目录

[一.老版本防篡改问题处理方法： 1](#_Toc38268435)

[1.1 客户端安装失败 1](#_Toc38268436)

[1.2 驱动状态显示黄色感叹号 2](#_Toc38268437)

[1.3 防护日志不产生或者额外产生 2](#_Toc38268438)

[1.4 中心服务启动失败/加载日志失败 3](#_Toc38268439)

[1.5 防护规则不生效 3](#_Toc38268440)

[二. 新版本防篡改10.5问题处理思路 4](#_Toc38268441)

[1.首页web验证码乱码或为空 4](#_Toc38268442)

[2.ssh断开，服务即停止 4](#_Toc38268443)

[3.发布端文件同步问题 4](#_Toc38268444)

[4.防护不生效或者防护生效后不产生告警日志 5](#_Toc38268445)

[5. 配置网站防护不能生效 6](#_Toc38268446)

[6. 父目录允许修改，子目录被阻止 6](#_Toc38268447)

[7. 添加许可后登录租户提示用户未授权 6](#_Toc38268448)

[8．端服务器的监控端口等信息在中心上不能显示 7](#_Toc38268449)

V1.0 二零二零年-四月二十号 汪志杰

维护三板斧：检查网络端口防火墙非法字符/重启/重装

## 一.老版本防篡改问题处理方法：

### 1.1 客户端安装失败

现场安装老版本端服务提示不能”could not load \*\*/WebGuardAgent.ko，no such file or directory”?

步骤1. 在服务器上执行uname -a 将内核版本信息，/lib/modules 和/usr/src/Kernel下的文件打包成tar.gz格式发给产品部项目经理进行服务器适配编译。

步骤2. 编译后的ko文件替换到客户端安装包目录下（Agent.tar.gz\WebProtect-Client\ko\x64或者x32）.

注意：假设拿到的ko文件是这样的：WebGuardAgent.ko-3.10.0-957.el7.x86\_64

但是服务器的内核信息是下图所示：



则需要将ko文件更名通内核信息一致，如改为：WebGuardAgent.ko-3.10.0-957.21.3.el7.x86\_64

将替换好ko文件的端安装包上传到服务器进行安装(执行安装脚本install.sh)，如果还安装失败，检查文件替换无误后再联系产品部解决

### 1.2 驱动状态显示黄色感叹号

管理中心显示端服务的驱动为黄色感叹号



出现该问题原因：中心和端服务驱动状态的交互是通过ko文件，三种情况下会出现该类问题：

问题类型1. 装端服务提示没有ko文件，编译后端服务安装成功，但是没将该ko文件替换到中心上

步骤1. 原因一：将编译好的ko文件（注意ko文件名称要和内核名称保持一致）也放到中心服务器目录下，/usr/local/WGSCentral/ko/x64或者x32），wins目录类似

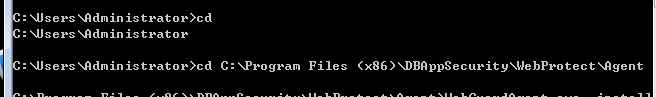
问题类型2. 平台运行一段时间因为环境原因导致端和中心上的ko文件md5值不一致

步骤1. 在端服务器上uname -r 查询到内核版本信息，在端目录（WebProtect-Client\ko\x64或者x32）下找到对应的ko文件，拷贝到中心服务器目录下，（/usr/local/WGSCentral/ko/x64或者x32），wins目录类似

问题类型3. 端服务器上得驱动服务没有安装成功，需要重新安装然后在管理端删除该设备（会再次自动连接上来）

步骤1. 在端服务器上执行：

1.1Wins：打开cmd窗口，查看驱动是否正常运行:sc query ppsdrv,，无驱动状态信息则手动安装，cd到端服务得安装目录下执行WebGuardAgent.exe -install (x86目录选择按tab键)



1.2如果安装驱动提示失败，则检查该环境下有没有其他安全软件和发布软件，将其卸载重启服务器后，重启WebProtector Agent服务（在服务管理器页面执行对该服务器得重启等操作）

1.3端服务重启后再次执行驱动安装命令即可：WebGuardAgent.exe -install

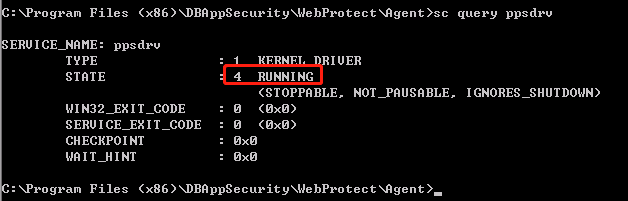
2.1Linux：连接端服务器后台：lsmod |grep WebGuard\* 如无驱动得运行状态，则cd到安装目录下执行ismond sysmon.ko,如安装失败则重启端服务/etc/init.d/ wgsclient restart 后再次执行安装驱动命令，安装驱动成功后可重启驱动：/etc/init.d/WebGuardAgent restart

### 1.3 防护日志不产生或者额外产生

防护生效状态下，无防护日志；或者是把需要防护的进程停止后还会产生该进程告警日志

该问题基本是：1.驱动有问题（驱动重新启动，重新下发规则） 2.添加的规则文件有空格等非法字符

win监控端sc query ppsdrv查看驱动状态，state：4表示运行



步骤1. 将驱动服务停止，并且也在wins服务管理里面把端服务停止

停止驱动：在cmd窗口下执行命令：net stop ppsdrv，如果命令停止失败则在服务管理里面停止驱动：



停止端服务：Agent Console



步骤2. 服务停止后，将端的安装目录下的WebGuardAgent.dat 规则文件删除，再按照前两步骤将端服务和端服务重新启动（net start ppsdrv）

步骤3. 服务启动后在管理端对端规则保存重新下发规则(注意：规则不能额外加上空格等字符)，触发规则验证有无日志产生

Linux监控端下操作方法同wins一致：只是驱动服务和端服务启动的命令有区别

步骤1.查看驱动是否启动lsmod |grep Web\* 状态是1表示运行

将驱动停止/重启/启动：/etc/init.d/WebGuardAgent stop/restart/start

步骤2.停止/启动/重启监控端服务命令

/etc/init.d/wgsclient stop/start/restart

步骤3.删除服务安装目录下的WebGuardAgent.dat后，再把驱动服务重新启动，最后在管理中心上把策略规则保存下（注意：规则不能额外加上空格等字符），再验证下问题是否修复

### 1.4 中心服务启动失败/加载日志失败

问题：服务安装所在的硬盘无剩余空间，导致服务重启失败。

问题原因:服务所在的数据库文件log.h2.db过大，大于2G，需要清理下，wins和Linux处理方法一样

处理方法：

步骤1.停止管理中心服务

步骤2.将管理中心安装目录Server/etc/下log.开头的文件(3个)删除

步骤3.从相同版本管理安装包里取log.h2.db放在管理端安装目录server/etc下

步骤4.重启启管理中心服务

### 1.5 防护规则不生效

在管理端上对端服务配置了策略并且保存后，触发防护规则不生效

处理方法：

步骤1. win监控端sc query ppsdrv查看驱动状态，linux查看驱动是否启动lsmod |grep Web\*

步骤2. 检查端服务器服务安装目录下的WebGuardAgent.dat规则文件是否有规则

步骤3. 删除现有的规则文件WebGuardAgent.dat，将驱动服务和端服务进行重启，重新下发规则（驱动和服务重启方法将前面的步骤参考1.3）

步骤4. 如果规则还是没有生效（注意添加得规则不要带空格等非法字符），确定驱动状态是1，则更改安装目录edr下得config.xml，debug\_log值改为1后，执行dmesg将内核日志信息输出到/tmp/1.log，发我

## 二. 新版本防篡改10.5问题处理思路

##### 本节主要面向具体的环境准备。

服务功能介绍、安装目录、及端口、排查日志

edrcenter服务：中心管理服务，平台所有的服务业务都由它下发管理，提供网页访问

安装目录：/usr/local/EDRCentral

服务端口：443

服务排错日志：/usr/local/EDRCentral/logs/server.log

服务启动方式：/etc/init.d/edrcenter restart

rpc-server服务：通信管理服务，负责与端agent服务的通信80端口（2010版本为10571端口）:

安装目录：/usr/local/dbappsecurity/rpc\_service

服务端口：10571

服务排错日志：/usr/local/dbappsecurity/rpc\_service/runlog/rpc\_service.rpc.log

/usr/local/dbappsecurity/rpc\_service/runlog/runlog.log

服务启动方式：/etc/init.d/rpc-server restart

edrdatacenter服务：负责对日志/报表数据/告警统计数据的写入和查询，对中心服务和es服务承上启下的作用，接受中心服务信令对es服务进行控制管理

安装目录：/usr/local/EDRDatacenter

服务端口：9400

服务排错日志：/usr/local/EDRDatacenter/log/data-center.log

服务启动方式：/etc/init.d/edrdatacenter restart

es服务: 提供动态数据的存储，如告警日志，防护日志等

安装目录：/opt/elasticsearch-7.5.1

服务端口：9200(主要端口) 9300

服务排错日志：/opt/elasticsearch-5.2.2/logs/edrlog.log

服务启动方式：/etc/init.d/es restart

mysql服务：提供静态数据的存储，如用户信息/许可信息等

安装目录：/opt/mysql

服务端口：3306  
 服务排错日志：/var/log/mysqld.log

服务启动方式：/etc/init.d/mysqld restart

edr-tomcat服务：提供离线升级包/病毒库/漏洞库等上传服务

安装目录：opt/tomcat9.0/

服务端口：8080

服务排错日志：opt/tomcat9.0/logs/catalina.out

服务启动方式：/etc/init.d/edr-tomcat restart

##### ****Q1.如何分配磁盘更合理？****

WPT的所有信息均存储在根目录（/）下，其中日志（es服务）和数据存储在/opt目录下，中心服务，datacenter服务rpc服务/更新包和库文件存储在/usr/local目录下。

**方案1**.根据[用户手册开局指南2.1.1](https://61.164.47.206:65526/2azbs/21.md)，对磁盘空间进行分配。如磁盘空间不足，建议对/目录挂载的的磁盘进行扩容，扩容方法百度很多；

**方案2**.新增2块磁盘，分别挂载到/opt和/usr。根据客户实际的情况判断日志数据和更新包（补丁包）的可能数量进行分配，一般建议比例为3:2，如需要扩容500G则/opt下挂载300G，/usr下挂载200G。

##### ****Q2.中心已安装，发现磁盘空间不足怎么办？****

WPT的所有信息均存储在/目录下，其中日志和数据存储在/opt目录下，更新包和库文件存储在/usr目录下。

**方案1**.对/目录挂载的的磁盘进行扩容(热扩容)，扩容方法百度查询；

**方案2**.有多余磁盘，重新进行磁盘挂载，操作步骤：

1、对服务器做镜像文件，便于异常回退，做镜像方法百度查询；

2、备份数据库，将备份的文件导出到本地：执行：mysqldump -u root -p xuerui123!@# >backup.sql，数据库密码联系项目经理或确认现场是否更改过密码。如提示bash:mysqldump:未找到命令，则执行：ln -fs /opt/mysql/bin/mysqldump /usr/bin/。

3、卸载wpt管理中心，在安装包解压目录执行unstall.sh；

4、参考Q1-方案2进行磁盘挂载处理；

5、重新上传安装包，安装edr；

6、将backup.sql传到任意目录，执行：mysql -u root -p -P3306 edrserver < backup.sql

7、重启中心服务edrcenter，/etc/init.d/edrcenter restart。

8、netstat -ntlp检查端口启动情况，确保端口正常启动。

**Q3.EDR磁盘满了导致服务起不来了怎么办？**

**步骤1.可清理的内容有：垃圾文件、补丁、运行日志、防护日志（占大头，一般防护日志清理后空间即可释放）。**

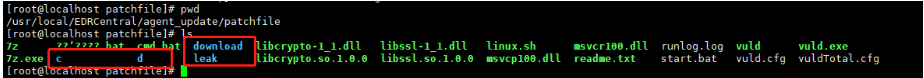
**垃圾文件**：

/usr/local/EDRCentral/upload/plateform/下所有文件

/usr/local/EDRCentral/upload/patch\_update/下所有文件

**补丁**：——该步骤执行结果会清空所有补丁

/usr/local/EDRCentral/agent\_update/patchfile/下的文件夹



**运行日志**：查看本节环境介绍

**防护日志**：（前提是es正常启动）——该步骤执行结果会清空所有防护日志

清除所有日志：curl -XDELETE '127.0.0.1:9200/edr-用户'，用户为当前租户名，此处为英文字母小写。

清除所有流量画像数据：curl -XDELETE '127.0.0.1:9200/traffic-用户'，用户为当前租户名，此处为英文字母小写。

**数据库：**——该步骤执行结果会清空系统性能监控信息

执行停止edrcenter服务service edrcenter stop

执行mysql -u root -p 输入密码（xuerui123!@#），use edrserver;

执行truncate table cpu\_performance; truncate table mem\_performance; truncate table net\_performance;

**步骤2.按以下顺序重启所有服务**:mysql es wpsdatacenter edr-tomcat rpc-server edrcenter

##### 本节主要面向客户方需求：修改各个服务的端口号；多网卡的情况、地址映射的情况、内外网均有客户端的情况；中心安装客户端；中心修改IP；中心迁移。

##### ****Q1.如何修改中心的RPC默认的80端口？****（2.0.10后版本为10571端口，修改步骤相同）

**步骤1.**修改/usr/local/dbappsecurity/rpc\_service/config.xml中的<var name="listen" value="80"/>，并保存。

**步骤2.**修改/usr/local/EDRCentral/conf/agent.conf中的rpc.port，并保存。

**步骤3.**CentOS7以下操作系统执行iptables -I INPUT -p tcp --dport [端口] -j ACCEPT防火墙开放端口。CentOS7及以上无需操作。

**步骤4.**执行/etc/init.d/rpc-server restart和/etc/init.d/edrcenter restart。

##### ****Q2.如何修改中心默认的443端口？****

**步骤1.**修改/etc/WebGuard/Server.conf中的HttpPort，并保存。

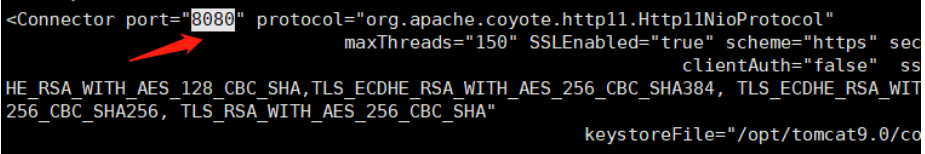
**步骤2.**修改/opt/tomcat9.0/webapps/ROOT/WEB-INF/classes/application.properties中的edr.url，并保存。

**步骤3.**CentOS7以下操作系统执行iptables -I INPUT -p tcp --dport [端口] -j ACCEPT防火墙开放端口。CentOS7及以上无需操作。

**步骤4.**执行/etc/init.d/edr-tomcat restart和/etc/init.d/edrcenter restart。

**Q3.如何修改中心tomcat默认的8080端口？**

**步骤1.**修改/opt/tomcat9.0/conf/server.xml中的Connector port，如下图，并保存。



**步骤2.**修改/usr/local/EDRCentral/conf/agent.conf中的update.port，并保存。

**步骤3.**CentOS7以下操作系统执行iptables -I INPUT -p tcp --dport [端口] -j ACCEPT防火墙开放端口。CentOS7及以上无需操作。

**步骤4.** 执行/etc/init.d/edr-tomcat restart和/etc/init.d/edrcenter restart。

##### ****Q4.内网环境部署的中心如何将平台映射到公网或其他网段使用？****

需修改中心配置文件/usr/local/EDRCentral/conf/agent.conf中四个参数：

先停止中心服务，再更改配置/etc/init.d/edrcenter stop

* domainName对应映射之后的IP
* domainPort对应edrcenter（443）映射之后的端口
* RpcDomainPort对应rpc-server（10571）映射之后的端口
* UpdateDomainPort对应edr-tomcat（8080）映射之后的端口

配置完成后执行/etc/init.d/edrcenter restart

##### Q5.如何配置WPT管理中心使内外网都可以下载安装包？

**步骤1.**确定已配置好映射（映射到公网或其他网段或多网卡）：

参考Q4配置，验证外网登录等功能是否正常

**步骤2.** 上述配置生效后，浏览器地址栏中的IP与WPT“添加资产”处提供的下载链接一定是一致的。通过访问对应的IP打开WPT管理中心，即可通过对应的地址下载安装包。

**步骤3.** 更换IP登录EDR管理中心后，安装包携带的配置参数通常是初始配置参数，需执行rm -rf /usr/local/EDRCentral/download/windows/租户名，删除旧的安装包，再打开网页使其产生新的安装包。Windows、Linux64位、Linux32位三个安装包对应的路径分别为：

* /usr/local/EDRCentral/download/windows/租户名
* /usr/local/EDRCentral/download/linux/x64/租户名
* /usr/local/EDRCentral/download/linux/x86/租户名

##### Q6.WPT****中心改IP的步骤****

登录中心服务器后台：更换IP后执行service edrcenter restart 重启中心服务

登录客户端服务器后台：

**步骤1.**停止agentservice服务。

Linux执行service rpc-server stop 或者 /etc/init.d/edr-server stop

Win命令行执行sc stop agentservice 或者 wins服务管理停止服务

**步骤2.**修改安装目录下的config.xml。

Linux默认位置：/usr/local/dbappsecurity/edr/

Win默认位置：C:\Program Files \\(x86\\)\DBAppSecurity\EDR\

**步骤3.**启动Agentservice服务。

Linux执行service rpc-server start 或者 /etc/init.d/edr-server start

Win命令行执行sc start agentservice 或者 wins服务管理启动服务

##### Q7.****如何在不影响客户端与中心绑定关系的情况下迁移中心？****

前提条件：新管理中心**租户名**与**IP**必须与老管理中心保持一致。

注意：如提示bash:mysqldump:未找到命令，则执行：ln -fs /opt/mysql/bin/mysqldump /usr/bin/

**步骤1.**登录老管理中心导出数据库。执行：mysqldump -u root -p edrserver >backup.sql，数据库密码联系项目经理

**步骤2.**登录新管理中心，将backup.sql传到任意目录，执行：mysql -u root -p -P3306 edrserver < backup.sql。

**步骤3.**执行mysql -u root -p 输入密码，执行use edrserver;，delete from user\_lic;，delete from lic;，/etc/init.d/edrcenter restart。

**步骤4.**原先的安装包携带的配置参数通常是初始配置参数，需执行rm -rf /usr/local/EDRCentral/download/windows/租户名，删除旧的安装包，再打开网页使其产生新的安装包。Windows、Linux64位、Linux32位三个安装包对应的路径分别为：

* /usr/local/EDRCentral/download/windows/租户名
* /usr/local/EDRCentral/download/linux/x64/租户名
* /usr/local/EDRCentral/download/linux/x86/租户名

**步骤5.**申请许可，导入许可即可。

**本节内容：查服务、查端口、查日志、查文件。**

##### ****Q1.WPT客户端日志在哪里？****

默认安装路径下：

Windows：C:\Program Files (x86)\DBAppSecurity\EDR\runlog

Linux：/usr/local/dbappsecurity/edr/runlog

##### ****Q2.中心上，客户端安装包所在的路径？****

Windows：/usr/local/EDRCentral/download/windows/

Linux64位：/usr/local/EDRCentral/download/linux/x64/

Linux32位：/usr/local/EDRCentral/download/linux/x86/

##### ****Q3.弱口令字典、隔离区、文件推送的路径？****

默认安装路径下：

Windows：

弱口令字典： C:\Program Files \(x86\)\DBAppSecurity\EDR\config\login\weakpsd.dat\

隔离区： C:\Program Files \(x86\)\DBAppSecurity\EDR\config\antiav\quarantine\

文件推送位置：C:\Program Files \(x86\)\DBAppSecurity\EDR\config\upload

Linux：

弱口令字典：/usr/local/dbappsecurity/edr/config/login/weakpsd.dat

隔离区：  
/usr/local/dbappsecurity/edr/config/antiav/quarantine/

文件推送位置：/usr/local/dbappsecurity/edr/config/upload

##### ****Q4.补丁的路径？****

中心：

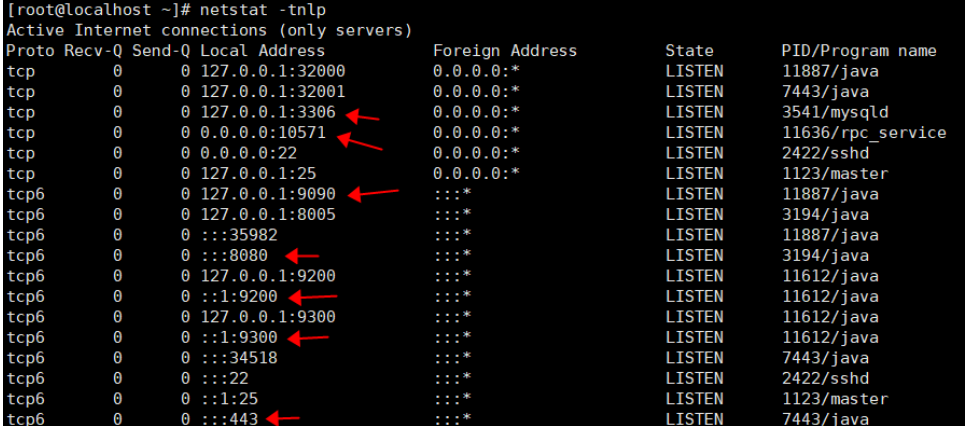
/usr/local/EDRCentral/agent\_update/patchfile/下的文件夹

windows客户端：

C:\Program Files (x86)\DBAppSecurity\EDR\hotfix

##### 本节讲述中心管理端异常处理办法：端口未开放、中心访问报错、界面转圈圈、日志无数据、客户端无法下载、中心上传失败。

##### 中心安装完成后，使用netstat -tnlp命令检查端口开放情况。是否如下图所示10571、443、3306、8080、9200、9300、9090正常开放，LISTEN状态。



排查思路：

1、服务未启动，重启服务，命令参考1.1Q1环境服务介绍

2、启动失败（基本是硬盘空间和内存空间不足），则检查基础环境，df -h 查看磁盘空间，要求根目录空闲空间>8GB且>15%，cat /proc/meminfo检查内存情况，要求MemFree+Buffers+Cached不可低于2G（极端情况）。

3、查看相应服务的日志，日志文件路径参考1.1Q1环境服务介绍

##### ****Q1.初次安装完中心程序查看到9200、9300端口未开放如何排查？****

es服务未启动，会导致Web首页和日志检索数据无法正常显示（告警日志等数据不能写入到es数据库中）。

**步骤1.**执行/etc/init.d/es start看是否可以直接启动。

**步骤2.**上步无法启动则排查是否是内存不足导致，执行cat /proc/meminfo，MemFree+Buffers+Cached不可低于2G（极端情况），若内存不足，考虑扩容

##### ****Q2.初次安装完中心程序查看到9400端口未开放如何排查？****

edrdatacenter服务未启动，会导致Web首页和日志检索数据无法正常显示(该服务得作用是将告警数据写入到es库中)

**步骤1.**执行/etc/init.d/edrdatacenter start看是否可以直接启动。

**步骤2.**上步无法启动则排查是否是内存不足导致，执行cat /proc/meminfo，MemFree+Buffers+Cached不可低于128M（极端情况），若内存不足，考虑扩容

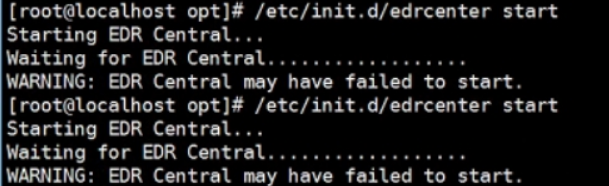
**Q3.初次安装完中心程序查看到8080端口（tomcat服务）未开放如何排查？**

**步骤1.**尝试执行/etc/init.d/edr-tomcat stop，和/etc/init.d/edr-tomcat start，重启tomcat服务。

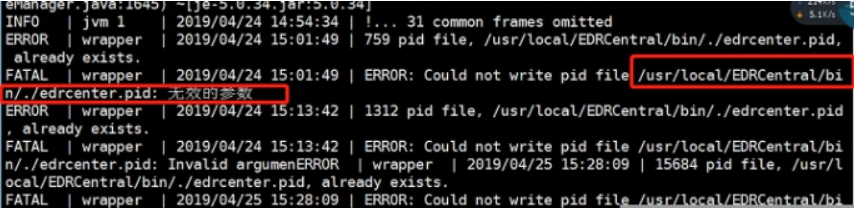
##### ****Q4.初次安装完中心程序查看到443端口未开放如何排查？****

**步骤1.**尝试执行/etc/init.d/edrcenter restart重启edrcenter服务。

##### Q5.****管理中心启动EDR central may have failed to start.****



**步骤1.**查看中心/usr/local/EDRCentral/logs/server.log日志。



**步骤2.**从日志里看到/usr/local/EDRCentral/bin/edrcenter.pid为无效参数，rm –f edrcenter.pid文件。

**步骤3.**重启中心服务/etc/init.d/edrcenter start。

##### Q6.****部署完成后，输入账号密码登录，登录界面不断刷新无法进入？****

**步骤1.**在中心执行/etc/init.d/edrcenter restart，然后重新登录。

**步骤2.**若步骤1无效，中心执行ifconfig查看中心IP和实际访问IP是否相同，如果是IP映射到公网或其他网段，中心也要进行配置，参考内外网映射配置

**步骤3.**ifconfig查看机器网卡信息，如果有2块网信息，访问的地址可能是另外一块网卡地址，则执行vi /usr/local/EDRCentral/conf/agent.conf，domainName=xxx.xx.xx.xx(另一块网卡地址)，domainPort=443(默认端口)，RpcDomainPort=80(默认端口)。

**步骤4.**重启中心服务/etc/init.d/edrcenter restart。

##### Q7.****访问中心报404（WPT的404界面）。****

可能是浏览器不满足Google Chrome 49+的条件，更换高点版本得谷歌浏览器

##### Q8.管理平台验证用户名密码错误?

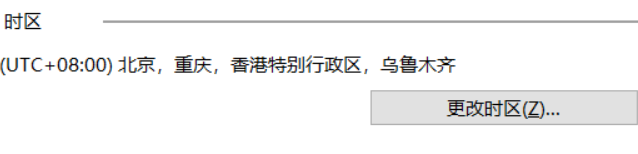
1、可能是管理端时区不对导致。需要更改为东八区，修改方法：

rm -f /etc/localtime

ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

/etc/init.d/edrcenter restart

2、访问管理平台页面的主机时区不对导致。需要更改为东八区（UTC+08:00）



3、联系项目经理获取恢复密码脚本。

##### Q9.****平台登录提示“该账户登录人数已达到上限”无法登录如何解决？****

**原因：**达到了租户的登录限制个数、未注销且未到超时时间。

**解决办法：**在管理中心服务器执行service edrcenter restart释放所有连接。

建议admin账户登录将租户的超时、锁定、登录限制个数建议设置为30、15、5。

##### Q10.****使用平台管理主机时无任何日志或首页无数据转圈是什么原因？****

安装完测试无日志和使用一段时间后开始无日志，都是es或wpsdatacenter服务未启动成功或异常停止导致。通过以下步骤排查：

**步骤1：**中心上执行netstat –tnlp，若是9200、9300端口没有开启则是es服务未启动。若是9400端口没有开启则是edrdatacenter服务未启动。执行service es restart或service edrdatacenter restart是否可以直接成功重启。

**步骤2：**重启失败则排查是否是内存不足导致。

es服务未启动：执行cat /proc/meminfo，MemFree+Buffers+Cached不可低于2G；

edrdatacenter服务未启动：执行cat /proc/meminfo，MemFree+Buffers+Cached不可低于128M；

**步骤3：**排查是否是磁盘空间不足导致

在/opt目录下执行df -hl，挂载点/的可用空间不足则无法继续写入日志。

**步骤4：**排除以上问题后，可能是数据中心的模板索引没有生成导致，执行以下命令：

service edrcenter stop

curl -XDELETE '127.0.0.1:9200/edr-用户名'

curl -XDELETE '127.0.0.1:9200/traffic-用户名'

cd /opt/EDR/edr（如果不是安装在/opt目录则/opt替换为相应的安装目录）

sh installESTemplate.sh

sh installTrafficTemplate.sh

service edrcenter restart

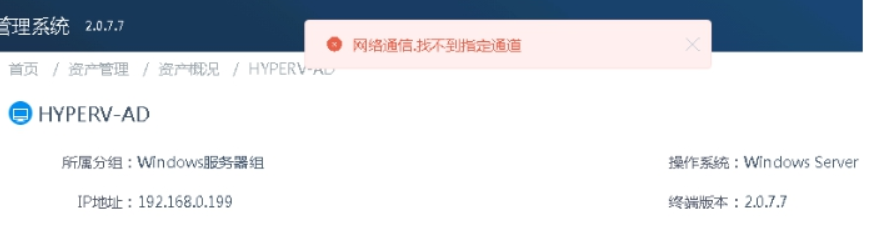
**步骤5：**查看/etc/hosts，如果中心hostname不是127.0.0.1，需要改为127.0.0.1，参考步骤6

（如果中心的hostname不是127.0.0.1且由于业务需求不能改，则修改EDR的wrapper，参考步骤7。）

**步骤6：**打开/etc/hosts，添加127.0.0.1 hostname，保存，执行service edrcenter restart。

**步骤7：**修改edrcenter的wrapper，在/usr/local/EDRCentral/wrapper/conf/wrapper.conf里添加wrapper.java.additional.5=-Djava.rmi.server.hostname=xxxxx，这里的xxx是/etc/hosts里的IP。保存，执行service edrcenter restart。

##### Q11.****网络通信找不到指定通道？****



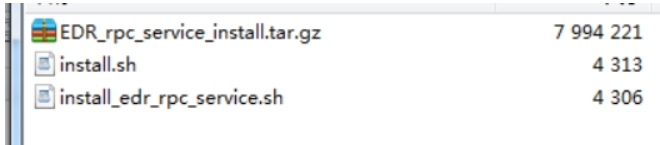
**步骤1.**登录管理中心后台，netstat –lnt查看10571端口是否监控，如果缺少10571端口，则rpc-server服务未启动或是异常。

**步骤2.**重启rpc服务/etc/init.d/rpc-server restart。

**步骤3.**启动rpc服务/etc/init.d/rpc-server restart如果启动异常，则需要重装rpc服务，见步骤4。

**步骤4.**用7z打包下载的edr.tar.gz安装包，将EDR\edr-rpc-service\下的文件拖出来，传到中心服务器上。

**步骤5.**执行install.sh安装rpc。



##### Q12.无法下载监控端安装程序？

**步骤1.**下载跳转的链接IP地址是否和跳转前一致。不一致检查管理中心的/usr/local/EDRCentral/conf/agent.conf中的rpc.ip是否和网卡地址一致、若配置了domainName则domain相关四个参数都不可为空。

**步骤2.**步骤1无异常则在管理中心操作系统执行netstat -tnlp查看10571端口是否开放,

**步骤3.**10571端口开放则在当前浏览器所在主机通过telnet测试10571端口是否通。不通则检查中心防火墙配置(中心服务得防火墙关闭：service iptablesstop)或其他网络设备是否拦截。

##### Q13.离线安装包上传失败怎么办？

每一步执行完成后，均需尝试下是否能成功上传，失败则再进行下一步确认；

**步骤1.**刷新浏览器缓存；

**步骤2**.检查网络通信，上传走8080（tomcat服务）端口，cmd执行telnet 中心IP 8080确认网络通信是否正常，不通则调整网络策略；

**步骤3**.检查上传包是否正确，是否为tar.gz后缀的压缩包（windows客户端为.exe）；

**步骤4.**确认是否进行了地址映射，该情况下需要进行配置，详见4.1-Q4；

**步骤5.**确认edrcenter端口是否有改动，如改动，则需要确认/opt/tomcat9.0/webapps/ROOT/WEB-INF/classes/application.properties中的edr.url端口号是否与修改后的edrcenter端口号一致；

**步骤6.**尝试重启edr-tomcat,命令：service edr-tomcat stop,service edr-tomcat start；

**步骤7.**检查根目录下磁盘剩余空间是否充足；

**步骤8.**查看edrcenter日志，查找失败原因。

**注意：**离线补丁包上传，压缩包是由客户自行压缩成tar.gz的，要确保压缩方式正确。

### Q14.WPT中心首页web验证码乱码或为空

**平台首页登录页面验证码为空或显示乱码，原因是服务器上缺少需要的字体（Arial,Courier,Helvetica）**

**步骤1. fc-list 查看环境，如无上述字体中的一种，可通过yum 和网上下载字体安装包解决**

**yum -y install Arial / Courier / Helvetica**

**步骤2. 如果提示没有fc-list命令也可以用yum安装 yum -y install fc-list**

**步骤3，若yum安装字体失败，则通过互联网下载字体tar包上传到服务器安装**

### Q15.中心管理服务器ssh连接断开，平台服务即停止

**安装好程序后，断开ssh连接，平台就登录不上**

**问题原因：centos7以上系统启动ssh服务的方式不同，需要将其改为service启动**

**出现改问题一般是系统centos7以上，问题原因是ssh启动的服务不同**

**步骤1. 改变启动ssh的服务由socket改为service，重装管理中心**

**步骤2. 如何改变ssh服务的启动服务参考博客：**

**https://zzz.buzz/zh/2015/12/26/configure-port-of-sshd-in-systemd-environment/**

### Q16.添加许可后登录租户提示用户未授权

**问题原因：1.许可授权生效时间与中心服务器时间存在差异 2.租户许可数量未配置添加**

**步骤1. 许可生效得与服务器时间不一致，校正服务器得时间(百度查询如何更改linux/wins服务器时间)**

**步骤2.删除许可信息表数据，在中心管理服务器后台上操作执行命令**

mysql -u root -p

输入密码： xuerui123!@#

use edrserver;

delete from lic；

delete from user\_lic;

### 17．端服务器的监控端口等信息在中心上不能显示

**问题原因：wins端服务器上的服务有中文名称的，我们的服务不能识别**

**处理步骤1. 查看端服务器上得任务管理器--服务有中文名称得服务，因为程序存在得bug，对于中文字符不能转义，所以端口信息会显示失败。临时解决办法把这个中文程序停止，后续程序修复这个bug ，如有问题将rpc日志发送给我**

##### 本节讲述客户端异常处理办法：驱动、安装、升级、卸载。

##### ****Q1.Windows主机上双击执行安装包闪退是什么原因？****

**步骤1.**系统核心服务Base Filtering Engine未开启，会造成网络驱动无法启动，开启Base Filtering Engine服务即可。

**步骤2.**可用内存小于300M会造成无法安装。

**步骤3.**当前磁盘空间小于200M会造成无法安装。

##### ****Q2.安装过程中弹窗报”与管理平台通信失败，错误信息为：Couldn’t connetc to server...”如何解决？****

**步骤1.**参考Q6到端上WPT安装路径下，查看config.xml中两处IP地址是否是正确的IP地址（内外网用同一个中心的话，保证当前访问的内/外网中心IP、端口可通）。

**步骤2.**步骤1无误，通常是网络问题，Windows端上cmd执行telnet中心IP （Linux端上执行命令相同），访问不通则是网络限制问题，需网络管理员自行排查直到端口通。（2.0.10端口合一，telnet 中心IP RPC端口，WPT中心新安装的PRC端口为10571，）

##### Q3.****Linux客户端安装完成报“can’t read‘netfilter\_edr.ko’”或“can’t read‘sysmon\_edr.ko’”?****

原因：是由于安装包里没有此操作系统的内核版本对应的上述驱动文件。

操作步骤：

1、执行uname -a将结果发给项目经理进行内核编译工作；

2、提供编译所需的内核头文件，将 /lib/modules下的文件和/usr/src/Kernel下的文件打包成.tar.gz发送给项目经理；

3、一小时到一天时间不等，完成一个版本的内核编译工作。

4、内核文件操作步骤：

方案一：端agent服务在服务器上已经安装成功只是无驱动

将项目经理提供的内核文件，分别更名为sysmon\_edr.ko和netfilter\_edr.ko，上传到/usr/local/dbappsecurity/edr目录下，重启edr-server即可

方案二：端agent服务未在服务器上执行安装脚本，则替换到整包中

将项目经理提供的内核文件，不更改名称，放到端服务得安装包目录下如：

\linux\_agent\_setup\_2.0.13.1.x64.tar.gz\linux\_agent\_setup.tar.gz\linux\_agent\_s\ko\x64或者x32

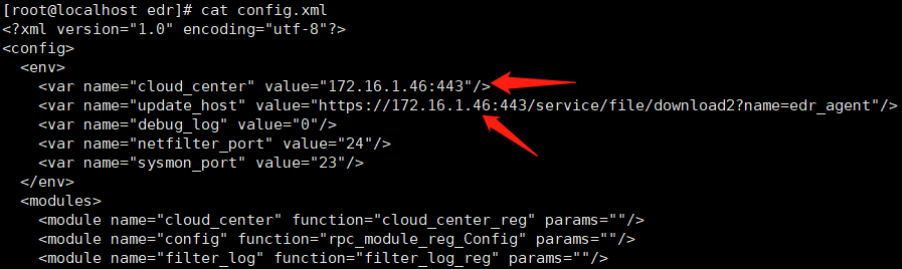
再将端服务得安装包以admin账户登录WPT平台，上传替换原本的Linux安装包即可正常安装。

##### ****Q4.客户端程序安装成功但平台上无显示如何排查？****

**步骤1.**登录平台查看许可是否有剩余数量或是否到期，通过增加许可数量或延期解决。

**步骤2.**Windows端上cmd执行telnet中心IP 10571（Linux端上执行命令相同），访问不通则是网络限制问题（通过关闭服务器防火墙），或需网络管理员自行排查直到端口通

**步骤3.**参考Q6到端上EDR安装路径下，查看config.xml中两处IP地址是否是正确的IP地址（内外网用同一个中心的话，保证当前访问的内/外网中心IP、端口可通）。正确的形式应如下图所示：



**步骤4.** 检查服务器编码格式是否为UTF-8，如不是，则调整为UTF-8。

**Q5.客户端程序安装成功平台上可见但是灰色（离线）如何排查？**

问题原因：驱动问题

**步骤1.**中心端口是否正常开放。执行netstat –tnlp 10571端口未开执行service rpc-server start。

**步骤2.**Windows端：AgentService服务是否启动成功。端上查看服务AgentService状态，状态为已停止则启动服务。Linux端：edr-server服务是否启动成功。通过执行service edr-server restart排除此问题。

**步骤3.**

**Wins版本：**

**查询驱动运行情况：sc query sysmon（4：runing表示正在运行）；**

**重启端服务：net stop/start Sysmon\_edr ，如命令启动失败，可在服务管理对agent-server服务进行重启**

**卸载驱动重装：先停止服务，再rmmod sysmon\_edr.ko ， 重新启动端服务， 该文件会自动生成（一般不用卸载驱动重新加载）**

**Linux版本：**

**查询驱动运行情况：lsmod |grep sysmon (sysmon\_edr 1表示运行 0表示停止，2表示异常)**

**重启端服务：/etc/init.d/edr-server stop / restart / start**

**卸载驱动重新加载：先停止服务，再rmmod sysmon\_edr.ko ，重新启动端服务，该文件会自动生成，再看下驱动运行状态（一般不用卸载驱动重新加载）**

**步骤4.**如上述检查完毕，仍无法解决，查询runlog.log。日志位置：

Windows：C:\Program Files (x86)\DBAppSecurity\EDR\runlog

Linux：/usr/local/dbappsecurity/edr

##### Q6.****客户端部分在线部分离线？****

**步骤1.**登录离线客户端，运行—cmd打开命令行窗口，sc stop agentservice停止服务。

**步骤2.**修改安装目录下C:\Program Files (x86)\DBAppSecurity\EDR\config.xml将<var name="debug\_log" value="0"/>处的“0”改为1。

**步骤3.**在命令行窗口cd C:\Program Files (x86)\DBAppSecurity\EDR 打开winscmd窗口执行AgentService.exe runcmd，如果日志有下以下报错



**步骤4.**修改中心安装目录vi /usr/local/EDRCentral/conf/agent.conf，查看rpc.ip=本机真实IP。

**步骤5.**重启中心服务/etc/init.d/edrcenter restart。

##### Q7.****客户端如何手动绑定中心？****

**Windows：**双击执行下安装目录下C:\Program Files (x86)\DBAppSecurity\EDR\bind.bat，粘贴由中心租户登录后，系统设置-添加资产页面获得的管理员识别码。回车即可。

**Linux：**执行/usr/local/dbappsecurity/edr/bind uuid，其中uuid是由中心租户登录后，系统设置-添加资产页面获得的管理员识别码。

##### Q8.****客户端如何手动升级？****

客户端安装路径下，cmd执行update.exe start。

##### Q9.客户端****升级失败，update.log报MD5 error等。****

所有上传到管理平台的文件，均会包含md5附加文件，以验证下载文件的完整性。出现MD5值不匹配有可能是因为中间件jetty本身的BUG会导致在网速慢的时候下载失败。网络较好的时候再尝试。

##### ****Q10.卸载WPT客户端时找不到卸载程序uninstall.exe是什么原因？此时如何卸载？****

可能是由于第一次执行卸载程序时，卸载行为触发了其他安全软件的防护机制，破坏了WPT程序的完整性，导致无法正常卸载。

**步骤1.**到其他安全软件隔离区是否可以找回重新执行。

**步骤2.**cmd分别执行sc stop agentservice、sc delete agentservice、sc stop nfw、sc delete nfw、sc stop sysmon、sc delete sysmon，到控制面板卸载程序。

**步骤3.**存在卸载残留或无法通过控制面板卸载则强制删除安装目录下剩余文件，并重启主机（正常卸载是不需要重启的，此时情况异常）。

##### ****Q11.中心是否可安装WPT客户端？如何安装？****

可以装在一起，尽量不这么做

**步骤1. 先**将客户端安装包下载到服务器上，然后停止通信服务service rpc-server stop。

**步骤2 .**删除/etc/ahedr/agent.conf （如无则不管）。

**步骤3. 手动解压**安装客户端，安装完成执行service rpc-server start开启rpc服务。

**步骤4.** 执行/usr/local/dbappsecurity/edr/bind uuid，其中uuid是由中心租户登录后，系统设置-添加资产页面获得的管理员识别码。

##### ****Q12.防护不生效或者防护生效后不产生告警日志****

**问题原因：1.驱动问题（驱动重启，重新下发规则） 2.es日志模板未导入成功需要重新导入**

**问题类型1：防护不生效问题：**

**Wins版本：**

**查询驱动运行情况：sc query sysmon（4：runing表示正在运行）；**

**重启端服务：net stop/start Sysmon\_edr ，如命令启动失败，可在服务管理对agent-server服务进行重启**

**卸载驱动重装：先停止驱动，再rmmod sysmon\_edr.ko ， 重新启动端服务，该文件会自动生成**

**Linux版本：**

**查询驱动运行情况：lsmod |grep sysmon (sysmon\_edr 1表示运行 0表示停止，2表示异常)**

**重启端服务：/etc/init.d/edr-server stop / restart / start**

**卸载驱动重新加载：先停止驱动，再rmmod sysmon\_edr.ko ，重新启动端服务，该文件会自动生成，再看下驱动运行状态**

**注意：如重启驱动后问题依旧存在，可以再次停止驱动后，将规则文件（WebGuardAgent.dat）删除，重启驱动后再在管理端重新对端进行规则策略下发:**

**若Linux下WebGuardAgent.dat规则文件不允许删除可以对内容清空（Linux 下命令echo 空格 >WebGuardAgent.dat）**

**重新启动驱动后，在管理中心上重新下发保存规则**

**注意：添加规则时候注意不能加上无意义的空格等非法字符哦**

**问题类型1：防护生效后不产生告警日志**

**问题原因：1.内存不足 2.es服务所在的硬盘空间不够 3.es模板问题**

**处理方法：**

**1.如果在部署中心服务时更改了es服务端口：需要更改datacenter配置文件中配置的es的端口再执行中心问题处理es模板重新导入**

##### ****Q13. 配置网站防护不能生效****

**问题原因: 1.java web防护模块未安装配置，2.web服务器jdk和tomcat使用环境没找对，文件替换错误 3.现场网络ip映射未确认实际需要屏蔽的ip**

**处理方法：**

**Wins版本：**

**jdk环境实际安装路径查找方法：**

**1.在cmd下输入java -verbose 最下面两行打印路径**

**2. 在cmd下输入：set java\_home**

**tomcat重启方法：cmd下：net stop/start tomcat 或者找到安装目录bin文件下找到执行脚本重启（start.bat / shutdown.bat）**

**Linux版本：**

**jdk环境实际安装路径---如配置了环境变量查询方法：echo $JAVA\_HOME**

**未配置java环境变量查找方法：1.which java 2. ls -ltr a （a:表示前一步的执行结果）找到实际使用的tomcat和java变量后进行防护模块的配置即可。**

**配置tomcat的web.xml文件时注意：直接从文档张贴配置内容可能因为wins和linux字符原因导致tomcat启动时读取web.xml文件失败，可以先把内容放到nodpad++中选择ntf-8编码格式后，再复制添加到web.xml配置文件中**

##### ****Q14. 父目录允许修改，子目录被阻止****

**配置策略允许改写的目录，其子目录还会被阻止**

**问题原因：驱动有关（重启驱动重新下发规则） 添加的规则存在额外的空格等非法字符**

**处理方法：**

**1). 停止驱动，删除规则后，启动驱动 重新下发规则 (参考前一步骤)**

**2). dmesg命令查看：insmod: page allocation failure: order:5，这个错误提示说明服务器内核得内存不够，规则就不能生效，需要手动触发服务器回收内核内存或者等服务器自动回收**

**.添加得规则进程名称不能有空格**

##### 本节讲述发布端异常处理办法

##### ****Q1. 发布端文件同步问题****

发布端同步文件失败，或者同步的文件发现少了？

问题原因：1.rsyns服务未启动 2.同步的目录文件过大性能不足

处理方法：

1). ps -ef |grep rsync 查看同步服务是否正常，将rsync服务重启

2). 查看发布目录要发布的文件的大小，同步的文件大于30G会因为性能问题导致同步时间过长或者同步后客户端少文件。将同步的目录改为当前目录的下一级目录，尽量避免每次同步文件太大