DS for VMware FAQ

* **阅读对象： SE/TAM/驻点/小蜜蜂**
* **阅读目的：本文档列出了DS for VMware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。**

目录

[**一．程序版本下载地址:** 3](#_Toc496449755)

[**二．安装部署问题** 4](#_Toc496449756)

[1.DS和VM之间的兼容性. 4](#_Toc496449757)

[2.DSM激活虚拟机防护时提示内部错误 4](#_Toc496449758)

[3.升级亚信DSM时提示需要升级数据库结构 4](#_Toc496449759)

[4.在windows2003/2008上安装DSA后出现防恶意引擎脱机。 4](#_Toc496449760)

[5.在NSX环境中部署GI和DSVA失败 4](#_Toc496449761)

[6.DS各平台所支持功能 5](#_Toc496449762)

[7.DS通讯端口列表 5](#_Toc496449763)

[**三．使用配置问题** 6](#_Toc496449764)

[1.DSM上查询隔离文件最多只能显示100条，是否可以修改限制？ 6](#_Toc496449765)

[2.linux部署DSA后系统缓慢 7](#_Toc496449766)

[3.linux安装DSA后使用EICAR文件测试，DSA没有隔离EICAR。 7](#_Toc496449767)

[4.在仅启用了DPI情况下，DS仍旧出现防火墙事件。 7](#_Toc496449768)

[5.安装DSA后，在message中看到很多GSCH告警。 7](#_Toc496449769)

[6.DSVA的网卡类型是否固定？可以更换为其他类型的网卡吗？ 8](#_Toc496449770)

[7.无代理模式下，Eicar文件没有被隔离。 8](#_Toc496449771)

[8.DS9.6环境中，增加虚拟机的CPU资源后，虚拟机自动重启 9](#_Toc496449772)

[9.DSVA/DSA 不能检测病毒样本，相同样本可以被OSCE检测。 9](#_Toc496449773)

[10.DSR离线更新失败 9](#_Toc496449774)

[**四． 其他** 10](#_Toc496449775)

[1. DS出现问题时该收集哪些日志？ 10](#_Toc496449776)

[2.NSX环境下是否有必要调整Heap Memory 10](#_Toc496449777)

[3.DSM数据库密码更换导致DSM无法访问 10](#_Toc496449778)

[4.Masteradmin帐号被锁定 10](#_Toc496449779)

## **一．程序版本下载地址:**

亚信版DS

http://support.asiainfo-sec.com/TM-Product/Product/Deep\_Security/DS\_for\_VM/9.6\_SP1\_JV/

趋势版DS

https://help.deepsecurity.trendmicro.com/software-9-6.html

Kernel

http://files.trendmicro.com/documentation/guides/deep\_security/Kernel%20Support/9.6/Deep\_Security\_96\_SP1\_kernels\_EN.html

## **二．安装部署问题**

### 1.DS和VM之间的兼容性.

参考

https://success.trendmicro.com/solution/1060499-deep-security-and-vmware-compatibility-matrix

### 2.DSM激活虚拟机防护时提示内部错误

已知问题，在9.6 SP1之后的版本中已经解决。请升级最新的DSM版本

### 3.升级亚信DSM时提示需要升级数据库结构

 可以使用趋势版本升级工具

 https://esupport.trendmicro.com/media/13785588/TrendDBUpgrade-042017.zip

### 4.在windows2003/2008上安装DSA后出现防恶意引擎脱机。

 由于windows证书过期导致AMSP引擎安装失败。

 参考下列KB导入comodo证书后重新安装DSA

 https://success.trendmicro.com/solution/1104241

### 5.在NSX环境中部署GI和DSVA失败

 GI和DSVA需要部署在集群共享存储上并使用分布式交换机

 如不是共享存储和分布式交换机，则会出现若干Esxi无法访问部署路径的情况。

### 6.DS各平台所支持功能

参考

http://docs.trendmicro.com/all/ent/ds/v9.6\_sp1/en-us/Deep\_Security\_96\_SP1\_feature\_matrix\_EN.pdf

### 7.DS通讯端口列表



## **三．使用配置问题**

### 1.DSM上查询隔离文件最多只能显示100条，是否可以修改限制？

可以通过数据库修改查询限制

参考

We have settings to control the display of quarantined files page in table administratorsettings, the default value is showed as below.
------------------------------
all.maxDatabaseRows=5000 --> 后台从数据库中最多读取的记录条数
all.maxDisplay=500 --> 显示在页面的最多条数
all.optimalNumberOfItems=100 --> 页面的表格中每页的条数
------------------------------

In DS 7.5 that we simply can change the below settings directly.
For example:
all.maxDatabaseRows=10000
all.maxDisplay=10000
all.optimalNumberOfItems=10000

But in DS 9.6 that is different due to the settings actually applied to each admin user. So you need to change those said settings by checking current admin user ID.

Steps:
1. Please do back up your database before any operations.
2. Create a new Admin account if possible.
3. Stop DSM service now.
4. Refer to below sample script, for example change the value to 20000, for user MasterAdmin and change those 3 settings at the same time. You may change each setting separately if you want.
------------------------------------------
update administratorsettingvalues set Value='20000' from dbo.administratorsettingvalues where ( AdministratorSettingID <=3 and AdministratorID = (select AdministratorID from dbo.administrators where Username ='MasterAdmin'))
-------------------------------------------
5.Start DSM service and login with the specific account.

### 2.linux部署DSA后系统缓慢

 请将相关应用进程添加到DSA扫描例外中，由于linux环境下DSA不支持通配符。因此需要写全进程完整路径

### 3.linux安装DSA后使用EICAR文件测试，DSA没有隔离EICAR。

 EICAR文件位于共享存储或者ISCSI或者NFS等网络存储上。

 Linux环境下DSA不支持扫描网络存储上的文件。

### 4.在仅启用了DPI情况下，DS仍旧出现防火墙事件。

DPI和防火墙共用一套引擎，因此当启用DPI后，防火墙的底层驱动也会被激活。

### 5.安装DSA后，在message中看到很多GSCH告警。

调整GSCH日志级别来解决

---------------------------------------------------------------------
1. Open shell script file under /opt/ds\_agent/ds\_am.init
2. Find the place of load\_module() and add one line "echo 5 > /proc/driver/gsch/debug" before return 0
=======================
if moduleIsLoaded $

{moduleTwoName}

; then
echo 5 > /proc/driver/gsch/debug
return 0;
=======================
3. Restart DSA service

### 6.DSVA的网卡类型是否固定？可以更换为其他类型的网卡吗？

不行，网卡类型已写入DSVA ovf中，无法更改。

### 7.无代理模式下，Eicar文件没有被隔离。

这种一般发生在Eicar文件位于共享目录中。DSVA会清除Eicar文件内的代码，留下一个空文件。

由于这个问题是VMware对EPSec的限制导致，R&D目前无改善计划。

8.DS9.6环境中，增加虚拟机的CPU资源后，虚拟机自动重启。

 已知问题，请升级DSVA/DSA到U11版本

### 9.DSVA/DSA 不能检测病毒样本，相同样本可以被OSCE检测。

请升级最新的DSVA/DSA版本

这种情况通常是检测病毒样本需要最新的扫描引擎。

DSVA/DSA的扫描引擎通过版本更新来升级。

### 10.DSR离线更新失败

TMUDUMP日志显示无法打开本地文件

在DSM上去掉更新设置中的下载9.0相关选项。

## **四． 其他**

### 1. DS出现问题时该收集哪些日志？

参考

https://success.trendmicro.com/solution/1110818

### 2.NSX环境下是否有必要调整Heap Memory

 NSX环境下不再使用Dvfilter，因此不需要调整Heap Memory

### 3.DSM数据库密码更换导致DSM无法访问

停止DSM服务

打开C:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties

搜索SqlServer.password字段

将字段后的内容替换成当前密码。

重启DSM服务

### 4.Masteradmin帐号被锁定

 打开CMD窗口

 切换路径到DSM安装路径下

 运行命令

 dsm\_c –action unlockout –username Masteradmin