18. Content Marshalling/Providers .......................................................... 65
  18.1. Default Providers and default JAX-RS Content Marshalling .......... 65
  18.2. Content Marshalling with @Provider classes ................................. 65
  18.3. Providers Utility Class ............................................................... 66
  18.4. Configuring Document Marshalling .............................................. 68
19. JAXB providers ............................................................................. 71
  19.1. JAXB Decorators ....................................................................... 72
  19.2. Pluggable JAXBContext's with ContextResolvers .............................. 73
  19.3. JAXB + XML provider ................................................................... 74
    19.3.1. @XmlHeader and @Stylesheet ................................................... 74
  19.4. JAXB + JSON provider .................................................................. 76
  19.5. JAXB + FastInfoSet provider ........................................................... 81
  19.6. Arrays and Collections of JAXB Objects ......................................... 81
    19.6.1. JSON and JAXB Collections/arrays ........................................... 84
  19.7. Maps of JAXB Objects ................................................................... 85
    19.7.1. JSON and JAXB maps ............................................................... 87
    19.7.2. Possible Problems with Jettison Provider .................................... 88
  19.8. Interfaces, Abstract Classes, and JAXB .......................................... 89
  19.9. Configurating JAXB Marshalling .................................................... 89
20. Resteasy Atom Support ................................................................... 91
  20.1. Resteasy Atom API and Provider .................................................... 91
  20.2. Using JAXB with the Atom Provider ............................................. 92
21. JSON Support via Jackson ............................................................... 95
  21.1. Using Jackson 1.9.x Outside of JBoss AS7 ....................................... 95
  21.2. Using Jackson 1.9.x Inside of JBoss AS7 ......................................... 95
  21.3. Using Jackson 2.2.x Outside of JBoss AS7 ....................................... 95
  21.4. Using Jackson 2.2.x Inside of JBoss AS7 ......................................... 96
  21.5. Additional Resteasy Specifics ........................................................... 96
  21.6. Possible Conflict With JAXB Provider ............................................ 98
  21.7. JSONP Support ............................................................................ 98
22. JSON Support via Java EE 7 JSON-P API ......................................... 101
23. Multipart Providers ...................................................................... 103
  23.1. Input with multipart/mixed ............................................................ 103
  23.2. java.util.List with multipart data ................................................ 105
  23.3. Input with multipart/form-data .................................................... 105
  23.4. java.util.Map with multipart/form-data ....................................... 106
  23.5. Input with multipart/related .......................................................... 106
  23.6. Output with multipart ................................................................. 107
  23.7. Multipart Output with java.util.List .......................................... 108
  23.8. Output with multipart/form-data ................................................ 109
  23.9. Multipart FormData Output with java.util.Map ............................ 110
  23.10. Output with multipart/related ..................................................... 110
### Table of Contents

23.11. @MultipartForm and POJOs ................................................................. 111  
23.12. XML-binary Optimized Packaging (Xop) ................................................ 113  
23.13. Note about multipart parsing and working with other frameworks .......... 115  
23.14. Overwriting the default fallback content type for multipart messages ..... 115  
23.15. Overwriting the content type for multipart messages .......................... 116  
23.16. Overwriting the default fallback charset for multipart messages .......... 116  

24. YAML Provider .................................................................................. 119  
25. String marshalling for String based @*Param ........................................... 121  
26. Responses using javax.ws.rs.core.Response ......................................... 123  

27. Exception Handling ........................................................................... 125  
27.1. Exception Mappers ........................................................................... 125  
27.2. Resteasy Built-in Internally-Thrown Exceptions ................................... 126  
27.3. Overriding Resteasy Builtin Exceptions ............................................. 127  

29. GZIP Compression/Decompression ....................................................... 131  
30. CORS .................................................................................................. 133  
31. Content-Range Support ...................................................................... 135  
32. Resteasy Caching Features .................................................................. 137  
32.1. @Cache and @NoCache Annotations ................................................. 137  
32.2. Client "Browser" Cache .................................................................... 138  
32.3. Local Server-Side Response Cache .................................................... 139  

33. Filters and Interceptors ........................................................................ 141  
33.1. Server Side Filters .......................................................................... 141  
33.2. Client Side Filters .......................................................................... 142  
33.3. Reader and Writer Interceptors ......................................................... 142  
33.4. Per Resource Method Filters and Interceptors ................................... 143  
33.5. Ordering .......................................................................................... 143  

34. Asynchronous HTTP Request Processing ............................................ 145  
35. Asynchronous Job Service ................................................................. 147  
35.1. Using Async Jobs ............................................................................ 147  
35.2. OneWay: Fire and Forget .................................................................. 148  
35.3. Setup and Configuration .................................................................. 148  

36. Embedded Containers ........................................................................ 151  
36.1. Undertow ......................................................................................... 151  
36.2. Sun JDK HTTP Server ...................................................................... 153  
36.3. TJWS Embeddable Servlet Container .............................................. 154  
36.4. Netty .............................................................................................. 155  

37. Server-side Mock Framework .............................................................. 157  
38. Securing JAX-RS and RESTeasy .......................................................... 159  
39. OAuth 2.0 and Resteasy Skeleton Key .................................................. 163  
39.1. System Requirements ...................................................................... 164  
39.2. Generate the Security Domain Key Pair ........................................... 164  
39.3. Setting up the Auth Server ............................................................... 164  
39.3.1. Setting up your Security Domain ................................................... 164
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>39.3.2. Auth Server Config File</td>
<td>165</td>
</tr>
<tr>
<td>39.3.3. Set up web.xml</td>
<td>167</td>
</tr>
<tr>
<td>39.3.4. Set up jboss-web.xml</td>
<td>167</td>
</tr>
<tr>
<td>39.3.5. Set up jboss-deployment-structure.xml</td>
<td>167</td>
</tr>
<tr>
<td>39.3.6. Tweak your login page</td>
<td>168</td>
</tr>
<tr>
<td>39.4. Setting Up An App for SSO</td>
<td>168</td>
</tr>
<tr>
<td>39.4.1. SSO config file</td>
<td>168</td>
</tr>
<tr>
<td>39.4.2. Set up web.xml</td>
<td>170</td>
</tr>
<tr>
<td>39.4.3. Set up jboss-web.xml</td>
<td>170</td>
</tr>
<tr>
<td>39.4.4. Set up jboss-deployment-structure.xml</td>
<td>170</td>
</tr>
<tr>
<td>39.5. Bearer Token only Setup</td>
<td>170</td>
</tr>
<tr>
<td>39.5.1. Bearer token auth config file</td>
<td>170</td>
</tr>
<tr>
<td>39.5.2. Set up web.xml</td>
<td>171</td>
</tr>
<tr>
<td>39.5.3. Set up jboss-web.xml</td>
<td>171</td>
</tr>
<tr>
<td>39.5.4. Set up jboss-deployment-structure.xml</td>
<td>171</td>
</tr>
<tr>
<td>39.6. Obtaining an access token programmatically</td>
<td>172</td>
</tr>
<tr>
<td>39.7. Access remote services securely in a secure web session</td>
<td>173</td>
</tr>
<tr>
<td>39.8. Check Out the OAuth2 Example!</td>
<td>174</td>
</tr>
<tr>
<td>39.9. Auth Server Action URLs</td>
<td>174</td>
</tr>
<tr>
<td>40. Authentication</td>
<td>175</td>
</tr>
<tr>
<td>40.1. OAuth core 1.0a</td>
<td>175</td>
</tr>
<tr>
<td>40.1.1. Authenticating with OAuth 1.0a</td>
<td>175</td>
</tr>
<tr>
<td>40.1.2. Accessing protected resources</td>
<td>176</td>
</tr>
<tr>
<td>40.1.3. Implementing an OAuthProvider</td>
<td>177</td>
</tr>
<tr>
<td>41. JSON Web Signature and Encryption (JOSE-JWT)</td>
<td>179</td>
</tr>
<tr>
<td>41.1. JSON Web Signature (JWS)</td>
<td>179</td>
</tr>
<tr>
<td>41.2. JSON Web Encryption (JWE)</td>
<td>179</td>
</tr>
<tr>
<td>42. Doseta Digital Signature Framework</td>
<td>183</td>
</tr>
<tr>
<td>42.1. Maven settings</td>
<td>185</td>
</tr>
<tr>
<td>42.2. Signing API</td>
<td>185</td>
</tr>
<tr>
<td>42.2.1. @Signed annotation</td>
<td>186</td>
</tr>
<tr>
<td>42.3. Signature Verification API</td>
<td>187</td>
</tr>
<tr>
<td>42.3.1. Annotation-based verification</td>
<td>188</td>
</tr>
<tr>
<td>42.4. Managing Keys via a KeyRepository</td>
<td>189</td>
</tr>
<tr>
<td>42.4.1. Create a KeyStore</td>
<td>189</td>
</tr>
<tr>
<td>42.4.2. Configure Restreasy to use the KeyRepository</td>
<td>189</td>
</tr>
<tr>
<td>42.4.3. Using DNS to Discover Public Keys</td>
<td>191</td>
</tr>
<tr>
<td>43. Body Encryption and Signing via SMIME</td>
<td>193</td>
</tr>
<tr>
<td>43.1. Maven settings</td>
<td>193</td>
</tr>
<tr>
<td>43.2. Message Body Encryption</td>
<td>193</td>
</tr>
<tr>
<td>43.3. Message Body Signing</td>
<td>195</td>
</tr>
<tr>
<td>43.4. application/pkcs7-signature</td>
<td>197</td>
</tr>
<tr>
<td>44. EJB Integration</td>
<td>199</td>
</tr>
<tr>
<td>45. Spring Integration</td>
<td>201</td>
</tr>
</tbody>
</table>
46. **CDI Integration** ................................................................. 205
   46.1. Using CDI beans as JAX-RS components .......................... 205
   46.2. Default scopes .......................................................... 205
   46.3. Configuration within JBoss 6 M4 and Higher ...................... 206
   46.4. Configuration with different distributions ...................... 206
47. **Seam Integration** ......................................................... 207
48. **Guice 3.0 Integration** .................................................. 209
   48.1. Request Scope .......................................................... 210
   48.2. Binding JAX-RS utilities .............................................. 211
   48.3. Configuring Stage ..................................................... 211
   48.4. Custom Injector creation ............................................ 212
49. **Resteasy Client API** .................................................... 215
   49.1. JAX-RS 2.0 Client API ................................................. 215
   49.2. Resteasy Proxy Framework .......................................... 215
   49.3. Apache HTTP Client 4.x and other backends ..................... 218
50. **AJAX Client** .............................................................. 223
   50.1. Generated JavaScript API .............................................. 223
       50.1.1. JavaScript API servlet ......................................... 223
       50.1.2. JavaScript API usage .......................................... 224
       50.1.3. Work with @Form .............................................. 226
       50.1.4. MIME types and unmarshalling. ............................. 227
       50.1.5. MIME types and marshalling. ............................... 229
   50.2. Using the JavaScript API to build AJAX queries ............... 230
       50.2.1. The REST object .............................................. 230
       50.2.2. The REST.Request class ................................. 231
   50.3. Caching Features ..................................................... 232
51. **Validation** ............................................................... 233
   51.1. Violation reporting ................................................ 234
   51.2. Bean Validation 1.1 ................................................ 238
   51.3. Bean Validation 1.0 ................................................ 239
   51.4. Validation Service Providers ................................... 240
52. **Maven and RESTEasy** .................................................. 245
53. **JBoss AS 5.x Integration** ............................................. 249
54. **JBoss AS 6/7 Integration** ............................................ 251
55. **Documentation Support** .............................................. 253
56. **Migration from older versions** ..................................... 255
   56.1. Migrating from 3.0.7 to 3.0.9 ................................... 255
   56.2. Migrating from 3.0.6 to 3.0.7 ................................... 255
   56.3. Migrating from 3.0 to 3.0.4 ..................................... 255
   56.4. Migrating from 3.0-beta-6 and 3.0-rc-1 ......................... 255
   56.5. Migrating from 3.0-beta-5 and 3.0-beta-6 ..................... 256
   56.6. Migrating from 3.0-beta-4 and 3.0-beta-5 ..................... 256
   56.7. Migrating from 3.0-beta-2 and 3.0-beta-4 ..................... 256
   56.8. Migrating from 3.0-beta-1 and 3.0-beta-2 ..................... 257
56.9. Migrating from 2.x to 3.0-beta-1 ................................................................. 257
56.10. Migrating from 2.3.2 to 2.3.3 ................................................................. 257
56.11. Migrating from 2.3.0 to 2.3.1 ................................................................. 258
56.12. Migrating from 2.2.x to 2.3 ................................................................. 258
56.13. Migrating from 2.2.0 to 2.2.1 ................................................................. 258
56.14. Migrating from 2.1.x to 2.2 ................................................................. 258
56.15. Migrating from 2.0.x to 2.1 ................................................................. 259
56.16. Migrating from 1.2.x to 2.0 ................................................................. 259
56.17. Migrating from 1.2.GA to 1.2.1.GA ....................................................... 259
56.18. Migrating from 1.1 to 1.2 ................................................................. 259

57. Books You Can Read ................................................................................. 261
Preface

Commercial development support, production support and training for RESTEasy JAX-RS is available through JBoss, a division of Red Hat Inc. (see http://www.jboss.com/).

In some of the example listings, what is meant to be displayed on one line does not fit inside the available page width. These lines have been broken up. A `\` at the end of a line means that a break has been introduced to fit in the page, with the following lines indented. So:

```
Let's pretend to have an extremely \nlong line that \ndoes not fit
This one is short
```

Is really:

```
Let's pretend to have an extremely long line that does not fit
This one is short
```
Chapter 1. Overview

JAX-RS, JSR-311, is a new JCP specification that provides a Java API for RESTful Web Services over the HTTP protocol. Resteasy is an portable implementation of this specification which can run in any Servlet container. Tighter integration with JBoss Application Server is also available to make the user experience nicer in that environment. While JAX-RS is only a server-side specification, Resteasy has innovated to bring JAX-RS to the client through the RESTEasy JAX-RS Client Framework. This client-side framework allows you to map outgoing HTTP requests to remote servers using JAX-RS annotations and interface proxies.

- JAX-RS implementation
- Portable to any app-server/Tomcat that runs on JDK 5 or higher
- Embeddable server implementation for junit testing
- EJB and Spring integration
- Client framework to make writing HTTP clients easy (JAX-RS only define server bindings)
Chapter 2. License

RESTEasy is distributed under the ASL 2.0 license. It does not distribute any thirdparty libraries that are GPL. It does ship thirdparty libraries licensed under Apache ASL 2.0 and LGPL.
Chapter 3. Installation/Configuration

RESTEasy is installed and configured in different ways depending on which environment you are running in. If you are running in JBoss AS 6-M4 (milestone 4) or higher, resteasy is already bundled and integrated completely so there is very little you have to do. If you are running in a different distribution, there is some manual installation and configuration you will have to do.

3.1. Upgrading Resteasy Within JBoss AS 7

Resteasy is bundled with JBoss AS 7. You will likely have the need to upgrade Resteasy in AS7. The Resteasy distribution comes with a zip file called resteasy-jboss-modules-3.0.9.Final.zip. Unzip this file while with the modules/ directory of the JBoss AS7 distribution. This will overwrite some of the existing files there.

3.2. Upgrading Resteasy Within JBoss EAP 6.1

Resteasy is bundled with JBoss EAP 6.1. You will likely have the need to upgrade Resteasy in JBoss EAP 6.1. The Resteasy distribution comes with a zip file called resteasy-jboss-modules-3.0.9.Final.zip. Unzip this file while with the modules/system/layers/base/ directory of the JBoss EAP 6.1 distribution. This will overwrite some of the existing files there.

3.3. Upgrading Resteasy Within Wildfly

Resteasy is bundled with Wildfly. You will likely have the need to upgrade Resteasy in Wildfly. The Resteasy distribution comes with a zip file called resteasy-jboss-modules-wf8-3.0.9.Final.zip. Unzip this file while with the modules/system/layers/base/ directory of the Wildfly distribution. This will overwrite some of the existing files there.

3.4. Configuring in JBoss AS 7, EAP, and Wildfly

RESTEasy is bundled with JBoss/Wildfly and completely integrated as per the requirements of Java EE 6. First you must at least provide an empty web.xml file. You can of course deploy any custom servlet, filter or security constraint you want to within your web.xml, but the least amount of work is to create an empty web.xml file. Also, resteasy context-params are available if you want to tweak turn on/off any specific resteasy feature.

```xml
<web-app version="3.0" xmlns="http://java.sun.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
```
Since we're not using a jax-rs servlet mapping, we must define an Application class that is annotated with the @ApplicationPath annotation. If you return any empty set for by classes and singletons, your WAR will be scanned for JAX-RS annotation resource and provider classes.

```java
import javax.ws.rs.ApplicationPath;
import javax.ws.rs.core.Application;

@ApplicationPath("/root-path")
public class MyApplication extends Application {
    
}
```

The Resteasy distribution has ported the "Restful Java" O'Reilly workbook examples to AS7. You can find these under the directory examples/oreilly-workbook-as7.

### 3.4.1. Resteasy Modules in AS7, EAP6.1, Wildfly

Resteasy and JAX-RS are automatically loaded into your deployment's classpath, if and only if you are deploying a JAX-RS Application. If you only want to use the client library, you will have to create a dependency for it within your deployment. Also, only some resteasy features are automatically loaded. To bring in these libraries, you'll have to create a jboss-deployment-structure.xml file within your WEB-INF directory of your WAR file. Here's an example:

```xml
<jboss-deployment-structure>
    <deployment>
        <dependencies>
            <module name="org.jboss.resteasy.resteasy-yaml-provider" services="import"/>
        </dependencies>
    </deployment>
</jboss-deployment-structure>
```
The `services` attribute must be set to import for modules that have default providers that must be registered. The following table specifies which modules are loaded by default when JAX-RS services are deployed and which aren't.

**Table 3.1.**

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Loaded by Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>org.jboss.resteasy.resteasy-jaxrs</td>
<td>yes</td>
<td>Core resteasy libraries for server and client. You will need to include this in your deployment if you are only using JAX-RS client.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-cdi</td>
<td>yes</td>
<td>Resteasy CDI integration</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-jaxb-provider</td>
<td>yes</td>
<td>XML JAXB integration.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-atom-provider</td>
<td>yes</td>
<td>Resteasy's atom library.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-jackson-provider</td>
<td>yes</td>
<td>Integration with the JSON parser and object mapper, Jackson.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-jsapi</td>
<td>yes</td>
<td>Resteasy's Javascript API.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-multipart-provider</td>
<td>yes</td>
<td>Features for dealing with multipart formats.</td>
</tr>
<tr>
<td>org.jboss.resteasy.resteasy-crypto</td>
<td>no</td>
<td>S/MIME, DKIM, and support for other security formats.</td>
</tr>
<tr>
<td>org.jboss.resteasy.jose-jwt</td>
<td>no</td>
<td>JOSE-JWT library. JSON Web Token.</td>
</tr>
<tr>
<td>org.jboss.resteasy.jettison-provider</td>
<td>no</td>
<td>Alternative JAXB-like parser for JSON.</td>
</tr>
<tr>
<td>org.jboss.resteasy.yaml-provider</td>
<td>no</td>
<td>YAML marshalling.</td>
</tr>
<tr>
<td>org.jboss.resteasy.skeleton-key</td>
<td>no</td>
<td>OAuth2 support for AS7.</td>
</tr>
</tbody>
</table>

### 3.5. Standalone Resteasy in Servlet 3.0 Containers

If you are using resteasy outside of JBoss/Wildfly, in a standalone servlet container like Tomcat or Jetty you will need to include the core Resteasy jars in your WAR file. Resteasy provides integration with standalone Servlet 3.0 containers via the `ServletContainerInitializer`
integration interface. To use this, you must also include the resteasy-servlet-initializer artifact in your WAR file as well.

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-servlet-initializer</artifactId>
  <version>3.0.9.Final</version>
</dependency>
```

We strongly suggest that you use Maven to build your WAR files as RESTEasy is split into a bunch of different modules. You can see an example Maven project in one of the examples in the examples/ directory. If you are not using Maven, when you download RESTEasy and unzip it you will see a lib/ directory that contains the libraries needed by resteasy. Copy these into your /WEB-INF/lib directory. Place your JAX-RS annotated class resources and providers within one or more jars within /WEB-INF/lib or your raw class files within /WEB-INF/classes.

### 3.6. Standalone Resteasy in Older Servlet Containers

The resteasy-servlet-initializer artifact will not work in Servlet versions older than 3.0. You'll then have to manually declare the Resteasy servlet in your WEB-INF/web.xml file of your WAR project. For example:

```xml
<web-app>
  <display-name>Archetype Created Web Application</display-name>

  <servlet>
    <servlet-name>Resteasy</servlet-name>
    <servlet-class>
      org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher
    </servlet-class>
    <init-param>
      <param-name>javax.ws.rs.Application</param-name>
      <param-value>com.restfully.shop.services.ShoppingApplication</param-value>
    </init-param>

  </servlet>

  <servlet-mapping>
    <servlet-name>Resteasy</servlet-name>
    <url-pattern>/*</url-pattern>
  </servlet-mapping>
</web-app>
```
The Resteasy servlet is responsible for initializing some basic components of RESTeasy.

## 3.7. Configuration Switches

Resteasy receives configuration options from `<context-param>` elements.

**Table 3.2.**

<table>
<thead>
<tr>
<th>Option Name</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>resteasy.servlet.mapping.prefix</code></td>
<td>no default</td>
<td>If the url-pattern for the Resteasy servlet-mapping is not /*</td>
</tr>
<tr>
<td><code>resteasy.scan</code></td>
<td>false</td>
<td>Automatically scan WEB-INF/lib jars and WEB-INF/classes directory for both @Provider and JAX-RS resource classes (@Path, @GET, @POST etc..) and register them</td>
</tr>
<tr>
<td><code>resteasy.scan.providers</code></td>
<td>false</td>
<td>Scan for @Provider classes and register them</td>
</tr>
<tr>
<td><code>resteasy.scan.resources</code></td>
<td>false</td>
<td>Scan for JAX-RS resource classes</td>
</tr>
<tr>
<td><code>resteasy.providers</code></td>
<td>no default</td>
<td>A comma delimited list of fully qualified @Provider class names you want to register</td>
</tr>
<tr>
<td><code>resteasy.use.builtin.providers</code></td>
<td>true</td>
<td>Whether or not to register default, built-in @Provider classes. (Only available in 1.0-beta-5 and later)</td>
</tr>
<tr>
<td><code>resteasy.resources</code></td>
<td>no default</td>
<td>A comma delimited list of fully qualified JAX-RS resource class names you want to register</td>
</tr>
<tr>
<td><code>resteasy.jndi.resources</code></td>
<td>no default</td>
<td>A comma delimited list of JNDI names which reference objects you want to register as JAX-RS resources</td>
</tr>
<tr>
<td>Option Name</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>javax.ws.rs.Application</td>
<td>no default</td>
<td>Fully qualified name of Application class to bootstrap in a spec portable way</td>
</tr>
<tr>
<td>resteasy.media.type.mappings</td>
<td>no default</td>
<td>Replaces the need for an Accept header by mapping file name extensions (like .xml or .txt) to a media type. Used when the client is unable to use a Accept header to choose a representation (i.e. a browser). See JAX-RS Content Negotiation chapter for more details.</td>
</tr>
<tr>
<td>resteasy.language.mappings</td>
<td>no default</td>
<td>Replaces the need for an Accept-Language header by mapping file name extensions (like .en or .fr) to a language. Used when the client is unable to use a Accept-Language header to choose a language (i.e. a browser). See JAX-RS Content Negotiation chapter for more details.</td>
</tr>
<tr>
<td>resteasy.document.expand.entity.references</td>
<td>false</td>
<td>Expand external entities in org.w3c.dom.Document documents and JAXB object representations</td>
</tr>
<tr>
<td>resteasy.document.secure.processing.feature</td>
<td>true</td>
<td>Impose security constraints in processing org.w3c.dom.Document documents and JAXB object representations</td>
</tr>
<tr>
<td>resteasy.document.secure.disable.dTDs</td>
<td>true</td>
<td>Prohibit DTDs in org.w3c.dom.Document documents and JAXB object representations</td>
</tr>
<tr>
<td>resteasy.wider.request.matching</td>
<td>true</td>
<td>Turns off the JAX-RS spec defined class-level expression filtering and instead tries to match version every method’s full path.</td>
</tr>
<tr>
<td>Option Name</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>resteasy.use.container.form.params</td>
<td>true</td>
<td>Will use the HttpServletRequest.getParameterMap() method to obtain form parameters. Use this switch if you are calling this method within a servlet filter or eating the input stream within the filter.</td>
</tr>
</tbody>
</table>

The resteasy.servlet.mapping.prefix <context param> variable must be set if your servlet-mapping for the Resteasy servlet has a url-pattern other than /*. For example, if the url-pattern is

```
<servlet-mapping>
  <servlet-name>Resteasy</servlet-name>
  <url-pattern>/restful-services/*</url-pattern>
</servlet-mapping>
```

Then the value of resteasy-servlet.mapping.prefix must be:

```
<context-param>
  <param-name>resteasy.servlet.mapping.prefix</param-name>
  <param-value>/restful-services</param-value>
</context-param>
```

### 3.8. javax.ws.rs.core.Application

The javax.ws.rs.core.Application class is a standard JAX-RS class that you may implement to provide information on your deployment. It is simply a class that lists all JAX-RS root resources and providers.
* subclass of this abstract class.
*/
public abstract class Application
{
    private static final Set<Object> emptySet = Collections.emptySet();

    /**
     * Get a set of root resource and provider classes. The default lifecycle
     * for resource class instances is per-request. The default lifecycle for
     * providers is singleton.
     * <p>
     * Implementations should warn about and ignore classes that do not
     * conform to the requirements of root resource or provider classes.
     * Implementations should warn about and ignore classes for which
     * {@link #getSingletons()} returns an instance. Implementations MUST
     * NOT modify the returned set.</p>
     *<p>
     * @return a set of root resource and provider classes. Returning null
     * is equivalent to returning an empty set.
     */
    public abstract Set<Class<?>> getClasses();

    /**
     * Get a set of root resource and provider instances. Fields and properties
     * of returned instances are injected with their declared dependencies
     * (see {@link Context}) by the runtime prior to use.
     * <p>
     * Implementations should warn about and ignore classes that do not
     * conform to the requirements of root resource or provider classes.
     * Implementations should flag an error if the returned set includes
     * more than one instance of the same class. Implementations MUST
     * NOT modify the returned set.</p>
     *<p>
     * @return a set of root resource and provider instances. Returning null
     * is equivalent to returning an empty set.
     */
    public Set<Object> getSingletons()
    {
        return emptySet;
    }
}
To use Application you must set a servlet init-param, javax.ws.rs.Application with a fully qualified class that implements Application. For example:

```xml
<web-app>
  <listener>
    <listener-class>
      org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap
    </listener-class>
  </listener>
</web-app>
```

If you have this set, you should probably turn off automatic scanning as this will probably result in duplicate classes being registered.

### 3.9. RESTEasy as a ServletContextListener

This section is pretty much deprecated if you are using a Servlet 3.0 container or higher. Skip it if you are and read the configuration section above on installing in Servlet 3.0. The initialization of RESTEasy can be performed within a ServletContextListener instead of within the Servlet. You may need this if you are writing custom Listeners that need to interact with RESTEasy at boot time. An example of this is the RESTEasy Spring integration that requires a Spring ServletContextListener. The org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap class is a ServletContextListener that configures an instance of an ResteasyProviderFactory and Registry. You can obtain instances of a ResteasyProviderFactory and Registry from the ServletContext attributes org.jboss.resteasy.spi.ResteasyProviderFactory and org.jboss.resteasy.spi.Registry. From these instances you can programmatically interact with RESTEasy registration interfaces.
3.10. RESTEasy as a servlet Filter

This section is pretty much deprecated if you are using a Servlet 3.0 container or higher. Skip it if you are and read the configuration section above on installing in Servlet 3.0. The downside of running Resteasy as a Servlet is that you cannot have static resources like .html and .jpeg files in the same path as your JAX-RS services. Resteasy allows you to run as a Filter instead. If a JAX-RS resource is not found under the URL requested, Resteasy will delegate back to the base servlet container to resolve URLs.
3.11. RESTEasyLogging

RESTEasy supports logging via java.util.logging, Log4j, or Slf4j. How it picks which framework to delegate to is expressed in the following algorithm:

- If log4j is in the application's classpath, log4j will be used
- If slf4j is in the application's classpath, slf4j will be used
- java.util.logging is the default if neither log4j or slf4j is in the classpath
- If the servlet context param resteasy.logger.type is set to JUL, LOG4J, or SLF4J will override this default behavior

The logging categories are still a work in progress, but the initial set should make it easier to troubleshoot issues. Currently, the framework has defined the following log categories:

**Table 3.3.**

<table>
<thead>
<tr>
<th>Category</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>org.jboss.resteasy.core</td>
<td>Logs all activity by the core RESTEasy implementation</td>
</tr>
<tr>
<td>org.jboss.resteasy.plugins.providers</td>
<td>Logs all activity by RESTEasy entity providers</td>
</tr>
<tr>
<td>org.jboss.resteasy.plugins.server</td>
<td>Logs all activity by the RESTEasy server implementation.</td>
</tr>
<tr>
<td>org.jboss.resteasy.specimpl</td>
<td>Logs all activity by JAX-RS implementing classes</td>
</tr>
<tr>
<td>org.jboss.resteasy.mock</td>
<td>Logs all activity by the RESTEasy mock framework</td>
</tr>
</tbody>
</table>
Chapter 4. Using @Path and @GET, @POST, etc.

```java
@Path("/library")
public class Library {

    @GET
    @Path("/books")
    public String getBooks() {...}

    @GET
    @Path("/book/{isbn}")
    public String getBook(@PathParam("isbn") String id) {
        // search my database and get a string representation and return it
    }

    @PUT
    @Path("/book/{isbn}")
    public void addBook(@PathParam("isbn") String id, @QueryParam("name") String name) {...}

    @DELETE
    @Path("/book/{id}")
    public void removeBook(@PathParam("id") String id {...}
}
```

Let's say you have the Resteasy servlet configured and reachable at a root path of http://myhost.com/services. The requests would be handled by the Library class:

- GET http://myhost.com/services/library/books

The @javax.ws.rs.Path annotation must exist on either the class and/or a resource method. If it exists on both the class and method, the relative path to the resource method is a concatenation of the class and method.
In the `@javax.ws.rs` package there are annotations for each HTTP method. `@GET`, `@POST`, `@PUT`, `@DELETE`, and `@HEAD`. You place these on public methods that you want to map to that certain kind of HTTP method. As long as there is a `@Path` annotation on the class, you do not have to have a `@Path` annotation on the method you are mapping. You can have more than one HTTP method as long as they can be distinguished from other methods.

When you have a `@Path` annotation on a method without an HTTP method, these are called JAXRSResourceLocators.

### 4.1. `@Path` and regular expression mappings

The `@Path` annotation is not limited to simple path expressions. You also have the ability to insert regular expressions into `@Path`'s value. For example:

```java
@Path("/resources")
public class MyResource {

    @GET
    @Path("{var:.*}/stuff")
    public String get() {...}
}
```

The following GETs will route to the `getResource()` method:

- GET /resources/stuff
- GET /resources/foo/stuff
- GET /resources/on/and/on/stuff

The format of the expression is:

```
{" variable-name [":" regular-expression ] "}
```

The regular-expression part is optional. When the expression is not provided, it defaults to a wildcard matching of one particular segment. In regular-expression terms, the expression defaults to

```
"\([\]*\)"
```
For example:

```java
@Path("/resources/{var}/stuff")
```

will match these:

```plaintext
GET /resources/foo/stuff
GET /resources/bar/stuff
```

but will not match:

```plaintext
GET /resources/a/bunch/of/stuff
```
Chapter 5. @PathParam

@PathParam is a parameter annotation which allows you to map variable URI path fragments into your method call.

```java
@Path("/library")
public class Library {

    @GET
    @Path("/book/{isbn}")
    public String getBook(@PathParam("isbn") String id) {
        // search my database and get a string representation and return it
    }
}
```

What this allows you to do is embed variable identification within the URIs of your resources. In the above example, an isbn URI parameter is used to pass information about the book we want to access. The parameter type you inject into can be any primitive type, a String, or any Java object that has a constructor that takes a String parameter, or a static valueOf method that takes a String as a parameter. For example, lets say we wanted isbn to be a real object. We could do:

```java
@GET
@Path("/book/{isbn}")
public String getBook(@PathParam("isbn") ISBN id) {...}
```

```java
public class ISBN {
    public ISBN(String str) {...}
}
```

Or instead of a public String constructors, have a valueOf method:

```java
public class ISBN {
    public static ISBN valueOf(String isbn) {...}
}
```
5.1. Advanced @PathParam and Regular Expressions

There are a few more complicated uses of @PathParams not discussed in the previous section.

You are allowed to specify one or more path params embedded in one URI segment. Here are some examples:

1. @Path("/aaa{param}bbb")
2. @Path("/{name}-{zip}")
3. @Path("/foo{name}-{zip}bar")

So, a URI of "/aaa111bbb" would match #1. "/bill-02115" would match #2. "foobill-02115bar" would match #3.

We discussed before how you can use regular expression patterns within @Path values.

@GET
@Path("/aaa{param:b+}/(many:.*)/stuff")
public String getIt(@PathParam("param") String bs, @PathParam("many") String many) {...}

For the following requests, lets see what the values of the "param" and "many" @PathParams would be:

Table 5.1.

<table>
<thead>
<tr>
<th>Request</th>
<th>param</th>
<th>many</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /aaabb/some/stuff</td>
<td>bb</td>
<td>some</td>
</tr>
<tr>
<td>GET /aab/a/lot/of/stuff</td>
<td>b</td>
<td>a/lot/of</td>
</tr>
</tbody>
</table>

5.2. @PathParam and PathSegment

The specification has a very simple abstraction for examining a fragment of the URI path being invoked on javax.ws.rs.core.PathSegment:
public interface PathSegment {

    /**
     * Get the path segment.
     * @return the path segment
     */
    String getPath();

    /**
     * Get a map of the matrix parameters associated with the path segment
     * @return the map of matrix parameters
     */
    MultivaluedMap<String, String> getMatrixParameters();
}

You can have Resteasy inject a PathSegment instead of a value with your @PathParam.

@GET
@Path("/book/{id}")
public String getBook(@PathParam("id") PathSegment id) {...}

This is very useful if you have a bunch of @PathParams that use matrix parameters. The idea of matrix parameters is that they are an arbitrary set of name-value pairs embedded in a uri path segment. The PathSegment object gives you access to these parameters. See also MatrixParam.

A matrix parameter example is:

GET http://host.com/library/book;name=EJB 3.0;author=Bill Burke

The basic idea of matrix parameters is that it represents resources that are addressable by their attributes as well as their raw id.
Chapter 6. @QueryParam

The @QueryParam annotation allows you to map a URI query string parameter or url form encoded parameter to your method invocation.

GET /books?num=5

```java
@GET
public String getBooks(@QueryParam("num") int num) {
    ...
}
```

Currently since Resteasy is built on top of a Servlet, it does not distinguish between URI query strings or url form encoded parameters. Like PathParam, your parameter type can be an String, primitive, or class that has a String constructor or static valueOf() method.
Chapter 7. @HeaderParam

The @HeaderParam annotation allows you to map a request HTTP header to your method invocation.

GET /books?num=5

```java
@GET
public String getBooks(@HeaderParam("From") String from) {
    ...
}
```

Like PathParam, your parameter type can be an String, primitive, or class that has a String constructor or static valueOf() method. For example, MediaType has a valueOf() method and you could do:

```java
@PUT
public void put(@HeaderParam("Content-Type") MediaType contentType, ...)
Chapter 8. Linking resources

There are two mechanisms available in RESTEasy to link a resource to another, and to link resources to operations: the Link HTTP header, and Atom links inside the resource representations.

8.1. Link Headers


The main advantage of Link headers over Atom links in the resource is that those links are available without parsing the entity body.

8.2. Atom links in the resource representations

RESTEasy allows you to inject Atom links [http://tools.ietf.org/html/rfc4287#section-4.2.7] directly inside the entity objects you are sending to the client, via auto-discovery.

![Warning]

This is only available when using the Jettison or JAXB providers (for JSON and XML).

The main advantage over Link headers is that you can have any number of Atom links directly over the concerned resources, for any number of resources in the response. For example, you can have Atom links for the root response entity, and also for each of its children entities.

8.2.1. Configuration

There is no configuration required to be able to inject Atom links in your resource representation, you just have to have this maven artifact in your path:

Table 8.1. Maven artifact for Atom link injection

<table>
<thead>
<tr>
<th>Group</th>
<th>Artifact</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>org.jboss.resteasy</td>
<td>resteasy-links</td>
<td>3.0.9.Final</td>
</tr>
</tbody>
</table>

8.2.2. Your first links injected

You need three things in order to tell RESTEasy to inject Atom links in your entities:
Chapter 8. Linking resources

- Annotate the JAX-RS method with @AddLinks to indicate that you want Atom links injected in your response entity.

- Add RESTServiceDiscovery fields to the resource classes where you want Atom links injected.

- Annotate the JAX-RS methods you want Atom links for with @LinkResource, so that RESTEasy knows which links to create for which resources.

The following example illustrates how you would declare everything in order to get the Atom links injected in your book store:

```java
@Path("/")
@Consumes({"application/xml", "application/json"})
@Produces({"application/xml", "application/json"})
public interface BookStore {

    @AddLinks
    @LinkResource(value = Book.class)
    @GET
    @Path("books")
    public Collection<Book> getBooks();

    @LinkResource
    @POST
    @Path("books")
    public void addBook(Book book);

    @AddLinks
    @LinkResource
    @GET
    @Path("book/{id}" )
    public Book getBook(@PathParam("id") String id);

    @LinkResource
    @PUT
    @Path("book/{id}" )
    public void updateBook(@PathParam("id") String id, Book book);

    @LinkResource(value = Book.class)
    @DELETE
    @Path("book/{id}" )
    public void deleteBook(@PathParam("id") String id);
}
```

And this is the definition of the Book resource:
@Mapped(namespaceMap = @XmlNsMap(jsonName = "atom", namespace = "http://www.w3.org/2005/Atom"))
@XmlRootElement
@XmlAccessorType(XmlAccessType.NONE)
public class Book {
    @XmlAttribute
    private String author;

    @XmlID
    @XmlAttribute
    private String title;

    @XmlElementRef
    private RESTServiceDiscovery rest;
}

If you do a GET /order/foo you will then get this XML representation:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<book xmlns:atom="http://www.w3.org/2005/Atom" title="foo" author="bar">
    <atom:link href="http://localhost:8081/books" rel="list"/>
    <atom:link href="http://localhost:8081/books" rel="add"/>
</book>
```

And in JSON format:

```json
{
    "book": {
        "@title": "foo",
        "@author": "bar",
        "atom.link": [
            {"@href": "http://localhost:8081/books", "@rel": "list"},
            {"@href": "http://localhost:8081/books", "@rel": "add"},
        ]
    }
}
```
8.2.3. Customising how the Atom links are serialised

Because the RESTServiceDiscovery is in fact a JAXB type which inherits from List you are free to annotate it as you want to customise the JAXB serialisation, or just rely on the default with @XmlElementRef.

8.2.4. Specifying which JAX-RS methods are tied to which resources

This is all done by annotating the methods with the @LinkResource annotation. It supports the following optional parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Function</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Class</td>
<td>Declares an Atom link for the given type of resources.</td>
<td>Defaults to the entity body type (non-annotated parameter), or the method’s return type. This default does not work with Response or Collection types, they need to be explicitly specified.</td>
</tr>
<tr>
<td>rel</td>
<td>String</td>
<td>The Atom link relation list</td>
<td>For GET methods returning a Collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>self For GET methods returning a non-Collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>remove For DELETE methods</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>update For PUT methods</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>add For POST methods</td>
</tr>
</tbody>
</table>
You can add several @LinkResource annotations on a single method by enclosing them in a @LinkResources annotation. This way you can add links to the same method on several resource types. For example the /order/foo/comments operation can belongs on the Order resource with the comments relation, and on the Comment resource with the list relation.

### 8.2.5. Specifying path parameter values for URI templates

When RESTEasy adds links to your resources it needs to insert the right values in the URI template. This is done either automatically by guessing the list of values from the entity, or by specifying the values in the @LinkResource pathParameters parameter.

#### 8.2.5.1. Loading URI template values from the entity

URI template values are extracted from the entity from fields or Java Bean properties annotated with @ResourceID, JAXB's @XmlID or JPA's @Id. If there are more than one URI template value to find in a given entity, you can annotate your entity with @ResourceIDs to list the names of fields or properties that make up this entity's Id. If there are other URI template values required from a parent entity, we try to find that parent in a field or Java Bean property annotated with @ParentResource. The list of URI template values extracted up every @ParentResource is then reversed and used as the list of values for the URI template.

For example, let's consider the previous Book example, and a list of comments:

```java
@XmlElement
@AccessorType(XmlAccessType.NONE)
public class Comment {
    @ParentResource
    private Book book;

    @XmlElement
    private String author;

    @XmlID
    @XmlAttribute
    private String id;

    @XmlElementRef
    private RESTServiceDiscovery rest;
}
```

Given the previous book store service augmented with comments:

```java
@Path("/")
@Consumes({"application/xml", "application/json"})
@Produces({"application/xml", "application/json"})
public interface BookStore {
```
Whenever we need to make links for a `Book` entity, we look up the ID in the `Book`’s `@XmlID` property. Whenever we make links for `Comment` entities, we have a list of values taken from the `Comment`’s `@XmlID` and its `@ParentResource`: the `Book` and its `@XmlID`.

For a `Comment` with id "1" on a `Book` with title "foo" we will therefore get a list of URI template values of {"foo", "1"}, to be replaced in the URI template, thus obtaining either "/book/foo/comments" or "/book/foo/comment/1".

### 8.2.5.2. Specifying path parameters manually

If you do not want to annotate your entities with resource ID annotations (`@ResourceId`, `@ResourceIds`, `@XmlID` or `@Id`) and `@ParentResource`, you can also specify the URI template values inside the `@LinkResource` annotation, using Unified Expression Language expressions:

**Table 8.3.**
Specifying path parameter values for URI templates

**@LinkResource** URI template parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Function</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>pathParameters</td>
<td>String[]</td>
<td>Declares a list of UEL expressions to obtain the URI template values.</td>
<td>Defaults to using @ResourceId, @ResourceIDs, @XmlID or @Id and @ParentResource annotations to extract the values from the model.</td>
</tr>
</tbody>
</table>

The UEL expressions are evaluated in the context of the entity, which means that any unqualified variable will be taken as a property for the entity itself, with the special variable `this` bound to the entity we're generating links for.

The previous example of `Comment` service could be declared as such:

```java
@Path("/")
@Consumes({"application/xml", "application/json"})
@Produces({"application/xml", "application/json"})
public interface BookStore {

    @AddLinks
    @LinkResources{
        @LinkResource(value = Book.class, rel = "comments", pathParameters = "${title}"),
        @LinkResource(value = Comment.class, pathParameters = {"${book.title}", "${id}"})
    }
    @GET
    @Path("book/{id}/comments")
    public Collection<Comment> getComments(@PathParam("id") String bookId);

    @AddLinks
    @LinkResource(pathParameters = {"${book.title}", "${id}"})
    @GET
    @Path("book/{id}/comment/{cid}")
    public Comment getComment(@PathParam("id") String bookId, @PathParam("cid") String commentId);

    @LinkResource(pathParameters = {"${book.title}", "${id}"})
    @POST
    @Path("book/{id}/comments")
    public void addComment(@PathParam("id") String bookId, Comment comment);

    @LinkResource(pathParameters = {"${book.title}", "${id}"})
    @PUT
    @Path("book/{id}/comment/{cid}")
    public void updateComment(@PathParam("id") String bookId, @PathParam("cid") String commentId);
```
@LinkResource(Comment.class, pathParameters = {"${book.title}" , "${id}"})
@DELETE
@Path("book/{id}/comment/{cid}")
public void deleteComment(@PathParam("id") String bookId, @PathParam("cid") String commentId)
}

8.2.6. Securing entities

You can restrict which links are injected in the resource based on security restrictions for the client, so that if the current client doesn't have permission to delete a resource he will not be presented with the "delete" link relation.

Security restrictions can either be specified on the @LinkResource annotation, or using RESTEasy and EJB's security annotation @RolesAllowed on the JAX-RS method.

Table 8.4.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Function</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>constraint</td>
<td>String</td>
<td>A UEL expression which must evaluate to true to inject this method's link in the response entity.</td>
<td>Defaults to using @RolesAllowed from the JAX-RS method.</td>
</tr>
</tbody>
</table>

8.2.7. Extending the UEL context

We've seen that both the URI template values and the security constraints of @LinkResource use UEL to evaluate expressions, and we provide a basic UEL context with access only to the entity we're injecting links in, and nothing more.

If you want to add more variables or functions in this context, you can by adding a @LinkELProvider annotation on the JAX-RS method, its class, or its package. This annotation's value should point to a class that implements the ELProvider interface, which wraps the default ELContext in order to add any missing functions.

For example, if you want to support the Seam annotation s:hasPermission(target, permission) in your security constraints, you can add a package-info.java file like this:

```java
@LinkELProvider(SeamELProvider.class)
package org.jboss.resteasy.links.test;
import org.jboss.resteasy.links.*;
```
With the following provider implementation:

```java
package org.jboss.resteasy.links.test;

import javax.el.ELContext;
import javax.el.ELResolver;
import javax.el.FunctionMapper;
import javax.el.VariableMapper;

import org.jboss.seam.el.SeamFunctionMapper;

import org.jboss.resteasy.links.ELProvider;

public class SeamELProvider implements ELProvider {

    public ELContext getContext(final ELContext ctx) {
        return new ELContext() {
            private SeamFunctionMapper functionMapper;

            @Override
            public ELResolver getELResolver() {
                return ctx.getELResolver();
            }

            @Override
            public FunctionMapper getFunctionMapper() {
                if (functionMapper == null)
                    functionMapper = new SeamFunctionMapper(ctx
                        .getFunctionMapper());
                return functionMapper;
            }

            @Override
            public VariableMapper getVariableMapper() {
                return ctx.getVariableMapper();
            }
        };
    }
}
```

And then use it as such:

```java
@Path("/")
@Consumes({"application/xml", "application/json"})
@Produces({"application/xml", "application/json"})
```
```java
public interface BookStore {
    @AddLinks
    @LinkResources(
        @LinkResource(value = Book.class, rel = "comments", constraint = "${s:hasPermission(this, 'add-comment')}")
        ,
        @LinkResource(value = Comment.class, constraint = "${s:hasPermission(this, 'insert')}")
    )
    @GET
    @Path("book/{id}/comments")
    public Collection<Comment> getComments(@PathParam("id") String bookId);

    @AddLinks
    @LinkResource(constraint = "${s:hasPermission(this, 'read')}")
    @GET
    @Path("book/{id}/comment/{cid}")
    public Comment getComment(@PathParam("id") String bookId, @PathParam("cid") String commentId);

    @LinkResource(constraint = "${s:hasPermission(this, 'insert')}")
    @POST
    @Path("book/{id}/comments")
    public void addComment(@PathParam("id") String bookId, Comment comment);

    @LinkResource(constraint = "${s:hasPermission(this, 'update')}")
    @PUT
    @Path("book/{id}/comment/{cid}")
    public void updateComment(@PathParam("id") String bookId, @PathParam("cid") String commentId,
        @LinkResource(Comment.class, constraint = "${s:hasPermission(this, 'delete')}")
        @DELETE
    @Path("book/{id}/comment/{cid}")
    public void deleteComment(@PathParam("id") String bookId, @PathParam("cid") String commentId);
}
```

### 8.2.8. Resource facades

Sometimes it is useful to add resources which are just containers or layers on other resources. For example if you want to represent a collection of `Comment` with a start index and a certain number of entries, in order to implement paging. Such a collection is not really an entity in your model, but it should obtain the "add" and "list" link relations for the `Comment` entity.

This is possible using resource facades. A resource facade is a resource which implements the `ResourceFacade<T>` interface for the type `T`, and as such, should receive all links for that type.
Since in most cases the instance of the $T$ type is not directly available in the resource facade, we need another way to extract its URI template values, and this is done by calling the resource facade's `pathParameters()` method to obtain a map of URI template values by name. This map will be used to fill in the URI template values for any link generated for $T$, if there are enough values in the map.

Here is an example of such a resource facade for a collection of `Comment`:

```java
@XmlElement
@XmlAccessorType(XmlAccessType.NONE)
public class ScrollableCollection implements ResourceFacade<Comment> {

    private String bookId;
    @XmlAttribute
    private int start;
    @XmlAttribute
    private int totalRecords;
    @XmlElement
    private List<Comment> comments = new ArrayList<Comment>();
    @XmlElementRef
    private RESTServiceDiscovery rest;

    public Class<Comment> facadeFor() {
        return Comment.class;
    }

    public Map<String, ? extends Object> pathParameters() {
        HashMap<String, String> map = new HashMap<String, String>();
        map.put("id", bookId);
        return map;
    }
}
```

This will produce such an XML collection:

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<collection xmlns:atom="http://www.w3.org/2005/Atom"
    totalRecords="2" start="0">
    <comment xmlid="0">
        <text>great book</text>
        <atom.link href="http://localhost:8081/book/foo/comment/0" rel="self"/>
        <atom.link href="http://localhost:8081/book/foo/comment/0" rel="update"/>
        <atom.link href="http://localhost:8081/book/foo/comment/0" rel="remove"/>
    </comment>
</collection>
```
Chapter 8. Linking resources

</comment>
<comment xmlid="1">
  <text>terrible book</text>
  <atom.link href="http://localhost:8081/book/foo/comment/1" rel="self"/>
  <atom.link href="http://localhost:8081/book/foo/comment/1" rel="update"/>
  <atom.link href="http://localhost:8081/book/foo/comment/1" rel="remove"/>
</comment>
</collection>
Chapter 9. @MatrixParam

The idea of matrix parameters is that they are an arbitrary set of name-value pairs embedded in a uri path segment. A matrix parameter example is:

GET http://host.com/library/book;name=EJB 3.0;author=Bill Burke

The basic idea of matrix parameters is that it represents resources that are addressable by their attributes as well as their raw id. The @MatrixParam annotation allows you to inject URI matrix parameters into your method invocation

```java
@GET
public String getBook(@MatrixParam("name") String name, @MatrixParam("author") String author) {...}
```

There is one big problem with @MatrixParam that the current version of the specification does not resolve. What if the same MatrixParam exists twice in different path segments? In this case, right now, its probably better to use PathParam combined with PathSegment.
The `@CookieParam` annotation allows you to inject the value of a cookie or an object representation of an HTTP request cookie into your method invocation.

```java
@GET
public String getBooks(@CookieParam("sessionid") int id) {
    ...
}

@GET
public String getBooks(@CookieParam("sessionid") javax.ws.rs.core.Cookie id) {
    ...
}
```

Like `PathParam`, your parameter type can be an `String`, primitive, or class that has a `String` constructor or `static valueOf()` method. You can also get an object representation of the cookie via the `javax.ws.rs.core.Cookie` class.
Chapter 11. @FormParam

When the input request body is of the type "application/x-www-form-urlencoded", a.k.a. an HTML Form, you can inject individual form parameters from the request body into method parameter values.

```html
<form method="POST" action="/resources/service">
First name:
<input type="text" name="firstname">
<br>
Last name:
<input type="text" name="lastname">
</form>
```

If you post through that form, this is what the service might look like:

```java
@Path("/")
public class NameRegistry {
    @Path("/resources/service")
    @POST
    public void addName(@FormParam("firstname") String first,
                        @FormParam("lastname") String last) {...}
}
```

You cannot combine @FormParam with the default "application/x-www-form-urlencoded" that unmarshalls to a MultivaluedMap<String, String>. i.e. This is illegal:

```java
@Path("/")
public class NameRegistry {
    @Path("/resources/service")
    @POST
    @Consumes("application/x-www-form-urlencoded")
    public void addName(@FormParam("firstname") String first,
                         MultivaluedMap<String, String> form) {...}
}
```
Chapter 12. @Form

This is a RESTEasy specific annotation that allows you to re-use any @*Param annotation within an injected class. RESTEasy will instantiate the class and inject values into any annotated @*Param or @Context property. This is useful if you have a lot of parameters on your method and you want to condense them into a value object.

```java
public class MyForm {

    @FormParam("stuff")
    private int stuff;

    @HeaderParam("myHeader")
    private String header;

    @PathParam("foo")
    public void setFoo(String foo) {...}
}

@POST
@Path("/myservice")
public void post(@Form MyForm form) {...}
```

When somebody posts to /myservice, RESTEasy will instantiate an instance of MyForm and inject the form parameter "stuff" into the "stuff" field, the header "myheader" into the header field, and call the setFoo method with the path param variable of "foo".

Also, @Form has some expanded @FormParam features. If you specify a prefix within the Form param, this will prepend a prefix to any form parameter lookup. For example, let's say you have one Address class, but want to reference invoice and shipping addresses from the same set of form parameters:

```java
public static class Person
{

    @FormParam("name")
    private String name;
```
Chapter 12. @Form

```java
@Form(prefix = "invoice")
private Address invoice;

@Form(prefix = "shipping")
private Address shipping;

public static class Address
{
    @FormParam("street")
    private String street;
}

@Path("person")
public static class MyResource
{
    @POST
    @Produces(MediaType.TEXT_PLAIN)
    @Consumes(MediaType.APPLICATION_FORM_URLENCODED)
    public String post(@Form Person p)
    {
        return p.toString();
    }
}
```

In this example, the client could send the following form parameters:

```
name=bill
invoice.street=xxx
shipping.street=yyy
```

The Person.invoice and Person.shipping fields would be populated appropriately. Also, prefix mappings also support lists and maps:

```java
public static class Person {
    @Form(prefix="telephoneNumbers") List<TelephoneNumber> telephoneNumbers;
    @Form(prefix="address") Map<String, Address> addresses;
}
```
public static class TelephoneNumber {
    @FormParam("countryCode") private String countryCode;
    @FormParam("number") private String number;
}

public static class Address {
    @FormParam("street") private String street;
    @FormParam("houseNumber") private String houseNumber;
}

@Path("person")
public static class MyResource {

    @POST
    @Consumes(MediaType.APPLICATION_FORM_URLENCODED)
    public void post (@Form Person p) {}  
}

The following form params could be submitted and the Person.telephoneNumbers and Person.addresses fields would be populated appropriately

```java
request.addFormHeader("telephoneNumbers[0].countryCode", "31");
request.addFormHeader("telephoneNumbers[0].number", "0612345678");
request.addFormHeader("telephoneNumbers[1].countryCode", "91");
request.addFormHeader("telephoneNumbers[1].number", "9717738723");
request.addFormHeader("address[INVOICE].street", "Main Street");
request.addFormHeader("address[INVOICE].houseNumber", "2");
request.addFormHeader("address[SHIPPING].street", "Square One");
request.addFormHeader("address[SHIPPING].houseNumber", "13");
```
Chapter 13. @DefaultValue

@DefaultValue is a parameter annotation that can be combined with any of the other @*Param annotations to define a default value when the HTTP request item does not exist.

```java
@GET
public String getBooks(@QueryParam("num") @DefaultValue("10") int num) {...}
```
Chapter 14. @Encoded and encoding

JAX-RS allows you to get encoded or decoded @*Params and specify path definitions and parameter names using encoded or decoded strings.

The @javax.ws.rs.Encoded annotation can be used on a class, method, or param. By default, inject @PathParam and @QueryParams are decoded. By additionally adding the @Encoded annotation, the value of these params will be provided in encoded form.

```java
@Path("/")
public class MyResource {

    @Path("/{param}")
    @GET
    public String get(@PathParam("param") @Encoded String param) {...}
}
```

In the above example, the value of the @PathParam injected into the param of the get() method will be URL encoded. Adding the @Encoded annotation as a paramater annotation triggers this affect.

You may also use the @Encoded annotation on the entire method and any combination of @QueryParam or @PathParam's values will be encoded.

```java
@Path("/")
public class MyResource {

    @Path("/{param}")
    @GET
    @Encoded
    public String get(@QueryParam("foo") String foo, @PathParam("param") String param) {};
}
```

In the above example, the values of the "foo" query param and "param" path param will be injected as encoded values.

You can also set the default to be encoded for the entire class.
The `@Path` annotation has an attribute called `encode`. Controls whether the literal part of the supplied value (those characters that are not part of a template variable) are URL encoded. If true, any characters in the URI template that are not valid URI character will be automatically encoded. If false then all characters must be valid URI characters. By default this is set to true. If you want to encoded the characters yourself, you may.

```java
@Path(encode=false)
@Path(value="hello%20world", encode=false)
```

Much like `Path.encode()`, this controls whether the specified query param name should be encoded by the container before it tries to find the query param in the request.

```java
@QueryParam(value="hello%20world", encode=false)
```
Chapter 15. @Context

Chapter 16. JAX-RS Resource Locators and Sub Resources

Resource classes are able to partially process a request and provide another "sub" resource object that can process the remainder of the request. For example:

```java
@Path("/")
public class ShoppingStore {

    @Path("/customers/{id}")
    public Customer getCustomer(@PathParam("id") int id) {
        Customer cust = ...; // Find a customer object
        return cust;
    }
}

public class Customer {

    @GET
    public String get() {...}

    @Path("/address")
    public String getAddress() {...}
}
```

Resource methods that have a @Path annotation, but no HTTP method are considered sub-resource locators. Their job is to provide an object that can process the request. In the above example ShoppingStore is a root resource because its class is annotated with @Path. The getCustomer() method is a sub-resource locator method.

If the client invoked:

```
GET /customer/123
```

The ShoppingStore.getCustomer() method would be invoked first. This method provides a Customer object that can service the request. The http request will be dispatched to the Customer.get() method. Another example is:
GET /customer/123/address

In this request, again, first the ShoppingStore.getCustomer() method is invoked. A customer object is returned, and the rest of the request is dispatched to the Customer.getAddress() method.

Another interesting feature of Sub-resource locators is that the locator method result is dynamically processed at runtime to figure out how to dispatch the request. So, the ShoppingStore.getCustomer() method does not have to declare any specific type.

```java
@Path("/")
public class ShoppingStore {

    @Path("/customers/{id}")
    public java.lang.Object getCustomer(@PathParam("id") int id) {
        Customer cust = ...; // Find a customer object
        return cust;
    }
}

public class Customer {

    @GET
    public String get() {...}

    @Path("/address")
    public String getAddress() {...}
}
```

In the above example, getCustomer() returns a java.lang.Object. Per request, at runtime, the JAX-RS server will figure out how to dispatch the request based on the object returned by getCustomer(). What are the uses of this? Well, maybe you have a class hierarchy for your customers. Customer is the abstract base, CorporateCustomer and IndividualCustomer are subclasses. Your getCustomer() method might be doing a Hibernate polymorphic query and doesn’t know, or care, what concrete class is it querying for, or what it returns.

```java
@Path("/")
public class ShoppingStore {

    @Path("/customers/{id}")
```
public java.lang.Object getCustomer(@PathParam("id") int id) {
    Customer cust = entityManager.find(Customer.class, id);
    return cust;
}

public class Customer {
    
    @GET
    public String get() {...}
    
    @Path("/address")
    public String getAddress() {...}

}

public class CorporateCustomer extends Customer {
    
    @Path("/businessAddress")
    public String getAddress() {...}

}
Chapter 17. JAX-RS Content Negotiation

The HTTP protocol has built in content negotiation headers that allow the client and server to specify what content they are transferring and what content they would prefer to get. The server declares content preferences via the @Produces and @Consumes headers.

@Consumes is an array of media types that a particular resource or resource method consumes. For example:

```java
@Consumes("text/*")
@Path("/library")
public class Library {

    @POST
    public String stringBook(String book) {...}

    @Consumes("text/xml")
    @POST
    public String jaxbBook(Book book) {...}
```

When a client makes a request, JAX-RS first finds all methods that match the path, then, it sorts things based on the content-type header sent by the client. So, if a client sent:

```
POST /library
content-type: text/plain

this is an ice book
```

The stringBook() method would be invoked because it matches to the default "text/*" media type. Now, if the client instead sends XML:

```
POST /library
content-type: text/xml
```
The `jaxbBook()` method would be invoked.

The `@Produces` is used to map a client request and match it up to the client’s Accept header. The Accept HTTP header is sent by the client and defines the media types the client prefers to receive from the server.

```java
@Produces("text/*")
@Path("/library")
public class Library {

  @GET
  @Produces("application/json")
  public String getJSON() {...}

  @GET
  public String get() {...}
```

So, if the client sends:

```
GET /library
Accept: application/json
```

The `getJSON()` method would be invoked

`@Consumes` and `@Produces` can list multiple media types that they support. The client’s Accept header can also send multiple types it might like to receive. More specific media types are chosen first. The client Accept header or `@Produces` `@Consumes` can also specify weighted preferences that are used to match up requests with resource methods. This is best explained by RFC 2616 section 14.1. Resteasy supports this complex way of doing content negotiation.

A variant in JAX-RS is a combination of media type, content-language, and content encoding as well as etags, last modified headers, and other preconditions. This is a more complex form of content negotiation that is done programmatically by the application developer using the `javax.ws.rs.Variant`, `VariantListBuilder`, and `Request` objects. Request is injected via `@Context`. Read the javadoc for more info on these.
17.1. URL-based negotiation

Some clients, like browsers, cannot use the Accept and Accept-Language headers to negotiation the representation's media type or language. RESTEasy allows you to map file name suffixes like (.xml, .txt, .en, .fr) to media types and languages. These file name suffixes take the place and override any Accept header sent by the client. You configure this using the resteasy.media.type.mappings and resteasy.language.mappings context-param variables within your web.xml.

```xml
<web-app>
  <display-name>Archetype Created Web Application</display-name>
  <context-param>
    <param-name>resteasy.media.type.mappings</param-name>
    <param-value>html : text/html, json : application/json, xml : application/xml</param-value>
  </context-param>
  <context-param>
    <param-name>resteasy.language.mappings</param-name>
  </context-param>
  <servlet>
    <servlet-name>Resteasy</servlet-name>
    <servlet-class>org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>Resteasy</servlet-name>
    <url-pattern>/*</url-pattern>
  </servlet-mapping>
</web-app>
```

Mappings are a comma delimited list of suffix/mediatype or suffix/language mappings. Each mapping is delimited by a ':'. So, if you invoked GET /foo/bar.xml.en, this would be equivalent to invoking the following request:

```
GET /foo/bar
Accept: application/xml
```
The mapped file suffixes are stripped from the target URL path before the request is dispatched to a corresponding JAX-RS resource.

### 17.2. Query String Parameter-based negotiation

RESTEasy can do content negotiation based in a parameter in query string. To enable this, the `web.xml` can be configured like follow:

```xml
<web-app>
    <display-name>Archetype Created Web Application</display-name>
    <context-param>
        <param-name>resteasy.media.type.param.mapping</param-name>
        <param-value>someName</param-value>
    </context-param>

    <servlet>
        <servlet-name>Resteasy</servlet-name>
        <servlet-class>org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>Resteasy</servlet-name>
        <url-pattern>/*</url-pattern>
    </servlet-mapping>
</web-app>
```

The `param-value` is the name of the query string parameter that RESTEasy will use in the place of the `Accept` header.

Invoking `http://service.foo.com/resource?someName=application/xml`, will give the `application/xml` media type the highest priority in the content negotiation.

In cases where the request contains both the parameter and the `Accept` header, the parameter will be more relevant.

It is possible to leave the `param-value` empty, what will cause the processor to look for a parameter named 'accept'.
Chapter 18. Content Marshalling/Providers

18.1. Default Providers and default JAX-RS Content Marshalling

Resteasy can automatically marshal and unmarshal a few different message bodies.

Table 18.1.

<table>
<thead>
<tr>
<th>Media Types</th>
<th>Java Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>application/<em>+xml, text/</em>+xml, application/<em>+json, application/</em>+fastinfoset, application/atom+*</td>
<td>JAXB annotated classes</td>
</tr>
<tr>
<td>application/<em>+xml, text/</em>+xml</td>
<td>org.w3c.dom.Document</td>
</tr>
<tr>
<td>/*</td>
<td>java.lang.String</td>
</tr>
<tr>
<td>/*</td>
<td>java.io.InputStream</td>
</tr>
<tr>
<td>text/plain</td>
<td>primitives, java.lang.String, or any type that has a String constructor, or static valueOf(String) method for input, toString() for output</td>
</tr>
<tr>
<td>/*</td>
<td>javax.activation.DataSource</td>
</tr>
<tr>
<td>/*</td>
<td>java.io.File</td>
</tr>
<tr>
<td>/*</td>
<td>byte[]</td>
</tr>
<tr>
<td>application/x-www-form-urlencoded</td>
<td>javax.ws.rs.core.MultivaluedMap</td>
</tr>
</tbody>
</table>

18.2. Content Marshalling with @Provider classes

The JAX-RS specification allows you to plug in your own request/response body reader and writers. To do this, you annotate a class with @Provider and specify the @Produces types for a writer and @Consumes types for a reader. You must also implement a MessageBodyReader/Writer interface respectively. Here is an example.

The Resteasy ServletContextLoader will automatically scan your WEB-INF/lib and classes directories for classes annotated with @Provider or you can manually configure them in web.xml. See Installation/Configuration
18.3. Providers Utility Class

javax.ws.rs.ext.Providers is a simple injectable interface that allows you to look up MessageBodyReaders, Writers, ContextResolvers, and ExceptionMappers. It is very useful, for instance, for implementing multipart providers. Content types that embed other random content types.

```java
public interface Providers {

    /**
     * Get a message body reader that matches a set of criteria. The set of
     * readers is first filtered by comparing the supplied value of
     * {0code mediaType} with the value of each reader's
     * {0link javax.ws.rs.Consumes}, ensuring the supplied value of
     * {0code type} is assignable to the generic type of the reader, and
     * eliminating those that do not match.
     * The list of matching readers is then ordered with those with the best
     * matching values of {0link javax.ws.rs.Consumes} (x/y > x&#47;* > *&#47;*)
     * sorted first. Finally, the
     * {0link MessageBodyReader#isReadable}
     * method is called on each reader in order using the supplied criteria and
     * the first reader that returns {0code true} is selected and returned.
     * *
     * @param type        the class of object that is to be written.
     * @param mediaType   the media type of the data that will be read.
     * @param genericType the type of object to be produced. E.g. if the
     *                     message body is to be converted into a method
     *                     parameter, this will be
     *                     the formal type of the method parameter as returned by
     *                     <code>Class.getGenericParameterTypes</code>.
     * @param annotations an array of the annotations on the declaration of the
     *                     artifact that will be initialized with the produced
     *                     instance. E.g. if the
     *                     message body is to be converted into a method
     *                     parameter, this will be
     *                     the annotations on that parameter returned by
     *                     <code>Class.getParameterAnnotations</code>.
     * @return a MessageBodyReader that matches the supplied criteria or null
     *         if none is found.
     */
    <T> MessageBodyReader<T> getMessageBodyReader(Class<T> type,
                                                 Type genericType, Annotation
                                                 annotations[], MediaType mediaType);

    /**
```
* Get a message body writer that matches a set of criteria. The set of
* writers is first filtered by comparing the supplied value of
* `{@code mediaType}` with the value of each writer's
* `{@link javax.ws.rs.Produces}`, ensuring the supplied value of
* `{@code type}` is assignable to the generic type of the reader, and
* eliminating those that do not match.
* The list of matching writers is then ordered with those with the best
* matching values of `{@link javax.ws.rs.Produces} (x/y > x/#7;* > *#/7;*)`
* sorted first. Finally, the
* `{@link MessageBodyWriter#isWriteable}`
* method is called on each writer in order using the supplied criteria and
* the first writer that returns `{@code true}` is selected and returned.
*
* `{@param mediaType} the media type of the data that will be written.
* `{@param type} the class of object that is to be written.
* `{@param genericType} the type of object to be written. E.g. if the
* message body is to be produced from a field, this will be
* the declared type of the field as returned by
* `<code>Field.getGenericType</code>`.
* `{@param annotations} an array of the annotations on the declaration of the
* artifact that will be written. E.g. if the
* message body is to be produced from a field, this will be
* the annotations on that field returned by
* `<code>Field.getDeclaredAnnotations</code>`.
* `{@return} a MessageBodyReader that matches the supplied criteria or null
* if none is found.
*`*/

```java
<T> MessageBodyWriter<T> getMessageBodyWriter(Class<T> type,
                                            Type genericType, Annotation
                                            annotations[], MediaType mediaType);
```

/**
* Get an exception mapping provider for a particular class of exception.
* Returns the provider whose generic type is the nearest superclass of
* `{@code type}.
*`*
* `{@param type} the class of exception
* `{@return} an `{@link ExceptionMapper}` for the supplied type or null if none
* is found.
*`*/

```java
<T extends Throwable> ExceptionMapper<T> getExceptionMapper(Class<T> type);
```

/**
* Get a context resolver for a particular type of context and media type.
* The set of resolvers is first filtered by comparing the supplied value of
* `{@code mediaType}` with the value of each resolver's
* `{@link javax.ws.rs.Produces}`, ensuring the generic type of the context
* resolver is assignable to the supplied value of `{@code contextType}`, and
* eliminating those that do not match. If only one resolver matches the
criteria then it is returned. If more than one resolver matches then the
list of matching resolvers is ordered with those with the best
matching values of (\cite{javax.ws.rs.Produces} x/y > x&47;* > *&47;*)
sorted first. A proxy is returned that delegates calls to
\cite{ContextResolver#getContext(java.lang.Class)} to each matching context
resolver in order and returns the first non-null value it obtains or null
if all matching context resolvers return null.

* @param contextType the class of context desired
* @param mediaType the media type of data for which a context is required.
* @return a matching context resolver instance or null if no matching
context providers are found.
*/
<T> ContextResolver<T> getContextResolver(Class<T> contextType,
                MediaType mediaType);
}

A Providers instance is injectable into MessageBodyReader or Writers:

```java
@Provider
@Consumes("multipart/fixed")
public class MultipartProvider implements MessageBodyReader {

    private @Context Providers providers;

    ...

}
```

### 18.4. Configuring Document Marshalling

XML document parsers are subject to a form of attack known as the XXE (Xml eXternal Entity) Attack (\cite{http://www.securiteam.com/securitynews/6D0100A5PU.html}), in which expanding an external entity causes an unsafe file to be loaded. For example, the document

```xml
<?xml version="1.0"?>
<!DOCTYPE foo
[<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
<search>
```
could cause the passwd file to be loaded.

By default, Resteasy's built-in unmarshaller for org.w3c.dom.Document documents will not expand external entities, replacing them by the empty string instead. It can be configured to replace external entities by values defined in the DTD by setting the context parameter to "true" in the web.xml file:

```
<context-param>
  <param-name>resteasy.document.expand.entity.references</param-name>
  <param-value>true</param-value>
</context-param>
```

Another way of dealing with the problem is by prohibiting DTDs, which Resteasy does by default. This behavior can be changed by setting the context parameter to "false".

Documents are also subject to Denial of Service Attacks when buffers are overrun by large entities or too many attributes. For example, if a DTD defined the following entities

```
<!ENTITY foo 'foo'>
<!ENTITY foo1 '&foo;&foo;&foo;&foo;&foo;&foo;&foo;&foo;&foo;&foo;'>
<!ENTITY foo2 '&foo1;&foo1;&foo1;&foo1;&foo1;&foo1;&foo1;&foo1;&foo1;&foo1;'>
<!ENTITY foo3 '&foo2;&foo2;&foo2;&foo2;&foo2;&foo2;&foo2;&foo2;&foo2;&foo2;'>
<!ENTITY foo4 '&foo3;&foo3;&foo3;&foo3;&foo3;&foo3;&foo3;&foo3;&foo3;&foo3;'>
<!ENTITY foo5 '&foo4;&foo4;&foo4;&foo4;&foo4;&foo4;&foo4;&foo4;&foo4;&foo4;'>
<!ENTITY foo6 '&foo5;&foo5;&foo5;&foo5;&foo5;&foo5;&foo5;&foo5;&foo5;&foo5;'>
```

then the expansion of &foo6; would result in 1,000,000 foos. By default, Resteasy will limit the number of expansions and the number of attributes per entity. The exact behavior depends on the underlying parser. The limits can be turned off by setting the context parameter to "false".
Chapter 19. JAXB providers

As required by the specification, RESTEasy JAX-RS includes support for (un)marshalling JAXB annotated classes. RESTEasy provides multiple JAXB Providers to address some subtle differences between classes generated by XJC and classes which are simply annotated with @XmlRootElement, or working with JAXBElement classes directly.

For the most part, developers using the JAX-RS API, the selection of which provider is invoked will be completely transparent. For developers wishing to access the providers directly (which most folks won’t need to do), this document describes which provider is best suited for different configurations.

A JAXB Provider is selected by RESTEasy when a parameter or return type is an object that is annotated with JAXB annotations (such as @XmlRootElement or @XmlType) or if the type is a JAXBElement. Additionally, the resource class or resource method will be annotated with either a @Consumes or @Produces annotation and contain one or more of the following values:

- text/*+xml
- application/*+xml
- application/*+fastinfoset
- application/*+json

RESTEasy will select a different provider based on the return type or parameter type used in the resource. This section describes how the selection process works.

@XmlRootElement When a class is annotated with a @XmlRootElement annotation, RESTEasy will select the JAXBXmlRootElementProvider. This provider handles basic marshaling and unmarshaling of custom JAXB entities.

@XmlType Classes which have been generated by XJC will most likely not contain an @XmlRootElement annotation. In order for these classes to marshalled, they must be wrapped within a JAXBElement instance. This is typically accomplished by invoking a method on the class which serves as the XmlRegistry and is named ObjectFactory.

The JAXBXmlTypeProvider provider is selected when the class is annotated with an XmlType annotation and not an XmlRootElement annotation.

This provider simplifies this task by attempting to locate the XmlRegistry for the target class. By default, a JAXB implementation will create a class called ObjectFactory and is located in the same package as the target class. When this class is located, it will contain a "create" method that takes the object instance as a parameter. For example, if the target type is called "Contact", then the ObjectFactory class will have a method:
public JAXBElem createContact(Contact value) {..}

JAXBElem<?> If your resource works with the JAXBElem class directly, the RESTEasy runtime will select the JAXBElemProvider. This provider examines the ParameterizedType value of the JAXBElem in order to select the appropriate JAXBContext.

19.1. JAXB Decorators

Resteasy’s JAXB providers have a pluggable way to decorate Marshaller and Unmarshaller instances. The way it works is that you can write an annotation that can trigger the decoration of a Marshaller or Unmarshaller. Your decorators can do things like set Marshaller or Unmarshaller properties, set up validation, stuff like that. Here’s an example. Let’s say we want to have an annotation that will trigger pretty-printing, nice formatting, of an XML document. If we were doing raw JAXB, we would set a property on the Marshaller of Marshaller.JAXB_FORMATTED_OUTPUT. Let’s write a Marshaller decorator.

First we define a annotation:

```java
import org.jboss.resteasy.annotations.Decorator;

@Target({ElementType.TYPE, ElementType.METHOD, ElementType.PARAMETER, ElementType.FIELD})
@Retention(RetentionPolicy.RUNTIME)
@Decorator(processor = PrettyProcessor.class, target = Marshaller.class)
public @interface Pretty {}
```

To get this to work, we must annotate our @Pretty annotation with a meta-annotation called @Decorator. The target() attribute must be the JAXB Marshaller class. The processor() attribute is a class we will write next.

```java
import org.jboss.resteasy.core.interception.DecoratorProcessor;
import org.jboss.resteasy.annotations.interception.DecorateTypes;

import javax.xml.bind.Marshaller;
import javax.xml.bind.PropertyException;
import javax.ws.rs.core.MediaType;
import javax.ws.rs.Produces;
import java.lang.annotation.Annotation;
```
Pluggable JAXBContext's with ContextResolvers

/**
 * @author <a href="mailto:bill@burkecentral.com">Bill Burke</a>
 * @version $Revision: 1 $
 */
@DecorateTypes({"text/*+xml", "application/*+xml"})
public class PrettyProcessor implements DecoratorProcessor<Marshaller, Pretty> {
    public Marshaller decorate(Marshaller target, Pretty annotation,
        Class type, Annotation[] annotations, MediaType mediaType) {
        target.setProperty(Marshaller.JAXB_FORMATTED_OUTPUT, Boolean.TRUE);
    }
}

The processor implementation must implement the DecoratorProcessor interface and should also be annotated with @DecorateTypes. This annotation specifies what media types the processor can be used with. Now that we've defined our annotation and our Processor, we can use it on our JAX-RS resource methods or JAXB types as follows:

@GET
@Pretty
@Produces("application/xml")
public SomeJAXBObject get() {...}

If you are confused, check the Resteasy source code for the implementation of @XmlHeader

19.2. Pluggable JAXBContext's with ContextResolvers

You should not use this feature unless you know what you're doing.

Based on the class you are marshalling/unmarshalling, RESTEasy will, by default create and cache JAXBContext instances per class type. If you do not want RESTEasy to create JAXBContexts, you can plug-in your own by implementing an instance of javax.ws.rs.ext.ContextResolver

public interface ContextResolver<T> {
    T getContext(Class<?> type);
}
You must provide a @Produces annotation to specify the media type the context is meant for. You must also make sure to implement ContextResolver<JAXBContext>. This helps the runtime match to the correct context resolver. You must also annotate the ContextResolver class with @Provider.

There are multiple ways to make this ContextResolver available.

1. Return it as a class or instance from a javax.ws.rs.core.Application implementation

2. List it as a provider with resteasy.providers

3. Let RESTEasy automatically scan for it within your WAR file. See Configuration Guide

4. Manually add it via ResteasyProviderFactory.getInstance().registerProvider(Class) or registerProviderInstance(Object)

19.3. JAXB + XML provider

Resteasy is required to provide JAXB provider support for XML. It has a few extra annotations that can help code your app.

19.3.1. @XmlHeader and @Stylesheet

Sometimes when outputting XML documents you may want to set an XML header. Resteasy provides the @org.jboss.resteasy.annotations.providers.jaxb.XmlHeader annotation for this. For example:
public String getName()
{
    return name;
}

public void setName(String name)
{
    this.name = name;
}
}

@Path("/test")
public static class TestService
{

    @GET
    @Path("/header")
    @Produces("application/xml")
    @XmlHeader("<?xml-stylesheet type='text/xsl' href='${baseuri}foo.xsl' ?>")
    public Thing get()
    {
        Thing thing = new Thing();
        thing.setName("bill");
        return thing;
    }
}

The @XmlHeader here forces the XML output to have an xml-stylesheet header. This header could also have been put on the Thing class to get the same result. See the javadocs for more details on how you can use substitution values provided by resteasy.

Resteasy also has a convenience annotation for stylesheet headers. For example:

@XmlRootElement
public static class Thing
{
    private String name;

    public String getName()
    {
        return name;
    }

    public void setName(String name)
{  
    this.name = name;  
  }
}

@Path("/test")
public static class TestService
{
  
  @GET  
  @Path("/stylesheet")  
  @Path("/stylesheet")  
  @Produces("application/xml")  
  @Produces("application/xml")  
  @Stylesheet(type="text/css", href=${basepath}foo.xsl")  
  @Stylesheet(type="text/css", href=${basepath}foo.xsl")  
  @Junk  
  @Junk  
  public Thing getStyle()  
  {  
    Thing thing = new Thing();  
    thing.setName("bill");  
    return thing;  
  }  
}

19.4. JAXB + JSON provider

RESTEasy allows you to marshall JAXB annotated POJOs to and from JSON. This provider wraps
the Jettison JSON library to accomplish this. You can obtain more information about Jettison and
how it works from:

http://jettison.codehaus.org/

To use this integration with Jettison you need to import the resteasy-jettison-provider Maven
module. Older versions of RESTEasy used to include this within the resteasy-jaxb-provider but
we decided to modularize it more.

Jettison has two mapping formats. One is BadgerFish the other is a Jettison Mapped Convention
format. The Mapped Convention is the default mapping.

For example, consider this JAXB class:

(XmlRootElement(name = "book")  
public class Book  
{  
private String author;  
private String ISBN;  
private String title;
public Book()
{
}

public Book(String author, String ISBN, String title)
{
    this.author = author;
    this.ISBN = ISBN;
    this.title = title;
}

@XmlElement
public String getAuthor()
{
    return author;
}

public void setAuthor(String author)
{
    this.author = author;
}

@XmlElement
public String getISBN()
{
    return ISBN;
}

public void setISBN(String ISBN)
{
    this.ISBN = ISBN;
}

@XmlAttribute
public String getTitle()
{
    return title;
}

public void setTitle(String title)
{
    this.title = title;
}
Notice that element values have a map associated with them and to get to the value of the element, you must access the "$" variable. Here's an example of accessing the book in Javascript:

```javascript
var data = eval("(" + xhr.responseText + ")");
document.getElementById("zone").innerHTML = data.book.$title;
document.getElementById("zone").innerHTML += data.book.$author;
```

To use the BadgerFish Convention you must use the `@org.jboss.resteasy.annotations.providers.jaxb.json.BadgerFish` annotation on the JAXB class you are marshalling/unmarshalling, or, on the JAX-RS resource method or parameter:

```java
@BadgerFish
@XmlElement(name = "book")
public class Book { ... }
```

If you are returning a book on the JAX-RS method and you don't want to (or can't) pollute your JAXB classes with RESTEasy annotations, add the annotation to the JAX-RS method:

```java
@BadgerFish
@GET
public Book getBook(...) { ... }
```

If a Book is your input then you put it on the parameter:
@POST
class public void newBook(@BadgerFish Book book) {...}

The default Jettison Mapped Convention would return JSON that looked like this:

```
{ "book" :
   {
      "@title":"EJB 3.0",
      "author":"Bill Burke",
      "ISBN":596529260
   }  
}
```

Notice that the @XmlAttribute "title" is prefixed with the '@' character. Unlike BadgerFish, the '$' does not represent the value of element text. This format is a bit simpler than the BadgerFish convention which is why it was chose as a default. Here's an example of accessing this in Javascript:

```
var data = eval("(" + xhr.responseText + ")");
document.getElementById("zone").innerHTML = data.book.@title;
document.getElementById("zone").innerHTML += data.book.author;
```

The Mapped Convention allows you to fine tune the JAXB mapping using the @org.jboss.resteasy.annotations.providers.jaxb.json.Mapped annotation. You can provide an XML Namespace to JSON namespace mapping. For example, if you defined your JAXB namespace within your package-info.java class like this:

```
@javax.xml.bind.annotation.XmlSchema(namespace="http://jboss.org/books")
package org.jboss.resteasy.test.books;
```

You would have to define a JSON to XML namespace mapping or you would receive an exception of something like this:
java.lang(IllegalStateException: Invalid JSON namespace: http://jboss.org/books
at
org.codehaus.jettison.mapped.MappedNamespaceConvention.getJSONNamespace(MappedNamespaceConvention.java:151)
at
org.codehaus.jettison.mapped.MappedNamespaceConvention.createKey(MappedNamespaceConvention.java:158)
at
org.codehaus.jettison.mapped.MappedXMLStreamWriter.writeStartElement(MappedXMLStreamWriter.java:190)
To fix this problem you need another annotation, @Mapped. You use the @Mapped annotation on your JAXB classes, on your JAX-RS resource method, or on the parameter you are unmarshalling

```java
import org.jboss.resteasy.annotations.providers.jaxb.json.Mapped;
import org.jboss.resteasy.annotations.providers.jaxb.json.XmlNsMap;
...

@GET
@Produces("application/json")
@Mapped(namespaceMap = {
    @XmlNsMap(namespace = "http://jboss.org/books", jsonName = "books")
})
public Book get() {...}
```

Besides mapping XML to JSON namespaces, you can also force @XmlAttribute's to be marshaled as XMLElements.

```java
@Mapped(attributeAsElements={"title"})
@XmlRootElement(name = "book")
public class Book {...}
```

If you are returning a book on the JAX-RS method and you don't want to (or can't) pollute your JAXB classes with RESTEasy annotations, add the annotation to the JAX-RS method:

```java
@Mapped(attributeAsElements={"title"})
@GET
```

80
If a Book is your input then you put it on the parameter:

@POST
public void newBook(@Mapped(attributeAsElements="title") Book book) {...}

19.5. JAXB + FastinfoSet provider

RESTEasy supports the FastinfoSet mime type with JAXB annotated classes. Fast info set documents are faster to serialize and parse, and smaller in size, than logically equivalent XML documents. Thus, fast info set documents may be used whenever the size and processing time of XML documents is an issue. It is configured the same way the XML JAXB provider is so really no other documentation is needed here.

To use this integration with FastinfoSet you need to import the resteasy-fastinfoSet-provider Maven module. Older versions of RESTEasy used to include this within the resteasy-jaxb-provider but we decided to modularize it more.

19.6. Arrays and Collections of JAXB Objects

RESTEasy will automatically marshal arrays, java.util.Set's, and java.util.List's of JAXB objects to and from XML, JSON, FastinfoSet (or any other new JAXB mapper Restasy comes up with).
The above resource can publish and receive JAXB objects. It is assumed that are wrapped in a collection element.
Arrays and Collections of JAXB Objects

You can change the namespace URI, namespace tag, and collection element name by using the `@org.jboss.resteasy.annotations.providers.jaxb.Wrapped` annotation on a parameter or method.

```java
@Target({ElementType.PARAMETER, ElementType.METHOD})
@Retention(RetentionPolicy.RUNTIME)
public @interface Wrapped {
    String element() default "collection";
    String namespace() default "http://jboss.org/resteasy";
    String prefix() default "resteasy";
}
```

So, if we wanted to output this XML:

```xml
<foo:list xmlns:foo="http://foo.org">
    <customer><name>bill</name></customer>
    <customer><name>monica</name></customer>
</foo:list>
```

We would use the `@Wrapped` annotation as follows:

```java
@GET
@Path("list")
@Produces("application/xml")
@Wrapped(element="list", namespace="http://foo.org", prefix="foo")
public List<Customer> getCustomerSet() {
```
Chapter 19. JAXB providers

```java
List<Customer> list = new ArrayList<Customer>();
list.add(new Customer("bill");
list.add(new Customer("monica");

return list;
}
```

19.6.1. JSON and JAXB Collections/arrays

Resteasy supports using collections with JSON. It encloses lists, sets, or arrays of returned JAXB objects within a simple JSON array. For example:

```java
@XmlElement
@XmlAccessorType(XmlAccessType.FIELD)
public static class Foo
{
  @XmlAttribute
  private String test;

  public Foo()
  {
  }

  public Foo(String test)
  {
    this.test = test;
  }

  public String getTest()
  {
    return test;
  }

  public void setTest(String test)
  {
    this.test = test;
  }
}
```

This a List or array of this Foo class would be represented in JSON like this:
It also expects this format for input

### 19.7. Maps of JAXB Objects

RESTEasy will automatically marshal maps of JAXB objects to and from XML, JSON, Fastinfoset (or any other new JAXB mapper Restasy comes up with). Your parameter or method return type must be a generic with a String as the key and the JAXB object's type.

```java
@XmlRootElement(namespace = "http://foo.com")
public static class Foo
{
  @XmlAttribute
  private String name;

  public Foo()
  {
  }

  public Foo(String name)
  {
    this.name = name;
  }

  public String getName()
  {
    return name;
  }
}
@Path("/map")
public static class MyResource
{
  @POST
  @Produces("application/xml")
  @Consumes("application/xml")
  public Map<String, Foo> post(Map<String, Foo> map)
  {
    Assert.assertEquals(2, map.size());
    Assert.assertNotNull(map.get("bill"));
```

The above resource can publish and receive JAXB objects within a map. By default, they are wrapped in a "map" element in the default namespace. Also, each "map" element has zero or more "entry" elements with a "key" attribute.

You can change the namespace URI, namespace prefix and map, entry, and key element and attribute names by using the @org.jboss.resteasy.annotations.providers.jaxb.WrappedMap annotation on a parameter or method.
So, if we wanted to output this XML

```xml
<hashmap>
  <hashentry hashkey="bill" xmlns:foo="http://foo.com">
    <foo:foo name="bill"/>
  </hashentry>
</hashmap>
```

We would use the `@WrappedMap` annotation as follows:

```java
@Path("/map")
public static class MyResource {
  
  @GET
  @Produces("application/xml")
  @WrappedMap(map="hashmap", entry="hashentry", key="hashkey")
  public Map<String, Foo> get()
  {
    ... return map;
  }
}
```

### 19.7.1. JSON and JAXB maps

Resteasy supports using maps with JSON. It encloses maps returned JAXB objects within a simple JSON map. For example:
Chapter 19. JAXB providers

```java
@XmlElement
@XmlAccessorType(XmlAccessType.FIELD)
public static class Foo
{
    @XmlAttribute
    private String test;

    public Foo()
    {
    }

    public Foo(String test)
    {
        this.test = test;
    }

    public String getTest()
    {
        return test;
    }

    public void setTest(String test)
    {
        this.test = test;
    }
}
```

This a List or array of this Foo class would be represented in JSON like this:

```json
{ "entry1" : {"foo":{"@test":"bill"}}, "entry2" : {"foo":{"@test":"monica"}}}"
```

It also expects this format for input

**19.7.2. Possible Problems with Jettison Provider**

If you have the resteasy-jackson-provider-xxx.jar in your classpath, the Jackson JSON provider will be triggered. This will screw up code that is dependent on the Jettison JAXB/JSon provider. If you had been using the Jettison JAXB/Json providers, you must either remove Jackson from your WEB-INF/lib or classpath, or use the @NoJackson annotation on your JAXB classes.
19.8. Interfaces, Abstract Classes, and JAXB

Some objects models use abstract classes and interfaces heavily. Unfortunately, JAXB doesn't work with interfaces that are root elements and RESTEasy can't unmarshal parameters that are interfaces or raw abstract classes because it doesn't have enough information to create a JAXBContext. For example:

```java
public interface IFoo {}

@XmlRootElement
public class RealFoo implements IFoo {}

@Path("/jaxb")
public class MyResource {

@PUT
@Consumes("application/xml")
public void put(IFoo foo) {...}
}
```

In this example, you would get an error from RESTEasy of something like "Cannot find a MessageBodyReader for...". This is because RESTEasy does not know that implementations of IFoo are JAXB classes and doesn't know how to create a JAXBContext for it. As a workaround, RESTEasy allows you to use the JAXB annotation @XmlSeeAlso on the interface to correct the problem. (NOTE, this will not work with manual, hand-coded JAXB).

```java
@XmlSeeAlso(RealFoo.class)
public interface IFoo {}
```

The extra @XmlSeeAlso on IFoo allows RESTEasy to create a JAXBContext that knows how to unmarshal RealFoo instances.

19.9. Configurating JAXB Marshalling

As a consumer of XML datasets, JAXB is subject to a form of attack known as the XXE (Xml eXternal Entity) Attack (http://www.securiteam.com/securitynews/6D0100A5PU.html), in which expanding an external entity causes an unsafe file to be loaded. Preventing the expansion of external entities is discussed in Section 18.4, "Configuring Document Marshalling". The same context parameter,
applies to JAXB unmarshallers as well.

Section 18.4, “Configuring Document Marshalling” also discusses the prohibition of DTDs and the imposition of limits on entity expansion and the number of attributes per element. The context parameters and discussed there, and their default values, also apply to the representation of JAXB objects.
Chapter 20. Resteasy Atom Support


"Atom is an XML-based document format that describes lists of related information known as "feeds". Feeds are composed of a number of items, known as "entries", each with an extensible set of attached metadata. For example, each entry has a title. The primary use case that Atom addresses is the syndication of Web content such as weblogs and news headlines to Web sites as well as directly to user agents."

Atom is the next-gen RSS feed. Although it is used primarily for the syndication of blogs and news, many are starting to use this format as the envelope for Web Services, for example, distributed notifications, job queues, or simply a nice format for sending or receiving data in bulk from a service.

20.1. Resteasy Atom API and Provider

RESTEasy has defined a simple object model in Java to represent Atom and uses JAXB to marshal and unmarshal it. The main classes are in the org.jboss.resteasy.plugins.providers.atom package and are Feed, Entry, Content, and Link. If you look at the source, you'd see that these are annotated with JAXB annotations. The distribution contains the javadocs for this project and are a must to learn the model. Here is a simple example of sending an atom feed using the Resteasy API.

```java
import org.jboss.resteasy.plugins.providers.atom.Content;
import org.jboss.resteasy.plugins.providers.atom.Entry;
import org.jboss.resteasy.plugins.providers.atom.Feed;
import org.jboss.resteasy.plugins.providers.atom.Link;
import org.jboss.resteasy.plugins.providers.atom.Person;

@Path("atom")
public class MyAtomService
{

    @GET
    @Path("feed")
    @Produces("application/atom+xml")
    public Feed getFeed() throws URISyntaxException
    {
        Feed feed = new Feed();
        feed.setId(new URI("http://example.com/42"));
        feed.setTitle("My Feed");
        feed.setUpdated(new Date());
        Link link = new Link();
        link.setHref(new URI("http://localhost"));
```
Because Resteasy's atom provider is JAXB based, you are not limited to sending atom objects using XML. You can automatically re-use all the other JAXB providers that Resteasy has like JSON and fastinfoset. All you have to do is have "atom+" in front of the main subtype. i.e. @Produces("application/atom+json") or @Consumes("application/atom+fastinfoset")

### 20.2. Using JAXB with the Atom Provider

The org.jboss.resteasy.plugins.providers.atom.Content class allows you to unmarshal and marshal JAXB annotated objects that are the body of the content. Here's an example of sending an Entry with a Customer object attached as the body of the entry's content.

```java
@XmlElement
private String name;

public Customer()
{

}

public Customer(String name)
{
    this.name = name;
}

public String getName()
{
    return name;
}
```
The `Content.setJAXBObject()` method is used to tell the content object you are sending back a Java JAXB object and want it marshalled appropriately. If you are using a different base format other than XML, i.e. "application/atom+json", this attached JAXB object will be marshalled into that same format.

If you have an atom document as your input, you can also extract JAXB objects from Content using the `Content.getJAXBObject(Class clazz)` method. Here is an example of an input atom document and extracting a Customer object from the content.

```java
@Path("atom")
public static class AtomServer {

    @Path("entry")
    @Produces("application/atom+xml")
    public Entry getEntry()
    {
        Entry entry = new Entry();
        entry.setTitle("Hello World");
        Content content = new Content();
        content.setJAXBObject(new Customer("bill"));
        entry.setContent(content);
        return entry;
    }
}
```
Chapter 21. JSON Support via Jackson

Besides the Jettision JAXB adapter for JSON, Resteasy also support integration with the Jackson project. Many users find the output from Jackson much much nicer than the Badger format or Mapped format provided by Jettison. Jackson lives at http://jackson.codehaus.org. It allows you to easily marshal Java objects to and from JSON. It has a Java Bean based model as well as JAXB like APIs. Resteasy integrates with the JavaBean model as described at this url: http://jackson.codehaus.org/Tutorial.

While Jackson does come with its own JAX-RS integration. Resteasy expanded it a little. To include it within your project, just add this maven dependency to your build. Resteasy supports both Jackson 1.9.x and Jackson 2.2.x. Read further on how to use each.

21.1. Using Jackson 1.9.x Outside of JBoss AS7

If you’re deploying Resteasy outside of JBoss AS7 add the resteasy jackson provider to your WAR pom.xml build

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-jackson-provider</artifactId>
  <version>3.0.9.Final</version>
</dependency>
```

21.2. Using Jackson 1.9.x Inside of JBoss AS7

If you’re deploying Resteasy with JBoss AS7, there’s nothing you need to do except to make sure you’ve updated your AS7 distribution with the latest and greatest Resteasy. See the installation sectio of this documentation for more details.

21.3. Using Jackson 2.2.x Outside of JBoss AS7

If you’re deploying Resteasy outside of JBoss AS7 add the resteasy jackson provider to your WAR pom.xml build

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-jackson2-provider</artifactId>
</dependency>
```
21.4. Using Jackson 2.2.x Inside of JBoss AS7

If you want to use Jackson 2.2.x inside of JBoss AS7 you'll have to create a jboss-deployment-structure.xml file within your WEB-INF directory. By default AS7 includes the Jackson 1.9.x JAX-RS integration, so you'll want to exclude it from your dependencies, and add the jackson2 ones.

```xml
<jboss-deployment-structure>
  <deployment>
    <exclusions>
      <module name="org.jboss.resteasy.resteasy-jackson-provider"/>
    </exclusions>
    <dependencies>
      <module name="org.jboss.resteasy.resteasy-jackson2-provider" services="import"/>
    </dependencies>
  </deployment>
</jboss-deployment-structure>
```

21.5. Additional Resteasy Specifics

The first extra piece that Resteasy added to the integration was to support "application/*+json". Jackson would only accept "application/json" and "text/json" as valid media types. This allows you to create json-based media types and still let Jackson marshal things for you. For example:

```java
@Path("/customers")
public class MyService {

  @GET
  @Produces("application/vnd.customer+json")
  public Customer[] getCustomers() {
  }
}
```

Another problem that occurs is when you are using the Resteasy JAXB providers alongside Jackson. You may want to use Jettison and JAXB to output your JSON instead of Jackson.
In this case, you must either not install the Jackson provider, or use the annotation @org.jboss.resteasy.annotations.providers.NoJackson on your JAXB annotated classes. For example:

```java
@XmlElement
@NoJackson
public class Customer {...}

@Path("/customers")
public class MyService {
  @GET
  @Produces("application/vnd.customer+json")
  public Customer[] getCustomers() {}  
}
```

If you can't annotate the JAXB class with @NoJackson, then you can use the annotation on a method parameter. For example:

```java
@XmlElement
public class Customer {...}

@Path("/customers")
public class MyService {

  @GET
  @Produces("application/vnd.customer+json")
  @NoJackson
  public Customer[] getCustomers() {}  

  @POST
  @Consumes("application/vnd.customer+json")
  public void createCustomer(@NoJackson Customer[] customers) {...}
}
```
21.6. Possible Conflict With JAXB Provider

If your Jackson classes are annotated with JAXB annotations and you have the resteasy-jaxb-provider in your classpath, you may trigger the Jettision JAXB marshalling code. To turn off the JAXB json marshaller use the @org.jboss.resteasy.annotations.providers.jaxb.IgnoreMediaTypes("application/*+json") on your classes.

21.7. JSONP Support

If you’re using Jackson, Resteasy has JSONP [http://en.wikipedia.org/wiki/JSONP] that you can turn on by adding the provider org.jboss.resteasy.plugins.providers.jackson.JacksonJsonpInterceptor (Jackson2JsonpInterceptor if you’re using the Jackson2 provider) to your deployments. If the media type of the response is json and a callback query parameter is given, the response will be a javascript snippet with a method call of the method defined by the callback parameter. For example:

GET /resources/stuff?callback=processStuffResponse

will produce this response:

processStuffResponse(<nomal JSON body>)

This supports the default behavior of jQuery [http://api.jquery.com/jQuery.ajax/].

You can change the name of the callback parameter by setting the callbackQueryParameter property.

21.8. Jackson JSON Decorator

If you are using the Jackson 2.2.x provider, Resteasy has provided a pretty-printing annotation similar with the one in JAXB provider:

org.jboss.resteasy.annotations.providers.jackson.Formatted

Here is an example:
Jackson JSON Decorator

```java
@GET
@Produces("application/json")
@Path("/formatted/{id}")
@Formatted
public Product getFormattedProduct()
{
    return new Product(333, "robot");
}
```

As the example shown above, the `@Formatted` annotation will enable the underlying Jackson option "SerializationFeature.INDENT_OUTPUT".
Chapter 22. JSON Support via Java EE 7 JSON-P API

No, this is not the JSONP you are thinking of! JSON-P is a new Java EE 7 JSON parsing API. Horrible name for a new JSON parsing API!! What were they thinking? Anyways, Resteasy has a provider for it. If you are using Wildfly, it is required by Java EE 7 so you will have it automatically bundled. Otherwise, use this maven dependency.

```xml
<dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-json-p-provider</artifactId>
    <version>3.0.9.Final</version>
</dependency>
```

It has built in support for JsonObject, JSONArray, and JsonStructure as request or response entities. It should not conflict with Jackson or Jettison if you have that in your path too.
Chapter 23. Multipart Providers

Resteasy has rich support for the "multipart/*" and "multipart/form-data" mime types. The multipart mime format is used to pass lists of content bodies. Multiple content bodies are embedded in one message. "multipart/form-data" is often found in web application HTML Form documents and is generally used to upload files. The form-data format is the same as other multipart formats, except that each inlined piece of content has a name associated with it.

RESTEasy provides a custom API for reading and writing multipart types as well as marshalling arbitrary List (for any multipart type) and Map (multipart/form-data only) objects

23.1. Input with multipart/mixed

When writing a JAX-RS service, RESTEasy provides an interface that allows you to read in any multipart mime type. org.jboss.resteasy.plugins.providers.multipart.MultipartInput

```java
package org.jboss.resteasy.plugins.providers.multipart;

public interface MultipartInput
{
    List<InputPart> getParts();

    String getPreamble();

    // You must call close to delete any temporary files created
    // Otherwise they will be deleted on garbage collection or on JVM exit
    void close();
}

class InputPart
{
    MultivaluedMap<String, String> getHeaders();

    String getBodyAsString();

    <T> T getBody(Class<T> type, Type genericType) throws IOException;

    <T> T getBody(org.jboss.resteasy.util.GenericType<T> type) throws IOException;

    MediaType getMediaType();

    boolean isContentTypeFromMessage();
}
```
MultipartInput is a simple interface that allows you to get access to each part of the multipart message. Each part is represented by an InputPart interface. Each part has a set of headers associated with it. You can unmarshall the part by calling one of the getBody() methods. The Type genericType parameter can be null, but the Class type parameter must be set. Resteasy will find a MessageBodyReader based on the media type of the part as well as the type information you pass in. The following piece of code is unmarshalling parts which are XML into a JAXB annotated class called Customer.

```java
@Path("/multipart")
public class MyService {
    @PUT
    @Consumes("multipart/mixed")
    public void put(MultipartInput input) {
        List<Customer> customers = new ArrayList...;
        for (InputPart part : input.getParts()) {
            Customer cust = part.getBody(Customer.class, null);
            customers.add(cust);
        }
        input.close();
    }
}
```

Sometimes you may want to unmarshall a body part that is sensitive to generic type metadata. In this case you can use the org.jboss.resteasy.util.GenericType class. Here’s an example of unmarshalling a type that is sensitive to generic type metadata.

```java
@Path("/multipart")
public class MyService {
    @PUT
    @Consumes("multipart/mixed")
    public void put(MultipartInput input) {
        for (InputPart part : input.getParts()) {
            List<Customer> cust = part.getBody(new GenericType<List<Customer>>() {});
            input.close();
        }
    }
}
```
Use of GenericType is required because it is really the only way to obtain generic type information at runtime.

### 23.2. java.util.List with multipart data

If your body parts are uniform, you do not have to manually unmarshall each and every part. You can just provide a java.util.List as your input parameter. It must have the type it is unmarshalling with the generic parameter of the List type declaration. Here’s an example again of unmarshalling a list of customers.

```java
t@Path("/multipart")
public class MyService
{
    @PUT
    @Consumes("multipart/mixed")
    public void put(List<Customer> customers)
    {
        ...  
    }
}
```

### 23.3. Input with multipart/form-data

When writing a JAX-RS service, RESTEasy provides an interface that allows you to read in multipart/form-data mime type. “multipart/form-data” is often found in web application HTML Form documents and is generally used to upload files. The form-data format is the same as other multipart formats, except that each inlined piece of content has a name associated with it. The interface used for form-data input is org.jboss.resteasy.plugins.providers.multipart.MultipartFormDataInput

```java
public interface MultipartFormDataInput extends MultipartInput
{
    @Deprecated
    Map<String, InputPart> getFormData();
    Map<String, List<InputPart>> getFormDataMap();
    <T> T getFormDataPart(String key, Class<T> rawType, Type genericType) throws IOException;
}
```
Chapter 23. Multipart Providers

```java
<T> T getFormDataPart(String key, GenericType<T> type) throws IOException;
}
```

It works in much the same way as MultipartInput described earlier in this chapter.

### 23.4. java.util.Map with multipart/form-data

With form-data, if your body parts are uniform, you do not have to manually unmarshall each and every part. You can just provide a java.util.Map as your input parameter. It must have the type it is unmarshalling with the generic parameter of the List type declaration. Here's an example of unmarshalling a Map of Customer objects which are JAXB annotated classes.

```java
@Path("/multipart")
public class MyService
{
    @PUT
    @Consumes("multipart/form-data")
    public void put(Map<String, Customer> customers)
    {
        ...
    }
}
```

### 23.5. Input with multipart/related

When writing a JAX-RS service, RESTEasy provides an interface that allows you to read in multipart/related mime type. A multipart/related is used to indicate that message parts should not be considered individually but rather as parts of an aggregate whole. One example usage for multipart/related is to send a web page complete with images in a single message. Every multipart/related message has a root/start part that references the other parts of the message. The parts are identified by their "Content-ID" headers. multipart/related is defined by RFC 2387. The interface used for related input is org.jboss.resteasy.plugins.providers.multipart.MultipartRelatedInput

```java
public interface MultipartRelatedInput extends MultipartInput
{
    String getType();

    String getStart();

    String getStartInfo();
}
```
It works in much the same way as MultipartInput described earlier in this chapter.

## 23.6. Output with multipart

RESTEasy provides a simple API to output multipart data.

```java
package org.jboss.resteasy.plugins.providers.multipart;

public class MultipartOutput {
    public OutputPart addPart(Object entity, MediaType mediaType)
    public OutputPart addPart(Object entity, GenericType type, MediaType mediaType)
    public OutputPart addPart(Object entity, Class type, Type genericType, MediaType mediaType)
    public List<OutputPart> getParts()
    public String getBoundary()
    public void setBoundary(String boundary)
}

public class OutputPart {
    public MultivaluedMap<String, Object> getHeaders()
    public Object getEntity()
    public Class getType()
    public Type getGenericType()
    public MediaType getMediaType()
}
```
When you want to output multipart data it is as simple as creating a MultipartOutput object and calling addPart() methods. Resteasy will automatically find a MessageBodyWriter to marshall your entity objects. Like MultipartInput, sometimes you may have marshalling which is sensitive to generic type metadata. In that case, use GenericType. Most of the time though passing in an Object and its MediaType is enough. In the example below, we are sending back a "multipart/mixed" format back to the calling client. The parts are Customer objects which are JAXB annotated and will be marshalling into "application/xml".

@Path("/multipart")
public class MyService {
    @GET
    @Produces("multipart/mixed")
    public MultipartOutput get() {
        MultipartOutput output = new MultipartOutput();
        output.addPart(new Customer("bill"), MediaType.APPLICATION_XML_TYPE);
        output.addPart(new Customer("monica"), MediaType.APPLICATION_XML_TYPE);
        return output;
    }
}

23.7. Multipart Output with java.util.List

If your body parts are uniform, you do not have to manually marshall each and every part or even use a MultipartOutput object. You can just provide a java.util.List. It must have the generic type it is marshalling with the generic parameter of the List type declaration. You must also annotate the method with the @PartType annotation to specify what media type each part is. Here's an example of sending back a list of customers back to a client. The customers are JAXB objects.

@Path("/multipart")
public class MyService {
    @GET
    @Produces("multipart/mixed")
    @PartType("application/xml")
    public List<Customer> get() {
        ...
    }
}
23.8. Output with multipart/form-data

RESTEasy provides a simple API to output multipart/form-data.

```java
package org.jboss.resteasy.plugins.providers.multipart;

public class MultipartFormDataOutput extends MultipartOutput{
    public OutputPart addFormData(String key, Object entity, MediaType mediaType){
    }
    public OutputPart addFormData(String key, Object entity, GenericType type, MediaType mediaType){
    }
    public OutputPart addFormData(String key, Object entity, Class type, Type genericType, MediaType mediaType){
    }
    public Map<String, OutputPart> getFormData(){
    }
}
```

When you want to output multipart/form-data it is as simple as creating a MultipartFormDataOutput object and calling addFormData() methods. Resteasy will automatically find a MessageBodyWriter to marshall your entity objects. Like MultipartInput, sometimes you may have marshalling which is sensitive to generic type metadata. In that case, use GenericType. Most of the time though passing in an Object and its MediaType is enough. In the example below, we are sending back a "multipart/form-data" format back to the calling client. The parts are Customer objects which are JAXB annotated and will be marshalling into "application/xml".

```java
@Path("/form")
public class MyService{
    @GET
    @Produces("multipart/form-data")
    public MultipartFormDataOutput get(){
        MultipartFormDataOutput output = new MultipartFormDataOutput();
        output.addPart("bill", new Customer("bill"), MediaType.APPLICATION_XML_TYPE);
        output.addPart("monica", new Customer("monica"), MediaType.APPLICATION_XML_TYPE);
        return output;
    }
}
```
23.9. Multipart FormData Output with java.util.Map

If your body parts are uniform, you do not have to manually marshall each and every part or even use a MultipartFormDataOutput object. You can just provide a java.util.Map. It must have the generic type it is marshalling with the generic parameter of the Map type declaration. You must also annotate the method with the @PartType annotation to specify what media type each part is. Here's an example of sending back a list of customers back to a client. The customers are JAXB objects.

```java
@Path("/multipart")
public class MyService {
    @GET
    @Produces("multipart/form-data")
    @PartType("application/xml")
    public Map<String, Customer> get() {
        ...
    }
}
```

23.10. Output with multipart/related

RESTEasy provides a simple API to output multipart/related.

```java
package org.jboss.resteasy.plugins.providers.multipart;

public class MultipartRelatedOutput extends MultipartOutput {
    public OutputPart getRootPart() {
        public OutputPart addPart(Object entity, MediaType mediaType, String contentId, String contentTransferEncoding)
        public String getStartInfo()
        public void setStartInfo(String startInfo)
    }
}
```
When you want to output multipart/related it is as simple as creating a MultipartRelatedOutput object and calling addPart() methods. The first added part will be used as the root part of the multipart/related message. Resteasy will automatically find a MessageBodyWriter to marshall your entity objects. Like MultipartInput, sometimes you may have marshalling which is sensitive to generic type metadata. In that case, use GenericType. Most of the time though passing in an Object and its MediaType is enough. In the example below, we are sending back a "multipart/related" format back to the calling client. We are sending a html with 2 images.

```java
@Path("/related")
public class MyService {
  @GET
  @Produces("multipart/related")
  public MultipartRelatedOutput get() {
      MultipartRelatedOutput output = new MultipartRelatedOutput();
      output.setStartInfo("text/html");

      Map<String, String> mediaTypeParameters = new LinkedHashMap<String, String>();
      mediaTypeParameters.put("charset", "UTF-8");
      mediaTypeParameters.put("type", "text/html");
      output
          .addPart("<html><body>
          + "This is me: <img src='cid:http://example.org/me.png' />
          + "This is you: <img src='cid:http://example.org/you.png' />
          + "</body></html>",
          new MediaType("text", "html", mediaTypeParameters),
          "<mymessage.xml@example.org>", "8bit");
      output.addPart("// binary octets for me png",
          new MediaType("image", "png"), "<http://example.org/me.png>";
      output.addPart("// binary octets for you png",
          new MediaType("image", "png"),
          "<http://example.org/you.png>");
      client.putRelated(output);
      return output;
  }
}
```

### 23.11. `@MultipartFile` and POJOs

If you have a exact knowledge of your multipart/form-data packets, you can map them to and from a POJO class to and from multipart/form-data using the
Chapter 23. Multipart Providers

@org.jboss.resteasy.annotations.providers.multipart.MultipartForm annotation and the JAX-RS @FormParam annotation. You simple define a POJO with at least a default constructor and annotate its fields and/or properties with @FormParams. These @FormParams must also be annotated with @org.jboss.resteasy.annotations.providers.multipart.PartType if you are doing output. For example:

```java
public class CustomerProblemForm {
    @FormParam("customer")
    @PartType("application/xml")
    private Customer customer;

    @FormParam("problem")
    @PartType("text/plain")
    private String problem;

    public Customer getCustomer() { return customer; }
    public void setCustomer(Customer cust) { this.customer = cust; }
    public String getProblem() { return problem; }
    public void setProblem(String problem) { this.problem = problem; }
}
```

After defining your POJO class you can then use it to represent multipart/form-data. Here's an example of sending a CustomerProblemForm using the RESTEasy client framework:

```java
@Path("portal")
public interface CustomerPortal {

    @Path("issues/{id}")
    @Consumes("multipart/form-data")
    @PUT
    public void putProblem(@MultipartForm CustomerProblemForm,
                            @PathParam("id") int id);
}

{  
    CustomerPortal portal = ProxyFactory.create(CustomerPortal.class, "http://example.com");
    CustomerProblemForm form = new CustomerProblemForm();
    form.setCustomer(...);
    form.setProblem(...);

    portal.putProblem(form, 333);
}
```
You see that the @MultipartForm annotation was used to tell RESTEasy that the object has @FormParam and that it should be marshalled from that. You can also use the same object to receive multipart data. Here is an example of the server side counterpart of our customer portal.

```java
@Path("portal")
public class CustomerPortalServer {

    @Path("issues/{id}")
    @Consumes("multipart/form-data")
    @PUT
    public void putIssue(@MultipartForm CustomerProblemForm,
                          @PathParam("id") int id) {
        ... write to database...
    }
}
```

### 23.12. XML-binary Optimized Packaging (Xop)

RESTEasy supports Xop messages packaged as multipart/related. What does this mean? If you have a JAXB annotated POJO that also holds some binary content you may choose to send it in such a way where the binary does not need to be encoded in any way (neither base64 neither hex). This results in faster transport while still using the convenient POJO. More about Xop can be read here: [http://www.w3.org/TR/xop10/](http://www.w3.org/TR/xop10/). Now lets see an example:

First we have a JAXB annotated POJO to work with. @XmlMimeType tells JAXB the mime type of the binary content (its not required to do XOP packaging but it is recommended to be set if you know the exact type):

```java
@XmlRootElement
@XmlAccessorType(XmlAccessType.FIELD)
public static class Xop {
    private Customer bill;
    private Customer monica;

    @XmlMimeType(MediaType.APPLICATION_OCTET_STREAM)
    private byte[] myBinary;

    @XmlMimeType(MediaType.APPLICATION_OCTET_STREAM)
    private DataHandler myDataHandler;

    // methods, other fields ...
}
```
In the above POJO myBinary and myDataHandler will be processed as binary attachments while the whole Xop object will be sent as xml (in the places of the binaries only their references will be generated). javax.activation.DataSource is the most general supported type so if you need an java.io.InputStream or a javax.activation.DataSource you need to go with the DataHandler. Some other special types are supported too: java.awt.Image and javax.xml.transform.Source. Let's assume that Customer is also JAXB friendly POJO in the above example (of course it can also have binary parts). Now let's see an example Java client that sends this:

```java
// our client interface:
@Path("mime")
public static interface MultipartClient {
    @Path("xop")
    @PUT
    @Consumes(MultipartConstants.MULTIPART_RELATED)
    public void putXop(@XopWithMultipartRelated Xop bean);
}

// Somewhere using it:
{
    MultipartClient client = ProxyFactory.create(MultipartClient.class, "http://www.example.org");
    Xop xop = new Xop(new Customer("bill"), new Customer("monica"), "Hello Xop World!".getBytes("UTF-8"),
            new DataHandler(new ByteArrayDataSource("Hello Xop World!".getBytes("UTF-8"),
                MediaType.APPLICATION_OCTET_STREAM)));
    client.putXop(xop);
}
```

We used @Consumes(MultipartConstants.MULTIPART_RELATED) to tell RESTEasy that we want to send multipart/related packages (that's the container format that will hold our Xop message). We used @XopWithMultipartRelated to tell RESTEasy that we want to make Xop messages. So we have a POJO and a client service that is willing to send it. All we need now a server that can read it:

```java
@Path("/mime")
public class XopService {
    @PUT
    @Path("xop")
    @Consumes(MultipartConstants.MULTIPART_RELATED)
    public void putXopWithMultipartRelated(@XopWithMultipartRelated Xop xop) {
        // do very important things here
    }
}
```
We used `@Consumes(MultipartConstants.MULTIPART_RELATED)` to tell RESTEasy that we want to read multipart/related packages. We used `@XopWithMultipartRelated` to tell RESTEasy that we want to read Xop messages. Of course we could also produce Xop return values but we would than also need to annotate that and use a Produce annotation, too.

### 23.13. Note about multipart parsing and working with other frameworks

There are a lot of frameworks doing multipart parsing automatically with the help of filters and interceptors. Like `org.jboss.seam.web.MultipartFilter` in Seam or `org.springframework.web.multipart.MultipartResolver` in Spring. However the incoming multipart request stream can be parsed only once. Resteasy users working with multipart should make sure that nothing parses the stream before Resteasy gets it.

### 23.14. Overwriting the default fallback content type for multipart messages

By default if no Content-Type header is present in a part, "text/plain; charset=us-ascii" is used as fallback. This is the value defined by the MIME RFC. However for example some web clients (like most, if not all, web browsers) do not send Content-Type headers for all fields in a multipart/form-data request (only for the file parts). This can cause character encoding and unmarshalling errors on the server side. To correct this there is an option to define an other, non-rfc compliant fallback value. This can be done dynamically per request with the PreProcessInterceptor infrastructure of RESTEasy. In the following example we will set ":/; charset=UTF-8" as the new default fallback:

```java
import org.jboss.resteasy.plugins.providers.multipart.InputPart;

@Provider
@ServerInterceptor
public class ContentTypeSetterPreProcessorInterceptor implements
    PreProcessInterceptor {

    public ServerResponse preProcess(HttpRequest request,
        ResourceMethod method) throws Failure, WebApplicationException {
        request.setAttribute(InputPart.DEFAULT_CONTENT_TYPE_PROPERTY,
            ":/; charset=UTF-8"));
        return null;
    }
}
```
23.15. Overwriting the content type for multipart messages

Using an interceptor and the `InputPart.DEFAULT_CONTENT_TYPE_PROPERTY` attribute allows setting a default Content-Type, but it is also possible to override the Content-Type, if any, in any input part by calling `org.jboss.resteasy.plugins.providers.multipart.InputPart.setMediaType()`. For example:

```java
@POST
@Path("query")
@Consumes(MediaType.MULTIPART_FORM_DATA)
@Produces(MediaType.TEXT_PLAIN)
public Response setMediaType(MultipartInput input) throws IOException {
    List<InputPart> parts = input.getParts();
    InputPart part = parts.get(0);
    part.setMediaType(MediaType.valueOf("application/foo+xml"));
    String s = part.getBody(String.class, null);
    ...
}
```

23.16. Overwriting the default fallback charset for multipart messages

Sometimes, a part may have a Content-Type header with no charset parameter. If the `InputPart.DEFAULT_CONTENT_TYPE_PROPERTY` property is set and the value has a charset parameter, that value will be appended to an existing Content-Type header that has no charset parameter. It is also possible to specify a default charset using the constant `InputPart.DEFAULT_CHARSET_PROPERTY` (actual value "resteasy.provider.multipart.inputpart.defaultCharset"):

```java
import org.jboss.resteasy.plugins.providers.multipart.InputPart;

@Provider
@ServerInterceptor
public class ContentTypeSetterPreProcessorInterceptor implements PreProcessInterceptor {
    public ServerResponse preProcess(HttpRequest request, ResourceMethod method) throws Failure, WebApplicationException {
```

116
request.setAttribute(InputPart.DEFAULT_CHARSET_PROPERTY, "UTF-8");
return null;
}
}

If both InputPart.DEFAULT_CONTENT_TYPE_PROPERTY and InputPart.DEFAULT_CHARSET_PROPERTY are set, then the value of InputPart.DEFAULT_CHARSET_PROPERTY will override any charset in the value of InputPart.DEFAULT_CONTENT_TYPE_PROPERTY.
Chapter 24. YAML Provider

Since 3.0.9.Final release, resteasy comes with built in support for YAML using the SnakeYAML library. To enable YAML support, you need to drop in the SnakeYaml 1.8 jar and the resteasy-yaml-provider.jar (whatever the current version is) in RestEASY's classpath.

SnakeYaml jar file can either be downloaded from Google code at http://code.google.com/p/snakeyaml/downloads/list

Or if you use maven, the SnakeYaml jar is available through SonaType public repositories and included using this dependency:

```
<dependency>
    <groupId>org.yaml</groupId>
    <artifactId>snakeyaml</artifactId>
    <version>1.8</version>
</dependency>
```

When starting resteasy look out in the logs for a line stating that the YamlProvider has been added - this indicates that resteasy has found the Jyaml jar:

2877 Main INFO org.jboss.resteasy.plugins.providers.RegisterBuiltin - Adding YamlProvider

The Yaml provider recognises three mime types:

- text/x-yaml
- text/yaml
- application/x-yaml

This is an example of how to use Yaml in a resource method.

```
import javax.ws.rs.Consumes;
import javax.ws.rs.GET;
import javax.ws.rs.Path;
import javax.ws.rs.Produces;

@Path("/yaml")
public class YamlResource
```
public MyObject getMyObject() {
    return createMyObject();
}
...

Chapter 25. String marshalling for String based @*Param

@PathParam, @QueryParam, @MatrixParam, @FormParam, and @HeaderParam are represented as strings in a raw HTTP request. The specification says that these types of injected parameters can be converted to objects if these objects have a valueOf(String) static method or a constructor that takes one String parameter. What if you have a class where valueOf() or this string constructor doesn't exist or is inappropriate for an HTTP request? JAX-RS 2.0 has the javax.ws.rs.ext.ParamConverterProvider to help in this situation. See javadoc for more details.
Chapter 26. Responses using javax.ws.rs.core.Response

You can build custom responses using the javax.ws.rs.core.Response and ResponseBuilder classes. If you want to do your own streaming, your entity response must be an implementation of javax.ws.rs.core.StreamingOutput. See the java doc for more information.
Chapter 27. Exception Handling

27.1. Exception Mappers

ExceptionMappers are custom, application provided, components that can catch thrown application exceptions and write specific HTTP responses. They are classes annotated with @Provider and that implement this interface:

```java
package javax.ws.rs.ext;

import javax.ws.rs.core.Response;

/**
 * Contract for a provider that maps Java exceptions to
 * @link javax.ws.rs.core.Response]. An implementation of this interface
 * must
 * be annotated with @link Provider).
 *
 * @see Provider
 * @see javax.ws.rs.core.Response
 */
public interface ExceptionMapper<E>
{

  /**
   * Map an exception to a @link javax.ws.rs.core.Response).
   * @param exception the exception to map to a response
   * @return a response mapped from the supplied exception
   */
  Response toResponse(E exception);
}
```

When an application exception is thrown it will be caught by the JAX-RS runtime. JAX-RS will then scan registered ExceptionMappers to see which one support marshalling the exception type thrown. Here is an example of ExceptionMapper:

```java
@Provider
public class EJBExceptionMapper implements ExceptionMapper<javax.ejb.EJBException>
```
You register ExceptionMappers the same way you do MessageBodyReader/Writers. By scanning, through the resteasy provider context-param (if you're deploying via a WAR file), or programmatically through the ResteasyProviderFactory class.

### 27.2. Resteasy Built-in Internally-Thrown Exceptions

Resteasy has a set of built-in exceptions that are thrown by it when it encounters errors during dispatching or marshalling. They all revolve around specific HTTP error codes. You can find them in RESTEasy's javadoc under the package org.jboss.resteasy.spi. Here's a list of them:

<table>
<thead>
<tr>
<th>Exception</th>
<th>HTTP Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReaderException</td>
<td>400</td>
<td>All exceptions thrown from MessageBodyReaders are wrapped within this exception. If there is no ExceptionMapper for the wrapped exception or if the exception isn't a WebApplicationException, then resteasy will return a 400 code by default.</td>
</tr>
<tr>
<td>WriterException</td>
<td>500</td>
<td>All exceptions thrown from MessageBodyWriters are wrapped within this exception. If there is no ExceptionMapper for the wrapped exception or if the exception isn't a WebApplicationException, then resteasy will return a 400 code by default.</td>
</tr>
<tr>
<td>o.j.r.plugins.providers.jaxb.JAXBUnmarshallerException</td>
<td></td>
<td>The JAXB providers (XML and Jettison) throw this exception on reads. They may be wrapping...</td>
</tr>
</tbody>
</table>
### Overriding Resteasy Builtin Exceptions

You may override Resteasy built-in exceptions by writing an ExceptionMapper for the exception. For that matter, you can write an ExceptionMapper for any thrown exception including WebApplicationException.

<table>
<thead>
<tr>
<th>Exception</th>
<th>HTTP Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAXBExceptions. This class extends ReaderException</td>
<td></td>
<td></td>
</tr>
<tr>
<td>o.j.r.plugins.providers.jaxb.JAXBMarshalException</td>
<td>500</td>
<td>The JAXB providers (XML and Jettison) throw this exception on writes. They may be wrapping JAXBExceptions. This class extends WriterException</td>
</tr>
<tr>
<td>ApplicationException</td>
<td>N/A</td>
<td>This exception wraps all exceptions thrown from application code. It functions much in the same way as InvocationTargetException. If there is an ExceptionMapper for wrapped exception, then that is used to handle the request.</td>
</tr>
<tr>
<td>Failure</td>
<td>N/A</td>
<td>Internal Resteasy. Not logged</td>
</tr>
<tr>
<td>LoggableFailure</td>
<td>N/A</td>
<td>Internal Resteasy error. Logged</td>
</tr>
<tr>
<td>DefaultOptionsMethodException</td>
<td>N/A</td>
<td>If the user invokes HTTP OPTIONS and no JAX-RS method for it, Resteasy provides a default behavior by throwing this exception</td>
</tr>
</tbody>
</table>

#### 27.3. Overriding Resteasy Builtin Exceptions

You may override Resteasy built-in exceptions by writing an ExceptionMapper for the exception. For that matter, you can write an ExceptionMapper for any thrown exception including WebApplicationException.
Chapter 28. Configuring Individual JAX-RS Resource Beans

If you are scanning your path for JAX-RS annotated resource beans, your beans will be registered in per-request mode. This means an instance will be created per HTTP request served. Generally, you will need information from your environment. If you are running within a servlet container using the WAR-file distribution, in Beta-2 and lower, you can only use the JNDI lookups to obtain references to Java EE resources and configuration information. In this case, define your EE configuration (i.e. ejb-ref, env-entry, persistence-context-ref, etc...) within web.xml of the resteasy WAR file. Then within your code do jndi lookups in the java:comp namespace. For example:

web.xml

```xml
<ejb-ref>
    <ejb-ref-name>ejb/foo</ejb-ref-name>
    ...
</ejb-ref>
```

resource code:

```java
@Path("/")
public class MyBean {

    public Object getSomethingFromJndi() {
        new InitialContext().lookup("java:comp/ejb/foo");
    }
    ...
}
```

You can also manually configure and register your beans through the Registry. To do this in a WAR-based deployment, you need to write a specific ServletContextListener to do this. Within the listener, you can obtain a reference to the registry as follows:

```java
public class MyManualConfig implements ServletContextListener
```
{ public void contextInitialized(ServletContextEvent event)
{

    Registry registry = (Registry)
    event.getServletContext().getAttribute(Registry.class.getName());

}
...
}

Please also take a look at our Spring Integration as well as the Embedded Container's Spring Integration
Chapter 29. GZIP Compression/Decompression

Resteasy has automatic GZIP decompression support. If the client framework or a JAX-RS service receives a message body with a Content-Encoding of "gzip", it will automatically decompress it. The client framework automatically sets the Accept-Encoding header to be "gzip, deflate". So you do not have to set this header yourself.

Resteasy also supports automatic compression. If the client framework is sending a request or the server is sending a response with the Content-Encoding header set to "gzip", Resteasy will do the compression. So that you do not have to set the Content-Encoding header directly, you can use the @org.jboss.resteasy.annotation.GZIP annotation.

```java
@Path("/")
public interface MyProxy {

    @Consumes("application/xml")
    @PUT
    public void put(@GZIP Order order);
}
```

In the above example, we tag the outgoing message body, order, to be gzip compressed. You can use the same annotation to tag server responses.

```java
@Path("/")
public class MyService {

    @GET
    @Produces("application/xml")
    @GZIP
    public String getData() {...}
}
```
Chapter 30. CORS

Resteasy has a ContainerRequestFilter that can be used to handle CORS preflight and actual requests. org.jboss.resteasy.plugins.interceptors.CorsFilter. You must allocate this and register it as a singleton provider from your Application class. See the javadoc or its various settings.

```java
CorsFilter filter = new CorsFilter();
filter.getAllowedOrigins().add("http://localhost");
```
Chapter 31. Content-Range Support

Resteasy supports Range requests for java.io.File response entities.

```java
@Path("/")
public class Resource {
    @GET
    @Path("file")
    @Produces("text/plain")
    public File getFile()
    {
        return file;
    }
}

Response response = client.target(generateURL("/file")).request()
    .header("Range", "1-4").get();
Assert.assertEquals(response.getStatus(), 206);
Assert.assertEquals(4, response.getLength());
System.out.println("Content-Range: " + response.getHeaderString("Content-Range"));
```
Chapter 32. Resteasy Caching

Features

Resteasy provides numerous annotations and facilities to support HTTP caching semantics. Annotations to make setting Cache-Control headers easier and both server-side and client-side in-memory caches are available.

32.1. @Cache and @NoCache Annotations

Resteasy provides an extension to JAX-RS that allows you to automatically set Cache-Control headers on a successful GET request. It can only be used on @GET annotated methods. A successful @GET request is any request that returns 200 OK response.

```java
package org.jboss.resteasy.annotations.cache;

public @interface Cache {
    int maxAge() default -1;
    int sMaxAge() default -1;
    boolean noStore() default false;
    boolean noTransform() default false;
    boolean mustRevalidate() default false;
    boolean proxyRevalidate() default false;
    boolean isPrivate() default false;
}

public @interface NoCache {
    String[] fields() default {};
}
```

While @Cache builds a complex Cache-Control header, @NoCache is a simplified notation to say that you don’t want anything cached i.e. Cache-Control: nocache.

These annotations can be put on the resource class or interface and specifies a default cache value for each @GET resource method. Or they can be put individually on each @GET resource method.
32.2. Client "Browser" Cache

Resteasy has the ability to set up a client-side, browser-like, cache. You can use it with the Client Proxy Framework, or with raw ClientRequests. This cache looks for Cache-Control headers sent back with a server response. If the Cache-Control headers specify that the client is allowed to cache the response, Resteasy caches it within local memory. The cache obeys max-age requirements and will also automatically do HTTP 1.1 cache revalidation if either or both the Last-Modified and/or ETag headers are sent back with the original response. See the HTTP 1.1 specification for details on how Cache-Control or cache revalidation works.

It is very simple to enable caching. Here's an example of using the client cache with the Client Proxy Framework

```java
@Path("/orders")
public interface OrderServiceClient {

    @Path("{id}")
    @GET
    @Produces("application/xml")
    public Order getOrder(@PathParam("id") String id);
}
```

To create a proxy for this interface and enable caching for that proxy requires only a few simple steps:

```java
import org.jboss.resteasy.client.ProxyFactory;
import org.jboss.resteasy.client.cache.CacheFactory;
import org.jboss.resteasy.client.cache.LightweightBrowserCache;

public static void main(String[] args) throws Exception {
    RegisterBuiltin.register(ResteasyProviderFactory.getInstance());
    OrderServiceClient proxy = ProxyFactory.create(OrderServiceClient.class,
    generateBaseUrl());

    // This line enables caching
    LightweightBrowserCache cache = CacheFactory.makeCacheable(proxy);
}
```

If you are using the ClientRequest class to make invocations rather than the proxy framework, it is just as easy
import org.jboss.resteasy.client.ProxyFactory;
import org.jboss.resteasy.client.cache.CacheFactory;
import org.jboss.resteasy.client.cache.LightweightBrowserCache;

public static void main(String[] args) throws Exception
{
    RegisterBuiltin.register(ResteasyProviderFactory.getInstance());

    // This line enables caching
    LightweightBrowserCache cache = new LightweightBrowserCache();

    ClientRequest request = new ClientRequest("http://example.com/orders/333");
    CacheFactory.makeCacheable(request, cache);
}

The LightweightBrowserCache, by default, has a maximum 2 megabytes of caching space. You can change this programmatically by calling its setMaxBytes() method. If the cache gets full, the cache completely wipes itself of all cached data. This may seem a bit draconian, but the cache was written to avoid unnecessary synchronizations in a concurrent environment where the cache is shared between multiple threads. If you desire a more complex caching solution or if you want to plug in a thirdparty cache please contact our resteasy-developers list and discuss it with the community.

### 32.3. Local Server-Side Response Cache

Resteasy has a server-side cache that can sit in front of your JAX-RS services. It automatically caches marshalled responses from HTTP GET JAX-RS invocations if, and only if your JAX-RS resource method sets a Cache-Control header. When a GET comes in, the Resteasy Server Cache checks to see if the URI is stored in the cache. If it does, it returns the already marshalled response without invoking your JAX-RS method. Each cache entry has a max age to whatever is specified in the Cache-Control header of the initial request. The cache also will automatically generate an ETag using an MD5 hash on the response body. This allows the client to do HTTP 1.1 cache revalidation with the IF-NONE-MATCH header. The cache is also smart enough to perform revalidation if there is no initial cache hit, but the jax-rs method still returns a body that has the same ETag.

The cache is also automatically invalidated for a particular URI that has PUT, POST, or DELETE invoked on it. You can also obtain a reference to the cache by injecting a org.jboss.resteasy.plugins.cache.ServerCache via the @Context annotation

```java
@Context
ServerCache cache;
```
To set up the server-side cache you must register an instance of org.jboss.resteasy.plugins.cache.server.ServerCacheFeature via your Application getSingletons() or getClasses() methods. The underlying cache is Infinispan. By default, Resteasy will create an Infinispan cache for you. Alternatively, you can create and pass in an instance of your cache to the ServerCacheFeature constructor. You can also configure Infinispan by specifying various context-param variables in your web.xml. First, if you are using Maven you must depend on the resteasy-cache-core artifact:

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-cache-core</artifactId>
  <version>3.0.9.Final</version>
</dependency>
```

The next thing you should probably do is set up the Infinispan configuration in your web.xml.

```xml
<web-app>
  <context-param>
    <param-name>server.request.cache.infinispan.config.file</param-name>
    <param-value>infinispan.xml</param-value>
  </context-param>

  <context-param>
    <param-name>server.request.cache.infinispan.cache.name</param-name>
    <param-value>MyCache</param-value>
  </context-param>
</web-app>
```

server.request.cache.infinispan.config.file can either be a classpath or a file path. server.request.cache.infinispan.cache.name is the name of the cache you want to reference that is declared in the config file.
Chapter 33. Filters and Interceptors

JAX-RS 2.0 has two different concepts for interceptions: Filters and Interceptors. Filters are mainly used to modify or process incoming and outgoing request headers or response headers. They execute before and after request and response processing.

33.1. Server Side Filters

On the server-side you have two different types of filters. ContainerRequestFilters run before your JAX-RS resource method is invoked. ContainerResponseFilters run after your JAX-RS resource method is invoked. As an added caveat, ContainerRequestFilters come in two flavors: pre-match and post-matching. Pre-matching ContainerRequestFilters are designated with the @PreMatching annotation and will execute before the JAX-RS resource method is matched with the incoming HTTP request. Pre-matching filters often are used to modify request attributes to change how it matches to a specific resource method (i.e. strip .xml and add an Accept header). ContainerRequestFilters can abort the request by calling ContainerRequestContext.abortWith(Response). A filter might want to abort if it implements a custom authentication protocol.

After the resource class method is executed, JAX-RS will run all ContainerResponseFilters. These filters allow you to modify the outgoing response before it is marshalling and sent to the client. So given all that, here’s some pseudo code to give some understanding of how things work.

```java
// execute pre match filters
for (ContainerRequestFilter filter : preMatchFilters) {
    filter.filter(requestContext);
    if (isAborted(requestContext)) {
        sendAbortionToClient(requestContext);
        return;
    }
}

// match the HTTP request to a resource class and method
JaxrsMethod method = matchMethod(requestContext);

// Execute post match filters
for (ContainerRequestFilter filter : postMatchFilters) {
    filter.filter(requestContext);
    if (isAborted(requestContext)) {
        sendAbortionToClient(requestContext);
        return;
    }
}

// execute resource class method
method.execute(request);
```
Chapter 33. Filters and Inter...

```java
// execute response filters
for (ContainerResponseFilter filter : responseFilters) {
    filter.filter(requestContext, responseContext);
}
```

### 33.2. Client Side Filters

On the client side you also have two types of filters: ClientRequestFilter and ClientResponseFilter. ClientRequestFilters run before your HTTP request is sent over the wire to the server. ClientResponseFilters run after a response is received from the server, but before the response body is unmarshalled. ClientRequestFilters are also allowed to abort the execute of the request and provide a canned response without going over the wire to the server. ClientResponseFilters can modify the Response object before it is handed back to application code. Here’s some pseudo code to illustrate things.

```java
// execute request filters
for (ClientRequestFilter filter : requestFilters) {
    filter.filter(requestContext);
    if (isAborted(requestContext)) {
        return requestContext.getAbortedResponseObject();
    }
}

// send request over the wire
response = sendRequest(request);

// execute response filters
for (ClientResponseFilter filter : responseFilters) {
    filter.filter(requestContext, responseContext);
}
```

### 33.3. Reader and Writer Interceptors

While filters modify request or response headers, interceptors deal with message bodies. Interceptors are executed in the same call stack as their corresponding reader or writer. ReaderInterceptors wrap around the execution of MessageBodyReaders. WriterInterceptors wrap around the execution of MessageBodyWriters. They can be used to implement a specific content-encoding. They can be used to generate digital signatures or to post or pre-process a Java object model before or after it is marshalled.
33.4. Per Resource Method Filters and Interceptors

Sometimes you want a filter or interceptor to only run for a specific resource method. You can do this in two different ways: register an implementation of DynamicFeature or use the @NameBinding annotation. The DynamicFeature interface is executed at deployment time for each resource method. You just use the Configurable interface to register the filters and interceptors you want for the specific resource method. @NameBinding works a lot like CDI interceptors. You annotate a custom annotation with @NameBinding and then apply that custom annotation to your filter and resource method.

```java
@NameBinding
public @interface DoIt {}

@DoIt
public class MyFilter implements ContainerRequestFilter {...}

@Path("/root")
public class MyResource {

    @GET
    @DoIt
    public String get() {...}
}
```

33.5. Ordering

Ordering is accomplished by using the @BindingPriority annotation on your filter or interceptor class.
Chapter 34. Asynchronous HTTP Request Processing

Asynchronous HTTP Request Processing is a relatively new technique that allows you to process a single HTTP request using non-blocking I/O and, if desired in separate threads. Some refer to it as COMET capabilities. The primary use case for Asynchronous HTTP is in the case where the client is polling the server for a delayed response. The usual example is an AJAX chat client where you want to push/pull from both the client and the server. These scenarios have the client blocking a long time on the server’s socket waiting for a new message. What happens in synchronous HTTP where the server is blocking on incoming and outgoing I/O is that you end up having a thread consumed per client connection. This eats up memory and valuable thread resources. Not such a big deal in 90% of applications (in fact using asynchronous processing may actually hurt your performance in most common scenarios), but when you start getting a lot of concurrent clients that are blocking like this, there’s a lot of wasted resources and your server does not scale that well.

The JAX-RS 2.0 specification has added asynchronous HTTP support via two classes. The @Suspended annotation, and AsyncResponse interface.

Injecting an AsynchronousResponse as a parameter to your jax-rs methods tells Resteasy that the HTTP request/response should be detached from the currently executing thread and that the current thread should not try to automatically process the response.

The AsyncResponse is the callback object. The act of calling one of the resume() methods will cause a response to be sent back to the client and will also terminate the HTTP request. Here is an example of asynchronous processing:

```java
import javax.ws.rs.Suspend;
import javax.ws.rs.core.AsynchronousResponse;

@Path("/")
public class SimpleResource
{

    @GET
    @Path("basic")
    @Produces("text/plain")
    public void getBasic(@Suspended final AsyncResponse response) throws Exception
    {
        Thread t = new Thread()
        {
            @Override
            public void run()
            {
```
try {
    Response jaxrs = Response.ok("basic").type(MediaType.TEXT_PLAIN).build();
    response.resume(jaxrs);
} catch (Exception e) {
    e.printStackTrace();
}
}
t.start();

AsyncResponse also has other methods to cancel the execution. See javadoc for more details.

NOTE: The old Resteasy proprietary API for async http has been deprecated and may be removed as soon as Resteasy 3.1.
Chapter 35. Asynchronous Job Service

The Resteasy Asynchronous Job Service is an implementation of the Asynchronous Job pattern defined in O'Reilly's "Restful Web Services" book. The idea of it is to bring asynchronicity to a synchronous protocol.

35.1. Using Async Jobs

While HTTP is a synchronous protocol it does have a faint idea of asynchronous invocations. The HTTP 1.1 response code 202, "Accepted" means that the server has received and accepted the response for processing, but the processing has not yet been completed. The Resteasy Asynchronous Job Service builds around this idea.

POST http://example.com/myservice?asynch=true

For example, if you make the above post with the asynch query parameter set to true, Resteasy will return a 202, "Accepted" response code and run the invocation in the background. It also sends back a Location header with a URL pointing to where the response of the background method is located.

HTTP/1.1 202 Accepted
Location: http://example.com/asynch/jobs/3332334

The URI will have the form of:

/asynch/jobs/{job-id}?wait={millisconds}|nowait=true

You can perform the GET, POST, and DELETE operations on this job URL. GET returns whatever the JAX-RS resource method you invoked returned as a response if the job was completed. If the job has not completed, this GET will return a response code of 202, Accepted. Invoking GET does not remove the job, so you can call it multiple times. When Resteasy's job queue gets full, it will evict the least recently used job from memory. You can manually clean up after yourself by calling DELETE on the URI. POST does a read of the JOB response and will remove the JOB it has been completed.
Both GET and POST allow you to specify a maximum wait time in milliseconds, a "wait" query parameter. Here's an example:

```
POST http://example.com/asynch/jobs/122?wait=3000
```

If you do not specify a "wait" parameter, the GET or POST will not wait at all if the job is not complete.

NOTE!! While you can invoke GET, DELETE, and PUT methods asynchronously, this breaks the HTTP 1.1 contract of these methods. While these invocations may not change the state of the resource if invoked more than once, they do change the state of the server as new Job entries with each invocation. If you want to be a purist, stick with only invoking POST methods asynchronously.

Security NOTE! Resteasy role-based security (annotations) does not work with the Asynchronous Job Service. You must use XML declarative security within your web.xml file. Why? It is impossible to implement role-based security portably. In the future, we may have specific JBoss integration, but will not support other environments.

35.2. Oneway: Fire and Forget

Resteasy also supports the notion of fire and forget. This will also return a 202, Accepted response, but no Job will be created. This is as simple as using the oneway query parameter instead of asynch. For example:

```
POST http://example.com/myservice?oneway=true
```

Security NOTE! Resteasy role-based security (annotations) does not work with the Asynchronous Job Service. You must use XML declarative security within your web.xml file. Why? It is impossible to implement role-based security portably. In the future, we may have specific JBoss integration, but will not support other environments.

35.3. Setup and Configuration

You must enable the Asynchronous Job Service in your web.xml file as it is not turned on by default.

```
<web-app>
    <!-- enable the Asynchronous Job Service -->
    <context-param>
        <param-name>resteasy.async.job.service.enabled</param-name>
```

<param-value>true</param-value>
</context-param>

<!-- The next context parameters are all optional. Their default values are shown as example param-values -->

<!-- How many jobs results can be held in memory at once? -->
<context-param>
    <param-name>resteasy.async.job.service.max.job.results</param-name>
    <param-value>100</param-value>
</context-param>

<!-- Maximum wait time on a job when a client is querying for it -->
<context-param>
    <param-name>resteasy.async.job.service.max.wait</param-name>
    <param-value>300000</param-value>
</context-param>

<!-- Thread pool size of background threads that run the job -->
<context-param>
    <param-name>resteasy.async.job.service.thread.pool.size</param-name>
    <param-value>100</param-value>
</context-param>

<!-- Set the base path for the Job uris -->
<context-param>
    <param-name>resteasy.async.job.service.base.path</param-name>
    <param-value>/asynch/jobs</param-value>
</context-param>

<listener>
    <listener-class>
        org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap
    </listener-class>
</listener>

<servlet>
    <servlet-name>Resteasy</servlet-name>
    <servlet-class>
        org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher
    </servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>Resteasy</servlet-name>
    <url-pattern>/*</url-pattern>
</servlet-mapping>

</web-app>
Chapter 36. Embedded Containers

Resteasy has a few different plugins for different embeddable HTTP and/or Servlet containers if you use Resteasy in a test environment, or within an environment where you do not want a Servlet engine dependency.

36.1. Undertow

Undertow is a new Servlet Container that is used by Wildfly (JBoss Community Server). You can embed Undertow as you wish. Here's a a test that shows it in action.

```java
import io.undertow.servlet.api.DeploymentInfo;
import org.jboss.resteasy.plugins.server.undertow.UndertowJaxrsServer;
import org.jboss.resteasy.test.TestPortProvider;
import org.junit.AfterClass;
import org.junit.Assert;
import org.junit.BeforeClass;
import org.junit.Test;
import javax.ws.rs.ApplicationPath;
import javax.ws.rs.GET;
import javax.ws.rs.Path;
import javax.ws.rs.Produces;
import javax.ws.rs.client.Client;
import javax.ws.rs.client.ClientBuilder;
import javax.ws.rs.core.Application;
import java.util.HashSet;
import java.util.Set;

/**
 * @author <a href="mailto:bill@burkecentral.com">Bill Burke</a>
 * @version $Revision: 1 $
 */
public class UndertowTest
{
    private static UndertowJaxrsServer server;

    @Path("/test")
    public static class Resource
    {
        @GET
        @Produces("text/plain")
        public String get()
        {
            return "hello world";
        }
    }
```
Chapter 36. Embedded Containers

```java
@ApplicationPath("/base")
public static class MyApp extends Application {
    @Override
    public Set<Class<?>> getClasses() {
        HashSet<Class<?>> classes = new HashSet<Class<?>>();
        classes.add(Resource.class);
        return classes;
    }
}

@BeforeClass
public static void init() throws Exception {
    server = new UndertowJaxrsServer().start();
}

@AfterClass
public static void stop() throws Exception {
    server.stop();
}

@Test
public void testApplicationPath() throws Exception {
    server.deploy(MyApp.class);
    Client client = ClientBuilder.newClient();
    String val = client.target(TestPortProvider.generateURL("/base/test"))
        .request().get(String.class);
    Assert.assertEquals("hello world", val);
    client.close();
}

@Test
public void testApplicationContext() throws Exception {
    server.deploy(MyApp.class, "/root" plunged into the main class.
    Client client = ClientBuilder.newClient();
    String val = client.target(TestPortProvider.generateURL("/root/test"))
        .request().get(String.class);
    Assert.assertEquals("hello world", val);
    client.close();
}

@Test
```
public void testDeploymentInfo() throws Exception
{
    DeploymentInfo di = server.undertowDeployment(MyApp.class);
    di.setContextPath("/di");
    di.setDeploymentName("DI");
    server.deploy(di);
    Client client = ClientBuilder.newClient();
    String val = client.target(TestPortProvider.generateURL("/di/base/test"))
        .request().get(String.class);
    Assert.assertEquals("hello world", val);
    client.close();
}

36.2. Sun JDK HTTP Server

The Sun JDK comes with a simple HTTP server implementation (com.sun.net.httpserver.HttpServer) which you can run Resteasy on top of.

HttpServer httpServer = HttpServer.create(new InetSocketAddress(port), 10);
contextBuilder = new HttpContextBuilder();
contextBuilder.getDeployment().getActualResourceClasses().add(SimpleResource.class);
HttpContext context = contextBuilder.bind(httpServer);
context.getAttributes().put("some.config.info", "42");
httpServer.start();

contextBuilder.cleanup();
httpServer.stop(0);

Create your HttpServer the way you want then use the org.jboss.resteasy.plugins.server.sun.http.HttpContextBuilder to initialize Resteasy and bind it to an HttpContext. The HttpContext attributes are available by injecting in a org.jboss.resteasy.spi.ResteasyConfiguration interface using @Context within your provider and resource classes.

Maven project you must include is:

<dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-jdk-http</artifactId>
</dependency>
36.3. TJWS Embeddable Servlet Container

RESTeasy integrates with the TJWS Embeddable Servlet container. It comes with this distribution, or you can reference the Maven artifact. You must also provide a servlet API dependency as well.

```
<dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>tjws</artifactId>
    <version>3.0.9.Final</version>
</dependency>

<dependency>
    <groupId>javax.servlet</groupId>
    <artifactId>servlet-api</artifactId>
    <version>2.5</version>
</dependency>
```

From the distribution, move the jars in resteasy-jaxrs.war/WEB-INF/lib into your classpath. You must both programmatically register your JAX-RS beans using the embedded server's Registry. Here's an example:

```java
@Path("/")
public class MyResource {

    @GET
    public String get() { return "hello world"; }

    public static void main(String[] args) throws Exception {
    TJWSEmbeddedJaxrsServer tjws = new TJWSEmbeddedJaxrsServer();
tjws.setPort(8080);
tjws.start();
tjws.getRegistry().addPerRequestResource(RestEasy485Resource.class);
    }
}
```
The server can either host non-encrypted or SSL based resources, but not both. See the Javadoc for TJWSEmbeddedJaxrsServer as well as its superclass TJWSServletServer. The TJWS website is also a good place for information.

If you want to use Spring, see the SpringBeanProcessor. Here’s a pseudo-code example

```java
public static void main(String[] args) throws Exception {
    final TJWSEmbeddedJaxrsServer tjws = new TJWSEmbeddedJaxrsServer();
    tjws.setPort(8081);
    tjws.start();
    org.jboss.resteasy.plugins.server.servlet.SpringBeanProcessor processor = new SpringBeanProcessor(tjws.getDeployment().getRegistry(),
    tjws.getDeployment().getFactory();
    ConfigurableBeanFactory factory = new XmlBeanFactory(...);
    factory.addBeanPostProcessor(processor);
}
```

### 36.4. Netty

Resteasy has integration with the popular Netty project as well.

```java
public static void start(ResteasyDeployment deployment) throws Exception {
    netty = new NettyJaxrsServer();
    netty.setDeployment(deployment);
    netty.setPort(TestPortProvider.getPort());
    netty.setRootResourcePath("")
    netty.setSecurityDomain(null);
    netty.start();
}
```

Maven project you must include is:

```xml
<dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-netty</artifactId>
    <version>3.0.9.Final</version>
</dependency>
```
</dependency>
Chapter 37. Server-side Mock Framework

Although RESTEasy has an Embeddable Container, you may not be comfortable with the idea of starting and stopping a web server within unit tests (in reality, the embedded container starts in milliseconds), or you might not like the idea of using Apache HTTP Client or java.net.URL to test your code. RESTEasy provides a mock framework so that you can invoke on your resource directly.

```java
import org.jboss.resteasy.mock.*;
...

Dispatcher dispatcher = MockDispatcherFactory.createDispatcher();
POJOResourceFactory noDefaults = new POJOResourceFactory(LocatingResource.class);
dispatcher.getRegistry().addResourceFactory(noDefaults);
{
    MockHttpRequest request = MockHttpRequest.get("/locating/basic");
    MockHttpResponse response = new MockHttpResponse();

    dispatcher.invoke(request, response);

    Assert.assertEquals(HttpServletResponse.SC_OK, response.getStatus());
    Assert.assertEquals("basic", response.getContentAsString());
}
```

See the RESTEasy Javadoc for all the ease-of-use methods associated with MockHttpRequest, and MockHttpResponse.
Chapter 38. Securing JAX-RS and RESTeasy

Because Resteasy is deployed as a servlet, you must use standard web.xml constraints to enable authentication and authorization.

Unfortunately, web.xml constraints do not mesh very well with JAX-RS in some situations. The problem is that web.xml URL pattern matching is very very limited. URL patterns in web.xml only support simple wildcards, so JAX-RS resources like:

```
/{pathparam1}/foo/bar/{pathparam2}
```

Cannot be mapped as a web.xml URL pattern like:

```
/*/foo/bar/*/ 
```

To get around this problem you will need to use the security annotations defined below on your JAX-RS methods. You will still need to set up some general security constraint elements in web.xml to turn on authentication.

Resteasy JAX-RS supports the @RolesAllowed, @PermitAll and @DenyAll annotations on JAX-RS methods. By default though, Resteasy does not recognize these annotations. You have to configure Resteasy to turn on role-based security by setting a context parameter. NOTE!!! Do not turn on this switch if you are using EJBs. The EJB container will provide this functionality instead of Resteasy.

```
<web-app>
  ...
  <context-param>
    <param-name>resteasy.role_based.security</param-name>
    <param-value>true</param-value>
  </context-param>
</web-app>
```

There is a bit of quirkiness with this approach. You will have to declare all roles used within the Resteasy JAX-RS war file that you are using in your JAX-RS classes and set up a security
constraint that permits all of these roles access to every URL handled by the JAX-RS runtime. You'll just have to trust that Resteasy JAX-RS authorizes properly.

How does Resteasy do authorization? Well, it's really simple. It just sees if a method is annotated with @RolesAllowed and then just does HttpServletRequest.isUserInRole. If one of the @RolesAllowed passes, then allow the request, otherwise, a response is sent back with a 401 (Unauthorized) response code.

So, here's an example of a modified RESTEasy WAR file. You'll notice that every role declared is allowed access to every URL controlled by the Resteasy servlet.

```
<web-app>
  <context-param>
    <param-name>resteasy.role.based.security</param-name>
    <param-value>true</param-value>
  </context-param>

  <listener>
    <listener-class>org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap</listener-class>
  </listener>

  <servlet>
    <servlet-name>Resteasy</servlet-name>
    <servlet-class>org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher</servlet-class>
  </servlet>

  <servlet-mapping>
    <servlet-name>Resteasy</servlet-name>
    <url-pattern>/*</url-pattern>
  </servlet-mapping>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Resteasy</web-resource-name>
      <url-pattern>/security</url-pattern>
    </web-resource-collection>

    <auth-constraint>
      <role-name>admin</role-name>
      <role-name>user</role-name>
    </auth-constraint>
  </security-constraint>
</web-app>
```
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>Test</realm-name>
</login-config>

<security-role>
  <role-name>admin</role-name>
</security-role>
<security-role>
  <role-name>user</role-name>
</security-role>

</web-app>
Chapter 39. OAuth 2.0 and Resteasy Skeleton Key

The overall goal of Resteasy Skeleton Key is to provide a unified way for both Browser and JAX-RS clients to be secured in an integrated and seamless fashion. We want to support a network of applications and services so that if one server needs to execute or forward requests to another, there is a secure and scalable way to do this without hitting a central authentication server each and every request.

The OAuth 2.0 [http://tools.ietf.org/html/rfc6749] Authorization Framework enables a third-party to obtain access to an HTTP resource on behalf of a resource owner without the third-party having to know the credentials of the resource owner. It does this by issuing access tokens via a browser redirect protocol, or by a direct grant. The access tokens can then be transmitted by the OAuth2 Bearer Token [http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-23] protocol to access the protected resource.

Resteasy Skeleton Key is an OAuth 2.0 implementation that allows you to use existing JBoss AS7 security infrastructure to secure your web applications and restful services. You can turn an existing web app into an OAuth 2.0 Access Token Provider or you can turn a JBoss AS7 Security Domain into a central authentication and authorization server that a whole host of applications and services can use. Here are the features in a nutshell:

• Turn an existing servlet-form-auth-based web application into an OAuth 2.0 provider.

• Provide Distributed Single-Sign-On (SSO) from a central authentication server. Log in once, and you can securely access any browser-based app configured to work in the domain.

• Provide Distributed Logout. Following one link from any application can log you out of all your distributed applications configured to use SSO.

• Web apps can interact securely with any remote restful service by forwarding access tokens through the standard Authorization header.

• Access tokens are digitally signed by the oauth2 framework and can be used to access any service configured to work in the domain. The tokens contain both identity and role mapping information. Because they are digitally signed, there's no need to overload the central authentication server with each request to verify identity and to determine permissions.

Important

The Resteasy distribution comes with an OAuth2 Skeleton key example. This is a great way to see OAuth2 in action and how it is configured. You may also want to use this as a template for your applications.
39.1. System Requirements

- JBoss AS 7.1.x or higher
- HTTPS is required. See the JBoss 7 documentation on how to enable SSL for web applications
- Resteasy 3.0 or higher must be installed within your AS7 distribution. View how to upgrade AS7 to the latest version of Resteasy.
- A username/password based JBoss security domain
- Browser-based apps must be configured to use servlet FORM authentication and web.xml security constraints

39.2. Generate the Security Domain Key Pair

Access tokens are digitally signed and verified by an RSA keypair. You must generate this keypair using the JDK's keytool command or by something like openssl.

```
$ keytool -genkey -alias mydomain -keyalg rsa -keystore realm.jks
```

This will ask you a series of questions that will be used to create the X509 public certificate. Basic PKI stuff that you hopefully are already familiar with. Move this keystore file into a directory that you can reference from a configuration file. I suggest the standalone/configuration directory of your JBoss AS7 distribution.

39.3. Setting up the Auth Server

The next thing you're gonna want to do is set up a web application to be your OAuth2 provider. This can be an existing web app or you can create a new WAR to be your central authentication server. An existing web app must be configured to use servlet FORM authentication. Enabling OAuth2 within this app will not change how normal users interact with it.

39.3.1. Setting up your Security Domain

You can use any set of JBoss AS7 login modules you want to store your username, passwords and role mappings. Each security domain will be comprised of regular users, oauth clients, and admins. OAuth clients represent either a web application that wants to use the auth-server to do SSO, or they are traditional oauth clients that want access permission to act on behalf of another user (the traditional OAuth use case). Every oauth client must have a username, password, and a specific role mapping that gives them various permissions to participate in OAuth 2 protocols. There is a role that grants an oauth client permission to login as a specific user (default is login. This is the SSO case. There is a role that grants a client permission to request permission to act on behalf of a user (default is oauth). Additional role mappings assigned to the oauth client define
what additional permissions they are allowed to have. These additional permissions are the role mappings of the application and are the intersection of the permissions given to the user the client is acting on behalf of. This is better explained by an example role mapping file:

```
wburke=user,admin
loginclient=login
oauthclient1=oauth,*
oauthclient2=oauth,user
```

In the above role mapping file with have a simple user wburke. He has application role permissions of user and admin. One oauth client user is loginclient. It has been given a role mapping of login. This client is allowed to login as the user and is given all roles of the user. The oauthclient1 user is not allowed to login as the user, but is allowed to obtain an OAuth grant to act on behalf of the user. The * role means that oauthclient1 is granted the same roles as the user it is acting on behalf of. If oauthclient1 acts on behalf of wburke then it will have both user and admin permissions. The oauthclient2 is also allowed to use the oauth grant protocol, but it will only ever be granted user permissions.

You are not confined to login, oauth, and * as role mapping names. You can configure them to be whatever you want.

Why have different login and oauth role mappings? login clients are allowed to bypass entering username and password if the user has already logged in once and has an existing authenticated session with the server. oauth clients are always required to enter username and password. You probably don't want to grant permission automatically to an oauth client. A user will want to look at who is requesting permission. This role distinction gives you this capability.

### 39.3.2. Auth Server Config File

You must create a configuration file that holds all the configuration for OAuth2. This is json formatted. If you name it resteasy-oauth.json and put it within the WEB-INF/ directory of your war, that's all you have to do. Otherwise, you must specify the full path to this configuration file within a context-param within your web.xml file. The name of this param is skeleton.key.config.file. You can reference System properties within the value of this context-param by enclosing them within `${VARIABLE}`. Here's an example configuration:

```
{
    "realm" : "mydomain",
    "admin-role" : "admin",
    "login-role" : "login",
    "oauth-client-role" : "oauth",
    "wildcard-role" : "*",
    "realm-keystore" : "${jboss.server.config.dir}/realm.jks",
}```
Let's go over what each of these config variables represent:

realm
   Name of the realm representing the users of your distributed applications and services

admin-role
   Admin role mapping used for admins. You must have this defined if you want to do distributed logout.

login-role
   Role mapping for login clients.

oauth-client-role
   Role mapping for regular oauth clients.

wildcard-role
   Role mapping for assigning all roles to an oauth client wishing to act on behalf of a user.

realm-keystore
   Absolute path pointing to the keystore that contains the realm's keypair. This keypair is used to digitally sign access tokens. You may use `${VARIABLE}` to reference System properties. The example is referencing the JBoss config dir.

realm-key-alias
   Key alias for the key pair stored in your realm-keystore file.

realm-keystore-password
   Password to access the keystore.

realm-private-key-password
   Password to access the private realm key within the keystore

access-code-lifetime
   The access code is obtained via a browser redirect after you log into the central server. This access code is then transmitted in a separate request to the auth server to obtain an access
token. This variable is the lifetime of this access code. In how many seconds will it expire. You want to keep this value short. The default is 300 seconds.

token-lifetime
This is how long in seconds the access token is viable after it was first created. The default is one hour. Depending on your security requirements you may want to extend or shorten this default.

truststore
Used for outgoing client HTTPS communications. This contains one or more trusted host certificates or certificate authorities. This is OPTIONAL if you are not using distributed logout.

truststore-password
Password for the truststore keystore.

resources
Root URLs of applications using this auth-server for SSO. This is OPTIONAL and only needed if you want to allow distributed logout.

39.3.3. Set up web.xml

Set up your security constraints however you like. You must though use FORM authentication.

39.3.4. Set up jboss-web.xml

In jboss-web.xml in your WEB-INF directory, point to your security domain as a normal secured web app does, and also use a specific valve.

```xml
<jboss-web>
  <security-domain>java:/jaas/commerce</security-domain>
  <valve>
    <class-name>org.jboss.resteasy.skeleton.key.as7.OAuthAuthenticationServerValve</class-name>
  </valve>
</jboss-web>
```

39.3.5. Set up jboss-deployment-structure.xml

You must import the skeleton key modules so that the classes are visible to this application. Include this file within WEB-INF

```xml
<jboss-deployment-structure>
  <deployment>
    <dependencies>
```

167
39.3.6. Tweak your login page

The action url used by your login form is dependent on the oauth protocol. Skeleton key defines a request attribute called `OAUTH_FORM_ACTION` which is the URL you should use for the form's action. Here's an example login.jsp page that uses this attribute:

```html
<form action="" method="post">
  <p><strong>Please Enter Your User Name: </strong>
  <input type="text" name="j_username" size="25"></p>
  <p><strong>Please Enter Your Password: </strong>
  <input type="password" size="15" name="j_password"></p>
  <input type="submit" value="Submit">
  <input type="reset" value="Reset">
</form>
```

39.4. Setting Up An App for SSO

This section specifies how you can use the central auth-server for SSO. Following these directions will use the auth-server for browser log in. The server will also be able to do bearer token authentication as well.

39.4.1. SSO config file

The best way to create the config file for your application is to ask the central authentication server you configured in the last section. So, boot up the auth server and go to `https://auth-server-context-root/j_oauth_realm_info.html`. For example: `https://localhost:8443/auth-server/j_oauth_realm_info.html`. This will show template configurations depending on which valve you are using. You want the `OAuthManagedResourceValve` config. It will look something like this:

```json
{
    "realm" : "mydomain",
    "realm-public-key" : "MIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoXXyi7oAq5ecsYy+tJr154N2TtKAskWEDmzvSPU+muA2/3qHcxucZakG74Z49410tn5Iiu2CXX1k9CuKcpXvK
```
Let's go over what each of these config variables represent:

**realm**
Name of the realm representing the users of your distributed applications and services

**realm-public-key**
PEM format of public key.

**admin-role**
Admin role mapping used for admins. You must have this defined if you want to do distributed logout.

**auth-url**
URL of the auth server's login page.

**code-url**
URL to turn an access code into an access token. (Part of the OAuth2 protocol)

**truststore**
Used for outgoing client HTTPS communications. This contains one or more trusted host certificates or certificate authorities. This is REQUIRED as you must talk HTTPS to the auth server to turn an access code into an access token. You can create this truststore by extracting the public certificate of the auth server's SSL keystore. The google knows if you want to know how to do this.

**truststore-password**
Password for the truststore keystore.

**client-id**
Username of the login client. This server will send client-id and password when turning an access code into an access token. Internally, the server will do an HTTPS invocation to the auth-server passing this information using Basic AUTH.

**client-credentials**
Must specify the password of the oauth login client.
39.4.2. Set up web.xml

Set up your security constraints however you like. You must though use FORM authentication.

39.4.3. Set up jboss-web.xml

In jboss-web.xml in your WEB-INF directory you need to use a specific valve.

```xml
<jboss-web>
  <valve>
    <class-name>org.jboss.resteasy.skeleton.key.as7.OAuthManagedResourceValve</class-name>
  </valve>
</jboss-web>
```

39.4.4. Set up jboss-deployment-structure.xml

You must import the skeleton key modules so that the classes are visible to this application. Include this file within WEB-INF

```xml
<jboss-deployment-structure>
  <deployment>
    <dependencies>
      <module name="org.jboss.resteasy.resteasy-jaxrs" services="import"/>
      <module name="org.jboss.resteasy.resteasy-jackson-provider" services="import"/>
      <module name="org.jboss.resteasy.skeleton-key"/>
    </dependencies>
  </deployment>
</jboss-deployment-structure>
```

39.5. Bearer Token only Setup

If you have a web app that you want only to allow Bearer token authentication, i.e. a set of JAX-RS services then follow these directions.

39.5.1. Bearer token auth config file

The best way to create the config file for your application is to ask the central authentication server you configured in the last section. So, boot up the auth server and go to https://auth-server-context-root/j_oauth_realm_info.html. For example: https://localhost:8443/auth-server/
j_oauth_realm_info.html. This will show template configurations depending on which valve you are using. You want the BearerTokenAuthenticatorValve config. It will look something like this.

```json
{
  "realm" : "mydomain",
  "realm-public-key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCo8XXyi7oAq5ecsYy+tJr154N2TtKakxuWEDmzvSPU+mUA2/3qHcxucZakG74Z49410tn51u2CXXl9CuKcpXvKh+cPBzmC1Nmbd+4Me1RVV2nvogyPICs8h3sNTAMNdFI6hDc5/MfVQ9m50ZrkBN3dY50mTi/ExnJ51WPqXQIDAQAB",
}
```

All that is needed is the realm name, and the public key of the realm. Let's go over what each of these config variables represent:

- **realm**
  Name of the realm representing the users of your distributed applications and services

- **realm-public-key**
  PEM format of the realm's public key. Used to verify tokens.

### 39.5.2. Set up web.xml

Set up your security constraints however you like. You must though use FORM authentication.

### 39.5.3. Set up jboss-web.xml

In jboss-web.xml in your WEB-INF directory you need to use a specific valve.

```xml
<jboss-web>
  <valve>
    <class-name>org.jboss.resteasy.skeleton.key.as7.BearerTokenAuthenticatorValve</class-name>
  </valve>
</jboss-web>
```

### 39.5.4. Set up jboss-deployment-structure.xml

You must import the skeleton key modules so that the classes are visible to this application. Include this file within WEB-INF
39.6. Obtaining an access token programmatically.

You can request an access token from the auth-server by doing a simple HTTPS invocation. You must use BASIC authentication to identify your user, and you will get back a signed access token for that user. Here’s an example using a JAX-RS 2.0 client:

```java
ResteasyClient client = new ResteasyClientBuilder()
    .truststore(truststore)
    .build();

Form form = new Form().param("grant_type", "client_credentials");
ResteasyWebTarget target = client.target("https://localhost:8443/auth-server/j_oauth_token_grant");
target.configuration().register(new BasicAuthentication("bburke@redhat.com", "password"));
AccessTokenResponse res = target.request()
    .post(Entity.form(form), AccessTokenResponse.class);
```

The above makes a simple POST to the context root of the auth server with \texttt{j\_oauth\_token\_grant} at the end of the target URL. This resource is responsible for creating access tokens.

```java
try {
        .header(HttpHeaders.AUTHORIZATION, "Bearer " + res.getToken()).get();
    String xml = response.readEntity(String.class);
} finally {
    client.close();
}
```
The access token is a simple string. To invoke on a service protected by bearer token auth, just set the **Authorization** header of your HTTPS request with a value of **Bearer** and then the access token string.

## 39.7. Access remote services securely in a secure web session

If you have an application secured by one of the methods described in this chapter, you can obtain the access token of the current web session so that you can use it to invoke on other remote services securely using bearer token authentication. Each `HttpServletRequest` in a secure web session has an attribute called `org.jboss.resteasy.skeleton.key.SkeletonKeySession` which points to an instance of a class with the same name. This class contains the access token and also points to the truststore you configured. You can then extract this info and make secure remote invocations. Here's an example of that.

```java
public List<String> getCustomers(HttpServletRequest request) {
    SkeletonKeySession session = (SkeletonKeySession) request.getAttribute(SkeletonKeySession.class.getName());
    ResteasyClient client = new ResteasyClientBuilder()
        .truststore(session.getMetadata().getTruststore())
        .build();
    try {
            .header(HttpHeaders.AUTHORIZATION, "Bearer " + session.getToken()).get();
        return response.readEntity(new GenericType<List<String>>{});
    } finally {
        client.close();
    }
}
```

If you are within a JAX-RS environment you can inject a `SkeletonKeySession` using the `@Context` annotation.
39.8. Check Out the OAuth2 Example!

Important

The Resteasy distribution comes with an example project that shows all of these different features in action! Check it out!

39.9. Auth Server Action URLs

For reference, here is the set of relative URL actions that the auth server will publish.

*login page*

The is the url of your login page. OAuth clients will redirect to it. This is application specific.

*j_oauth_resolve_access_code*

Used by oauth clients to turn an access code into an access token.

*j_oauth_logout*

Do a GET request to this URL and it will perform a distributed logout.

*j_oauth_token_grant*

Do a POST with BASIC Auth to obtain an access token for a specific user.

*j_oauth_realm_info.html*

Displays an HTML page with template configurations for using this realm.
Chapter 40. Authentication

Since Resteasy runs within a servlet container you can use most (all?) mechanism available in your servlet container for authentication. Basic and Digest authentication are probably the easiest to set up and fit nicely into REST’s stateless principle. Form security can be used, but requires passing the session’s cookie value with each request. We have done some preliminary work on OAuth and also plan to work on OpenID and SAML integration in the future.

40.1. OAuth core 1.0a

RESTEasy has preliminary support for OAuth core 1.0a [http://oauth.net/core/1.0a]. This includes support for authenticating with OAuth (as described by the spec section 6 [http://oauth.net/core/1.0a#rfc.section.6]) and OAuth authentication for protected resources (as described by the spec section 7 [http://oauth.net/core/1.0a#rfc.section.7]).

Important

This API is deprecated and will be removed in subsequent versions of Resteasy unless there is an outcry from the community. We’re focusing on OAuth 2.0 protocols. Please see our OAuth 2.0 Work.

40.1.1. Authenticating with OAuth 1.0a

OAuth authentication is the process in which Users grant access to their Protected Resources without sharing their credentials with the Consumer.

OAuth Authentication is done in three steps:

1. The Consumer obtains an unauthorized Request Token. This part is handled by RESTEasy.

2. The User authorizes the Request Token. This part is not handled by RESTEasy because it requires a user interface where the User logs in and authorizes or denies the Request Token. This cannot be implemented automatically as it needs to be integrated with your User login process and user interface.

3. The Consumer exchanges the Request Token for an Access Token. This part is handled by RESTEasy.

In order for RESTEasy to provide the two URL endpoints where the Client will request unauthorized Request Tokens and exchange authorized Request Tokens for Access Tokens, you need to enable the OAuthServlet in your web.xml:
The following configuration options are available using `<context-param>` elements:

**Table 40.1. OAuth 1.0a Servlet options**

<table>
<thead>
<tr>
<th>Option Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oauth.provider.provider-class</td>
<td><em>Required</em></td>
<td>Defines the fully-qualified class name of your OAuthProvider implementation</td>
</tr>
<tr>
<td>oauth.provider.tokens.request</td>
<td>/requestToken</td>
<td>This defines the endpoint URL for requesting unauthorized Request Tokens</td>
</tr>
<tr>
<td>oauth.provider.tokens.access</td>
<td>/accessToken</td>
<td>This defines the endpoint URL for exchanging authorized Request Tokens for Access Tokens</td>
</tr>
</tbody>
</table>

### 40.1.2. Accessing protected resources

After successfully receiving the Access Token and Token Secret, the Consumer is able to access the Protected Resources on behalf of the User.

RESTEasy supports OAuth authentication for protected resources using a servlet filter which should be mapped in your `web.xml` for all protected resources:

<!-- The OAuth Filter handles authentication for protected resources -->
<filter>
  <filter-name>OAuth Filter</filter-name>
  <filter-class>org.jboss.RESTEasy.auth.oauth.OAuthFilter</filter-class>
</filter>
Implementing an OAuthProvider

```xml
<filter>
<!-- This defines the URLs which should require OAuth authentication for your protected resources -->
<filter-mapping>
  <filter-name>OAuth Filter</filter-name>
  <url-pattern>/rest/*</url-pattern>
</filter-mapping>
</filter>

The following configuration options are available using `<context-param>` elements:

Table 40.2. OAuth Filter options

<table>
<thead>
<tr>
<th>Option Name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oauth.provider.provider-class</td>
<td><em>Required</em></td>
<td>Defines the fully-qualified class name of your OAuthProvider implementation</td>
</tr>
</tbody>
</table>

Once authenticated, the OAuth Servlet Filter will set your request's Principal and Roles, which can then be accessed using the JAX-RS SecurityContext. You can also protect your resources using Roles as described in the section "Securing JAX-RS and RESTeasy".

40.1.3. Implementing an OAuthProvider

In order for RESTEasy to implement OAuth it needs you to provide an instance of `OAuthProvider` which will provide access to the list of Consumer, Request and Access Tokens. Because one size doesn’t fit all we cannot know if you wish to store your Tokens and Consumer credentials in a configuration file, in memory, or on persistent storage.

All you need to do is implement the `OAuthProvider` interface:

```java
public interface OAuthProvider {
  String getRealm();

  OAuthConsumer getConsumer(String consumerKey) throws OAuthException;
  OAuthToken getRequestToken(String consumerKey, String requestToken) throws OAuthException;
  OAuthToken getAccessToken(String consumerKey, String accessToken) throws OAuthException;
  OAuthToken makeRequestToken(String consumerKey, String callback) throws OAuthException;
```
OAuthToken makeAccessToken(String consumerKey, String requestToken, String verifier) throws OAuthException;

String authoriseRequestToken(String consumerKey, String requestToken) throws OAuthException;

void checkTimestamp(OAuthToken token, long timestamp) throws OAuthException;

If a Consumer Key, or Token doesn’t exist, or if the timestamp is not valid, simply throw an OAuthException.

The rest of the interfaces used in OAuthProvider are:

public interface OAuthConsumer {
    String getKey();
    String getSecret();
}

public interface OAuthToken {
    OAuthConsumer getConsumer();
    String getToken();
    String getSecret();
    Principal getPrincipal();
    Set<String> getRoles();
}
Chapter 41. JSON Web Signature and Encryption (JOSE-JWT)

JSON Web Signature and Encryption (JOSE JWT) is a new specification that can be used to encode content as a string and either digitally sign or encrypt it. I won't go over the spec here. Do a Google search on it if you're interested.

41.1. JSON Web Signature (JWS)

To digitally sign content using JWS, use the `org.jboss.resteasy.jose.jws.JWSBuilder` class. To unpack and verify a JWS, use the `org.jboss.resteasy.jose.jws.JWSInput` class. (TODO, write more doco here!) Here's an example:

```java
@Test
public void testRSAWithContentType() throws Exception {
    KeyPair keyPair = KeyPairGenerator.getInstance("RSA").generateKeyPair();

    String encoded = new JWSBuilder()
        .contentType(MediaType.TEXT_PLAIN_TYPE)
        .content("Hello World", MediaType.TEXT_PLAIN_TYPE)
        .rsa256(keyPair.getPrivate());

    System.out.println(encoded);

    JWSInput input = new JWSInput(encoded,
        ResteasyProviderFactory.getInstance());
    System.out.println(input.getHeader());
    String msg = (String)input.readContent(String.class);
    Assert.assertEquals("Hello World", msg);
    Assert.assertTrue(RSAProvider.verify(input, keyPair.getPublic()));
}
```

41.2. JSON Web Encryption (JWE)

To encrypt content using JWE, use the `org.jboss.resteasy.jose.jwe.JWEBuilder` class. To decrypt content using JWE, use the `org.jboss.resteasy.jose.jwe.JWEInput` class. (TODO, write more doco here!) Here's an example:
@Test
public void testRSA() throws Exception {
    KeyPair keyPair = KeyPairGenerator.getInstance("RSA").generateKeyPair();
    String content = "Live long and prosper."
    String encoded = new JWEBuilder().contentBytes(content.getBytes()).RSA1_5((RSAPublicKey)keyPair.getPublic());
    System.out.println("encoded: " + encoded);
    byte[] raw = new JWEInput(encoded).decrypt((RSAPrivateKey)keyPair.getPrivate()).getRawContent();
    String from = new String(raw);
    Assert.assertEquals(content, from);
}

String encoded = new JWEBuilder().contentBytes(content.getBytes()).RSA_OAEP((RSAPublicKey)keyPair.getPublic());
    System.out.println("encoded: " + encoded);
    byte[] raw = new JWEInput(encoded).decrypt((RSAPrivateKey)keyPair.getPrivate()).getRawContent();
    String from = new String(raw);
    Assert.assertEquals(content, from);
}

String encoded = new JWEBuilder().contentBytes(content.getBytes()).A128CBC_HS256().RSA1_5((RSAPublicKey)keyPair.getPublic());
    System.out.println("encoded: " + encoded);
    byte[] raw = new JWEInput(encoded).decrypt((RSAPrivateKey)keyPair.getPrivate()).getRawContent();
    String from = new String(raw);
    Assert.assertEquals(content, from);
}

String encoded = new JWEBuilder().contentBytes(content.getBytes()).A128CBC_HS256().RSA_OAEP((RSAPublicKey)keyPair.getPublic());
    System.out.println("encoded: " + encoded);
    byte[] raw = new JWEInput(encoded).decrypt((RSAPrivateKey)keyPair.getPrivate()).getRawContent();
    String from = new String(raw);
    Assert.assertEquals(content, from);
}

@Test
public void testDirect() throws Exception
{
    String content = "Live long and prosper.";
    String encoded = new JWEBuilder().contentBytes(content.getBytes()).dir("geheim");
    System.out.println("encoded: " + encoded);
    byte[] raw = new JWEInput(encoded).decrypt("geheim").getRawContent();
    String from = new String(raw);
    Assert.assertEquals(content, from);
}

Chapter 42. Doseta Digital Signature Framework

Digital signatures allow you to protect the integrity of a message. They are used to verify that a message sent was sent by the actual user that sent the message and was modified in transit. Most web apps handle message integrity by using TLS, like HTTPS, to secure the connection between the client and server. Sometimes though, we have representations that are going to be forwarded to more than one recipient. Some representations may hop around from server to server. In this case, TLS is not enough. There needs to be a mechanism to verify who sent the original representation and that they actually sent that message. This is where digital signatures come in.

While the mime type multiple/signed exists, it does have drawbacks. Most importantly it requires the receiver of the message body to understand how to unpack. A receiver may not understand this mime type. A better approach would be to put signatures in an HTTP header so that receivers that don't need to worry about the digital signature, don't have to.

The email world has a nice protocol called Domain Keys Identified Mail [http://dkim.org] (DKIM). Work is also being done to apply this header to protocols other than email (i.e. HTTP) through the DOSETA specifications [https://tools.ietf.org/html/draft-crocker-doseta-base-02]. It allows you to sign a message body and attach the signature via a DKIM-Signature header. Signatures are calculated by first hashing the message body then combining this hash with an arbitrary set of metadata included within the DKIM-Signature header. You can also add other request or response headers to the calculation of the signature. Adding metadata to the signature calculation gives you a lot of flexibility to piggyback various features like expiration and authorization. Here's what an example DKIM-Signature header might look like.

```
DKIM-Signature: v=1;
a=rsa-sha256;
d=example.com;
s=burke;
c=simple/simple;
h=Content-Type;
x=002342311111;
bh=2342322111;
b=M232234=
```

As you can see it is a set of name value pairs delimited by a ';'. While its not THAT important to know the structure of the header, here's an explanation of each parameter:

- **v**
Algorithm used to hash and sign the message. RSA signing and SHA256 hashing is the only supported algorithm at the moment by Resteasy.

Domain of the signer. This is used to identify the signer as well as discover the public key to use to verify the signature.

Selector of the domain. Also used to identify the signer and discover the public key.

Canonical algorithm. Only simple/simple is supported at the moment. Basically this allows you to transform the message body before calculating the hash

Semi-colon delimited list of headers that are included in the signature calculation.

When the signature expires. This is a numeric long value of the time in seconds since epoch. Allows signer to control when a signed message's signature expires

Timestamp of signature. Numeric long value of the time in seconds since epoch. Allows the verifier to control when a signature expires.

Base 64 encoded hash of the message body.

Base 64 encoded signature.

To verify a signature you need a public key. DKIM uses DNS text records to discover a public key. To find a public key, the verifier concatenates the Selector (s parameter) with the domain (d parameter)

It then takes that string and does a DNS request to retrieve a TXT record under that entry. In our above example burke._domainKey.example.com would be used as a string. This is a every interesting way to publish public keys. For one, it becomes very easy for verifiers to find public keys. There's no real central store that is needed. DNS is a infrastructure IT knows how to deploy. Verifiers can choose which domains they allow requests from. Resteasy supports discovering public keys via DNS. It also instead allows you to discover public keys within a local Java KeyStore if you do not want to use DNS. It also allows you to plug in your own mechanism to discover keys.

If you're interested in learning the possible use cases for digital signatures, here's a blog [http://bill.burkecentral.com/2011/02/21/multiple-uses-for-content-signature/] you might find interesting.
42.1. Maven settings

You must include the resteasy-crypto project to use the digital signature framework.

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-crypto</artifactId>
  <version>3.0.9.Final</version>
</dependency>
```

42.2. Signing API

To sign a request or response using the Resteasy client or server framework you need to create an instance of `org.jboss.resteasy.security.doseta.DKIMSignature`. This class represents the DKIM-Signature header. You instantiate the `DKIMSignature` object and then set the "DKIM-Signature" header of the request or response. Here's an example of using it on the server-side:

```java
import org.jboss.resteasy.security.doseta.DKIMSignature;
import java.security.PrivateKey;

@Path("/signed")
public static class SignedResource
{
  @GET
  @Path("manual")
  @Produces("text/plain")
  public Response getManual()
  {
    PrivateKey privateKey = ....; // get the private key to sign message

    DKIMSignature signature = new DKIMSignature();
    signature.setSelector("test");
    signature.setDomain("samplezone.org");
    signature.setPrivateKey(privateKey);

    Response.ResponseBuilder builder = Response.ok("hello world");
    builder.header(DKIMSignature.DKIM_SIGNATURE, signature);
    return builder.build();
  }
}
```

// client example
To sign a message you need a PrivateKey. This can be generated by KeyTool or manually using regular, standard JDK Signature APIs. Resteasy currently only supports RSA key pairs. The DKIMSignature class also allows you to add and control how various pieces of metadata are added to the DKIM-Signature header and the signature calculation. See the javadoc for more details.

If you are including more than one signature, then just add additional DKIMSignature instances to the headers of the request or response.

### 42.2.1. `@Signed` annotation

Instead of using the API, Resteasy also provides you an annotation alternative to the manual way of signing using a DKIMSignature instances is to use the `@org.jboss.resteasy.annotations.security.doseta.Signed` annotation. It is required that you configure a KeyRepository as described later in this chapter. Here's an example:

```java
@GET
@Produces("text/plain")
@Path("signedresource")
@Signed(selector="burke", domain="sample.com", timestamped=true,
expires=@After(hours=24))
public String getSigned()
{
    return "hello world";
}
```

The above example using a bunch of the optional annotation attributes of `@Signed` to create the following Content-Signature header:

```
DKIM-Signature: v=1;
a=rsa-sha256;
c=simple/simple;
domain=sample.com;
s=burke;
```
This annotation also works with the client proxy framework.

42.3. Signature Verification API

If you want fine grain control over verification, this is an API to verify signatures manually. It's a little tricky because you'll need the raw bytes of the HTTP message body in order to verify the signature. You can get at an unmarshalled message body as well as the underlying raw bytes by using a org.jboss.resteasy.spi.MarshalledEntity injection. Here's an example of doing this on the server side:

```java
import org.jboss.resteasy.spi.MarshalledEntity;

@POST
@Consumes("text/plain")
@Path("verify-manual")
public void verifyManual(@HeaderParam("Content-Signature") DKIMSignature signature,
                       @Context KeyRepository repository,
                       @Context HttpHeaders headers,
                       MarshalledEntity<String> input) throws Exception {
    Verifier verifier = new Verifier();
    Verification verification = verifier.addNew();
    verification.setRepository(repository);
    verification.setStaleCheck(true);
    verification.setStaleSeconds(100);
    try {
        verifier.verifySignature(headers.getRequestHeaders(),
                      input.getMarshalledBytes, signature);
    } catch (SignatureException ex) {
    }
    System.out.println("The text message posted is: " + input.getEntity());
}
```

MarshalledEntity is a generic interface. The template parameter should be the Java type you want the message body to be converted into. You will also have to configure a KeyRepository. This is describe later in this chapter.

The client side is a little bit different:
ClientRequest request = new ClientRequest("http://localhost:9095/signed"));

ClientResponse<String> response = request.get(String.class);
Verifier verifier = new Verifier();
Verification verification = verifier.addNew();
verification.setRepository(repository);
response.getProperties().put(Verifier.class.getName(), verifier);

// signature verification happens when you get the entity
String entity = response.getEntity();

On the client side, you create a verifier and add it as a property to the
ClientResponse. This will trigger the verification interceptors.

42.3.1. Annotation-based verification

The easiest way to verify a signature sent in a HTTP request on the server side is to use
the @@org.jboss.resteasy.annotations.security.doseta.Verify (or @Verifications which is used to
verify multiple signatures). Here's an example:

```java
@POST
@Consumes("text/plain")
@Verify
public void post(String input)
{
}
```

In the above example, any DKIM-Signature headers attached to the posted message body will
be verified. The public key to verify is discovered using the configured KeyRepository (discussed
later in this chapter). You can also specify which specific signatures you want to verify as well
as define multiple verifications you want to happen via the @Verifications annotation. Here's a
complex example:

```java
@POST
@Consumes("text/plain")
@Verifications(
        @Verify(identifierName="d", identifierValue="inventory.com",
        stale=@After(days=2)),
        @Verify(identifierName="d", identifierValue="bill.com")
    )
```
Managing Keys via a KeyRepository

```java
public void post(String input) {...}
```

The above is expecting 2 different signature to be included within the DKIM-Signature header.

Failed verifications will throw an `org.jboss.resteasy.security.doseta.UnauthorizedSignatureException`. This causes a 401 error code to be sent back to the client. If you catch this exception using an ExceptionHandler you can browse the failure results.

42.4. Managing Keys via a KeyRepository

Resteasy manages keys for you through a `org.jboss.resteasy.security.doseta.KeyRepository`. By default, the KeyRepository is backed by a Java KeyStore. Private keys are always discovered by looking into this KeyStore. Public keys may also be discovered via a DNS text (TXT) record lookup if configured to do so. You can also implement and plug in your own implementation of KeyRepository.

42.4.1. Create a KeyStore

Use the Java keytool to generate RSA key pairs. Key aliases MUST HAVE the form of:

```xml
<selector>._domainKey.<domain>
```

For example:

```
$ keytool -genkeypair -alias burke._domainKey.example.com -keyalg RSA -keysize 1024 -keystore my-apps.jks
```

You can always import your own official certificates too. See the JDK documentation for more details.

42.4.2. Configure Resteasy to use the KeyRepository

Next you need to configure the KeyRepository in your web.xml file so that it is created and made available to Resteasy to discover private and public keys. You can reference a Java key store you want the Resteasy signature framework to use within web.xml using either `resteasy.keystore.classpath` or `resteasy.keystore.filename` context parameters. You must also specify the password (sorry its clear text) using the `resteasy.keystore.password` context parameter. The `resteasy.context.objects` is used to create the instance of the repository. For example:

```
<context-param>
  <param-name>resteasy.doseta.keystore.classpath</param-name>
  <param-value>test.jks</param-value>
</context-param>
```
You can also manually register your own instance of a KeyRepository within an Application class.
For example:

```java
import org.jboss.resteasy.core.Dispatcher;
import org.jboss.resteasy.security.doseta.KeyRepository;
import org.jboss.resteasy.security.doseta.DosetaKeyRepository;
import javax.ws.rs.core.Application;
import javax.ws.rs.core.Context;

public class SignatureApplication extends Application {
    private HashSet<Class<?>> classes = new HashSet<Class<?>>();
    private KeyRepository repository;

    public SignatureApplication(@Context Dispatcher dispatcher) {
        classes.add(SignedResource.class);

        repository = new DosetaKeyRepository();
        repository.setKeyStorePath("test.jks");
        repository.setKeyStorePassword("password");
        repository.setUseDns(false);
        repository.start();

        dispatcher.getDefaultContextObjects().put(KeyRepository.class, repository);
    }

    @Override
    public Set<Class<?>> getClasses() {
        return classes;
    }
}
```
On the client side, you can load a KeyStore manually, by instantiating an instance of org.jboss.resteasy.security.doseta.DosetaKeyRepository. You then set a request attribute, "org.jboss.resteasy.security.doseta.KeyRepository", with the value of the created instance. Use the ClientRequest.getAttributes() method to do this. For example:

```java
dosetaKeyRepository = new DosetaKeyRepository();
repository.setKeyStorePath("test.jks");
repository.setKeyStorePassword("password");
repository.setUseDns(false);
repository.start();

dkimsSignature = new DKIMSignature();
signature.setDomain("example.com");

ClientRequest request = new ClientRequest("http://...");
request.getAttributes().put(KeyRepository.class.getName(), repository);
request.header("DKIM-Signature", signatures);
```

### 42.4.3. Using DNS to Discover Public Keys

Public keys can also be discovered by a DNS text record lookup. You must configure web.xml to turn this feature:

```xml
<context-param>
  <param-name>restateasy.doseta.use.dns</param-name>
  <param-value>true</param-value>
</context-param>
<context-param>
  <param-name>restateasy.doseta.dns.uri</param-name>
  <param-value>dns://localhost:9095</param-value>
</context-param>
```

The restateasy.doseta.dns.uri context-param is optional and allows you to point to a specific DNS server to locate text records.

#### 42.4.3.1. Configuring DNS TXT Records

DNS TXT Records are stored via a format described by the DOSETA specification. The public key is defined via a base 64 encoding. You can obtain this text encoding by exporting your public keys from your keystore, then using a tool like openssl to get the text-based format. For example:
$ keytool -export -alias bill._domainKey.client.com -keystore client.jks -file bill.der
$ openssl x509 -noout -pubkey -in bill.der -inform der > bill.pem

The output will look something like:

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKxct5GHz8dFw0mzAMfVNju2b3oeAv/EOPfVb9mD73Wn+CIJXVnryh2o99Y/q47urWYWAF/bqH9AMyMfibPr6IlP8mO9pNYf/Zsqup/7oJxrvzJU7T0IGdLN1hHcC+qRnwKkdNmD8UPEQ4BXiX4xFxbTjNvKWLZVKGQMyy6EFVQIDAQAB
-----END PUBLIC KEY-----

The DNS text record entry would look like this:

test2._domainKey        IN      TXT
"v=DKIM1; p=MIGfMA0GCSqGSIb3DQEBAQUA4GNADCBiQKBgQCIKFLFwUqFdfBug688BJ0dazQ/x+GENH443KpnBK8agpJXSqFAPh1Rvf0yhqHeuI+J5onsSOo9Rn4fKaFQaQNBfCQpHSnZpBc3X0G5Bc1HWq1AtB1621rbyPen4CmGYOyRzDBU01W6n8K47bf3hvoSxpqY1pH+wIDAQAB; t=s"

Notice that the newlines are take out. Also, notice that the text record is a name value ';;' delimited list of parameters. The p field contains the public key.
Chapter 43. Body Encryption and Signing via SMIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. MIME data being a set of headers and a message body. Its most often seen in the email world when somebody wants to encrypt and/or sign an email message they are sending across the internet. It can also be used for HTTP requests as well which is what the RESTEasy integration with S/MIME is all about. RESTEasy allows you to easily encrypt and/or sign an email message using the S/MIME standard. While the API is described here, you may also want to check out the example projects that come with the RESTEasy distribution. It shows both Java and Python clients exchanging S/MIME formatted messages with a JAX-RS service.

43.1. Maven settings

You must include the resteasy-crypto project to use the smime framework.

```
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-crypto</artifactId>
  <version>3.0.9.Final</version>
</dependency>
```

43.2. Message Body Encryption

While HTTPS is used to encrypt the entire HTTP message, S/MIME encryption is used solely for the message body of the HTTP request or response. This is very useful if you have a representation that may be forwarded by multiple parties (for example, HornetQ's REST Messaging integration!) and you want to protect the message from prying eyes as it travels across the network. RESTEasy has two different interfaces for encrypting message bodies. One for output, one for input. If your client or server wants to send an HTTP request or response with an encrypted body, it uses the org.jboss.resteasy.security.smime.EnvelopedOutput type. Encrypting a body also requires an X509 certificate which can be generated by the Java keytool command-line interface, or the openssl tool that comes installed on many OS's. Here's an example of using the EnvelopedOutput interface:

```
// server side

@Path("encrypted")
@GET
public EnvelopedOutput getEncrypted()
```
An EnvelopedOutput instance is created passing in the entity you want to marshal and the media
type you want to marshal it into. So in this example, we’re taking a Customer class and marshalling
it into XML before we encrypt it. RESTEasy will then encrypt the EnvelopedOutput using the
BouncyCastle framework’s SMIME integration. The output is a Base64 encoding and would look
something like this:

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"

MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMiAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
MIAGCSqGSIb3DQEHATA8CMIAACAqAxghgM2w0DQQDQEElMDgQLDQgMIAw
```

Decrypting an S/MIME encrypted message requires using the
org.jboss.resteasy.security.smime.EnvelopedInput interface. You also need both the private key
and X509Certificate used to encrypt the message. Here’s an example:
// server side

@Path("encrypted")
@POST
public void postEncrypted(EnvelopedInput<Customer> input)
{
    PrivateKey privateKey = ...;
    X509Certificate certificate = ...;
    Customer cust = input.getEntity(privateKey, certificate);
}

// client side

ClientRequest request = new ClientRequest("http://localhost:9095/smime/encrypted");
EnvelopedInput input = request.getTarget(EnvelopedInput.class);
Customer cust = (Customer)input.getEntity(Customer.class, privateKey, cert);

Both examples simply call the getEntity() method passing in the PrivateKey and X509Certificate instances requires to decrypt the message. On the server side, a generic is used with EnvelopedInput to specify the type to marshal to. On the server side this information is passed as a parameter to getEntity(). The message is in MIME format: a Content-Type header and body, so the EnvelopedInput class now has everything it needs to know to both decrypt and unmarshal the entity.

43.3. Message Body Signing

S/MIME also allows you to digitally sign a message. It is a bit different than the Doseta Digital Signing Framework. Doseta is an HTTP header that contains the signature. S/MIME uses the multipart/signed data format which is a multipart message that contains the entity and the digital signature. So Doseta is a header, S/MIME is its own media type. Generally I would prefer Doseta as S/MIME signatures require the client to know how to parse a multipart message and Doseta doesn’t. Its up to you what you want to use.

Resteasy has two different interfaces for creating a multipart/signed message. One for input, one for output. If your client or server wants to send an HTTP request or response with a multipart/signed body, it uses the org.jboss.resteasy.security.smime.SignedOutput type. This type requires both the PrivateKey and X509Certificate to create the signature. Here’s an example of signing an entity and sending a multipart/signed entity.

// server-side

@Path("signed")
@GET


@Produces("multipart/signed")
public SignedOutput getSigned()
{
    Customer cust = new Customer();
    cust.setName("Bill");

    SignedOutput output = new SignedOutput(cust,
        MediaType.APPLICATION_XML_TYPE);
    output.setPrivateKey(privateKey);
    output.setCertificate(certificate);
    return output;
}

// client side
Client client = new ResteasyClient();
WebTarget target = client.target("http://localhost:9095/smime/signed");
Customer cust = new Customer();
    cust.setName("Bill");
    SignedOutput output = new SignedOutput(cust, "application/xml");
    output.setPrivateKey(privateKey);
    output.setCertificate(cert);
    Response res = target.request().post(Entity.entity(output, "multipart/signed");

An SignedOutput instance is created passing in the entity you want to marshal and the media type
you want to marshal it into. So in this example, we’re taking a Customer class and marshalling it
into XML before we sign it. RESTEasy will then sign the SignedOutput using the BouncyCastle
framework’s SMIME integration. The output iwould look something like this:

Content-Type: multipart/signed; protocol="application/pkcs7-signature";
  micalg=sha1; boundary="-----_Part_0_1083228271.1313024422098"

------=_Part_0_1083228271.1313024422098
Content-Type: application/xml
Content-Transfer-Encoding: 7bit

<customer name="bill"/>

------=_Part_0_1083228271.1313024422098
Content-Type: application/pkcs7-signature; name=smime.p7s; smime-type=signed-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAjBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAA...
To unmarshal and verify a signed message requires using the org.jboss.resteasy.security.smime.SignedInput interface. You only need the X509Certificate to verify the message. Here's an example of unmarshalling and verifying a multipart/signed entity.

```java
// server side
@Path("signed")
@POST
@Consumes("multipart/signed")
public void postSigned(SignedInput<Customer> input) throws Exception {
    Customer cust = input.getEntity();
    if (!input.verify(certificate)) {
        throw new WebApplicationException(500);
    }
}

// client side
Client client = new ResteasyClient();
WebTarget target = client.target("http://localhost:9095/smime/signed");
SignedInput input = target.request().get(SignedInput.class);
Customer cust = (Customer)input.getEntity(Customer.class);
input.verify(cert);
```

### 43.4. application/pkcs7-signature

application/pkcs7-signature is a data format that includes both the data and the signature in one ASN.1 binary encoding.

SignedOutput and SignedInput can be used to return application/pkcs7-signature format in binary form. Just change the @Produces or @Consumes to that media type to send back that format.

Also, if your @Produces or @Consumes is text/plain instead, SignedOutput will be base64 encoded and sent as a string.
Chapter 44. EJB Integration

To integrate with EJB you must first modify your EJB's published interfaces. Resteasy currently only has simple portable integration with EJBs so you must also manually configure your Resteasy WAR.

Resteasy currently only has simple integration with EJBs. To make an EJB a JAX-RS resource, you must annotate an SLSB's @Remote or @Local interface with JAX-RS annotations:

```java
@Local
@Path("/Library")
public interface Library {

    @GET
    @Path("/books/{isbn}")
    public String getBook(@PathParam("isbn") String isbn);
}

@Stateless
public class LibraryBean implements Library {
...
}
```

Next, in RESTeasy's web.xml file you must manually register the EJB with RESTeasy using the resteasy.jndi.resources <context-param>:

```xml
<web-app>
    <display-name>Archetype Created Web Application</display-name>
    <context-param>
        <param-name>resteasy.jndi.resources</param-name>
        <param-value>LibraryBean/local</param-value>
    </context-param>
    <listener>
        <listener-class>org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap</listener-class>
    </listener>
</web-app>
```
<servlet>
  <servlet-name>Resteasy</servlet-name>
  <servlet-class>org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>Resteasy</servlet-name>
  <url-pattern>/*</url-pattern>
</servlet-mapping>

</web-app>

This is the only portable way we can offer EJB integration. Future versions of RESTeasy will have tighter integration with JBoss AS so you do not have to do any manual registrations or modifications to web.xml. For right now though, we're focusing on portability.

If you're using Resteasy with an EAR and EJB, a good structure to have is:

```
my-ear.ear
  |----myejb.jar
  |----resteasy-jaxrs.war
  |
  \----WEB-INF/web.xml
  \----WEB-INF/lib (nothing)
  \----lib/
       \----All Resteasy jar files
```

From the distribution, remove all libraries from WEB-INF/lib and place them in a common EAR lib. OR. Just place the Resteasy jar dependencies in your application server's system classpath. (i.e. In JBoss put them in server/default/lib)

An example EAR project is available from our testsuite here.
Chapter 45. Spring Integration

RESTEasy integrates with Spring 3.0.x. We are interested in other forms of Spring integration, so please help contribute.

45.1. Basic Integration

For Maven users, you must use the resteasy-spring artifact. Otherwise, the jar is available in the downloaded distribution.

```xml
<dependency>
  <groupId>org.jboss.resteasy</groupId>
  <artifactId>resteasy-spring</artifactId>
  <version>whatever version you are using</version>
</dependency>
```

RESTEasy comes with its own Spring ContextLoaderListener that registers a RESTEasy specific BeanPostProcessor that processes JAX-RS annotations when a bean is created by a BeanFactory. What does this mean? RESTEasy will automatically scan for @Provider and JAX-RS resource annotations on your bean class and register them as JAX-RS resources.

Here is what you have to do with your web.xml file

```xml
<web-app>
  <display-name>Archetype Created Web Application</display-name>

  <listener>
    <listener-class>org.jboss.resteasy.plugins.server.servlet.ResteasyBootstrap</listener-class>
  </listener>

  <listener>
    <listener-class>org.jboss.resteasy.plugins.spring.SpringContextLoaderListener</listener-class>
  </listener>

  <servlet>
    <servlet-name>Resteasy</servlet-name>
  </servlet>
</web-app>
```
The SpringContextLoaderListener must be declared after ResteasyBootstrap as it uses ServletContext attributes initialized by it.

If you do not use a Spring ContextLoaderListener to create your bean factories, then you can manually register the RESTeasy BeanFactoryPostProcessor by allocating an instance of org.jboss.resteasy.plugins.spring.SpringBeanProcessor. You can obtain instances of a ResteasyProviderFactory and Registry from the ServletContext attributes org.jboss.resteasy.spi.ResteasyProviderFactory and org.jboss.resteasy.spi.Registry. (Really the string FQN of these classes). There is also a org.jboss.resteasy.plugins.spring.SpringBeanProcessorServletAware, that will automatically inject references to the Registry and ResteasyProviderFactory from the Servlet Context. (that is, if you have used RestasyBootstrap to bootstrap Resteasy).

Our Spring integration supports both singletons and the "prototype" scope. RESTEasy handles injecting @Context references. Constructor injection is not supported though. Also, with the "prototype" scope, RESTEasy will inject any @*Param annotated fields or setters before the request is dispatched.

NOTE: You can only use auto-proxied beans with our base Spring integration. You will have undesirable affects if you are doing handcoded proxying with Spring, i.e., with ProxyFactoryBean. If you are using auto-proxied beans, you will be ok.

### 45.2. Spring MVC Integration

RESTEasy can also integrate with the Spring DispatcherServlet. The advantages of using this are that you have a simpler web.xml file, you can dispatch to either Spring controllers or Resteasy from under the same base URL, and finally, the most important, you can use Spring ModelAndView objects as return arguments from @GET resource methods. Setup requires you using the Spring DispatcherServlet in your web.xml file, as well as importing the springmvc-resteasy.xml file into your base Spring beans xml file. Here's an example web.xml file:
Spring MVC Integration

```xml
<display-name>Archetype Created Web Application</display-name>

<servlet>
  <servlet-name>Spring</servlet-name>
  <servlet-class>org.springframework.web.servlet.DispatcherServlet;</servlet-class>
</servlet>

<servlet-mapping>
  <servlet-name>Spring</servlet-name>
  <url-pattern>/*</url-pattern>
</servlet-mapping>
</web-app>

Then within your main Spring beans xml, import the springmvc-resteasy.xml file

```xml
<beans xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>
  <!-- Import basic SpringMVC Resteasy integration -->
  <import resource="classpath:springmvc-resteasy.xml"/>
  ....
</beans>
```

You can specify resteasy configuration options by overriding the resteasy.deployment bean which is an instance of org.jboss.resteasy.spi.ResteasyDeployment. Here's an example of adding media type suffix mappings as well as enabling the Resteasy asynchronous job service.

```xml

```
<import resource="classpath:springmvc-resteasy.xml" /> 

<!-- override the bean definition for deployment -->
<bean id="resteasy.deployment" class="org.jboss.resteasy.spi.ResteasyDeployment" init-method="start" destroy-method="stop">
  <property name="asyncJobServiceEnabled" value="true"/>
  <property name="mediaTypeMappings">
    <map>
      <entry key="json" value="application/json" />
      <entry key="xml" value="application/xml" />
    </map>
  </property>
</bean>

...
Chapter 46. CDI Integration

This module provides integration with JSR-299 (Contexts and Dependency Injection for the Java EE platform)

46.1. Using CDI beans as JAX-RS components

Both the JAX-RS and CDI specifications introduce their own component model. On the one hand, every class placed in a CDI archive that fulfills a set of basic constraints is implicitly a CDI bean. On the other hand, explicit decoration of your Java class with @Path or @Provider is required for it to become a JAX-RS component. Without the integration code, annotating a class suitable for being a CDI bean with JAX-RS annotations leads into a faulty result (JAX-RS component not managed by CDI) The resteasy-cdi module is a bridge that allows RESTEasy to work with class instances obtained from the CDI container.

During a web service invocation, resteasy-cdi asks the CDI container for the managed instance of a JAX-RS component. Then, this instance is passed to RESTEasy. If a managed instance is not available for some reason (the class is placed in a jar which is not a bean deployment archive), RESTEasy falls back to instantiating the class itself.

As a result, CDI services like injection, lifecycle management, events, decoration and interceptor bindings can be used in JAX-RS components.

46.2. Default scopes

A CDI bean that does not explicitly define a scope is @Dependent scoped by default. This pseudo scope means that the bean adapts to the lifecycle of the bean it is injected into. Normal scopes (request, session, application) are more suitable for JAX-RS components as they designate component's lifecycle boundaries explicitly. Therefore, the resteasy-cdi module alters the default scoping in the following way:

- If a JAX-RS root resource does not define a scope explicitly, it is bound to the Request scope.
- If a JAX-RS Provider or javax.ws.rs.Application subclass does not define a scope explicitly, it is bound to the Application scope.

**Warning**

Since the scope of all beans that do not declare a scope is modified by resteasy-cdi, this affects session beans as well. As a result, a conflict occurs if the scope of a stateless session bean or singleton is changed automatically as the spec prohibits these components to be @RequestScoped. Therefore, you need to explicitly define a scope when using stateless session beans or singletons. This requirement is likely to be removed in future releases.
46.3. Configuration within JBoss 6 M4 and Higher

CDI integration is provided with no additional configuration with JBoss AS 6-M4 and higher.

46.4. Configuration with different distributions

Provided you have an existing RESTEasy application, all that needs to be done is to add the resteasy-cdi jar into your project's WEB-INF/lib directory. When using maven, this can be achieved by defining the following dependency.

```xml
<dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-cdi</artifactId>
    <version>${project.version}</version>
</dependency>
```

Furthermore, when running a pre-Servlet 3 container, the following context parameter needs to be specified in web.xml. (This is done automatically via web-fragment in a Servlet 3 environment)

```xml
<context-param>
    <param-name>resteasy.injector.factory</param-name>
    <param-value>org.jboss.resteasy.cdi.CdiInjectorFactory</param-value>
</context-param>
```

When deploying an application to a Servlet container that does not support CDI out of the box (Tomcat, Jetty, Google App Engine), a CDI implementation needs to be added first. Weld-servlet module [http://docs.jboss.org/weld/reference/latest/en-US/html/environments.html] can be used for this purpose.
Chapter 47. Seam Integration

RESTEasy integrates quite nicely with the JBoss Seam framework. This integration is maintained by the Seam developers and documented there as well. Check out Seam documentation [http://docs.jboss.org/seam/latest/en-US/html/webservices.html#d0e22078].
Chapter 48. Guice 3.0 Integration

RESTEasy has some simple integration with Guice 3.0. RESTEasy will scan the binding types for a Guice Module for @Path and @Provider annotations. It will register these bindings with RESTEasy. The guice-hello project that comes in the RESTEasy examples/ directory gives a nice example of this.

```java
@Path("hello")
public class HelloResource
{
    @GET
    @Path("{name}")
    public String hello(@PathParam("name") final String name) {
        return "Hello " + name;
    }
}
```

First you start off by specifying a JAX-RS resource class. The HelloResource is just that. Next you create a Guice Module class that defines all your bindings:

```java
import com.google.inject.Module;
import com.google.inject.Binder;

public class HelloModule implements Module
{
    public void configure(final Binder binder)
    {
        binder.bind(HelloResource.class);
    }
}
```

You put all these classes somewhere within your WAR WEB-INF/classes or in a JAR within WEB-INF/lib. Then you need to create your web.xml file. You need to use the GuiceResteasyBootstrapServletContextListener as follows:

```xml
<web-app>
    <display-name>Guice Hello</display-name>
    <context-param>
```

209
GuiceResteasyBootstrapServletContextListener is a subclass of ResteasyBootstrap, so you can use any other RESTEasy configuration option within your web.xml file. Also notice that there is a resteasy.guice.modules context-param. This can take a comma delimited list of class names that are Guice Modules.

### 48.1. Request Scope

Add the RequestScopeModule to your modules to allow objects to be scoped to the HTTP request by adding the @RequestScoped annotation to your class. All the objects injectable via the @Context annotation are also injectable, except ServletConfig and ServletContext.

```java
import javax.inject.Inject;
import javax.servlet.http.HttpServletRequest;
import javax.ws.rs.core.Context;
import org.jboss.resteasy.plugins.guice.RequestScoped;

@RequestScoped
```
public class MyClass
{
    @Inject @Context
    private HttpRequest request;
}

48.2. Binding JAX-RS utilities


48.3. Configuring Stage

You can configure the stage Guice uses to deploy your modules by specific a context param, resteasy.guice.stage. If this value is not specified, Resteasy uses whatever Guice’s default is.

```xml
<web-app>
    <display-name>Guice Hello</display-name>
    <context-param>
        <param-name>resteasy.guice.modules</param-name>
        <param-value>org.jboss.resteasy.examples.guice.hello.HelloModule</param-value>
    </context-param>
    <context-param>
        <param-name>resteasy.guice.stage</param-name>
        <param-value>PRODUCTION</param-value>
    </context-param>
    <listener>
        <listener-class>
            org.jboss.resteasy.plugins.guice.GuiceResteasyBootstrapServletContextListener
        </listener-class>
    </listener>
    <servlet>
        <servlet-name>Resteasy</servlet-name>
        <servlet-class>
            org.jboss.resteasy.plugins.server.servlet.HttpServletDispatcher
        </servlet-class>
    </servlet>
</web-app>
```
48.4. Custom Injector creation

GuiceResteasyBootstrapServletContextListener can be extended to allow more flexibility in the way the Injector and Modules are created. Three methods can be overridden: getModules(), withInjector() and getStage(). Register your subclass as the listener in the web.xml.

Override getModules() when you need to pass arguments to your modules' constructor or perform more complex operations.

Override withInjector(Injector) when you need to interact with the Injector after it has been created.

Override getStage(ServletContext) to set the Stage yourself.
injector.getInstance(PersistService.class).start();
}
Chapter 49. Resteasy Client API

49.1. JAX-RS 2.0 Client API

JAX-RS 2.0 introduces a new client API so that you can make http requests to your remote RESTful web services. It is a 'fluent' request building API with really 3 main classes: Client, WebTarget, and Response. The Client interface is a builder of WebTarget instances. WebTarget represents a distinct URL or URL template from which you can build more sub-resource WebTargets or invoke requests on.

There are really two ways to create a Client. Standard way, or you can use the ResteasyClientBuilder class. The advantage of the latter is that it gives you a few more helper methods to configure your client.

```java
Client client = ClientBuilder.newClient();
... or...
Client client = ClientBuilder.newBuilder().build();
WebTarget target = client.target("http://foo.com/resource");
Response response = target.request().get();
String value = response.readEntity(String.class);
response.close();  // You should close connections!

ResteasyClient client = new ResteasyClientBuilder().build();
ResteasyWebTarget target = client.target("http://foo.com/resource");
```

Resteasy will automatically load a set of default providers. (Basically all classes listed in all META-INF/services/javax.ws.rs.ext.Providers files). Additionally, you can manually register other providers, filters, and interceptors through the Configuration object provided by the method call Client.configuration(). Configuration also lets you set various configuration properties that may be needed.

Each WebTarget has its own Configuration instance which inherits the components and properties registered with its parent. This allows you to set specific configuration options per target resource. For example, username and password.

49.2. Resteasy Proxy Framework

The Resteasy Proxy Framework is the mirror opposite of the JAX-RS server-side specification. Instead of using JAX-RS annotations to map an incoming request to your RESTful Web Service method, the client framework builds an HTTP request that it uses to invoke on a remote RESTful Web Service. This remote service does not have to be a JAX-RS service and can be any web resource that accepts HTTP requests.
Resteasy has a client proxy framework that allows you to use JAX-RS annotations to invoke on a remote HTTP resource. The way it works is that you write a Java interface and use JAX-RS annotations on methods and the interface. For example:

```java
public interface SimpleClient
{
    @GET
    @Path("basic")
    @Produces("text/plain")
    String getBasic();

    @PUT
    @Path("basic")
    @Consumes("text/plain")
    void putBasic(String body);

    @GET
    @Path("queryParam")
    @Produces("text/plain")
    String getQueryParam(@QueryParam("param")String param);

    @GET
    @Path("matrixParam")
    @Produces("text/plain")
    String getMatrixParam(@MatrixParam("param")String param);

    @GET
    @Path("uriParam/{param}")
    @Produces("text/plain")
    int getUriParam(@PathParam("param")int param);
}
```

Resteasy has a simple API based on Apache HttpClient. You generate a proxy then you can invoke methods on the proxy. The invoked method gets translated to an HTTP request based on how you annotated the method and posted to the server. Here's how you would set this up:

```java
Client client = ClientFactory.newClient();
WebTarget target = client.target("http://example.com/base/uri");
ResteasyWebTarget rtarget = (ResteasyWebTarget)target;

SimpleClient simple = rtarget.proxy(SimpleClient.class);
client.putBasic("hello world");
```
Alternatively you can use the Resteasy client extension interfaces directly:

```java
ResteasyClient client = new ResteasyClientBuilder().build();
ResteasyWebTarget target = client.target("http://example.com/base/uri");
SimpleClient simple = target.proxy(SimpleClient.class);
client.putBasic("hello world");
```

@CookieParam works the mirror opposite of its server-side counterpart and creates a cookie header to send to the server. You do not need to use @CookieParam if you allocate your own javax.ws.rs.core.Cookie object and pass it as a parameter to a client proxy method. The client framework understands that you are passing a cookie to the server so no extra metadata is needed.

The framework also supports the JAX-RS locator pattern, but on the client side. So, if you have a method annotated only with @Path, that proxy method will return a new proxy of the interface returned by that method.

### 1. Abstract Responses

Sometimes you are interested not only in the response body of a client request, but also either the response code and/or response headers. The Client-Proxy framework has two ways to get at this information

You may return a javax.ws.rs.core.Response.Status enumeration from your method calls:

```java
@Path("/")
public interface MyProxy {
    @POST
    Response.Status updateSite(MyPojo pojo);
}
```

Internally, after invoking on the server, the client proxy internals will convert the HTTP response code into a Response.Status enum.

If you are interested in everything, you can get it with the javax.ws.rs.core.Response class:
Chapter 49. Resteasy Client API

```java
@Path("/")
public interface LibraryService {

    @GET
    @Produces("application/xml")
    Response getAllBooks();
}
```

2. Sharing an interface between client and server

It is generally possible to share an interface between the client and server. In this scenario, you just have your JAX-RS services implement an annotated interface and then reuse that same interface to create client proxies to invoke on the client-side.

49.3. Apache HTTP Client 4.x and other backends

Network communication between the client and server is handled in Resteasy, by default, by HttpClient (4.x) from the Apache HttpComponents project. In general, the interface between the Resteasy Client Framework and the network is found in an implementation of `org.jboss.resteasy.client.jaxrs.ClientHttpEngine`, and `org.jboss.resteasy.client.jaxrs.engines.ApacheHttpClient4Engine`, which uses HttpClient (4.x), is the default implementation. Resteasy also ships with the following client engines, all found in the `org.jboss.resteasy.client.jaxrs.engines` package:

- `URLConnectionClientExecutor`: uses `java.net.HttpURLConnection`;
- `InMemoryClientExecutor`: dispatches requests to a server in the same JVM.

and a client executor may be passed to a specific `ClientRequest`:

```java
ResteasyClient client = new ResteasyClientBuilder().httpEngine(engine).build();
```

Resteasy and HttpClient make reasonable default decisions so that it is possible to use the client framework without ever referencing HttpClient, but for some applications it may be necessary to drill down into the HttpClient details. `ApacheHttpClient4Engine` can be supplied with an instance of `org.apache.http.client.HttpClient` and an instance of `org.apache.http.protocol.HttpContext`, which can carry additional configuration details into the HttpClient layer. For example, authentication may be configured as follows:

```java
// Configure HttpClient to authenticate preemptively
// by prepopulating the authentication data cache.
```
// 1. Create AuthCache instance
AuthCache authCache = new BasicAuthCache();

// 2. Generate BASIC scheme object and add it to the local auth cache
AuthScheme basicAuth = new BasicScheme();
authCache.put(new HttpHost("sippycups.bluemonkeydiamond.com"), basicAuth);

// 3. Add AuthCache to the execution context
BasicHttpContext localContext = new BasicHttpContext();
localContext.setAttribute(ClientContext.AUTH_CACHE, authCache);

// 4. Create client executor and proxy
DefaultHttpClient httpClient = new DefaultHttpClient();
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient,
localContext);
ResteasyClient client = new ResteasyClientBuilder().httpEngine(engine).build();

One default decision made by HttpClient and adopted by Resteasy is the use of
org.apache.http.impl.conn.SingleClientConnManager, which manages a single socket at
any given time and which supports the use case in which one or more invocations are made
serially from a single thread. For multithreaded applications, SingleClientConnManager may be
replaced by org.apache.http.impl.conn.tsccm.ThreadSafeClientConnManager:

ClientConnectionManager cm = new ThreadSafeClientConnManager();
HttpClient httpClient = new DefaultHttpClient(cm);
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient);

For more information about HttpClient (4.x), see the documentation at http://hc.apache.org/
html/].

**Note.** It is important to understand the difference between "releasing" a connection and "closing" a
connection. **Releasing** a connection makes it available for reuse. **Closing** a connection frees
its resources and makes it unusable.

SingleClientConnManager manages a single socket, which it allocates to at most a single
invocation at any given time. Before that socket can be reused, it has to be released from its
current use, which can occur in one of two ways. If an execution of a request or a call on a proxy
returns a class other than Response, then Resteasy will take care of releasing the connection.
For example, in the fragments

```java
// 1. Create AuthCache instance
AuthCache authCache = new BasicAuthCache();

// 2. Generate BASIC scheme object and add it to the local auth cache
AuthScheme basicAuth = new BasicScheme();
authCache.put(new HttpHost("sippycups.bluemonkeydiamond.com"), basicAuth);

// 3. Add AuthCache to the execution context
BasicHttpContext localContext = new BasicHttpContext();
localContext.setAttribute(ClientContext.AUTH_CACHE, authCache);

// 4. Create client executor and proxy
DefaultHttpClient httpClient = new DefaultHttpClient();
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient,
localContext);
ResteasyClient client = new ResteasyClientBuilder().httpEngine(engine).build();

One default decision made by HttpClient and adopted by Resteasy is the use of
org.apache.http.impl.conn.SingleClientConnManager, which manages a single socket at
any given time and which supports the use case in which one or more invocations are made
serially from a single thread. For multithreaded applications, SingleClientConnManager may be
replaced by org.apache.http.impl.conn.tsccm.ThreadSafeClientConnManager:

ClientConnectionManager cm = new ThreadSafeClientConnManager();
HttpClient httpClient = new DefaultHttpClient(cm);
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient);

For more information about HttpClient (4.x), see the documentation at http://hc.apache.org/
html/].

**Note.** It is important to understand the difference between "releasing" a connection and "closing" a
connection. **Releasing** a connection makes it available for reuse. **Closing** a connection frees
its resources and makes it unusable.

SingleClientConnManager manages a single socket, which it allocates to at most a single
invocation at any given time. Before that socket can be reused, it has to be released from its
current use, which can occur in one of two ways. If an execution of a request or a call on a proxy
returns a class other than Response, then Resteasy will take care of releasing the connection.
For example, in the fragments

```java
// 1. Create AuthCache instance
AuthCache authCache = new BasicAuthCache();

// 2. Generate BASIC scheme object and add it to the local auth cache
AuthScheme basicAuth = new BasicScheme();
authCache.put(new HttpHost("sippycups.bluemonkeydiamond.com"), basicAuth);

// 3. Add AuthCache to the execution context
BasicHttpContext localContext = new BasicHttpContext();
localContext.setAttribute(ClientContext.AUTH_CACHE, authCache);

// 4. Create client executor and proxy
DefaultHttpClient httpClient = new DefaultHttpClient();
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient,
localContext);
ResteasyClient client = new ResteasyClientBuilder().httpEngine(engine).build();

One default decision made by HttpClient and adopted by Resteasy is the use of
org.apache.http.impl.conn.SingleClientConnManager, which manages a single socket at
any given time and which supports the use case in which one or more invocations are made
serially from a single thread. For multithreaded applications, SingleClientConnManager may be
replaced by org.apache.http.impl.conn.tsccm.ThreadSafeClientConnManager:

ClientConnectionManager cm = new ThreadSafeClientConnManager();
HttpClient httpClient = new DefaultHttpClient(cm);
ApacheHttpClient4Engine engine = new ApacheHttpClient4Engine(httpClient);

For more information about HttpClient (4.x), see the documentation at http://hc.apache.org/
html/].

**Note.** It is important to understand the difference between "releasing" a connection and "closing" a
connection. **Releasing** a connection makes it available for reuse. **Closing** a connection frees
its resources and makes it unusable.

SingleClientConnManager manages a single socket, which it allocates to at most a single
invocation at any given time. Before that socket can be reused, it has to be released from its
current use, which can occur in one of two ways. If an execution of a request or a call on a proxy
returns a class other than Response, then Resteasy will take care of releasing the connection.
WebTarget target = client.target("http://localhost:8081/customer/123");
String answer = target.request().get(String.class);

or

ResteasyWebTarget target = client.target("http://localhost:8081/customer/123");
RegistryStats stats = target.proxy(RegistryStats.class);
RegistryData data = stats.get();

Resteasy will release the connection under the covers. The only counterexample is the case in which the response is an instance of InputStream, which must be closed explicitly.

On the other hand, if the result of an invocation is an instance of Response, then Response.close() method must be used to released the connection.

WebTarget target = client.target("http://localhost:8081/customer/123");
Response response = target.request().get();
System.out.println(response.getStatus());
response.close();

You should probably execute this in a try/finally block. Again, releasing a connection only makes it available for another use. It does not normally close the socket.

On the other hand, ApacheHttpClient4Engine.finalize() will close any open sockets, but only if it created the HttpClient it has been using. If an HttpClient has been passed into the ApacheHttpClient4Executor, then the user is responsible for closing the connections:

HttpClient httpClient = new DefaultHttpClient();
ApacheHttpClient4Engine executor = new ApacheHttpClient4Engine(httpClient);
...
httpClient.getConnectionManager().shutdown();

Note that if ApacheHttpClient4Engine has created its own instance of HttpClient, it is not necessary to wait for finalize() to close open sockets. The ClientHttpEngine interface has a close() method for this purpose.
Finally, if your `javax.ws.rs.client.Client` class has created the engine automatically for you, you should call `Client.close()` and this will clean up any socket connections.
Chapter 50. AJAX Client

RESTEasy resources can be accessed in JavaScript using AJAX using a proxy API generated by RESTEasy.

50.1. Generated JavaScript API

RESTEasy can generate a JavaScript API that uses AJAX calls to invoke JAX-RS operations.

Example 50.1. First JAX-RS JavaScript API example

Let's take a simple JAX-RS API:

```java
@Path("orders")
public interface Orders {
    @Path("{id}")
    @GET
    public String getOrder(@PathParam("id") String id){
        return "Hello "+id;
    }
}
```

The preceding API would be accessible using the following JavaScript code:

```javascript
var order = Orders.getOrder({id: 23});
```

50.1.1. JavaScript API servlet

In order to enable the JavaScript API servlet you must configure it in your web.xml file as such:

```xml
<servlet>
    <servlet-name>RESTEasy JSAPI</servlet-name>
    <servlet-class>org.jboss.resteasy.jsapi.JSAPIServlet</servlet-class>
</servlet>

<servlet-mapping>
    <servlet-name>RESTEasy JSAPI</servlet-name>
    <url-pattern>/rest-js</url-pattern>
</servlet-mapping>
```
50.1.2. JavaScript API usage

Each JAX-RS resource class will generate a JavaScript object of the same name as the declaring
class (or interface), which will contain every JAX-RS method as properties.

Example 50.2. Structure of JAX-RS generated JavaScript

For example, if the JAX-RS resource X defines methods Y and Z:

```java
@Path("/")
public interface X {
    @GET
    public String Y();
    @PUT
    public void Z(String entity);
}
```

Then the JavaScript API will define the following functions:

```javascript
var X = {
    Y : function(params){…},
    Z : function(params){…}
};
```

Each JavaScript API method takes an optional object as single parameter where each property
is a cookie, header, path, query or form parameter as identified by their name, or the following
special parameters:

**Warning**
The following special parameter names are subject to change.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$entity</td>
<td></td>
<td>The entity to send as a PUT, POST request.</td>
</tr>
<tr>
<td>$contentType</td>
<td>As determined by @Consumes.</td>
<td>The MIME type of the body entity sent as the Content-Type header.</td>
</tr>
<tr>
<td>$accepts</td>
<td>Determined by @Provides, defaults to &quot;/&quot;.</td>
<td>The accepted MIME types sent as the Accept header.</td>
</tr>
</tbody>
</table>
### JavaScript API usage

<table>
<thead>
<tr>
<th>Property name</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$callback</td>
<td></td>
<td>Set to a function(httpCode, xmlHttpRequest, value) for an asynchronous call. If not present, the call will be synchronous and return the value.</td>
</tr>
<tr>
<td>$apiURL</td>
<td>Determined by container</td>
<td>Set to the base URI of your JAX-RS endpoint, not including the last slash.</td>
</tr>
<tr>
<td>$username</td>
<td></td>
<td>If username and password are set, they will be used for credentials for the request.</td>
</tr>
<tr>
<td>$password</td>
<td></td>
<td>If username and password are set, they will be used for credentials for the request.</td>
</tr>
</tbody>
</table>

### Example 50.3. Using the API

Here is an example of JAX-RS API:

```java
@Path("foo")
public class Foo{
    @Path({"id"})
    @GET
    public String get(@QueryParam("order") String order, @HeaderParam("X-Foo") String header,
                       @MatrixParam("colour") String colour, @CookieParam("Foo-Cookie") String cookie){
        &
    }
    @POST
    public void post(String text){
    }
}
```

We can use the previous JAX-RS API in JavaScript using the following code:

```javascript
var text = Foo.get({order: 'desc', 'X-Foo': 'hello', colour: 'blue', 'Foo-Cookie': 123987235444});
Foo.put({$entity: text});
```
50.1.3. Work with @Form

@Form is a RESTEasy specific annotation that allows you to re-use any @*Param annotation within an injected class. The generated JavaScript API will expand the parameters for use automatically. Support we have the following form:

```java
public class MyForm {
    @FormParam("stuff")
    private String stuff;

    @FormParam("number")
    private int number;

    @HeaderParam("myHeader")
    private String header;
}
```

And the resource is like:

```java
@Path("/")
public class MyResource {

    @POST
    public String postForm(@Form MyForm myForm) { ... }
}
```

Then we could call the method from JavaScript API like following:

```javascript
MyResource.postForm({stuff:"A", myHeader:"B", number:1});
```

Also, @Form supports prefix mappings for lists and maps:

```java
public static class Person {
    @Form(prefix="telephoneNumbers") List<TelephoneNumber> telephoneNumbers;
    @Form(prefix="address") Map<String, Address> addresses;
}
```

```java
public static class TelephoneNumber {
    @FormParam("countryCode") private String countryCode;
    @FormParam("number") private String number;
}
```
public static class Address {
    @FormParam("street") private String street;
    @FormParam("houseNumber") private String houseNumber;
}

@Path("person")
public static class MyResource {
    @POST
    public void postForm(@Form Person p) {...}
}

From JavaScript we could call the API like this:

```javascript
MyResource.postForm({
    telephoneNumbers:[
        {"telephoneNumbers[0].countryCode":31},
        {"telephoneNumbers[0].number":12345678},
        {"telephoneNumbers[1].countryCode":91},
        {"telephoneNumbers[1].number":9717738723}
    ],
    address:[
        {"address[INVOICE].street":"Main Street"},
        {"address[INVOICE].houseNumber":2},
        {"address[SHIPPING].street":"Square One"},
        {"address[SHIPPING].houseNumber":13}
    ]
});
```

50.1.4. MIME types and unmarshalling.

The Accept header sent by any client JavaScript function is controlled by the $accepts parameter, which overrides the @Produces annotation on the JAX-RS endpoint. The returned value however is controlled by the Content-Type header sent in the response as follows:

Table 50.2. Return values by MIME type

<table>
<thead>
<tr>
<th>MIME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text/xml,application/xml,xml,application/*+xml</td>
<td>The response entity is parsed as XML before being returned. The return value is thus a DOM Document.</td>
</tr>
<tr>
<td>application/json</td>
<td>The response entity is parsed as JSON before being returned. The return value is thus a JavaScript Object.</td>
</tr>
<tr>
<td>Anything else</td>
<td>The response entity is returned raw.</td>
</tr>
</tbody>
</table>
Example 50.4. Unmarshalling example

The RESTEasy JavaScript client API can automatically unmarshall JSON and XML:

```java
@Path("orders")
public interface Orders {

    @XmlRootElement
    public static class Order {
        @XmlElement
        private String id;

        public Order(){
        }
        public Order(String id){
            this.id = id;
        }
    }

    @Path("{id}/xml")
    @GET
    @Produces("application/xml")
    public Order getOrderXML(@PathParam("id") String id){
        return new Order(id);
    }

    @Path("{id}/json")
    @GET
    @Produces("application/json")
    public Order getOrderJSON(@PathParam("id") String id){
        return new Order(id);
    }
}
```

Let us look at what the preceding JAX-RS API would give us on the client side:

```javascript
// this returns a JSON object
var orderJSON = Orders.getOrderJSON({'id': '23'});
orderJSON.id == '23';

// this one returns a DOM Document whose root element is the order, with one
// whose child is the text node value
var orderXML = Orders.getOrderXML({'id': '23'});
orderXML.documentElement.childNodes[0].childNodes[0].nodeValue == '23';
```
50.1.5. MIME types and marshalling.

The Content-Type header sent in the request is controlled by the $contentType parameter which overrides the @Consumes annotation on the JAX-RS endpoint. The value passed as entity body using the $entity parameter is marshalled according to both its type and content type:

<table>
<thead>
<tr>
<th>Type</th>
<th>MIME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOM Element</td>
<td>Empty or text/xml,application/xml</td>
<td>The DOM Element is marshalled to XML before being sent.</td>
</tr>
<tr>
<td>JavaScript Object (JSON)</td>
<td>Empty or application/json</td>
<td>The JSON object is marshalled to a JSON string before being sent.</td>
</tr>
<tr>
<td>Anything else</td>
<td>Anything else</td>
<td>The entity is sent as is.</td>
</tr>
</tbody>
</table>

Example 50.5. Marshalling example

The RESTEasy JavaScript client API can automatically marshall JSON and XML:

```java
@Path("orders")
public interface Orders {

    @XmlRootElement
    public static class Order {
        @XmlElement
        private String id;

        public Order(){}

        public Order(String id){
            this.id = id;
        }
    }

    @Path("{id}/xml")
    @PUT
    @Consumes("application/xml")
    public void putOrderXML(Order order){
        // store order
    }

    @Path("{id}/json")
    @PUT
    @Consumes("application/json")
```
public void putOrderJSON(Order order){
  // store order
}

Let us look at what the preceding JAX-RS API would give us on the client side:

```java
// this saves a JSON object
Orders.putOrderJSON({$entity: {id: "23"}});

// It is a bit more work with XML
var order = document.createElement("order");
var id = document.createElement("id");
order.appendChild(id);
id.appendChild(document.createTextNode("23"));
Orders.putOrderXML({$entity: order});
```

## 50.2. Using the JavaScript API to build AJAX queries

The RESTEasy JavaScript API can also be used to manually construct your requests.

### 50.2.1. The REST object

The REST object contains the following read-write properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiURL</td>
<td>Set by default to the JAX-RS root URL, used by every JavaScript client API functions when constructing the requests.</td>
</tr>
<tr>
<td>log</td>
<td>Set to a function(string) in order to receive RESTEasy client API logs. This is useful if you want to debug your client API and place the logs where you can see them.</td>
</tr>
</tbody>
</table>

### Example 50.6. Using the REST object

The REST object can be used to override RESTEasy JavaScript API client behaviour:

```java
// Change the base URL used by the API:
REST.apiURL = "http://api.service.com";

// log everything in a div element
```
50.2.2. The REST.Request class

The REST.Request class is used to build custom requests. It has the following members:

**Table 50.5. The REST.Request class**

<table>
<thead>
<tr>
<th>Member</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>execute(callback)</td>
<td>Executes the request with all the information set in the current object. The value is never returned but passed to the optional argument callback.</td>
</tr>
<tr>
<td>setAccepts(acceptHeader)</td>
<td>Sets the Accept request header. Defaults to &quot;/&quot;.</td>
</tr>
<tr>
<td>setCredentials(username, password)</td>
<td>Sets the request credentials.</td>
</tr>
<tr>
<td>setEntity(entity)</td>
<td>Sets the request entity.</td>
</tr>
<tr>
<td>setContentType(contentTypeHeader)</td>
<td>Sets the Content-Type request header.</td>
</tr>
<tr>
<td>setURI(uri)</td>
<td>Sets the request URI. This should be an absolute URI.</td>
</tr>
<tr>
<td>setMethod(method)</td>
<td>Sets the request method. Defaults to GET.</td>
</tr>
<tr>
<td>setAsync(async)</td>
<td>Controls whether the request should be asynchronous. Defaults to true.</td>
</tr>
<tr>
<td>addCookie(name, value)</td>
<td>Sets the given cookie in the current document when executing the request. Beware that this will be persistent in your browser.</td>
</tr>
<tr>
<td>addQueryParameter(name, value)</td>
<td>Adds a query parameter to the URI query part.</td>
</tr>
<tr>
<td>addMatrixParameter(name, value)</td>
<td>Adds a matrix parameter (path parameter) to the last path segment of the request URI.</td>
</tr>
<tr>
<td>addHeader(name, value)</td>
<td>Adds a request header.</td>
</tr>
</tbody>
</table>

**Example 50.7. Using the REST.Request class**

The REST.Request class can be used to build custom requests:

```javascript
var r = new REST.Request();
r.setURI("http://api.service.com/orders/23/json");
r.setMethod("PUT");
r.setContentType("application/json");
r.setEntity({id: "23");
r.addMatrixParameter("JSESSIONID", "12309812378123");
```
50.3. Caching Features

RESTEasy AJAX Client works well with server side caching features. But the buggy browsers cache will always prevent the function to work properly. If you'd like to use RESTEasy's caching feature with its AJAX client, you can enable 'antiBrowserCache' option:

```javascript
REST.antiBrowserCache = true;
```

The above setting should be set once before you call any APIs.
Chapter 51. Validation

RESTEasy provides the support for validation mandated by the JAX-RS: Java API for RESTful Web Services 2.0 [http://www.jcp.org/en/jsr/detail?id=339], given the presence of an implementation of the Bean Validation specification 1.1 [http://beanvalidation.org/1.1/spec/] such as Hibernate Validator 5.x [http://www.hibernate.org/subprojects/validator.html].

Validation provides a declarative way of imposing constraints on fields and properties of beans, bean classes, and the parameters and return values of bean methods. For example, in

```java
@Path("all")
@TestClassConstraint(5)
public class TestResource {

    @Size(min=2, max=4)
    @PathParam("s")
    String s;

    private String t;

    @Size(min=3)
    public String getT() {
        return t;
    }

    @PathParam("t")
    public void setT(String t) {
        this.t = t;
    }

    @POST
    @Path("/{s}/{t}/{u}")
    @Pattern(regexp="[a-c]+")
    public String post(@PathParam("u") String u) {
        return u;
    }
}
```

the field \( s \) is constrained by the Bean Validation built-in annotation `@Size` to have between 2 and 4 characters, the property \( t \) is constrained to have at least 3 characters, and the `TestResource` object is constrained by the application defined annotation `@TestClassConstraint` to have the combined lengths of \( s \) and \( t \) less than 5:
@Constraint(validatedBy = TestClassValidator.class)
@Target({TYPE})
@Retention(RUNTIME)
public @interface TestClassConstraint
{
    String message() default "Concatenation of s and t must have length > \{value\}";
    Class<?>[] groups() default {};
    Class<? extends Payload>[] payload() default {};
    int value();
}

public class TestClassValidator implements ConstraintValidator<TestClassConstraint, TestResource>
{
    int length;

    public void initialize(TestClassConstraint constraintAnnotation)
    {
        length = constraintAnnotation.value();
    }

    public boolean isValid(TestResource value, ConstraintValidatorContext context)
    {
        boolean b = value.retrieveS().length() + value.getT().length() < length;
    }
}

See the links above for more about how to create validation annotations.

Also, the method parameter u is constrained to have no more than 5 characters, and the return value of method post is constrained by the built-in annotation @Pattern to match the regular expression "\[a-c]\+".

The sequence of validation constraint testing is as follows:

1. Create the resource and validate field, property, and class constraints.
2. Validate the resource method parameters.
3. If no violations have been detected, call the resource method and validate the return value

51.1. Violation reporting

If a validation problem occurs, either a problem with the validation definitions or a constraint violation, Resteasy will set the return
Violation reporting

header org.jboss.resteasy.api.validation.Validation.VALIDATION_HEADER ("validation-exception") to "true".

If Resteasy detects a structural validation problem, such as a validation annotation with a missing validator class, it will return a String representation of a javax.validation.ValidationException. For example

javax.validation.ValidationException: HV000028: Unexpected exception during isValid call.[org.jboss.resteasy.test.validation.TestValidationExceptions$OtherValidationException]

If any constraint violations are detected, Resteasy will return a report in one of a variety of formats. If one of "application/xml" or "application/json" occur in the "Accept" request header, Resteasy will return an appropriately marshalled instance of org.jboss.resteasy.api.validation.ViolationReport:

@XmlElement(name="violationReport")
@AccessorType(XmlAccessType.FIELD)
public class ViolationReport
{
...

    public ArrayList<ResteasyConstraintViolation> getFieldViolations()
    {
        return fieldViolations;
    }

    public ArrayList<ResteasyConstraintViolation> getPropertyViolations()
    {
        return propertyViolations;
    }

    public ArrayList<ResteasyConstraintViolation> getClassViolations()
    {
        return classViolations;
    }

    public ArrayList<ResteasyConstraintViolation> getParameterViolations()
    {
        return parameterViolations;
    }

    public ArrayList<ResteasyConstraintViolation> getReturnValueViolations()
    {

Chapter 51. Validation

```java
return returnValueViolations;
}
...
}

where org.jboss.resteasy.api.validation.ResteasyConstraintViolation is defined:

@XmlElement(name="resteasyConstraintViolation")
@XmlAccessorType(XmlAccessType.FIELD)
public class ResteasyConstraintViolation implements Serializable
{
...
/**
 * @return type of constraint
 */
public ConstraintType.Type getConstraintType()
{
    return constraintType;
}

/**
 * @return description of element violating constraint
 */
public String getPath()
{
    return path;
}

/**
 * @return description of constraint violation
 */
public String getMessage()
{
    return message;
}

/**
 * @return object in violation of constraint
 */
public String getValue()
{
    return value;
}
```
/**
 * @return String representation of violation
 */
public String toString()
{
    return "[" + type() + "]\r[" + path + "]\r[" + message + "]\r[" + value + "]\r";
}

/**
 * @return String form of violation type
 */
public String type()
{
    return constraintType.toString();
}

and org.jboss.resteasy.api.validation.ConstraintType is the enumeration

public class ConstraintType
{
    public enum Type {CLASS, FIELD, PROPERTY, PARAMETER, RETURN_VALUE};
}

If both "application/xml" or "application/json" occur in the "Accept" request header, the media type is chosen according to the ranking given by implicit or explicit "q" parameter values. In the case of a tie, the returned media type is indeterminate.

If neither "application/xml" or "application/json" occur in the "Accept" request header, Resteasy returns a report with a String representation of each ResteasyConstraintViolation, where each field is delimited by [" and "], followed by a \r, with a final \r at the end. For example,

[FIELD]
[s]
[size must be between 2 and 4]
[a]

[PROPERTY]
[t]
[size must be between 3 and 5]
[z]

[CLASS]
[]
[Concatenation of s and t must have length > 5]
[org.jboss.resteasy.validation.TestResource868467a6f]

[PARAMETER]
[test.<cross-parameter>]
[Parameters must total <= 7]
[[5, 7]]

[RETURN_VALUE]
[g.<return value>]
[size must be between 2 and 4]
[abcde]

where the four fields are

1. type of constraint
2. path to violating element (e.g., field name, class name, method name and parameter name)
3. message
4. violating element

The ViolationReport can be reconstituted from the String as follows:

ResteasyClient client = new ResteasyClientBuilder().build();
Invocation.Builder request = client.target(...).request();
Response response = request.get();
if (Boolean.valueOf(response.getHeaders().getFirst(Validation.VALIDATION_HEADER)))
{
    String s = response.getEntity(String.class);
    ViolationReport report = new ViolationReport(s);
}

If the path field is considered to be too much server side information, it can be suppressed by setting the context parameter "resteasy.validation.suppress.path" to "true". In that case, "***" will be returned in the path fields.

51.2. Bean Validation 1.1

The form of validation mandated by the JAX-RS 2.0 specification, based on Bean Validation 1.1, is supported by the RESTEasy module resteasy-validator-provider-11, which produces the artifact resteasy-validator-provider-11-<version>.jar. Validation is turned on by default (assuming resteasy-validator-provider-11-<version>.jar is available), though parameter and return value
validation can be turned off or modified in the validation.xml configuration file. See the Hibernate Validator [http://docs.jboss.org/hibernate/validator/5.0/reference/en-US/html/] documentation for the details. Wildfly 8.x will ship with Hibernate Validator 5.x.

51.3. Bean Validation 1.0

Validation is not included in the original JAX-RS specification, but RESTEasy 2.x provides a form of validation, including parameter and return value validation, based on Bean Validation 1.0 plus Hibernate 4.x extensions. For applications running in the context of Hibernate Validation 4.x, RESTEasy 3.x inherits the validation semantics from RESTEasy 2.x. This version of validation is in the RESTEasy module resteasy-hibernatevalidate-provider, which produces the artifact resteasy-hibernatevalidate-provider-<version>.jar. It follows the validation sequence given in the first section, detecting field, property, class, parameter, and return value constraints, though with a somewhat less rich semantics than resteasy-validator-provider-11.

Unlike resteasy-validator-provider-11, resteasy-hibernatevalidate-provider does not do validation testing by default. Validation must be turned on. There are two relevant annotations - org.jboss.resteasy.plugins.validation.hibernate.ValidateRequest and org.jboss.resteasy.plugins.validation.hibernate.DoNotValidateRequest - that are used to indicate what needs validation or not. We can tell RESTEasy to validate any method in a resource annotating the resource:

```java
@Path("resourcePath")
@ValidateRequest
public interface Resource {

    @POST
    @Path("insert")
    public String insert(...)

    @GET
    @Path("list")
    public String list(...)
}
```

We can tell it to validate just some methods in an interface:

```java
@Path("resourcePath")
public interface Resource {

    @POST
    @Path("insert")

    @POST
    @Path("update")
```
This way RESTEasy will only trigger validation in insert method. It's possible to say what methods you don't want to be validated:

```java
@Path("resourcePath")
@ValidateRequest
public interface Resource {

    @POST
    @Path("insert")
    public String insert(...)

    @GET
    @Path("list")
    @DoNotValidateRequest
    public String list(...)
}
```

### 51.4. Validation Service Providers

RESTEasy obtains a bean validation implementation by looking in the available META-INF/services/javax.ws.rs.Providers files for an implementation of `ContextResolver<GeneralValidator>`, where `org.jboss.resteasy.spi.GeneralValidator` is

```java
public interface GeneralValidator {
    /**
     * Validates all constraints on [@code object].
     * @param object object to validate
     * @param groups the group or list of groups targeted for validation (defaults to Default)
     * @return constraint violations or an empty set if none
     */
}
```
* @throws IllegalArgumentException if object is {code null}
* or if {code null} is passed to the varargs groups
* @throws ValidationException if a non recoverable error happens
* during the validation process
*/

public abstract void validate(HttpRequest request, Object object, Class<?>... groups);
/**
* Validates all constraints placed on the parameters of the given method.
* @param method the method for which the parameter constraints is validated
* @param parameterValues the values provided by the caller for the given method's
* @param groups the group or list of groups targeted for validation (defaults to
* {link Default})
* @return a set with the constraint violations caused by this validation;
* will be empty if no error occurs, but never {code null}
* @throws IllegalArgumentException if {code null} is passed for any of
* the parameters
* or if parameters don't match with each other
* @throws ValidationException if a non recoverable error happens during the
* validation process
*/

public abstract void validateAllParameters(HttpRequest request, Object object, Method method, Object[] parameterValues, Class<?>... groups);
/**
* Validates all return value constraints of the given method.
* @param method the method for which the return value constraints is validated
* @param returnvalue the value returned by the given method
* @param groups the group or list of groups targeted for validation (defaults to
* {link Default})
* @return a set with the constraint violations caused by this validation;
* will be empty if no error occurs, but never {code null}
* @throws IllegalArgumentException if {code null} is passed for any of
* the object, method or groups parameters or if parameters don't match with
* each other
* @throws ValidationException if a non recoverable error happens during the
* validation process
*/

public abstract void validateReturnValue{
HttpRequest request, Object object, Method method, Object returnValue,
Class<?>... groups);

/**
 * Indicates if validation is turned on for a class.
 * @param clazz Class to be examined
 * @return true if and only if validation is turned on for clazz
 */
public abstract boolean isValidatable(Class<?> clazz);

/**
 * Indicates if validation is turned on for a method.
 * @param method method to be examined
 * @return true if and only if validation is turned on for method
 */
public abstract boolean isMethodValidatable(Method method);

void checkViolations(HttpRequest request);

The methods and the javadoc are adapted from the Bean Validation 1.1 classes
javax.validation.Validator and javax.validation.executable.ExecutableValidator.

RESTEasy supplies two implementations of GeneralValidator, in the modules
resteasy-validator-provider-11 and resteasy-hibernatevalidator-provider. An alternative
implementation may be supplied by implementing ContextResolver<GeneralValidator> and
org.jboss.resteasy.spi.validation.GeneralValidator.

A validator intended to function in the presence of CDI must also implement the subinterface

public interface GeneralValidatorCDI extends GeneralValidator
{
  /**
   * Indicates if validation is turned on for a class.
   * @param clazz Class to be examined
   * @param injectorFactory the InjectorFactory used for clazz
   * @return true if and only if validation is turned on for clazz
   */
  public boolean isValidatable(Class<?> clazz, InjectorFactory injectorFactory);
Both supplied validators implement GeneralValidatorCDI.
Chapter 52. Maven and RESTEasy

JBoss's Maven Repository is at: http://repository.jboss.org/nexus/content/groups/public/

Here's the pom.xml fragment to use. Resteasy is modularized into various components. Mix and max as you see fit. Please replace 3.0.9.Final with the current Resteasy version you want to use.

```xml
<repositories>
  <repository>
    <id>jboss</id>
    <url>http://repository.jboss.org/nexus/content/groups/public/</url>
  </repository>
</repositories>

<dependencies>
  <!-- core library -->
  <dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-jaxrs</artifactId>
    <version>3.0.9.Final</version>
  </dependency>
  <dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-client</artifactId>
    <version>3.0.9.Final</version>
  </dependency>

  <!-- optional modules -->
  <!-- JAXB support -->
  <dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-jaxb-provider</artifactId>
    <version>3.0.9.Final</version>
  </dependency>

  <!-- multipart/form-data and multipart/mixed support -->
  <dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-multipart-provider</artifactId>
    <version>3.0.9.Final</version>
  </dependency>

  <!-- Resteasy Server Cache -->
  <dependency>
    <groupId>org.jboss.resteasy</groupId>
    <artifactId>resteasy-cache-core</artifactId>
    <version>3.0.9.Final</version>
  </dependency>
</dependencies>
```
There is also a pom that can be imported so the versions of the individual modules do not have to be specified. Note that maven 2.0.9 is required for this.
<type>pom</type>
<scope>import</scope>
</dependency>
</dependencies>
</dependencyManagement>
Chapter 53. JBoss AS 5.x Integration

Resteasy has no special integration with JBoss Application Server so it must be configured and installed like any other container. There are some issues though. You must make sure that there is not a copy of servlet-api-xxx.jar in your WEB-INF/lib directory as this may cause problems. Also, if you are running with JDK 6, make sure to filter out the JAXB jars as they come with JDK 6.
RESTEasy is preconfigured and completely integrated with JBoss 6-M4 and higher. You can use it with EJB and CDI and you can rely completely on JBoss for scanning for your JAX-RS services and deploying them. All you have to provide is your JAX-RS service classes packaged within a WAR either as POJOs, CDI beans, or EJBs and provide an empty web.xml file as follows:

```xml
<web-app version="3.0" xmlns="http://java.sun.com/xml/ns/javaee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
</web-app>
```
Chapter 55. Documentation Support

There’s a great javadoc engine that allows you to generate javadocs for JAX-RS and JAXB called JAX-Doclet [http://www.lunatech-labs.com/open-source/jax-doclets]. Follow the link for more details.
Chapter 56. Migration from older versions

56.1. Migrating from 3.0.7 to 3.0.9

- You may need to upgrade your JDK to the latest 1.7.x or 1.8 releases if you are using JAXB. There's some entity expansion security vulnerabilities that we had to patch and it seems the fix doesn't work on earlier versions of JDK 1.7.

- ContainerRequestContext.setRequestUri() method behavior has been changed to match the behavior of the JAXRS RI. The relative URI must be equal to are an extension of the base URI or it will not work. i.e.

```java
context.setRequestUri(URI.create("https://foo.com/base"),
    URI.create("https://foo.com/base/path"));  // legal
context.setRequestUri(URI.create("https://foo.com/base"),
    URI.create("/path"));  // "path" is ignored
// if base uri is "http://foo.com/base"
context.setRequestUri(URI.create("http://foo.com/base/path"));  // legal
context.setRequestUri(URI.create("/path"));  // ignored
```

56.2. Migrating from 3.0.6 to 3.0.7

- Scannotation has been removed. If you are not running within an application server you must use the ResteasyServletInitializer. See docs for more detail.

56.3. Migrating from 3.0 to 3.0.4

- Servlet 3.0 deployments within standalone Tomcat or Jetty can now use the Resteasy ServletContainerInitializer. This allows tighter integration with Resteasy much like you have within JBoss/Wildfly. Check out the installation/configuration section of this document for more information.

56.4. Migrating from 3.0-beta-6 and 3.0-rc-1

- Form parameters are now read via a provider where earlier they were read from HttpServletRequest.getParameterMap(). This may break deployments that depend on that behavior, i.e. if you have a servlet filter that calls that very method. For those situations I added the switch resteasy.use.container.form.params
Chapter 56. Migration from ol...

- The JAX-RS TCK has become very strict with a ton more tests. I can't remember them all, but there are a number of edge cases which earlier Resteasy releases misinterpreted.

- Any Failure exceptions in the SPI now have a corresponding JAX-RS 2.0 exception, so they have been deprecated. Resteasy no longer uses these old SPI exceptions internally. It now uses the JAX-RS 2.0 ones.

- A number of SPIs have changed. Shouldn't be an issue for those of you who use Restasy as-is. Specifically InjectorFactory and Registry have changed.

56.5. Migrating from 3.0-beta-5 and 3.0-beta-6

- The JAX-RS 2.0 TCK has become very very strict in terms of the matching algorithm. Unfortunately, the matching algorithm is quite poor so there are a number of resource schemes that will no longer match. For example, resource classes are scanned for a best match, other are ignored in the match. Resource locators are not visited unless they are a best match over resource methods. There is one config switch I added so that Resteasy will ignore the Spec defined class expression filtering step and instead match base on the full expressions of each JAX-RS method. resteasy.wider.request.matching. Set that to true and you will at least be able to avoid that.

- The JAX-RS TCK has become very strict with a ton more tests. I can't remember them all, but there are a number of edge cases which earlier Resteasy releases misinterpreted.

- Any Failure exceptions in the SPI now have a corresponding JAX-RS 2.0 exception, so they have been deprecated. Resteasy no longer uses these old SPI exceptions internally. It now uses the JAX-RS 2.0 ones.

- A number of SPIs have changed. Shouldn't be an issue for those of you who use Restasy as-is. Specifically InjectorFactory and Registry have changed.

56.6. Migrating from 3.0-beta-4 and 3.0-beta-5

- JSONP support is no longer on by default. A few users have complained that it is a security hole for their applications.

- A number of SPIs have changed. Shouldn't be an issue for those of you who use Restasy as-is. Specifically InjectorFactory and Registry have changed.

56.7. Migrating from 3.0-beta-2 and 3.0-beta-4

- The JAX-RS 2.0 class ClientFactory no longer exists. It has been replaced with ClientBuilder. You can still call newClient(), but there is now an additional builder interface. Likewise, there is no ResteasyClientFactory. We also have an extension to ClientBuilder called ResteasyClientBuilder. So docs for more details.
Migrating from 3.0-beta-1 and 3.0-beta-2

- Filter execution and exception handling now matches the JAX-RS 2.0 spec. Exceptions thrown from filters/interceptors can now be mapped if possible. Responses returned from ExceptionMappers are now filtered.

56.8. Migrating from 3.0-beta-1 and 3.0-beta-2

- The constructors for ResteasyClient class are no longer public. You need to use the new ResteasyClientBuilder class. One thing to note is that when a ResteasyClient is created by a builder, it no longer uses ResteasyProviderFactory.getInstance(), but instead instantiates a new one. This will probably not effect most uses.

56.9. Migrating from 2.x to 3.0-beta-1

- Resteasy manual client API, interceptors, StringConverters, StringParameterConverters, and Async HTTP APIs have all been deprecated and will be removed possibly in a later release. There is now a JAX-RS 2.0 equivalent for each of these things.

- resteasy-crypto: SignedInput and SignedOutput must have a multipart/signed content type set either through the request or response object, or by annotation @Consumes/@Produces

- Server-side cache setup has been changed. Please see documentation for more details.

- The security filters for @RolesAllowed, etc. now return 403, Forbidden instead of 401.

- Most add() methods have been removed or made protected in ResteasyProviderFactory. Use registerProvider() and registerProviderInstance() methods.

- The new JAX-RS 2.0 client-side filters will not be bound and run when you are using Resteasy's old client api.

- On server-side, all old Resteasy interceptors can run in parallel with the new JAX-RS 2.0 filter and interceptor interfaces.

- Some SPIs have changed. This should not effect applications unless you are doing something you aren't supposed to do.

- The async tomcat and async jboss web modules have been removed. If you are not running under Servlet 3.0, async HTTP server-side, will be faked and run synchronously in same request thread.

56.10. Migrating from 2.3.2 to 2.3.3

- MultipartInput has a new close() method. If you have a read body that is MultipartInput or one of its subinterfaces, then you must call this method to clean up any temporary files created. Otherwise, these possible temporary files are deleted on GC or JDK shutdown. Other multipart providers clean up automatically.
Chapter 56. Migration from ol...

56.11. Migrating from 2.3.0 to 2.3.1

• sjsxp has been removed as a dependency for the Resteasy JAXB provider

56.12. Migrating from 2.2.x to 2.3

• The Apache Abdera integration has been removed as a project. If you want the integration back, please ping our dev lists or open a JIRA.

• Apache HttpClient 4.x is now the default underlying client HTTP mechanism. If there are problems, you can change the default mechanism by calling ClientRequest.setDefaultExecutorClass().

• ClientRequest no longer supports a shared default executor. The createPerRequestInstance parameter has been removed from ClientRequest.setDefaultExecutorClass().

• resteasy-doseta module no longer exists. It is now renamed to the resteasy-crypto module and also includes other things beyond doseta.

• Doseta work has been refactored a bit and may have broken backward compatibility.

• Jackson has been upgraded from 1.6.3 to 1.8.5. Let me know if there are any issues.

• Form parameter processing behavior was modified because of RESTEASY-574. If you are having problems with form parameter processing on Tomcat after this fix, please log a JIRA or contact the resteasy-developers email list.

• Some subtle changes were made to ExceptionMapper handling so that you can write ExceptionMappers for any exception thrown internally or within your application. See JIRA Issue RESTEASY-595 for more details. This may have an effect on existing applications that have an ExceptionMapper for RuntimeException in that you will start to see Resteasy internal exceptions being caught by this kind of ExceptionMapper.

• The resteasy-cache (Server-side cache) will now invalidate the cache when a PUT, POST, or DELETE is done on a particular URI.

56.13. Migrating from 2.2.0 to 2.2.1

• Had to upgrade JAXB libs from 2.1.x to 2.2.4 as there was a concurrency bug in JAXB impl.

56.14. Migrating from 2.1.x to 2.2

• ClientRequest.getHeaders() always returns a copy. It also converts the values within ClientRequest.getHeadersAsObjects() to string. If you add values to the map returned by getHeaders() nothing happen. Instead add values to the getHeadersAsObjects() map. This
allows non-string header objects to propagate through the MessageBodyWriter interceptor and ClientExecutor interceptor chains.

56.15. Migrating from 2.0.x to 2.1

• Slf4j is no longer the default logging mechanism for resteasy. Resteasy also no longer ships with SLF4J libraries. Please read the logging section in the Installation and Configuration chapter for more details.

• The constructor used to instantiate resource and provider classes is now picked based on the requirements of the JAX-RS specification. Specifically, the public constructor with the most arguments is picked. This behavior varies from previous versions where a no-arg constructor is preferred.

56.16. Migrating from 1.2.x to 2.0

• TJWS has been forked to fix some bugs. The new groupId is org.jboss.resteasy, the artifactId is tjws. It will match the resteasy distribution version

• Please check out the JBoss 6 integration. It makes things a lot easier if you are deploying in that environment

• There is a new Filter implementation that is the preferred deployment mechanism. Servlet-based deployments are still supported, but it is suggested you use to using a FilterDispatcher. See documentation for more details.

• As per required by the spec List or array injection of empty values will return an empty collection or array, not null. I.e. (@QueryParam("name") List<String> param) param will be an empty List. Resteasy 1.2.x and earlier would return null.

• We have forked TJWS, the servlet container used for embedded testing into the group org.jboss.resteasy, with the artifact id of tjws. You will need to remove these dependencies from your maven builds if you are using any part of the resteasy embeddable server. TJWS has a number of startup/shutdown race conditions we had to fix in order to make unit testing viable.

• Spring integration compiled against Spring 3.0.3. It may or may not still work with 2.5.6 and lower

56.17. Migrating from 1.2.GA to 1.2.1.GA

Methods @Deprecated within 1.2.GA have been removed. This is in the Client Framework and has to do with all references to Apache HTTP Client. You must now create an ClientExecutor if you want to manage your Apache HTTP Client sessions.

56.18. Migrating from 1.1 to 1.2

• The resteasy-maven-import artifact has been renamed to resteasy-bom
• Jettison and Fastinfoset have been broken out of the resteasy-jaxb-provider maven module. You will now need to include resteasy-jettison-provider or resteasy-fastinfoset-provider if you use either of these libraries.

• The constructors for ClientRequest that have a HttpClient parameter (Apache Http Client 3.1 API) are now deprecated. They will be removed in the final release of 1.2. You must create a Apache HTTP Client Executor and pass it in as a parameter if you want to re-use existing Apache HttpClient sessions or do any special configuration. The same is true for the ProxyFactory methods.

• Apache HttpClient 4.0 support is available if you want to use it. I've had some trouble with it so it is not the default implementation yet for the client framework.

• It is no longer required to call RegisterBuiltin.register() to initialize the set of providers. Too many users forgot to do this (include myself!). You can turn this off by calling the static method ResteasyProviderFactory.setRegisterBuiltinByDefault(false)

• The Embedded Container’s API has changed to use org.jboss.resteasy.spi.ResteasyDeployment. Please see embedded documentation for more details.
Chapter 57. Books You Can Read

There are a number of great books that you can learn REST and JAX-RS from

- *RESTful Web Services* [http://oreilly.com/catalog/9780596529260/] by Leonard Richardson and Sam Ruby. A great introduction to REST.

- *RESTful Java with JAX-RS* [http://oreilly.com/catalog/9780596158040/] by Bill Burke. Overview of REST and detailed explanation of JAX-RS. Book examples are distributed with RESTEasy.

- *RESTful Web Services Cookbook* [http://oreilly.com/catalog/9780596808679/] by Subbu Allamaraju and Mike Amundsen. Detailed cookbook on how to design RESTful services.