配置 wallfilter

cutedemons edited this page on 11 Dec 2013 · 40 revisions

这个文档提供基于Spring的各种配置方式

使用缺省配置的WallFilter

```
<bean id="dataSource" class="com.alibaba.druid.pool.DruidDataSource" init-method
    ...
    <property name="filters" value="wall"/>
</bean>
```

结合其他Filter一起使用

WallFilter可以结合其他Filter一起使用，例如：

```
<bean id="dataSource" class="com.alibaba.druid.pool.DruidDataSource" init-method
    ...
    <property name="filters" value="wall,stat"/>
</bean>
```

这样，拦截检测的时间不在StatFilter统计的SQL执行时间内。

如果希望StatFilter统计的SQL执行时间内，则使用如下配置

```
<bean id="dataSource" class="com.alibaba.druid.pool.DruidDataSource" init-method
    ...
    <property name="filters" value="stat,wall"/>
</bean>
```

指定dbType

有时候，一些应用框架做了自己的JDBC Proxy Driver，是的DruidDataSource无法正确识别数据库的类型，则需要特别指定，如下：

```
<bean id="wall-filter" class="com.alibaba.druid.wall.WallFilter">
    <property name="dbType" value="mysql" />
</bean>

<bean id="dataSource" class="com.alibaba.druid.pool.DruidDataSource" init-method
    ...
    <property name="proxyFilters">
        <list>
            <ref bean="wall-filter"/>
        </list>
    </property>
</bean>
```

指定配置装载的目录

缺省情况下，配置装载的目录如下：

数据库类型	目录
mysql	META-INF/druid/wall/mysql
oracle	META-INF/druid/wall/oracle
sqlserver	META-INF/druid/wall/sqlserver
postgres	META-INF/druid/wall/postgres

从配置目录中以下文件中读取配置：

```
deny-variant.txt
deny-schema.txt
deny-function.txt
deny-table.txt
deny-object.txt
```

指定配置装载的目录是可以指定，例如：

```
<bean id="wall-filter-config" class="com.alibaba.druid.wall.WallConfig" init-met
    <!-- 指定配置装载的目录  -->
    <property name="dir" value="META-INF/druid/wall/mysql" />
</bean>
```

```
<bean id="wall-filter" class="com.alibaba.druid.wall.WallFilter">
    <property name="dbType" value="mysql" />
    <property name="config" ref="wall-filter-config" />
</bean>

<bean id="dataSource" class="com.alibaba.druid.pool.DruidDataSource" init-methoc
    ...
    <property name="proxyFilters">
        <list>
            <ref bean="wall-filter"/>
        </list>
    </property>
</bean>
```

WallConfig详细说明

本身的配置

配置项	缺省值
dir	按照dbType分别配置: mysql : META-INF/druid/wall/mysql oracle : META-INF/druid/wall/oracle sqlserver : META-INF/druid/wall/sqlserver

拦截配置 – 语句

配置项	缺省值	描述
selelctAllow	true	是否允许执行SELECT语句
selectAllColumnAllow	true	是否允许执行SELECT * FROM T这样的语句。如果设置 from t，但select * from (select id, name from t) a。这个选项是防御程序通过调用select *获得数据表的
selectIntoAllow	true	SELECT查询中是否允许INTO字句
deleteAllow	true	是否允许执行DELETE语句
updateAllow	true	是否允许执行UPDATE语句

insertAllow	true	是否允许执行INSERT语句
replaceAllow	true	是否允许执行REPLACE语句
mergeAllow	true	是否允许执行MERGE语句，这个只在Oracle中有用
callAllow	true	是否允许通过jdbc的call语法调用存储过程
setAllow	true	是否允许使用SET语法
truncateAllow	true	truncate语句是危险，缺省打开，若需要自行关闭
createTableAllow	true	是否允许创建表
alterTableAllow	true	是否允许执行Alter Table语句
dropTableAllow	true	是否允许修改表
commentAllow	false	是否允许语句中存在注释，Oracle的用户不用担心，Wa
noneBaseStatementAllow	false	是否允许非以上基本语句的其他语句，缺省关闭，通过
multiStatementAllow	false	是否允许一次执行多条语句，缺省关闭
useAllow	true	是否允许执行mysql的use语句，缺省打开
describeAllow	true	是否允许执行mysql的describe语句，缺省打开
showAllow	true	是否允许执行mysql的show语句，缺省打开
commitAllow	true	是否允许执行commit操作
rollbackAllow	true	是否允许执行roll back操作

如果把selectIntoAllow、deleteAllow、updateAllow、insertAllow、mergeAllow都设置为false，这就是一个只读数据源了。

拦截配置 – 永真条件

配置项	缺省值	描述
selectWhereAlwayTrueCheck	true	检查SELECT语句的WHERE子句是否是一个永真条
selectHavingAlwayTrueCheck	true	检查SELECT语句的HAVING子句是否是一个永真条
deleteWhereAlwayTrueCheck	true	检查DELETE语句的WHERE子句是否是一个永真条

deleteWhereNoneCheck	false	检查DELETE语句是否无where条件，这是有风险的
updateWhereAlayTrueCheck	true	检查UPDATE语句的WHERE子句是否是一个永真条
updateWhereNoneCheck	false	检查UPDATE语句是否无where条件，这是有风险的
conditionAndAlwayTrueAllow	false	检查查询条件(WHERE/HAVING子句)中是否包含AN
conditionAndAlwayFalseAllow	false	检查查询条件(WHERE/HAVING子句)中是否包含AN
conditionLikeTrueAllow	true	检查查询条件(WHERE/HAVING子句)中是否包含LI

其他拦截配置

配置项	缺省值	描述
selectIntoOutfileAllow	false	SELECT ... INTO OUTFILE 是否允许，这个是mysql注
selectUnionCheck	true	检测SELECT UNION
selectMinusCheck	true	检测SELECT MINUS
selectExceptCheck	true	检测SELECT EXCEPT
selectIntersectCheck	true	检测SELECT INTERSECT
mustParameterized	false	是否必须参数化，如果为True，则不允许类似WHERE
strictSyntaxCheck	true	是否进行严格的语法检测，Druid SQL Parser在某些场景不能覆盖所有的SQL语法，出现解析
conditionOpXorAllow	false	查询条件中是否允许有XOR条件。XOR不常用，很难
conditionOpBitwseAllow	true	查询条件中是否允许有"&"、"~"、"|"、"^"运算符。
conditionDoubleConstAllow	false	查询条件中是否允许连续两个常量运算表达式
minusAllow	true	是否允许SELECT * FROM A MINUS SELECT * FROM
intersectAllow	true	是否允许SELECT * FROM A INTERSECT SELECT *
constArithmeticAllow	true	拦截常量运算的条件，比如说WHERE FID = 3 - 1，其
limitZeroAllow	false	是否允许limit 0这样的语句

禁用对象检测配置

配置项	缺省值	描述
tableCheck	true	检测是否使用了禁用的表
schemaCheck	true	检测是否使用了禁用的Schema
functionCheck	true	检测是否使用了禁用的函数
objectCheck	true	检测是否使用了“禁用对对象”
variantCheck	true	检测是否使用了“禁用的变量”
readOnlyTables	空	指定的表只读，不能够在SELECT INTO、DELETE、UPDATE、INSERT、MERGE中作为"被修改表"

Jdbc相关配置

配置项	缺省值	描述
metadataAllow	true	是否允许调用Connection.getMetadata方法，这个方法调用会暴露
wrapAllow	true	是否允许调用Connection/Statement/ResultSet的isWrapFor和unv

WallFiler配置说明

配置项	缺省值	描述
logViolation	false	对被认为是攻击的SQL进行LOG.error输出
throwException	true	对被认为是攻击的SQL抛出SQLExcepton
config		
provider		

刚开始引入WallFilter的时候，把logViolation设置为true，而throwException设置为false。就可以观察是否存在违规的情况，同时不影响业务运行。