**P9.3版服务器注意事项**

# 版本号

P9.3-20200323（V40753）

# 注意事项

## 中转服务器授权

支持后台直接导入授权，暂不支持通过管理平台页面导入授权

## 支持异地S3（默认禁用，按需开启）

/var/lib/tomcat7/webapps/DLP/WEB-INF/classes/application.properties

/var/lib/tomcat7/webapps/operationService/WEB-INF/classes/application.properties

enable.off.site.data=false,是否启用异地S3 (true为启用,false为禁用)

data.store.bucket=version,异地S3桶名

说明：后台配置后，需重启tomcat7

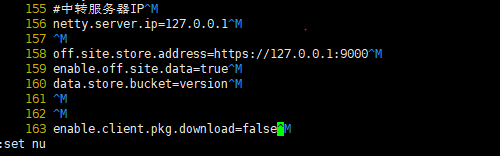
主服务器一体化部署、异地s3配置，dlp和operationService目录配置需同时开、关

## 登录页面的终端下载链接默认关闭

主服务器配置文件： /var/lib/tomcat7/webapps/DLP/WEB-INF/classes/appliaction.properties

添加配置项：enable.client.pkg.download=false

配置项说明：false为不显示，true为显示，默认为false



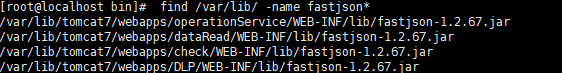
## 【安全要求】检查升级fastjson版本到1.2.67

升级完成后检查下列目录下只存在fastjson-1.2.67.jar不应存在其他版本：

* /var/lib/tomcat7/webapps/DLP/WEB-INF/lib/
* /var/lib/tomcat7/webapps/check/WEB-INF/lib/
* /var/lib/tomcat7/webapps/operationService/WEB-INF/lib/
* /var/lib/tomcat7/webapps/operationService/WEB-INF/lib/
* /var/lib/tomcat7/webapps/dateRead/WEB-INF/lib/
* /var/lib/tomcat7/webapps/operationServer/WEB-INF/lib/

如下截图为主服务器查看示例

# find /var/lib/ -name fastjson\*



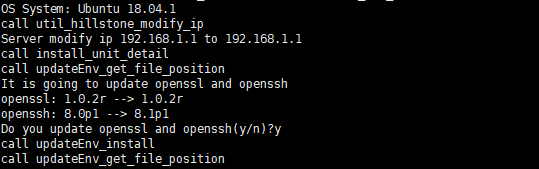
## 【安全要求】CentOS7.4系统下MySQL数据库升级

CentOS7.4系统下数据库版本升级到mariadb10.3.22



## 【安全要求】openssh升级至openssh8.1p1

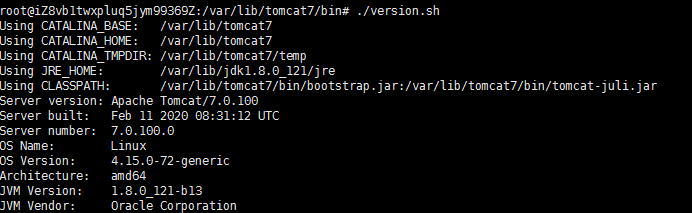
执行全新安装脚本/升级脚本第一步时会提示是否更新系统,升级OpenSSH到8.1p1，需手动确认升级，如下图：



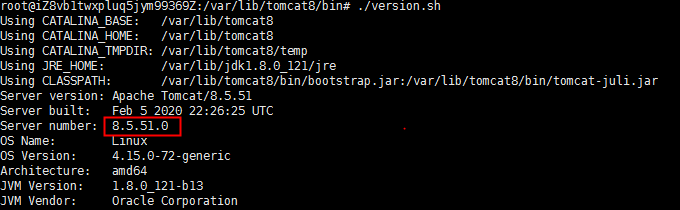
注：不支持centos7.2、不支持ubuntu14.04升级

## 【安全要求】tomcat7、8升级至最新版本

tomcat7最新版本为7.0.100.0



tomcat8最新版本为8.5.51.0



## 【安全要求】DLP管理平台访问的S3需默认关闭S3的WEB访问页面

s3配置文件写入配置MINIO\_BROWSER="off" ，实现s3web访问页面关闭

说明：

1 全新安装或者升级后（./upgrade.sh脚本执行后）配置默认写入

2如已有环境不进行升级，则手动修改配置文件

# vi /etc/default/minio

# 写入配置

# service minio stop 停止s3服务

# service minio start 启动s3服务

## 【安全要求】修补管理平台上mariadb5.6漏洞

方法：关闭mariadb服务，并使得服务器启动时也不自动启动

#systemctl stop mariadb

#systemctl disable mariadb

注意：以后用upgrade.sh升级管理平台，也执行上述两条命令

## 【安全要求】修补showmount -e 漏洞

方法：nfs服务有几个随机端口，更改配置，使得随机端口固定不变。并且设置防火墙只能指定的ip能访问nfs，可以运行showmount -e 显示nas共享目录

在提供nas共享的服务器上进行下列操作

具体步骤：

1 拷贝新的./util\_safe\_config.sh到/cirrusgate/bin目录下。(如果是新安装或升级过的，则/cirrusgate/bin/util\_safe\_config.sh下文件已经是最新的，可以跳过此步骤)

2 #cd /cirrusgate/bin

3 #./util\_safe\_config.sh -ip\_list\_save "nfs 192.168.44.140;192.168.44.145"

4 ./util\_safe\_config.sh -nfs\_config

5 查看一下/cirrusgate/config/cirrus\_firewall.ini文件，

有一行ip\_list\_nfs\_access=192.168.44.140;192.168.44.145

6 ./util\_safe\_config.sh

7 重启服务器

## dlp.log打印syslog内容

管理平台SYSLOG 配置后，后台dlp.log里面没有syslog的相关内容。需要在配置文件里switch置为true才可以

一级

[root@jszx-dlp-cs-01 classes]# cd /var/lib/tomcat7/webapps/DLP/WEB-INF/classes

[root@jszx-dlp-cs-01 classes]# cd /var/lib/tomcat7/webapps/operationService/WEB-INF/classes

二级

[root@jszx-dlp-cs-01 classes]# cd /var/lib/tomcat7/webapps/operationService/WEB-INF/classes

[root@jszx-dlp-cs-01 classes]# vi application.properties

Syslog.print.switch   由false-->true

[root@jszx-dlp-cs-01 work]#  systemctl stop tomcat7  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*停中间件

[root@jszx-dlp-cs-01 work]# cd  /var/lib/tomcat7/work/

[root@jszx-dlp-cs-01 work]# rm -rf \*                           \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*清缓存

[root@jszx-dlp-cs-01 work]# ls

[root@jszx-dlp-cs-01 work]# systemctl start tomcat7   \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*重启中间件

[root@jszx-dlp-cs-01 work]# ps -ef|grep tomcat7        \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*确认

## 触发终端熔断机制后策略再次生效操作

1. 触发终端熔断（终端熔断某一个策略）后，需要重新编辑保存这个策略才能在该终端上再生效
2. 触发策略熔断后，必须重新激活该策略，终端获取到新策略即可生效。

## 禁止使用root权限启动或停止服务器tomcat7/tomcat8服务

**特别重要：以下脚本禁止使用root权限启动或停止服务器tomcat7/tomcat8服务**

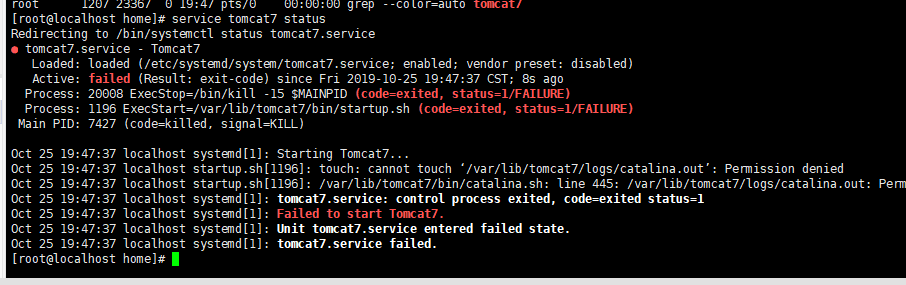
/var/lib/tomcat7/bin/shutdown.sh

/var/lib/tomcat7/bin/startup.sh

/var/lib/tomcat8/bin/shutdown.sh

/var/lib/tomcat8/bin/startup.sh

否则会出现如截图所示的报错，并导致服务启动异常无法登陆管理平台：



**特别重要：**tomcat重启是要用service或者systemctl命令去重启，不然会造成一些目录权限不对，页面会有一些问题，比如事件详情中截图出现裂图

## MAC终端白名单更新生效前提

MAC终端必须升级到最新版本才能同步生效服务器“终端白名单管理”中配置的白名单

## 【安全要求】MySQL数据库升级

本次全新安装的MySQL数据库已经是最新版本，从旧版本升级到P9之后可通过单独执行脚本进行数据库版本升级，但是由于MySOL数据库版本升级有可能对历史数据有未知影响风险，因此没有特别要求暂不建议升级MySQL数据库版本，除非项目安全需求必须升级版本再升级。

带数据升级MySQL数据库方法：

运行./install\_all\_falco\_with.log detail,选择others->Update to new version mysql

（升级过程中会先备份mysq的配置文件及数据库数据到/opt/backup\_cirrus/database）

注：数据库版本查看命令mysql -V

## 【安全要求】管理平台同一账号用户同时登录数配置

配置文件（/var/lib/tomcat7/webapps/DLP/WEB-INF/classes/spring-security.xml），默认值为100，即允许同一账号用户同时在线最大数为100；若只允许同一账号单用户登录，则把值改为1

## 【安全要求】增加对数据库限制访问IP功能

1. 安装包 ./config/setup.ini中配置默认mysql\_access\_ip\_list\_enable=1. 安装主服务器或mysql时，会要求输入可以访问MySQL的IP，只有这些IP和本机才能访问MySQL；如果不输入则允许所有IP连接数据库
2. 查看允许访问的IP，查看配置文件：/cirrusgate/config/cirrus\_firwall.ini
3. 如果限制了IP，需放开或者限制IP访问：

方法一：./install\_unit.sh 选择3) : Others 选择 3) : Config ip list mysql access

方法二：配置文件/cirrusgate/config/cirrus\_firewall.ini,在其中的ip\_list\_mysql\_access=填入允许访问MySQL的IP列表，用分号隔开，再运行/cirrusgate/bin/util\_safe\_config.sh,设置能访问MySQL的IP

注：install\_unit.sh可以用install\_all\_falco\_with\_log.sh detail代替，后者安装独立模块时也会记录日志到log/install\_unit.log中。（测试和实际使用时尽量用后者，便于从日志追溯安装过程。）

## 【安全要求】增加对Solr的限制访问IP功能

1. 当主服务器安装时，安装Solr时并不会提示输入指定IP访问Solr.
2. 可以用下面两种方式指定IP访问Solr：

方法一 运行./install\_unit.sh-->3) other->4) : Config ip list solr access,然后指定IP列表。

方法二 配置文件/cirrusgate/config/cirrus\_firewall.ini,在其中的ip\_list\_solr\_access=填入允许访问Solr的IP列表，用分号隔开；再运行/cirrusgate/bin/util\_safe\_config.sh,设置能访问Solr的IP

注：install\_unit.sh可以用install\_all\_falco\_with\_log.sh detail代替，后者安装独立模块时也会记录日志到log/install\_unit.log中。（测试和实际使用时尽量用后者，便于从日志追溯安装过程。）

## 【安全要求】数据库用户名、密码修正为默认加密存储

配置文件中application.properties中数据库的用户名、密码默认为加密存储。

## 【安全要求】部分目录或文件权限已修改为755、775或者644

1. 目录为755，目录下文件为644

/var/lib/tomcat7/sysauth/event  
/var/lib/tomcat7/sysauth/user  
/var/lib/tomcat7/sysauth/summary

1. 目录下文件权限改为775

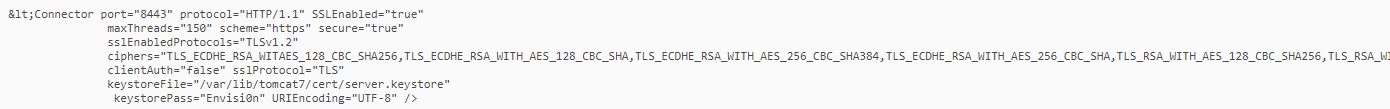
/cirrusgate/config/cirrus.ini  
/cirrusgate/config/calendar.dat  
/cirrusgate/config/checkConfig.json  
/cirrusgate/config/cirrus\_nas.ini  
/cirrusgate/config/ana.ini  
/cirrusgate/config/log4cplus.cfg  
/cirrusgate/config/license.lic

## 【安全要求】后台已去掉tomcat下默认应用

全新安装或升级后，在/var/lib/tomcat7/webapps和/var/lib/tomcat8/webapps目录下会删除如下目录docs,examples;host-manager;manager.

## 【安全要求】禁止3DES相关的加密算法

/var/lib/tomcat7/conf/server.xml中，设置如下ciphers



## Tomcat配置要求

从F3开始，再次明确要求：tomcat7、tomcat8配置如下：

-Xms1024m -Xmx4096m -XX:PermSize=512m -XX:MaxPermSize=2048m

将原来的Xmx 1024或2048 调整为4096

如果机器配置足够加大配置 可将四个参数的值都相应调大为：

-Xms2048m -Xmx8092m -XX:PermSize=1024m -XX:MaxPermSize=4096m

注：配置文件根据设置的内存大小，自适应写入值

## 意图分析

意图分析程序在CentOS操作系统下可能不支持。

## 桶扫描

1. 桶扫描，在/cirrus\_soft/cloud/config/cloud.ini中，缺省配置cloud\_enabled=0，表示安装了也不运行。cloud\_enabled=1，才能正常启动。
2. 配置完成后 /cirrus\_soft/cloud/bin目录，运行 ./cloud.sh –start 启动云桶扫描程序
3. 启用创建的云对象存储策略，开始扫描

## 文件溯源

1. 文件溯源功能，只支持针对文件后缀为.docx、.xlsx、.pptx的文件有效
2. 查询文件在多个终端上的流转溯源信息，可在最新一次某个终端上报的事件详情中，下载附件；然后在文件溯源页面，上传下载的附件查询该附件在哪些终端上流转过；
3. 开启此功能后，终端上操作以docx、xlsx、pptx 格式的文件时， 电脑管家可能会弹框“发现可疑程序正在修改文档”， 点击“阻止修改”后， 该功能失效。

开启文件溯源功能将影响终端运行性能，请谨慎使用。

## 终端加密功能注意事项

1. 升级前， 终端设置页面，勾选的终端加密设置、添加的白名单程序，在升级后，需要重新勾选配置、添加白名单。
2. 加密程序白名单，加密文件后缀应填写：.txt ;.xlsx (注意有个 点“.”)
3. 下发终端加密策略后，须重启终端后才能生效
4. 终端上的敏感文件被加密后，管理平台上即使关闭终端加密设置开关，已经被加密的文件，也不能看到明文内容，必须申请解密才行；
5. 开启文件加密功能将影响终端运行性能，且对终端本地源文件做了改动，存在一定风险，请谨慎使用。

## 二级负载服务器和流量探针服务器

升级后，需要重启tomcat7，且探针要删缓存后再重启

## 内置分类升级

升级前已存在的内置分类，升级后要重新发布一次才能继续生效。

## 文件属性分类

分类管理-->条件-->属性条件中的“文本文件”慎用，请在使用这一属性条件时尽量配上文件大小的约束条件。

## 结构化指纹、非结构化指纹

CentOS7.4系统下升级后，结构化指纹、非结构化指纹规则需要重新制作

# 网关配置注意事项

## HTTP中取不到文件名略过不扫

网关faloc.ini中配置skip\_all\_body\_file为1时，HTTP中取不到文件名的都略过不扫，但这种情况下有可能会丢事件。

## 关于DLP网关风险中存在的body文件的相关说明

1. DLP网关中，通过HTTP协议往外发数据，是通过POST方法实现，当传输文件时，大部分情况下将文件放在HTTP包体中，以MIME格式进行上传。这种情况下，通常可以从MIME中的subheader部分取得文件名称。
2. 很多情况下，外发部分的数据是直接放在HTTP的包体部分。这时，这些部分就没有确定的文件名，DLP软件将这些外发部分的数据（即HTTP包体）存成一个自定义的文件，文件名我们会取为类似http\_20180206\_120005\_body1这样的名称。当扫描到有风险时，会上报类似名称的风险文件。
3. webmail中的正文，主题，BBS，论坛的发言，所有的直接放到http包体，都是如此处理。
4. QQ的离线文件，某些切片传输的邮件或网盘，它们的数据也是直接放到包体里。虽然它们传输文件时，是带文件名的，但是它们实现时是文件名传输是一个POST过程完成，文件内容传输又是另一个POST完成，往往还不是一个连接中完成的。很难找到对应关系。所以，处理这些数据包时，也是将数据存储存成一个http\_2018xxxxx\_body的文件（因为无法取得文件名）。当然，也可以做一些特殊处理，这部分的处理某些情况下可以与情况1）做一些区别。比如发现时QQ传文件时，也要上报。但现在文件的命名与情况1）时无区分的。当body文件不上报时，也会丢失这些数据。
5. 目前版本中加了缺省的URL（域名）白名单，放在/cirrus/config/skipScan.conf中，一些经常产生类似事件的传输过程，如搜狗拼音等，会被滤掉，以此减少body文件的误报。
6. 除了已列出的内置域名外，过滤白名单也支持添加URL，可以更精细一些进行控制。

|  |  |
| --- | --- |
| diskapi.baidu.com | qurl.f.360.cn |
| pss.alicdn.com | \*. 3g.qq.com |
| ocsp.digicert.com | api.ad.xiaomi.com |
| ocsp.digicert.com | shup-ctfs.ftn.qq.com |
| szshort.weixin.qq.com | adashww.ut.taobao.com |
| 220.249.243.24 | szminorshort.weixin.qq.com |
| log.snssdk.com | qurl.f.360.cn |
| web.gleasy.com | notify.meihua.docer.com |
| pmir.3g.qq.com | \*.amap.com |
| \*. taobao.com | \*.alipaylog.com |
| \*.pinyin.sogou.com | \*.qqpy.sogou.com |
| \*.amap.com | gw.api.taobao.com |
| feedback.iqiyi.com | err.up.vivo.com.cn |
| bugreport.os.qiku.com | logs.quality.qiku.com |
| bugs.python.org | stat.www2.kugou.com |
| api.hdtv.letv.com | sz-btfs.yunup.ftn.qq.com |
| openapi.baidu.com | nexus.officeapps.live.com |
| api.platform.cp21.ott.cibntv.net | music.163.com |
| report.cgi.weiyun.com | gw.api.taobao.com |
| data.mix.sina.com.cn | tps10216.doubleverify.com |
| [www.wintalent.cn](http://www.wintalent.cn/) | dict.youdao.com |

## 增加对mpls流量的扫描

1. 流量带mpls标识，以前的版本在抓包时流量被直接过滤。现在在falco.ini中加入pac\_snap\_type=all,会将带mpls的流量也放进来扫描。
2. 另外，环境中发现MTU（最大传输单元）会大于1500，要将镜像网口的MTU设置为9000才会避免丢包。需要在网卡配置文件中填入mtu: 9000才能正确收取长的包。
3. 这两项均不应成为网关缺省选项，根据现场的具体情况进行配置。

## 网卡名是非eth0的探针或其他服务器

新cirrusgate.tar.gz解决，对于网卡名是非eth0的探针或其他服务器，需要在/cirrusgate/config/cirrus.ini手工修改

local\_ethernet=RealNetCardNameXXX RealNetCardNameXXX为实际的网卡名称

## 默认镜像ip由11.22.33.44改为192.168.1.1

1镜像ip默认192.168.1.1，也可配置为其它镜像ip

2 配置文件 安装包\config\setup.ini

3 参数为mirror\_netcard\_ip=192.168.1.1，如下截图

