

Weaver Software

上海市闵行区联航路1188号浦江智谷33号楼

邮政编码：201112

电话：+86 21 52262837

**Webservice白名单配置说明**

**Submitted By Weaver**

**设计说明书**

文档版本控制

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **文档简要信息：** | | | | | | | |
| 文档主题(Title) | | | | Ecology系统安全配置说明 | | | |
| 作者(Author) | | | | 柳炉 | | | |
| 审批者 (To Be Approved By) | | | |  | | | |
| 说明 (Comments) | | | | Ecology系统安全配置说明 | | | |
| 文件名称(File Name) | | | |  | | | |
| **文档版本历史：** | | | | | | | |
| 序号 | 日期 | 版本 | 变更说明 | | 修改人 | 审批人 | 注释 |
|  | 2015/03/20 | 1 | 新建 | | 柳炉 |  |  |

**目录**

[1 引言 3](#_Toc528249143)

[1.1 编写目的 3](#_Toc528249144)

[1.2 定义 3](#_Toc528249145)

[1.3 配置说明 3](#_Toc528249146)

[1.3.1 检测WEBSERVICE白名单检测功能是否开启 3](#_Toc528249147)

# 引言

## 编写目的

本文档主要描述了Ecology系统安全补丁包中启用webservice的白名单防御功能检测与说明。（**此项防御功能非常重要，由于涉及到客户端具体环境，无法统一开启，现告知配置方式，请务必按照本方案开启webservice白名单防御，避免被攻击出现安全问题**）

## 定义

下文中提及到的WEB-INF/securityXML/weaver\_security\_custom\_rules\_1.xml与WEB-INF/ weaver\_security\_rules.xml文件的格式完全一样。

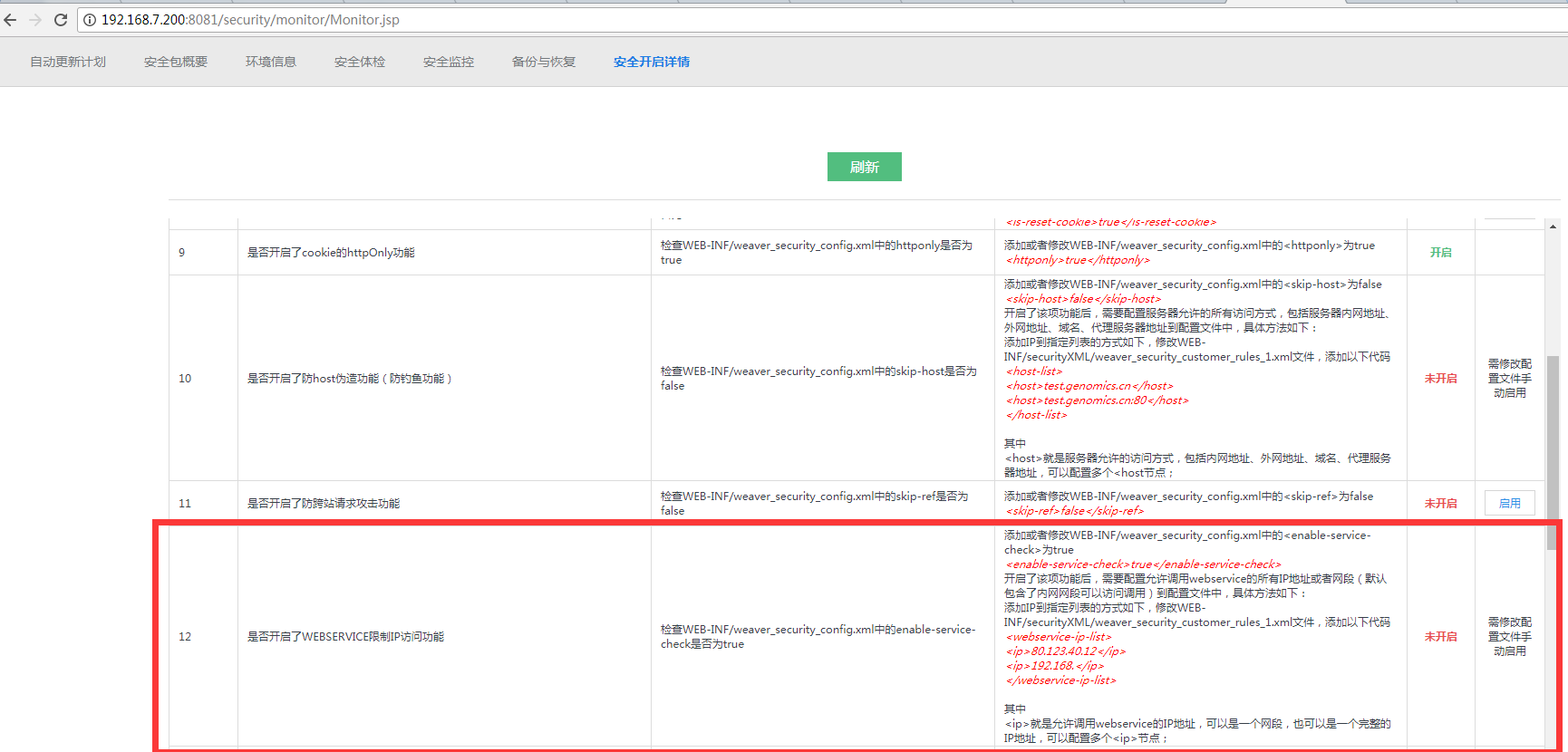
## 配置说明

部署安全包后，用sysadmin登录系统，访问如下地址：

**http://贵司OA访问地址/security/monitor/Monitor.jsp**

### 检测WEBSERVICE白名单检测功能是否开启

点击【安全开启详情】TAB页，查看第12条：【是否开启了WEBSERVICE限制IP访问功能】，如果该项显示为未开启，那么需要按照配置说明开启白名单防御。



**注：如果【安全开启详情】中所有的项都显示【未开启】，那么说明安全包没有生效，请先按照以下步骤开启安全补丁包：**

|  |
| --- |
| 1、用sysadmin登录系统，访问:/security/monitor/Monitor.jsp;  2、查看【环境信息】tab页，可以看到当前安全包版本；  3、在【安全概要】tab页，可以看到安全包是否生效；  4、如果显示为未开启，在【安全体检】里面点击【检测】，检测后会弹出【修复】按钮，点击【修复】；  5、修复完成后会弹出 具体的修复步骤（主要就是替换文件），按照修复步骤操作即可  6、如果按上面5步修复完成后仍显示未开启，请在【安全开启详情】tab页的第一项点击【开启】。  7、如果仍显示为未开启，则删除/ecology/WEB-INF/weaver\_security\_config.xml 文件，重启OA或者在【安全开启详情】界面点击【刷新】按钮 |

**白名单配置方法：**

**1、修改/ecology/WEB-INF/weaver\_security\_config.xml文件，在该文件中添加或者修改<enable-service-check>节点，将值改为true。**

|  |
| --- |
| **<enable-service-check>true</enable-service-check>** |

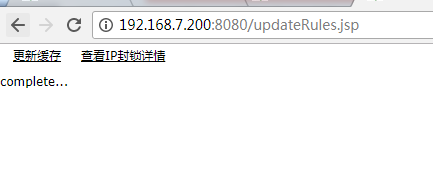
|  |
| --- |
| **2、将需要调用webservice的客户端IP地址加入到白名单中，具体格式见附件《weaver\_security\_custom\_rules\_ws\_20180206.xml》** |



**1、将允许访问webservice的客户端IP添加到上述文件中的<webservice-ip-list>下面添加一个<ip>节点即可。**

|  |
| --- |
| **<webservice-ip-list>**  **<ip>192.168.3.22</ip>**  **<ip>127.0.0.1</ip>**  **</webservice-ip-list>** |

**2 、将修改好的文件（文件名可以自定义，只要保证后缀是.xml即可）放到/ecology/WEB-INF/securityXML/目录下，用sysadmin登录，访问下/updateRules.jsp即可生效(如果是集群环境，需要每个节点都访问下该地址），无需重启OA服务。（重启服务也可以生效）。**



**开启后，默认会允许标准内网网段的地址调用，这些网段无需配置，包含以下IP地址段**：

|  |
| --- |
| <ip>localhost</ip>  <ip>127.0.0.1</ip>  <ip>192.168.</ip>  <ip>10.</ip>  <ip>172.16.</ip>  <ip>172.17.</ip>  <ip>172.18.</ip>  <ip>172.19.</ip>  <ip>172.20.</ip>  <ip>172.21.</ip>  <ip>172.22.</ip>  <ip>172.23.</ip>  <ip>172.24.</ip>  <ip>172.25.</ip>  <ip>172.26.</ip>  <ip>172.27.</ip>  <ip>172.28.</ip>  <ip>172.29.</ip>  <ip>172.30.</ip>  <ip>172.31.</ip> |