**DS for H3C FAQ**

* **阅读对象： SE/TAM/驻点/小蜜蜂**
* **阅读目的：本文档列出了DS for H3C的最新使用版本，下载地址，以及日常运维过程中会遇到的常见问题解决方案.**
* **使用技巧：可以根据右侧的文档目录来快速找到需要解决的问题。也可以使用CTRL+F快捷键搜索问题关键字来寻找相关问题的解决方法。**

# 程序版本地址:

**For\_CAS\_3.0**

**DSM: 7.5.8015**

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_H3C_CAS/7.5/For_CAS_3.0/DSM/>

**DSVA: 7.5.0.2055**

[http://support.asiainfo-sec.com/TM-Product/Product/Deep\_Security/DS\_for\_H3C\_CAS/7.5/For\_CAS\_3.0/DS后端/for\_CAS\_E0306H2/](http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_H3C_CAS/7.5/For_CAS_3.0/DS%E5%90%8E%E7%AB%AF/for_CAS_E0306H2/)

# 案件处理建议 ：

在用户反馈问题后，还请按照以下表格来确认用户使用的基本信息，以便后续案件排查。

|  |  |  |
| --- | --- | --- |
| ID | 检查列表 | 描叙 |
| 1 | 华三产品详细版本 | Eg:H3C CAS 3.0(E0306H06) |
| 2 | DSM版本 | 7.5.8015 |
| 3 | DS版本 | DSVA 2055 |
| 4 | ds服务状态 | ds\_agent ds\_am状态 |
| 5 | 前端驱动状态 | sc query kfileflt |
| 6 | 是否能杀毒 | 实时是否正常 手动扫描是否正常  |
| 7 | DSM防恶意配置文件 | 是否正常  |
| 8 | 华三页面上防病毒设置 | 是否正常  |
| 9 | 更新病毒 | 是否正常  |
| 10 | 环境中是否有其他的防病毒 | 360， 金山，瑞星，卡巴，赛门铁克 |

针对用户遇到的不同问题，可以按照此表格来收集相关的日志：

表格可以从此链接下载：

<https://www.ssfe.trendmicro.com.cn/app#folder/VBTJZ/H3C/DS7.5%20%E6%8E%92%E6%9F%A5%E8%A1%A8.xls?a=xiNqOYK_Qhc>

**常见问题：**

针对一些通讯，端口等基础问题，可以参考DS for VM的FAQ。如有遇到更多的常见问题，将会继续更新。

**问题一**

前端虚拟机卡慢，受DSHA保护的虚拟机出现大量脱机，甚至更新失败等现象

处理建议：

查看DS for CAS的版本，如果版本低于CAS\_E0306H2，还请建议升级。

下载链接：

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_H3C_CAS/7.5/For_CAS_3.0/DS%E5%90%8E%E7%AB%AF/>

**处理建议**

如果遇到上述现象，建议可以依照以下步骤，更新其中几台CVK，确认问题解决后，再批量部署

1.下载7.5.2043安装包，并上传到CVK中。然后登入CVK中进行升级如下。

2.解压补丁包：tar -xvf  dsva-agent\_7.5.0.2043\_amd64.tar.gz

3.升级：dpkg -i dsva-\*

4.验证是否更新成功：dpkg -l | grep dsva，看一下版本是不是7.5.0.2043

5.重启有问题的CVK

6．验证是否能是否还存在卡慢和观察是否能正常杀毒。

Note: 有客户的CVK主机上发生ds\_am进程卡死问题，造成更新没有完全，可以依照以下步骤处理

1. 检查是否有2个ds\_am进程存在，如果有就是不正常
ps –ef | grep ds\_am
2. 如果有2个ds\_am进程，kill -9 杀掉那些进程
3. 重启ds\_am服务

**问题二：**

在激活CVK对应的DSVA后，哪怕不开启任何rule，都会出现延迟的现象。（可能导致web应用无法打开或者延迟的现象）

**原因：**

在没有任何规则的情况下，有导流的时候，估计延迟会比没有导流的时候，多约20%，这个尤其在大量小数据包传送时更为严重， 实验数据如下
从下表可以看出，比较虚拟机未激活和激活0 rules 2栏位中延迟(tcp\_lat:)上半部使用小数据包测试时，throughput带宽受影响小，但是延迟明显。而下半部用大的数据包测试时，延迟就相对就较小
这是因为，目前无代理设计上，需要将数据包在系统（Linux上）中传送复制，虽然只有一次复制，但是这里在大量数据包时就会明显延迟。不幸的是，目前这里没有优化空间，这是系统和设计上限制


**处理建议**：

如果用户不开启DPI或者FW，可以尝试把导流的功能关闭。

编辑 /etc/default/openvswitch-switch，注销export FEATURE\_NETFILTER=on行，

再执行echo 0 > /sys/kernel/debug/openvswitch/feature\_mask

这样CAS就不再把流量导过来。但是要注意，以后如果升级ds\_agent时会需要再做一次

（因为ds\_agent安装默认会加入这个）

备：这个操作不会影响到用户的业务