NOD 32 全面維護 Linux 檔案伺服器防止病毒入侵網絡

Linux 上最流行的檔案伺服器便是 Samba，雖然 Samba 不會感染 Windows 的病毒，但這卻並不代表我們不需要爲 Samba 準備任何防毒方案。因爲一旦 Samba 成爲了公司的檔案伺服器時，全公司上下員工都可能透過 Samba 交換檔案。萬一檔案伺服器中含有針對 Windows 的病毒，而員工又是用 Windows 作客戶端工作的話，便有可能經由 Samba 散播病毒令 Windows 客戶端癱瘓。所以我們建議企業用戶使用 NOD32 的 Linux 檔案伺服器防毒方案，因爲 NOD32 能迅速地偵測和清除最新的病毒。

安裝檔案存取控制工具 Dazuko

要在 Samba 上部署防毒方案，大家首先要安裝檔案存取控制工具 Dazuko。Dazuko 是一個供 Linux 使用的開放源碼軟體，由 John Ogness 開發，是一個能提供檔案存取控制給第三者開發的軟體使用的核心模組。Dazuko 會監視系統的檔案存取狀況，及把這些資訊提供給第三者開發的軟體。當第三者開發的軟體發現有問題的檔案，便會透過 Dazuko 向核心轉送訊息，限制用戶存取有問題的檔案，第三者開發的軟體可以透過 Dazuko 獲得存取的種類、進程的 ID 和用戶 ID 等資訊。Dazuko 是供防毒軟體使用而開發的模組，可配合 NOD32 使用。

Dazuko 可從其官方網站 http://www.dazuko.org/下載，目前的最新版本爲 2.0.4。檔案名稱爲 dazuko-2.0.4.tar.gz，下載後進行解壓。

tar zxvf dazuko-2.0.4.tar.gz　(ENTER)

進入 dazuko 的安裝目錄：

cd dazuko-2.0.4　(ENTER)

然後檢查系統環境：

./configure (ENTER)

過程中可能需要重新編譯 Linux 核心。

編譯 Dazuko 模組

之後便要編譯供 Linux 核心使用的 dazuko 模組。在 dazuko 的安裝目錄內執行以下命令：

make (ENTER)

在當前目錄下會出現一個叫 dazuko.ko 的模組，我們把它複製到 2.6.5-1.358custom 的模組目錄下。

cp dazuko.ko /lib/modules/2.6.5-1.358custom/kernel/security　　(ENTER)

然後用 depmod 命令製作新的相依關係列表給 modprobe 使用。

depmod -ae 2.6.5-1.358custom　　(ENTER)

選擇「2.6.5-1.358custom」重新啓動後便可用 modprobe 命令掛上模組。

modprobe dazuko(ENTER)

如果你使用的 Linux 版本並未支援 devfs，便必須自行加上 dazuko 設定檔：

mknod -m 600 /dev/dazuko c 254 0 (ENTER)

至此 Dazuko 的安裝便算完成。

安裝防毒軟體 NOD32 及 Samba 的設定

防毒軟體可用 NOD 32 的 Linux 版本「NOD32 for Linux File Server」， 目前的最新版本爲 2.05，將光碟內的檔案解壓：

tar vxf nod32lfs-2.05-1.i386.rpm.tgz (ENTER)

然後進入目錄：

cd nod32lfs-2.05-1.i386.rpm (ENTER)

然後執行文字稿安裝即可。

./install (ENTER)

今次我們使用了一個最簡單的 Samba 設定檔，其內容如下：

[global]

workgroup = pilot

netbios name = antivirus

dos charset = CP950

unix charset = UTF-8

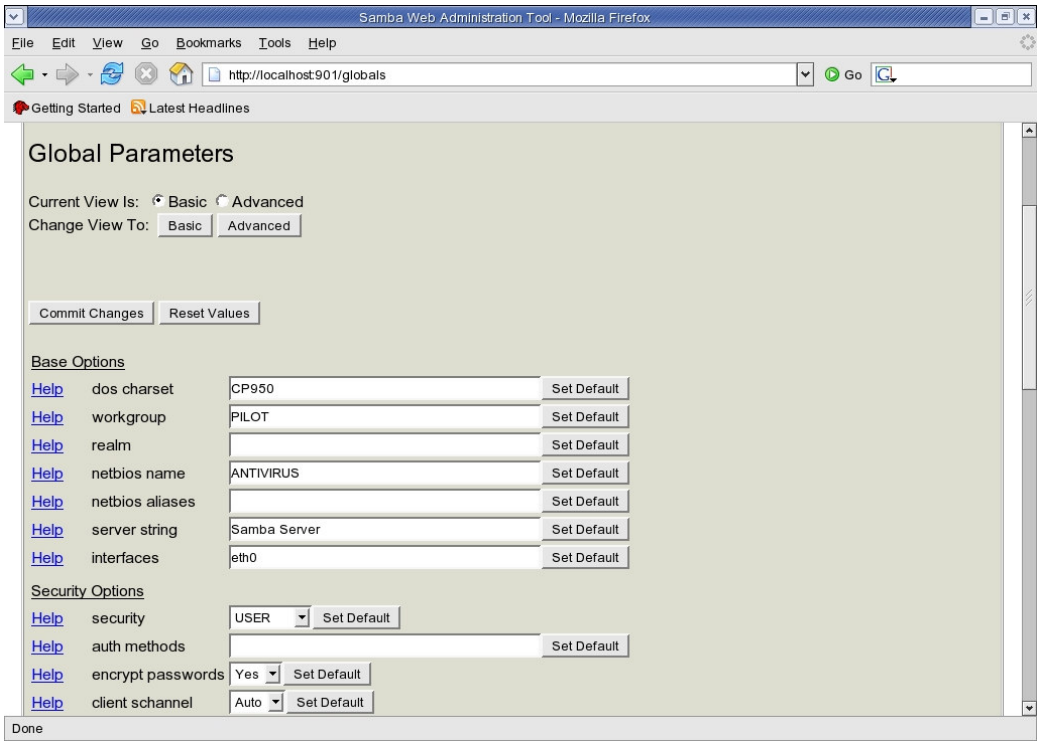
display charset = UTF-8

passdb backend = tdbsam

[home]

read only = No

browseable = No

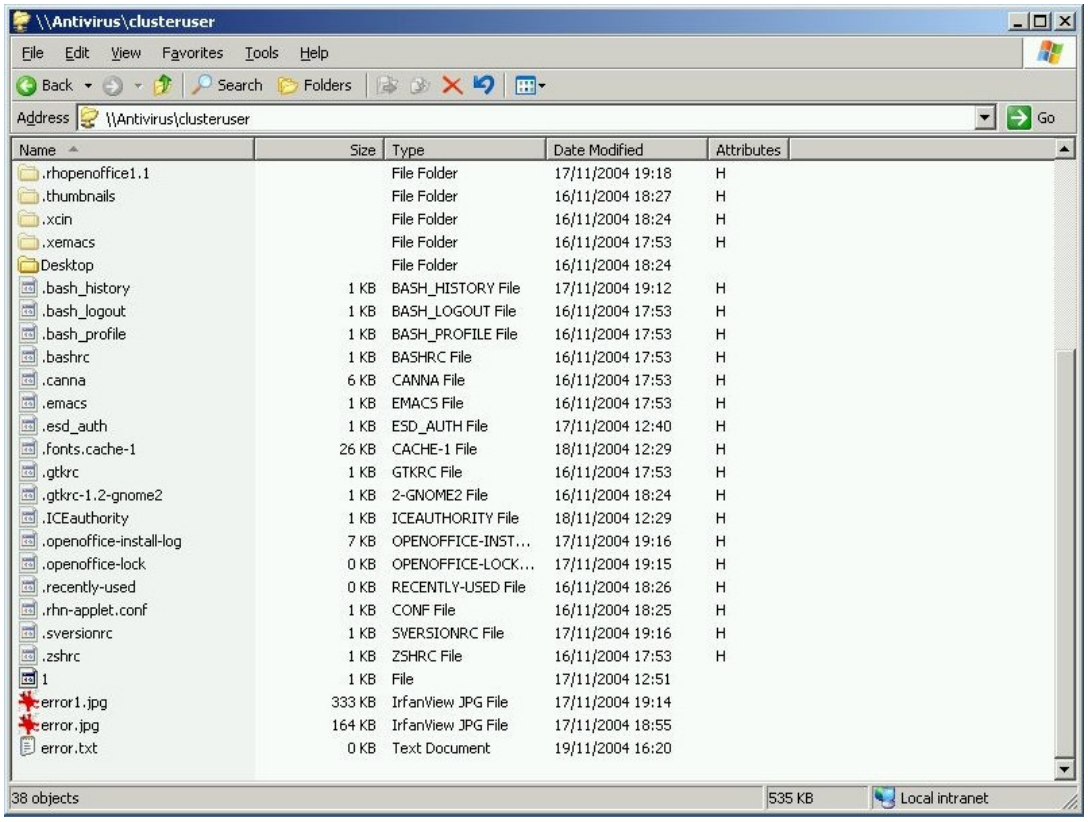


今次使用的簡單 Samba 設定。

留意當中沒有有關防毒軟體的設定，因爲有關的存取控制都已交給 NOD32 和 Dazuko 去執行。之後我們製作一個新的 Samba 用戶 clusteruser，執行以下命令即可。

useradd clusteruser (ENTER)

pdbedit -a clusteruser (ENTER)



從 Windows 客戶端存取 Samba 的情形。

防毒軟體 NOD32 的設定

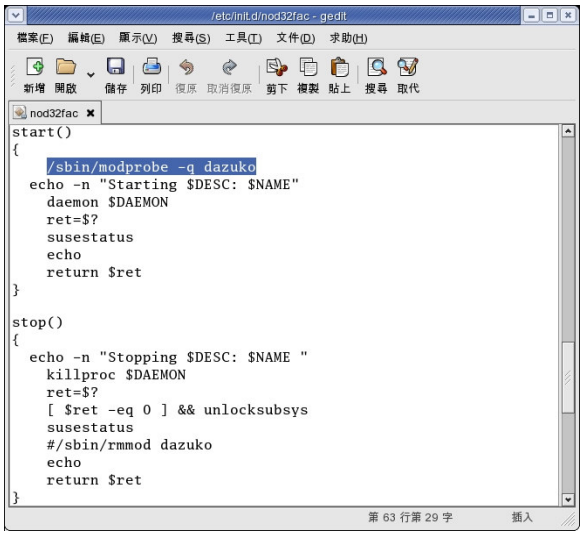
首先爲使系統在開機時載入 Dazuko 的模組，我們必須編輯/etc/init.d/nod32fac。打開後找出以下一行：

#/sbin/modprobe -q dazuko

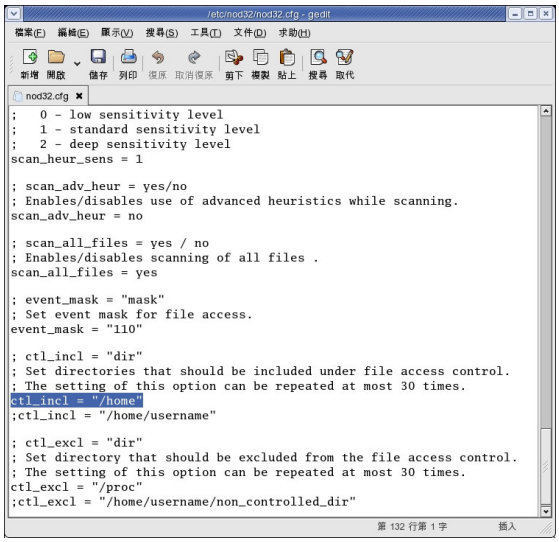
把前面的「#」除去，變成這樣：

/sbin/modprobe -q dazuko

以後每當 NOD32 啓動時都會自動載入 Dazuko 的模組。



編輯/etc/init.d/nod32fac。



指定需要 NOD32 實時監控的目錄。

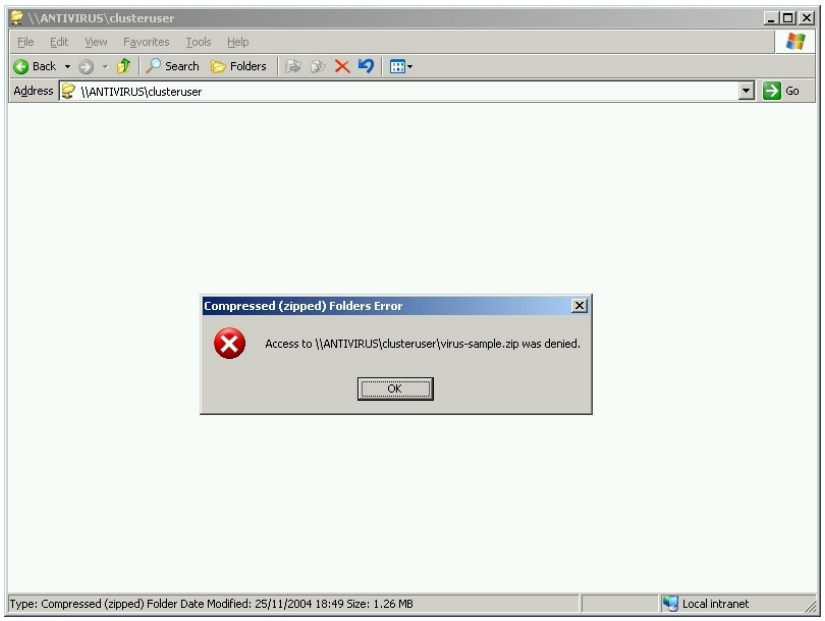
然後我們指定需要 NOD32 監控的目錄。例如我們希望 NOD32 監控/home 及其下的字目錄，便應編輯 /etc/nod32/nod32.cfg，在「fac」的部份找出「ctl_incl」加上以下一行：

ctl_incl = "/home"

「ctl_incl」可同時對 30 個目錄進行實時監控，只要把要實時監控的目錄依上述方法加入即可。完成設定後便可輸入以下命令啓動 NOD32。

service nod32fac start　(ENTER)

設定完成後，NOD32 便會發揮保護 Samba 檔案伺服器的功能，如果 NOD32 偵測得有病毒存在的話，便會馬上禁止其他用戶存取該檔案，NOD32 在預設值中已設定爲可偵測壓縮檔，之後系統管理員便可自行把該有問題的檔案刪除。至於病毒的記錄將被存放在/var/log/nod32fac.log。

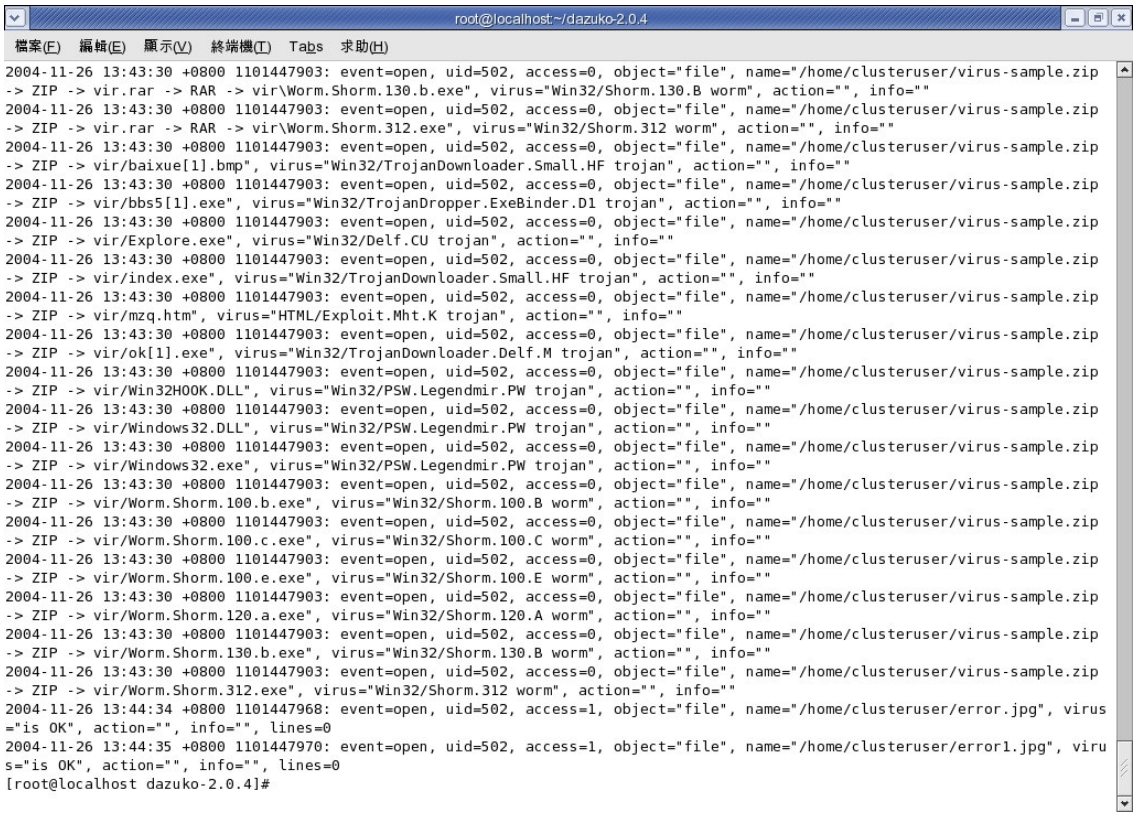


NOD32 會馬上禁止其他用戶存取該檔案。

至於病毒定義的更新方面，只要執行以下命令即可，但在更新之前必須編輯/etc/nod32/nod32.auth 檔加入由製造商提供的用戶名稱和密碼。

/usr/sbin/nod32_update (ENTER)

成功更新的話便可看到以下訊息。



要令 NOD32 定期自動更新，我們可以使用 Linux 的 crontab。輸入以下命令：

crontab -e　(ENTER)

鍵入「i」便可進入編輯模式，假設我們要在每天下午七時正麵自動進行自動更新，便可輸入以下文字。

0 19 * * * /usr/sbin/nod32_update

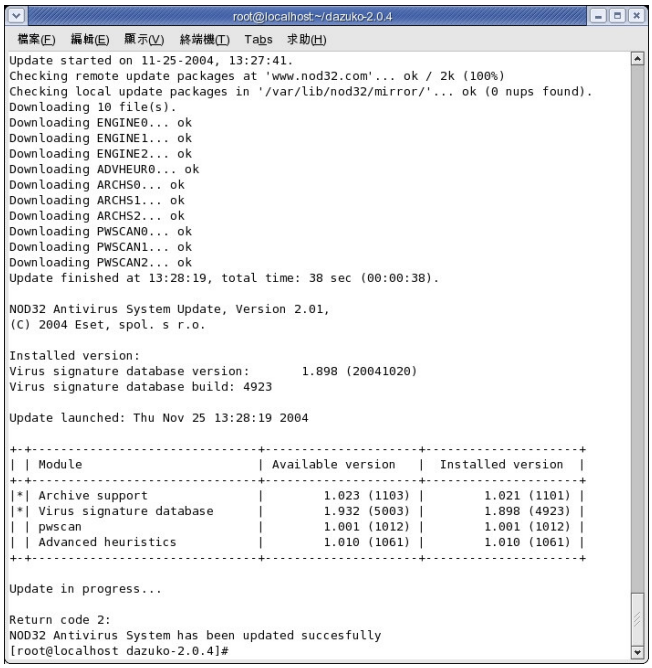
表示時間的數字以「分、時、日、月、星期」的順序排列。「*」代表「任何時間」，故全部設定爲「*」的時候，使會變成每分鐘執行一次。要指定每天的零時三十分、早上八時三十分、中午十二時三十分和晚上八時三十分更新的話，可輸入以下文字。

30 0,8,12,20 * * * /usr/sbin/nod32_update

完成設定後按「Esc」鍵，再輸入「:wq!」即可儲存並離開。

要確認剛才輸入的日程可用以下命令。

crontab -l　(ENTER)



成功更新的話便可看到有關訊息。