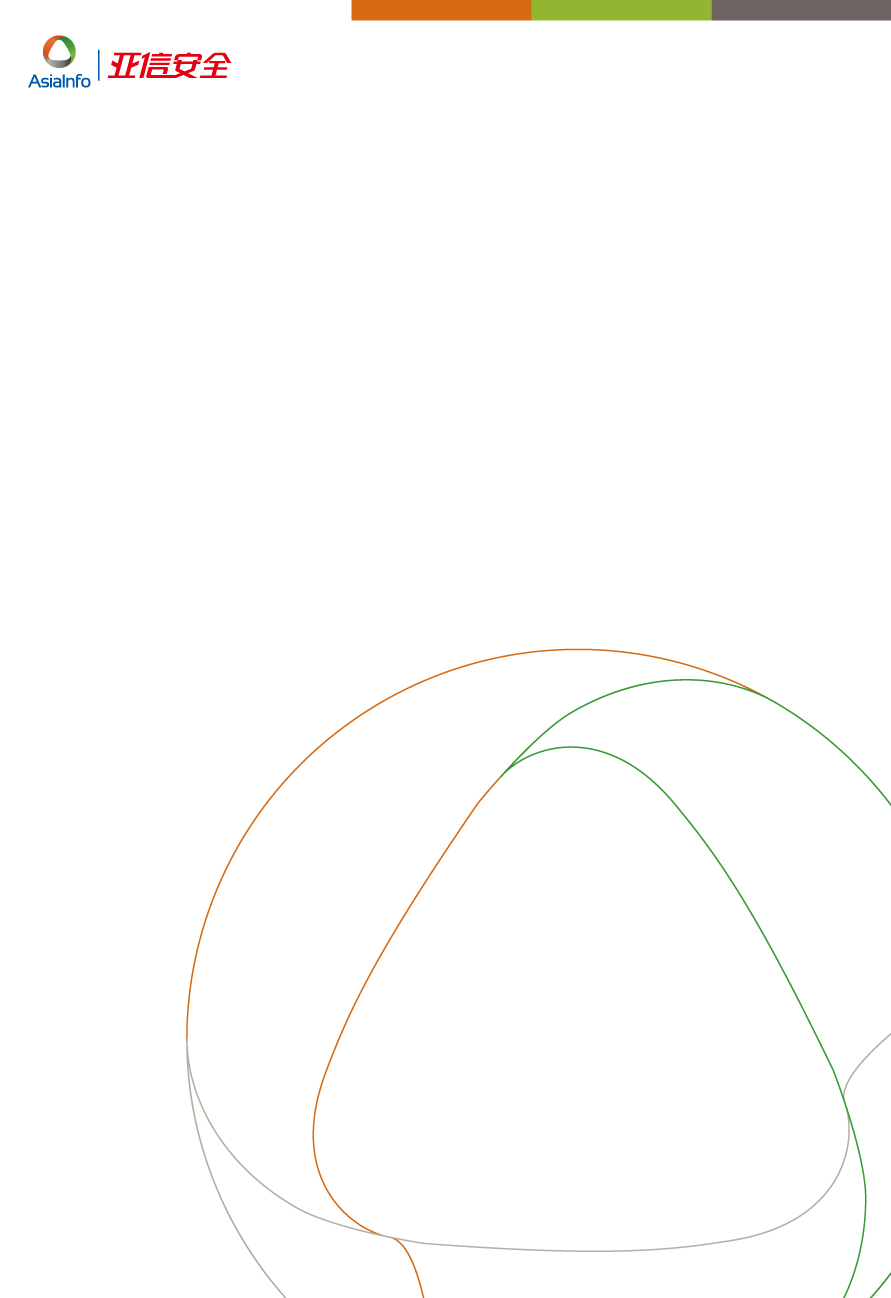
**DS for Fusion**



**FAQ**

作者: Michael Cao

日期：2017年10月

目录

[1.程序及文档下载地址 3](#_Toc496630683)

[2安装部署问题 4](#_Toc496630684)

[2.1通讯端口说明 4](#_Toc496630685)

[2.2Q:DS for Fusion支持的Fusion平台版本？ 5](#_Toc496630686)

[2.3Q:DS for Fusion 支持哪些功能？ 5](#_Toc496630687)

[2.4Q:DS for Fusion支持哪些操作系统？ 6](#_Toc496630688)

[2.5Q如何获取最新的防病毒（Antimalware）驱动？ 6](#_Toc496630689)

[2.6Q:如何获取最新的SVM（DSVA）？ 7](#_Toc496630690)

[2.7单台安全管理虚拟机可以设置安全用户虚拟机数量限制 7](#_Toc496630691)

[2.8SVM版本问题 8](#_Toc496630692)

[2.9 Q:如何设置SVM的IP地址？ 8](#_Toc496630693)

[3．使用配置问题 10](#_Toc496630694)

[3.1SVM防病毒选项调整问题 10](#_Toc496630695)

[3.2 DS FOR FUSION防火墙DPI功能不生效 10](#_Toc496630696)

[3.3日志过大问题（调整VIB日志等级） 11](#_Toc496630697)

[3.4SVM磁盘报警,SVM无法激活 11](#_Toc496630698)

[3.5 DSM PROTAL反应慢 12](#_Toc496630699)

[3.6 SVM脱机无法更新 12](#_Toc496630700)

[3.7 Q:如何处理防病毒功能失效问题？ 12](#_Toc496630701)

[4.更新相关问题 14](#_Toc496630702)

[4.1更新源 14](#_Toc496630703)

[4.2Q:如何离线更新？ 14](#_Toc496630704)

[4.3更新不成功：无法合并增量 14](#_Toc496630705)

[4.4.SVM补丁 15](#_Toc496630706)

[5其他常见问题 16](#_Toc496630707)

[5.1Q:SVM最新版本是什么？ 16](#_Toc496630708)

[5.2Q:SVM0918和SVM0307在功能上区别？ 16](#_Toc496630709)

[5.3Q:GVM版本是否需要更新？ 16](#_Toc496630710)

[5.4Q:0307和0918补丁是否推荐安装？ 16](#_Toc496630711)

[5.5Q:程序版本是否有更新？ 17](#_Toc496630712)

[5.6Q:DS for Fusion更新源？ 17](#_Toc496630713)

[5.7Q:ds for fusion其他资料 17](#_Toc496630714)

参考资料

特别鸣谢

## 1.程序及文档下载地址

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/>

**[文档]**

部署文档：

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/亚信安全服务器深度安全防护系统_FusionSphere_7.5版_安装手册_v1.12.pdf>

使用文档：

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/亚信安全服务器深度安全防护系统_FusionSphere_7.5版_使用手册_v1.12.pdf>

**[安装包]**

SVM

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/svm0307.rar>

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/SVM0918.zip>

DSM

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/Manager(for_FusionSphere_Hypervisor)-Windows-7.5.8021.x64.exe>

## 2安装部署问题

### 2.1通讯端口说明

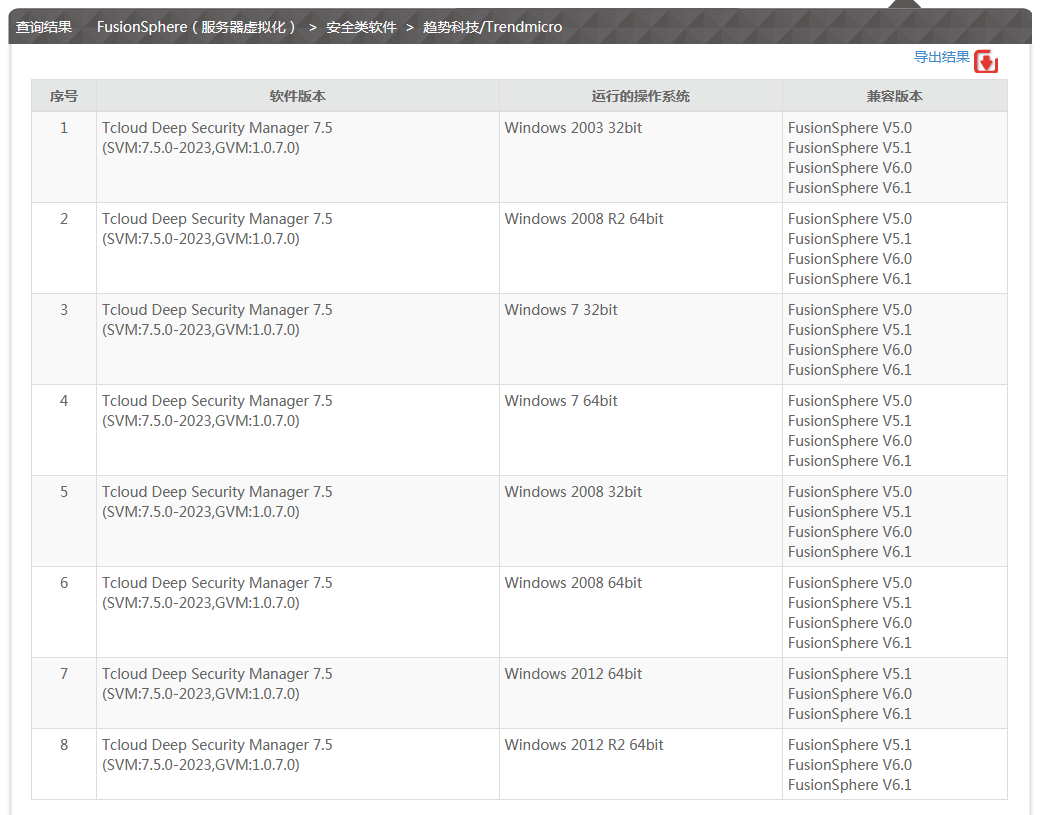
|  |  |  |  |
| --- | --- | --- | --- |
| **源应用** | **目标应用** | **目标应用开放端口** | **端口说明** |
| DSM | VRM | 7443 | HUAWEI Fusion开放出来得API， DSM需要调用，还有登入Fusion管理平台需要用的端口 |
| SSH tool | SVM | 22 | ssh连接 |
| DSM | 4118 | 用于与DSM通讯 |
| WEB | DSM | 4119 | Dsm web控制台 |
| SVM | 4120 | 波动信号 |
| 4122 | 与svm通讯 |

### 2.2Q:DS for Fusion支持的Fusion平台版本？

A:参考官方列表

<http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp>

FusionSphere(服务器虚拟化)>>安全类软件>>趋势科技



### **2.3Q:DS for Fusion 支持哪些功能？**

A:目前支持防病毒，防火墙和DPI功能。使用防火墙及DPI功能需搭配和华为 FusionSphere V100R006C00U1及SVM 0918版本。

### 2.4Q:DS for Fusion支持哪些操作系统？

A:防病毒功能依赖被保护虚机上的Antimalware驱动，而这个驱动由华为提供。

所以，**DS支持哪些操作系统，取决于华为是否有发布该操作系统的Antimalware驱动。**

截止至2017年10月为止，我们已知可以支持的操作系统：

Win 2003 x32

Win 2008 R2 x64

Win 7 x32

Win 7 x64

Win 2008 x32

Win 2008 x64

Win 2012x64

Win2012R2x64

### 2.5Q如何获取最新的防病毒（Antimalware）驱动？

A: 华为官网链接：

<http://support.huawei.com/enterprise/productNewOffering?idAbsPath=7919749|7919788|9856606|19916941&pid=19916941&productname=FusionSphere%20SIA>

进入后，选择【软件】下的最新版本，例如下图的V1.3.00.190

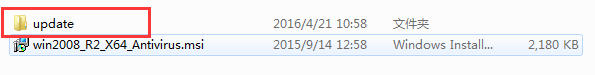


找到GVM驱动包（下载此包需要权限，权限需要相关产品的激活码）

cid:image004.png@01D1EDAC.988A18C0

2016/11月测试发现，虽然链接还是有锁的标记，但是已无需激活码，可以先试一下无激活码的前提能否下载。

注：每个驱动包中会有一个update文件夹



请安装update文件夹中的驱动，驱动版本为1.0.6。

### 2.6Q:如何获取最新的SVM（DSVA）？

A: 目前的SVM有2个版本：SVM0307和SVM0918，其中0918是最新的版本，如需使用DPI防火墙功能，需搭配0918版本，下载地址如下

<http://support.asiainfo-sec.com/TM-Product/Product/Deep_Security/DS_for_Fusion_JV/SVM0918.zip>

### 2.7单台安全管理虚拟机可以设置安全用户虚拟机数量限制



2.7.1：想了解DS for fusion是否有虚拟保护数量限制

没有限制。

2.7.2： 是华为还是亚信对保护虚拟机数量 进行了控制 ？如何能够修改安全用户虚机数量为50的限制？

咨询了华为的工程师，是华为fusion平台本生的限制，目前无法更改。

这个是系统限制。单位时间能处理的扫毒量就是大概50台左右。和硬件速度也有关系。理论上硬件可以的话是可以多过50的。不过如果瞬间大量，就会造成扫描来不及

但是50的限制，是华为页面做的限制

原因是华为设计在SVM和VM的沟通机制中，需要预先分配共享内存，而这个数字目前就是50份，这也是为什么在华为页面上就有如此限制

所以这个问题主要在设计架构问题。

### 2.8SVM版本问题

若ds\_agent版本为2023 SVM版本为0307

若ds\_agent版本为8013 SVM版本为0918

rpm -qa|grep ds\_

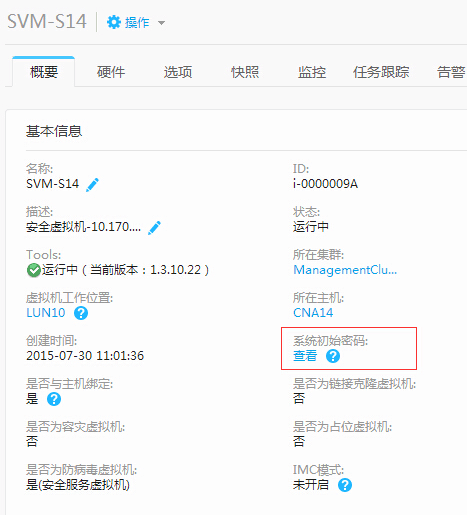
### 2.9 Q:如何设置SVM的IP地址？

A:

* VNC登陆SVM

用户名：root 密码：

注：密码在Funsion管理控制台的虚拟机摘要信息里，参考下图。



* 手动配置网卡

注意：配置之前，请先执行ifconfig，看看网卡是从eth0开始还是eth1开始

cd /etc/sysconfig/network-scripts

mv ifcfg-eth\* ifcfg-eth0 （如果ifconfig第一个网卡是eth0的话）

vi ifcfg-eth0

* 修改ifcfg-eth0文件中的ip:



* 重启网卡服务(或者直接重启SVM)

service network restart

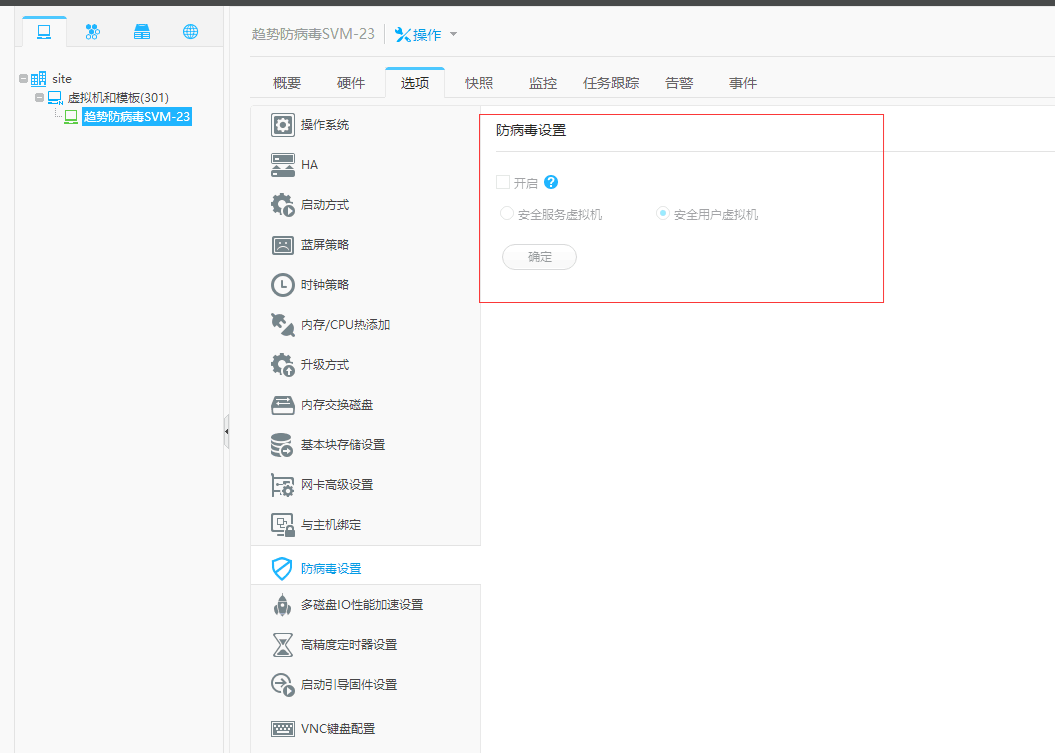
* 本地ping配置好的SVM地址，如果不通请重新检查SVM的IP网段

## **3**．使用配置问题

### 3.1SVM防病毒选项调整问题

通过Fusion的云管平台安装的扫描服务器 无防病毒功能开启选项（防毒选项为灰色）

该选项需要关机调整



### 3.2 DS FOR FUSION防火墙DPI功能不生效

若排错后功能不生效，可以参考以下方法收集下信息提供过来。

Root登录SVM后台，

请依照下面收集日志

         1.      检查封包。执行下面命令，并立刻Ctrl+C结束（因为会打印大量日志，执行后需快速按下）

#stop ds\_filter

#export LD\_LIBRARY\_PATH=/opt/ds\_guest\_agent/lib

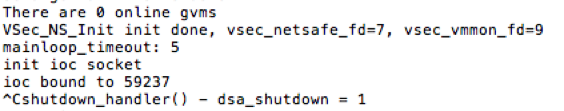
#/opt/ds\_guest\_agent/ds\_filter -l 8 –d

         2.      收取刚才打印在银幕上日志。尤其需要收集最开始部分

         3.      可以执行如下命令恢复。

#start ds\_filter

如果持续无输出，表示直没有侦测到开机的虚拟机 （直到^C结束时都没有），如果有，会有很多日志显示



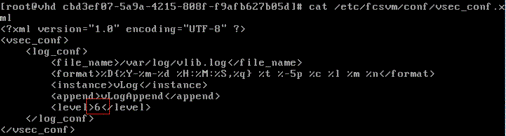
 这样需要请华为研发检查，为什么没有发送开机事件出来，可能是华为的svmroot这模块没有侦测到。

### 3.3日志过大问题（调整VIB日志等级）

问题可能是华为的ivshmem3打印太多日志到messages去了，

1.       检查messages内容，看是不是一堆ivshmem3的日志，如果是请华为减少ivshmem3的，可能要他们修改代码或配置

2.       vlib可以在/etc/fcsvm/conf/vsec\_conf.xml 调整日志级别，一般预设3就够了，如果还是很多，可能就要请华为那边看看，是不是有报错



3.       可以先删除比较久的日志压缩包

### 3.4SVM磁盘报警,SVM无法激活

C:\Users\Michael\AppData\Local\Temp\msohtmlclip1\02\clip_image001.jpg

请检查一下目前ds\_agent状态。如果是运行状态，尝试重新激活svm。

否则请按如下步骤操作：

1、  删除或者更改messages日志位置

2、  重启svm主机

3、  进到/opt/ds\_agent下，执行./resetagent.sh

4、  重启SVM

5、  再次激活。

6、  如果还不行，检查看看status ds\_agent是否还是没有running。如果是，请收一下/var/log/messages日志（新生成的日志）发给我们，做进一步分析

看来是档案毁损了

Dec 14 15:30:49 PANTV001-005 ds\_agent[2202]: Unable to load signed security profile from file /var/opt/ds\_agent/ds\_agent.config

Dec 14 15:30:49 PANTV001-005 ds\_agent[2202]: 1001|CLR\_CONFIG|-10 (Unknown error 18446744073709551606)

删除 /var/opt/ds\_agent/ds\_agent.config后，再start ds\_agent或重启SVM后，看看agent是否可以正常启动了

如果有可以激活看看。如果不行就试试resetagent.sh后再激活

如果还有问题，可能SVM毁损严重，这样一个个修了，怕也会有其他潜在问题

那就建议移除SVM再导入新的

并记得把vlib 日志级别从10降到3，以避免同样问题发生。

### 3.5 DSM PROTAL反应慢

排错后问题依然，可以先提供诊断包：

**SVM诊断包**:：双击一个svm，【支持】-【创建诊断数据包】

**vlib.log 和 message**：登录SVM，日志文件在/var/log下，收集对应日期的日志文件

### 3.6 SVM脱机无法更新

做过初步排查，SVM预留内存，CPU资源都足够。Vsec\_conf.xml配置文件的日志等级也已经调整到3，但是问题依然会出现。

收集了DSM/SVM诊断包

需要收集SVM上面的/var/log/messages 和 vlib.log需要收集这个，还有发生脱机日期或时间好定位

### 3.7 Q:如何处理防病毒功能失效问题？

* 确认gvm情况：

命令行运行cmd

查看服务状态，应该是running

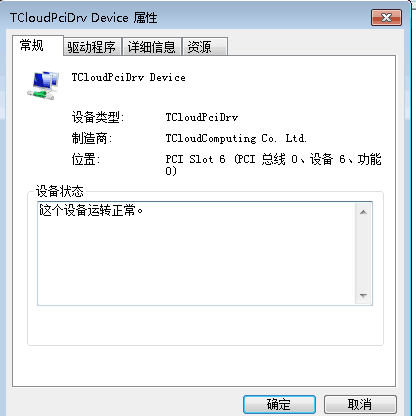
sc query kfileflt

验证服务能否正常启停

sc stop kfileflt

sc start kfileflt

* 设备管理器里面找到tcloud pci driver 看看是否正常运行



* 确认svm情况：

svm 查看服务状态

status ds\_am

status ds\_agent

* 在DSM上调整配置文件：

\*SVM配置文件必须为“无”

\*GVM根据扫描需要单独配置

注:可以尝试安装update版的防毒驱动，参考Q4

若检查无异常，收集日志：

**SVM诊断包**:：双击一个svm，【支持】-【创建诊断数据包】

**vlib.log 和 message**：登录SVM，日志文件在/var/log下，收集对应日期的日志文件

## 4.更新相关问题

### 4.1更新源

<http://dskvm75-huawei-p.activeupdate.asiainfo-sec.com/activeupdate/china>

### 4.2Q:如何离线更新？

A:目前的方案是使用TMUT，下载地址如下：

<https://www.ssfe.trendmicro.com.cn/TMFmF/DS%20for%20fusion/TMUT%20for%20fusion.zip?a=gp1OY1T0jfk>

### 4.3更新不成功：无法合并增量

Problem: 更新防恶意软件组件不成功: ActiveUpdate 無法合併漸進式修補程式檔案。請再試一次。如果問題持續存在，請聯絡趨勢科技客戶服務部門。(46)

初步解决步骤如下：

1. 删除并更新DSM病毒库：

1. 打开DSM页面-> 系统-> 更新-> 还原防恶意软件。
2. 打开DSM机器-> 进入 C:\Program Files\AsiaInfo\Deep Security Manager\-> 先备份au文件夹，再将au文件夹删除-> 进入service重启dsm服务
3. 打开DSM页面-> 系统-> 更新->立即更新
4. 打开DSM页面-> 系统-> 任务->每日组件更新->立即运行任务

二． 删除并更新Agent病毒库：

1. 打开SVM机器-> 进入/opt/ds\_agent/lib/-> 将AU\_Backup文件夹更名为AU\_Backup.bak
2. 进入/opt/ds\_agent/lib/ 将如下文件备份移至新建bak目录下

lpt$vpn.859  lpt$vpn.862  ssaptn.754  ssaptn.977  tmblack.141  tmblack.227  tmwhite.581  version.conf（不用在乎文件后面的数字号码）

进入/var/opt/ds\_agent/au/-> 将AU\_Data文件夹更名为AU\_Data.bak（备份可参考如下图）

1. 重启ds\_agent  ds\_am服务
2. 打开DSM页面-> 系统-> 更新->立即更新
3. 打开DSM页面-> 系统-> 任务->每日组件更新->立即运行任务

进行校验检测，能否更新成功并杀毒

### 4.4.SVM补丁

0307补丁

如果是大量扫毒造成SVM连线不正常，出现脱机现象可以安装以下补丁：

<https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Huawei/Builds/Hotfix/2017-03-29/?a=1-QbYm4gQso>

 0918补丁

<https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Huawei/Builds/Hotfix/2017-05-22/?a=Jsr4I_1aT0c>

## 5其他常见问题

### 5.1Q:SVM最新版本是什么？

使用防火墙及DPI功能需搭配和华为 FusionSphere V100R006C00U1及SVM 0918版本。SVM0918是否有后续版本发布？和华为现有FUSIONSphere最高可兼容版本是哪一个？

A: SVM0918是目前最新，预计明年才会有新SVM发布  
SVM0307, SVM0918都是兼容Fusion 6.0 U1以上的

### 5.2Q:SVM0918和SVM0307在功能上区别？

据我所知SVM0918和SVM0307在功能上区别0307只有防病毒功， 0918支持防火墙和dpi,在用户未购买防火墙和DPI功能的情况下，是否使用0307对性能方面会更好（之前有case遇到因为性能问题0918svm改装0307的），是否需要推荐安装该版本？

0918在其他方面对于0307是否有什么区别和优化？

A: 杀毒效能一样，但是SVM0307没有转发流量，所以不影响网路效能。如果确定不用FW，DPI，可以使用0307

### 5.3Q:GVM版本是否需要更新？

华为GVM驱动support站点上的版本为1.3.00.260

华为官网看到最新版本是1.3.10.300，目前正常使用的情况下是否需要更新？

A: 没有问题可以不用更新。有问题再更新为最新就好

### 5.4Q:0307和0918补丁是否推荐安装？

优化扫毒性能的补丁对于新装用户是否需要推荐其安装？

0307补丁

<https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Huawei/Builds/Hotfix/2017-03-29/?a=1-QbYm4gQso>

 0918补丁

<https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Huawei/Builds/Hotfix/2017-05-22/?a=Jsr4I_1aT0c>

 A: 新版本修复了大量杀毒时稳定性的问题，新版本是较稳定的，但是担心实施多一个步骤，可能有其他问题，所以如果没有问题，可能不需要特别建议  
目前预计明年会出一个新版本的SVM，会把这个补丁放进去。  
但是其实这个可以看遇到问题多不多，如果有增加趋势，可以考虑改成新用户就建议安装。这个其实我也没有很偏好哪一个。只是希望部署简单不要出错和后续解决方便这些考量而已。

### 5.5Q:程序版本是否有更新？

DSM7.5.8021版本是否有后续更新？

Supoort站点上使用手册和安装手册版本为1.12是否有更新版本？

安装手册中

DSM需要准备一台安装windows的机器，可以使用物理机或者虚拟机（可以使用Fusion创建的虚拟机）。

**内存：**4GB

* **磁盘空间：**50GB（建议使用 50GB）
* **操作系统**：Microsoft Windows Server 2008（32 位和 64 位）**、Windows Server 2008 R2**（64 位）**、**Windows 2003 Server SP2（32 位和 64 位）
* **数据库（建议可选）：** Oracle 11g、Oracle 10g、Microsoft SQL Server 2008 SP1、Microsoft SQL Server 2005 SP2
* **Web 浏览器：**Mozilla Firefox 3.x（启用 Cookie）、Internet Explorer 7.x（启用 Cookie）和 Internet Explorer 8.x（启用 Cookie）

系统要求和操作系统支持上是否有更新？

A: 没有更新。除非上新补丁，补丁部署文档会有特别说明系统需求是否要更改。如SVM补丁会建议多配置SVM RAM资源

### 5.6Q:DS for Fusion更新源？

资料中看到DS for fusion的更新源有3个

<http://dskvm75-h3c-p.activeupdate.asiainfo-sec.com/activeupdate/china>

<http://tmds75-p.activeupdate.trendmicro.com.cn/activeupdate/china>

<http://dskvm75-huawei-p.activeupdate.asiainfo-sec.com/activeupdate/china>

是否都可以用？

 A:  Fusion 用这个<http://dskvm75-huawei-p.activeupdate.asiainfo-sec.com/activeupdate/china>   （是给HUAWEI的），其他是其他产品的

### 5.7Q:ds for fusion其他资料

A: <https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Huawei/Documents/Best%20Practices/?a=h-XuKfpF4gM>  
这里有2个，一个是大量脱机的分析，排查和解决方案。在扫毒量过大时可以考虑  
另一个也是，如果扫毒量大到造成SVM CPU持续很高接近100%，可以参考这个文档配置减少扫毒量的压力  
<https://www.ssfe.trendmicro.com.cn/app#folder/CMTgz/Marketing/Sharing/%E7%A0%94%E5%8F%91%E9%9D%A2%E5%AF%B9%E9%9D%A2/?a=KKwDbkPqRic>

这里面的DS 7.5 排查表，有安装，或一些情境的可以查看那些日志，用哪些命令

参考资料：

1. DS for fusion FAQ ver1.0.3.doc
2. 亚信安全服务器深度安全防护系统 FusionSphere 7.5版 安装手册\_v1.12.pdf
3. 亚信安全服务器深度安全防护系统 FusionSphere 7.5版 使用手册\_v1.12.pdf
4. 历史案件

特别鸣谢：

Wesley Lee