

# ESET NOD32 Linux Security 安裝指南附加資料

適用的 ESETNOD32 版本: Linux desktop and Linux file server

適用的 Linux 版本: Redhat (RHEL, CentOS, Fedora)

ESET NOD32 Linux Security 提供的實時防護可以由兩個方法設定, Dazuko 及 preload libs (Samba) 。本附加資料會提供 Dazuko 的詳細安裝方法。而詳細的 SET NOD32 的設定請參考用戶手冊 或 LINUX 中的 MAN 檔。有關 LINUX 版本, Dazuko 或 其他第三方的程式的資料, 使用者可到互聯搜尋更多資料。

內容

安裝 ESET NOD32 Linux Security .....	1
編譯 Kernel 及安裝 dazuko.....	3
設定 ESET NOD32 Linux Security 的實時防護 .....	5

## 安裝 ESET NOD32 Linux Security

### 下載及安裝 puTTY

PuTTY 是一個提供 Telnet 或 SSH 連線的開放源碼軟體。用戶可以使用 Putty 登入 Linux Server 。

下載網址: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

### 下載及安裝 WinSCP

WinSCP 是一個提供 SFTP 連線的開放源碼軟體。用戶可以使用 WinSCP 登入 Linux Server, 然後上載或下載檔案。

下載網址: <http://winscp.net/eng/download.php>

### 登入 root 身份

```
# su
```

### 下載 ESET NOD32 安裝檔

```
# cd /usr/src/
```

```
# wget http://download.eset.com/download/unix/esets.i386.rpm.bin
```

Ps. 下載連結可參考 <http://www.nod32.com.hk/download/other>

#### 安裝 ESET NOD32

```
# chmod 755 esets.i386.rpm.bin
```

```
# ./esets.i386.rpm.bin
```

```
# rpm -i esets-2.71.2.i386.rpm
```

#### 初始化 ESET NOD32

```
# download the nod32.lic file
```

```
# cp nod32.lic /etc/esets/license/
```

在設定檔加入 **username/password**

```
# vi /etc/esets/esets.cfg
```

可以使用命令“/username” 搜尋 username 的位置。

...

#### 第一次更新 ESET NOD32

```
# /usr/sbin/esets_update
```

啟動 ESET NOD32 的服務

```
# /etc/init.d/esets_daemon start
```

## 編譯 Kernel 及安裝 dazuko

登入 root 身份

```
# su
```

下載 Kernel Source

```
# wget http://mirror.centos.org/centos/5/os/SRPMS/kernel-2.6.18-92.el5.src.rpm
```

Ps. 下載連結可參考 <http://mirror.centos.org/centos/5/os/SRPMS/>

更新相關模組

```
# yum install yum-utils rpmdevtools redhat-rpm-config rpm-build gcc ncurses-devel
```

編譯 kernel

```
# cd /usr/src/
```

```
# /usr/src/yum-builddep kernel-<version>.src.rpm
```

```
# /usr/src/rpm -Uvh kernel-<version>.src.rpm
```

PS. 可以不用理會以下警告

```
warning: user brewbuilder does not exist - using root
```

```
warning: group brewbuilder does not exist - using root
```

```
# cd /usr/src/redhat/SPECS/
```

```
# vi kernel-2.6.spec
```

```
# rpmbuild -bp --target=`uname -m` kernel-2.6.spec
```

```
# cd /usr/src/redhat/BUILD/kernel-2.6.21/linux-2.6.21.i686/
```

以下幾個編譯命令需時較耐, 可能要 1-2 小時。

```
# make menuconfig
```

```
# make
```

```
# make modules_install
```

```
# make install
```

在檔案 menu.1<sup>st</sup> 中找出 "default=?", 再設定開機使用的 KERNEL

```
# vi /boot/grub/menu.1st
```

```
# /sbin/shutdown -r now
```

載入指定的模塊 "commoncap"

```
# modprobe commoncap
```

## 安裝 dazuko

```
# cd /usr/src/  
下載 Dazuko  
# wget http://www.dazuko.de/files/dazuko-2.3.3.tar.gz  
# tar xfvz dazuko-2.3.3.tar.gz  
# cd dazuko-2.3.3  
# ./configure  
# make  
# /sbin/insmod dazuko.ko
```

## 測試 Dazuko

```
# less /proc/devices  
# cd /usr/src/dazuko-2.3.3/example_c/  
# make  
# ./example <一個測試 DAZUKO 的資料夾>
```

會出現:

```
DazukoIO version 2.3.3 (2.3.3.4)  
registered with Dazuko successfully  
Dazuko version 2.3.3 (2.3.3.4)  
set access mask successfully  
set scan path successfully
```

開啟另一個登入, 然後嘗試 TOUCH 其中一個檔案

```
# touch <測試 DAZUKO 的資料夾中的任何檔案>
```

出現檔案被閱讀或儲取的信息即表示 DAZUKO 成功運

編輯 ESETS\_DAEMON 的 SCRIPT, 在 "PATH=/usr/local....." 前插入 DAZUKO 的啟動命令。

```
# vi /etc/init.d/esets_daemon
```

啟動命令:

```
modprobe commoncap  
insmod /usr/src/dazuko-2.3.3/dazuko.ko
```

```
# /usr/sbin/shutdown -r now
```

# 設定 ESET NOD32 Linux Security 的實時防護

## 設定 ESET NOD32 Linux Security

設定 ESET NOD32 的實時防護對象及處理動作

```
# vi /etc/esets/esets.cfg
```

在 esets.cfg 中的[dac]部份:

```
[dac]
# Settings for ESETS Dazuko powered file Access Controler module.
# agent_enabled = yes/no
# Enables operation of the esets_dac.
agent_enabled = yes

# num_proc = value
# Keep value processes of esets_dac running in parallel.
num_proc = 1

# num_thrd = value
# Keep value threads per process of esets_dac running in parallel.
num_thrd = 2

# event_mask = "mask"
# The mask of (open, close, exec) events you wish to guard.
event_mask = "open"

# ctl_incl = "directory"
# Colon separated list of directories to scan files in.
ctl_incl = "/"

# ctl_excl = "directory"
# Colon separated list of directories to not scan files in.
ctl_excl = ""

# allow access to deleted files
action_av_deleted = "accept"
```

重新啟動 ESET NOD32 服務令設定生效

```
# /etc/init.d/esets_daemon restart
```

最後可以使用 EICAR 的防毒軟件測試檔，測試 ESET NOD32 的反應。

EICAR 病毒測試檔下 [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

當 ESET NOD32 偵測及處理病毒後，會在 /var/log/messages 記錄資料。例子:

```
Jul  1 02:45:21 localhost esets_daemon[3191]: summ[0c770220]: vdb=3085, agent=dac,
name="/root/eicar.com", virus="Eicar test file", action="cleaned by deleting - quarantined", info="",
avstatus="clean (deleted)", hop="accepted"
```