

# Audit akses file/direktori *shared* pada Samba server

By Henry Saptono < [boypyt@gmail.com](mailto:boypyt@gmail.com) >

Juli 2010

Ternyata untuk berbagi berkas/file dan direktori di linux sangat mudah dengan adanya samba ([www.samba.org](http://www.samba.org)). Direktori pada sistem linux yang di share dapat juga diakses oleh komputer lain yang menggunakan sistem operasi selain linux seperti microsoft windows. Sebenarnya kemampuan samba bukan hanya sekedar untuk berbagi berkas/file dan direktori saja, namun dapat pula digunakan untuk berbagi sumber daya lainnya seperti printer. Selain itu samba server dapat juga Anda konfigurasi agar berfungsi sebagai primary domain controller (PDC) menggantikan peran windows server sebagai PDC.

Umumnya komputer dengan sistem operasi linux sampai saat ini tidak rentan terhadap virus bahkan bisa dikatakan relatif lebih aman. Namun demikian ketika suatu direktori pada sistem linux, di *sharing* ke jaringan melalui service samba bukan berarti direktori tersebut tidak dapat disusupi oleh virus yang umumnya menyebar dan menyusup melalui aktifitas *sharing file* atau direktori yang dilakukan oleh komputer komputer yang ada didalam jaringan tersebut dimana umumnya menggunakan platform sistem operasi windows. Timbul pertanyaan, apakah samba server dapat melakukan pencegahan terhadap terjadi penyusupan virus kedalam direktori yang di *share*? Jawabannya bisa, yaitu menggunakan/memasang module virtual filesystem (vfs) khusus yang dapat dipasang pada samba server untuk melakukan scanning file-file bervirus yang akan ditulis kedalam direktori share pada samba server yaitu seperti **vscan-clamav**.

Meskipun kita bisa mencegah menyusupnya virus dari jaringan ke direktori yang di *share* oleh service samba dengan menambahkan module virtual filesystem (vfs) khusus tersebut namun ada baiknya mempertimbangkan dahulu pencegahan pada sisi komputer komputer klien windows dengan memasang program antivirus pada masing masing komputer windows karena justru disitulah akar masalahnya, sehingga samba server tidak dibebani dengan proses scanning virus saat file/direktori diakses oleh komputer komputer klien dari jaringan.

Terkait masalah seringnya share direktori disusupi oleh file bervirus maka penting bagi kita untuk menerapkan audit dan logging aktifitas akses file dan direktori yang terdapat pada direktori share samba server, agar kita dapat melacak dari komputer mana dan kapan file virus menyusup. Namun bagaimanakah caranya? Nah untuk itu penulis pada artikel kali ini sengaja akan membahas cara mengaktifkan kemampuan samba server dalam melakukan audit atau logging berbagai aktifitas terkait pengaksesan suatu file atau direktori pada direktori share samba yang juga relevan dengan permasalahan yang sebelumnya dipaparkan. Hal ini diangkat penulis juga karena adanya pertanyaan dari beberapa teman tentang mungkinkah kita dapat melacak aktifitas akses file dan direktori share pada samba server.

Dalam tulisan ini penulis tidak akan membahas secara detail bagaimana konfigurasi global samba server dan apa itu VFS (baca <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/VFS.html>), penulis akan fokus pada konfigurasi samba dengan peran standalone komputer, yaitu layaknya komputer windows klien ketika melakukan sharing direktori. Penulis akan memberikan contoh konfigurasi terkait proses audit aktifitas akses file atau direktori pada samba server. Untuk keperluan audit akses file dan direktori digunakan module virtual filesystem (vfs) **full\_audit** yang secara default sudah disertakan dalam paket software samba server. Dalam tulisan ini komputer yang berperan sebagai samba server menggunakan sitem operasi linux distribusi CentOS 5 (5.3).

## **Skenario**

Untuk memudahkan penjelasan tentang bagaimana implementasi audit atau logging aktifitas akses file/direktori yang dishare pada samba server maka berikut ini skenario konfigurasi samba server yang akan dijelaskan dalam tulisan kali ini:

- Komputer samba server memiliki peran sebagai **standalone** server bukan domain controller
- Nama workgroup samba server adalah **NANGNONG**
- Nama netbios samba server adalah **MYSAMBA01**
- Security level samba server yang digunakan adalah **SHARE**
- Nama direktori share adalah **CORETAN**
- Lokasi filesystem direktori share adalah **/opt/coretan**
- Sifat ijin akses ke direktori share CORETAN adalah siapapun(*public*) dapat mengakses dengan ijin **menulis**
- User public diasosiasikan ke user '**coretan**' dan group '**coretan**'
- Setiap aktifitas pengaksesan terhadap direktori share CORETAN dicatat kedalam file log **/var/log/samba/audit.log**
- Module VFS yang khusus digunakan untuk memungkinkan pencatatan log aktifitas akses file dan direktori adalah modul **vfs\_full\_audit**.
- Format pesan log yang akan tampak pada setiap baris dalam file log **/var/log/samba/audit.log** adalah menggunakan prefix **<username> | <IP/netbios name server> | <IP/netbios name client> | <nama share yang diakses>**
- Hanya Aksi sukses yang akan dicatat kedalam log, aksi tersebut adalah *aksi membuat direktori, merubah nama atau memindahkan file/direktori, menghapus file, menghapus direktori, dan membuat file.*
- Konfigurasi system logging (syslog), Facility log yang digunakan adalah **LOCAL6** dengan priority **NOTICE**
- Disumsikan paket software samba, samba-common, samba-client sudah diinstal saat instalasi sistem linux (untuk instalasi manual gunakan perintah **yum install samba samba-common samba-client**)

## Konfigurasi samba server

Langkah konfigurasi pertama yang harus dilakukan adalah konfigurasi samba server dengan mengedit file konfigurasi `/etc/samba/smb.conf` dan atur beberapa nilai parameter sehingga parameter minimal yang harus disesuaikan nilainya agar sesuai skenario adalah seperti berikut ini:

```
[global]
    workgroup = NANGNONG
    server string = Samba Server Version %v
    netbios name = MYSAMBA01
    security = share

[coretan]
    path = /opt/coretan
    public = yes
    browseable = yes
    read only = no
    force user = coretan
    force group = coretan
    vfs objects = full_audit
    full_audit:prefix = %u|%i|%m|%S
    full_audit:success = mkdir rename unlink rmdir pwrite
    full_audit:failure = none
    full_audit:facility = LOCAL6
    full_audit:priority = NOTICE
```

Selanjutnya jika direktori `/opt/coretan` belum ada maka buatlah dengan perintah berikut ini:

```
# mkdir /opt/coretan
```

Kemudian buatlah user sistem linux dengan nama user `coretan` dan group `coretan` dan jangan lupa untuk menambahkan user `coretan` sebagai user service samba juga , seperti berikut ini:

```
# useradd coretan
# smbpasswd -a coretan
```

Kemudian ubah kepemilikan direktori `/opt/coretan` menjadi milik user dan group `coretan` dengan perintah berikut ini:

```
# chown coretan.coretan /opt/coretan
```

## Konfigurasi Syslog

Agar catatan log dari aktifitas akses file dan direktori share pada samba server dapat ditulis kedalam file `/var/log/samba/audit.log` dengan jenis facility LOCAL6 (baca manual syslog) dan priority log NOTICE maka kita harus melakukan konfigurasi service logging yang disediakan oleh syslog daemon. Konfigurasi dilakukan dengan mengedit file `/etc/syslog.conf`, entri konfigurasi yang ditambahkan pada akhir file `/etc/syslog.conf` seperti berikut ini:

```
local6.* /var/log/samba/audit.log
```

Kemudian agar perubahan konfigurasi berpengaruh maka restart service syslog seperti berikut ini:

```
# service syslog restart
```

Selanjutnya restart juga service samba seperti berikut ini:

```
# service smb restart
```

## Uji coba

Untuk menguji hasil konfigurasi samba dan syslog apakah bekerja sebagaimana skenario yang telah dibuat cobalah Anda akses direktori share samba yang bernama share CORETAN dari komputer lain misalnya dari komputer windows menggunakan file manager yang ada seperti windows explorer, kemudian cobalah membuat dan menghapus direktori ataupun membuat dan menghapus file pada direktori share tersebut, kemudian amati file log `/var/log/samba/audit.log`, maka Anda akan melihat output pada file log tersebut yang menjelaskan aktifitas yang dilakukan komputer klien terhadap direktori share CORETAN, berikut ini contoh output yang akan tampak jika Anda membuat direktori baru dengan nama `'data'` pada direktori share CORETAN:

```
# tail /var/log/samba/audit.log
Jun 24 00:49:37 cen smbd_audit: coretan|192.168.1.65|192.168.1.229|
CORETAN|mkdir|ok|untitled folder
Jun 24 00:49:39 cen smbd_audit: coretan|192.168.1.65|192.168.1.229|
CORETAN|rename|ok|./untitled folder|./data
```