

大树叶 技术专栏

骨灰攻城狮 架构师

目录视图

摘要视图

RSS 订阅

个人资料



大树叶

原创	粉丝	喜欢	评论
403	129	77	49



等级：博客 1 访问量：83万+

积分：1万+ 排名：1355

JAVA 序列化 和 反序列化 （ Externalizable Serializable ） 那些事

标签： JAVA 序列化 反序列化 Externalizable Seriala

2016年01月13日 21:19:03

906人阅读

评论(0)

收藏

举报

分类： java (417)

版权声明：本文为博主原创文章，未经博主允许不得转载。 https://blog.csdn.net/bigtree_3721/article/details/50513295

序列化控制

- 当我们对序列化进行控制时，可能某个特定子对象不想让Java序列化机制自动保存与恢复。如果子对象表示的是我们不希望将其序列化的敏感信息（如密码），通常会面临这种情况。即使对象中的这些信息是private属性，一经序列化处理，人们就可以通过读取文件或者拦截网络传输的方式来访问到它。有两种办法可以防止对象的敏感部分被序列化：
 - 实现Externalizable代替实现Serializable接口来对序列化过程进行控制，Externalizable继承了Serializable接口，同时增添了两个方法：writeExternal()和readExternal()。

两者在反序列化时的区别：

- 对Serializable对象反序列化时，由于Serializable对象完全以它存储的二进制位为基础来构造，因此并不会调用任何构造函数，因此Serializable类无需默认构造函数，但是当Serializable类的父类没有实现Serializable接口时，反序列化过程会调用父类的默认构造函数，因此该父类必需有默认构造函数，否则会抛异常。
- 对Externalizable对象反序列化时，会先调用类的不带参数的构造方法，这是有别于默认反序列方式的。如果把类的不带参数的构造方法删除，或者把该构造方法的访问权限设置为private、默认或protected级别，会抛出java.io.InvalidException: no valid constructor异常，因此Externalizable对象必须有默认构造函数，而且必需是public的。
- Externalizable的替代方法：如果不是特别坚持实现Externalizable接口，那么还有另一种方法。我们可以实现Serializable接口，并添加writeObject()和readObject()的方法。一旦对象被序列化或者重新装配，就会分别调用那两个方法。也就是说，只要提供了这两个方法，就会优先使用它们，而不考虑默认的序列化机制。

这些方法必须含有下列准确的签名：

```
private void writeObject(ObjectOutputStream stream) throws IOException;
private void readObject(ObjectInputStream stream) throws IOException, ClassNotFoundException
```

- 可以用transient关键字逐个字段地关闭序列化，它的意思是“不用麻烦你保存或恢复数据—我自己会处理的”。由于Externalizable对象在默认情况下不保存它们的任何字段，所以transient关键字只能和Serializable对象一起使用。

- 上一篇 Java7 新特性：try() 语句 即 try-with-resources
- 下一篇 Java ServerSocket Socket 网络通讯的那些事

您还没有登录,请[登录](#)或[注册](#)

Externalizable和Serializable

1、Serializable序列化时不会调用默认的构造器，而Externalizable序列化时会调用默认构造器的！！！2、Serializable：一个对象想要被序列化，那么它的类就要实现 此接...

Externalizable 接口例子



namecyf

2012年10月10日 19:48

1365

被Serializable接口声明的类的对象的内容都将被序列化，如果现在用户希望自己指定序列化的内容，则可以让一个类实现Externalizable接口，此接口定义如下： public inte...

架构与分布式系统	(58)
nginx	(30)
web service	(14)
Restful	(13)
thrift	(2)
JVM	(21)
并发	(21)
网络编程	(28)
网络安全	(13)
数据结构	(20)
maven	(7)
jquery	(3)
velocity	(4)
tbschedule	(5)
mybatis	(11)
ecache	(2)
redis	(32)
json	(16)
秒杀系统	(9)
分布式调度框架	(12)
zookeeper	(8)
kafka	(24)
druid	(7)
mongodb	(1)
dubbo	(4)
sharding-jdbc	(1)
RocketMQ	(4)
java并发	(12)
UML	(1)
算法	(7)
mycat	(5)
lintcode	(2)
springmvc	(7)
netflix	(2)
jsp	(2)
安全	(1)
angular	(3)
微服务	(17)
大数据	(15)
K8S	(16)
istio	(5)
devops	(1)
黑白子	(1)
区块链	(1)

文章存档

2018年4月

(16)

2018年3月

(18)

2018年2月

(14)

2018年1月

(10)

2017年12月



(23)



展开

阅读排行	
分析和解决JAVA 内存泄露的...	(32251)
redis 最好的 GUI 客户端工具	(27496)
如何通过 Mybatis 向Mysql ...	(13506)
Spring transaction事务之roll...	(12319)
JAVA 中无锁的线程安全整数 ...	(12147)
mysql 聚簇索引 和聚簇索引 ...	(11484)
Spring中 PROPAGATION R...	(10387)
maven 编译时报错：编码 UT...	(9001)
JQuery 中 AJAX 如何实现 Ex...	(8579)
解决：Eclipse 提示内存不足	(7771)

最新评论
inginx搭建文件上传下载服务器 zhugeaming2018：老铁,看完楼主的这个帖子之后，学习了谢谢！
javax.servlet.http... HelloWorld20151118：<script>alert(/xs s/)</script...
javax.servlet.http...



Java中的Externalizable接口	 hirohrj123	2013年09月25日 10:16	 1428
源码：package java.io; import java.io.ObjectOutput; import java.io.ObjectInput; public interface Ext...			

Serializable和Externalizable	 lovergo	2016年11月21日 14:07	 908
无论是Serializable,还是Externalizable,他们都是实现序列化或者持久化的接口. 先解释下什么叫序列化,序列化就是对象保存到磁盘上,或者是对象由一台机器发送过来并保存下来就是序...			

Java序列化几点注意事项	 tayanxunhua	2014年02月28日 09:25	 4750
序列化保存的是对象的状态，而静态变量是类的状态。 1、基本类型的数据可以直接序列化 2、对象要被序列化，它的类必须要实现Serializable接口；如果一个类中有引用类型的实例变量，这个引用类...			


JAVA的可序列化	 jajavaja	2012年09月19日 10:36	 1248
http://rabbitsfish-163-com.iteye.com/blog/1121318 什么是序列化 java中的序列化(serialization)机制能够将一个实例对象的状态信息...			



序列化--Serializable接口和Externalizable接口	 zhai010101	2010年10月24日 19:47	 297
序列化--Serializable接口和Externalizable接口序列化就是将对象转化为流的过程；反序列化就是把流中的数据转化为对象。要实现序列化与反序列化，则类必须实现Serializable...			


java对象序列化与反序列化中的构造方法问题	 Deep_Mind	2016年07月27日 21:28	 1683
老规矩，先上代码再总结：import java.io.FileInputStream; import java.io.FileOutputStream; import java.io.IOExcept...			



对象反序列化时，如果父类未实现序列化接口，则反序列出的对象会再次调用父类的构造...

对象反序列化时，如果父类未实现序列化接口，则反序列出的对象会再次调用父类的构造函数来完成属于父类那部分内容的初始化。 1、当将一个父类没有实现序列化的对象son使用ObjectOutputStream...



 wanping321	2017年04月20日 20:43	 566
--	-------------------	---



Java中类序列化构造函数的调用问题	 fuyin11	2016年04月10日 22:51	 1625
public class Person implements Serializable{ public Person(){ System.out.println("Person..."); }...			

程序员不会英语怎么行？	
老司机教你一个数学公式秒懂天下英语	

Java的序列化和反序列化，我所遇到的坑	 w958796636	2017年01月19日 18:04	 1593
有时需要为对象做持久化，就是把内存里的对象保存到磁盘（暂且叫做磁盘吧，可以等同于sp、db、文件、网络等）上，等以后需要这个对象的时候再从磁盘上还原到内存，因此需要序列化和反序列化。 坑1、类里面...			

由Java反序列化对象异常想到的	 baosxie	2017年03月14日 23:06	 2290
由Java反序列化对象异常想到的serialVersionUID问题。			

java序列化与反序列化系列问题	 mawming	2016年07月20日 11:05	 2345
很多商业项目用到数据库、内存映射文件和普通文件来完成项目中的序列化处理的需求，但是这些方法很少会依靠于Java序列化。本文也不是用来解释序列化的，而是一起来看看面试中有关序列化的问题，这些问题你很有可...			

Java序列化问题总结	 kjfcgua	2013年02月19日 16:33	 5431
下面是一些复杂对象情况下一些总结： l 当父类继承Serializable接口，所有子类都可以被序列化 l 子类实现了Serializable接口，父类没有，父类中的属性不能序列化...			

HelloWorld20151118 : <script>alert ("uot;asd&quo...

druid中 如何从本地批(ba... zhugeaming2018 : 谢谢分享，相互学习！

推荐：Druid + Grafan... zhugeaming2018 : 老铁,顶，互相多学习！

redis 如何 把文件对象存进去 嘻嘻嘻嘻哈哈 : 全是错的 redis里面保存的是 文件地址对象 不是文件内容对象 全是错的 草

redis 如何 把文件对象存进去 嘻嘻嘻嘻哈哈 : 全是错的 redis里面保存的是 文件地址对象 不是文件内容对象 全是错的 草

redis 如何 把文件对象存进去 嘻嘻嘻嘻哈哈 : 全是错的 redis里面保存的是 文件地址对象 不是文件内容对象 全是错的 草

EJB 标注那些事 Super_gaohui : @Stateless @Remote 请教一下上面两个注解依赖哪个 jar 包

kafka与Spring的集成 fdfsfsdsaf : 你好,我根据你这个配置老是报Cause d by: java.lang.ClassNotFoundE...

联系我们



请扫描二维码联系客服

✉ webmaster@csdn.net

☎ 400-660-0108

💬 QQ客服 🗨 客服论坛

关于 招聘 广告服务 🐾 百度

©1999-2018 CSDN版权所有

京ICP证09002463号

经营性网站备案信息

网络110报警服务

中国互联网举报中心

北京互联网违法和不良信息举报中心

java反序列化漏洞解决方案

 OXiaoMianYiJiu 2016年01月22日 16:50 📖 4609

测解决方案是针对weblogic10.3.6.0版本的 方案一： 删除weblogic中com.bea.core.apache.commons.collections_3.2.0.jar包中的...

Java 序列化简单理解,serializable与externalizable区别？

什么是对象序列化？把Java对象状态保存为一组字节（序列化），之后还可以把这些字节组装成对象（反序列化）。为什么要使用对象序列化？1. 使用RMI（远程方法调用）2. 网络中传递对象（Ja...

 love_world_ 2013年12月24日 21:46 📖 1979

JAVA 对象序列化（三）——transient以及Externalizable的一种替代方法（使用Seri...

transient(瞬时)关键字 当我们队序列化进行控制时，可能某个特定子对象不想让Java的序列化机制自动保存与恢复。如果子对象表示的是我们不希望将其序列化的敏感信息（如密码），通...

 djun100 2014年01月11日 17:49 📖 1441

Java 利用 Externalizable 实现序列化

 hewusheng10 2013年01月21日 10:51 📖 444

原地址：http://201211131343.iteye.com/blog/1772780 Java 利用 Externalizable 实现序列化 博客分类：Java extern...

17万欧起全家三代定居希腊！

全家三代享受免费教育与公立医疗，最快60天起即可定居希腊！



Java对象的序列化和反序列化Serializable

 lingzhm 2015年04月14日 21:02 📖 2150

对象的序列化 对象序列化就是把一个对象变为二进制数据流的一种方法。 一个类要想被序列化，就行必须实现java.io.Serializabl e接口。虽然这个接口中没有任何方法，就如同之前的cloneab...

IDictionary 序列化一定要实现父类实现了ISerializable接口的，子类也必须有序列化构...

```
//public class ThreadSafeDictionary : IDictionary, ICloneable [Serializable] public class Th...
```

 fyifei0558 2013年01月22日 18:46 📖 1587