O Samba oferece também um recurso de geração de log. Ele pode ser ativado adicionando as opções abaixo na seção [global]do smb.conf:

log level = 1  
log file = /var/log/samba.log  
max log size = 1000

A opção “log level” indica o nível das mensagens (de 0 a 10), sendo que o nível 0 mostra apenas mensagens críticas, o nível 1 mostra alguns detalhes sobre os acessos e os demais mostram diversos níveis de informações de debug, úteis a desenvolvedores. A opção “log file” indica o arquivo onde ele será gerado e a “max log size” indica o tamanho máximo, em kbytes.

A partir do Samba 3.04 foi incluído um módulo de auditoria, que permite logar os acessos e as modificações feitas de uma forma muito mais completa que o log tradicional. Isso é feito através do módulo “full\_audit”, que (do ponto de vista técnico) funciona de forma similar ao módulo “recycle” usado pela lixeira.

O primeiro passo é ativar o módulo, o que é feito através da linha abaixo:

vfs objects = full\_audit

O próximo passo é definir quais operações devem ser logadas através da opção “full\_audit:success”, como em:

full\_audit:success = open, opendir, write, unlink, rename, mkdir, rmdir, chmod, chown  
(as opções formam uma única linha)

As opções que incluí no exemplo são open (ler um arquivo), opendir (ver os arquivos dentro de uma pasta), write (alterar um arquivo), unlink (deletar um arquivo), rename (renomear um arquivo), mkdir (criar um diretório), rmdir (remover um diretório), chmod (alterar as permissões de acesso de um arquivo) e chown (mudar o dono de um arquivo).

Você pode remover algumas destas opções, deixando apenas as opções desejadas, ou ver uma lista completa das opções que podem ser incluídas no manual do vfs\_full\_audit, disponível no:  
<http://samba.org/samba/docs/man/manpages-3/vfs_full_audit.8.html>

Continuando a configuração, especificamos as informações que desejamos que sejam incluídas no log, usando a opção “full\_audit:prefix”. Aqui podemos utilizar as variáveis que mostrei no tópico sobre o compartilhamento [homes], como a “%u” (o nome do usuário), “%I” (o IP da máquina) e “%S” (o nome do compartilhamento onde foi feito o acesso ou a alteração). Não é necessário incluir a variável referente ao nome da máquina, pois o nome é incluído automaticamente:

full\_audit:prefix = %u|%I|%S

Por padrão, o módulo loga não apenas os acessos e modificações, mas também um grande volume de mensagens de alerta e erros gerados durante a operação. A opção “full\_audit:failure = none” evita que estas mensagens sejam logadas, fazendo com que o log fique muito mais limpo e seja mais fácil encontrar as opções que realmente interessam:

full\_audit:failure = none

Concluindo, especificamos o nível dos alertas, entre os suportados pelo syslog, como em:

full\_audit:facility = local5  
full\_audit:priority = notice

Juntando tudo, temos:

vfs objects = full\_audit  
full\_audit:success = open, opendir, write, unlink, rename, mkdir, rmdir, chmod, chown  
full\_audit:prefix = %u|%I|%S  
full\_audit:failure = none  
full\_audit:facility = local5  
full\_audit:priority = notice

Esta configuração pode ser tanto incluída dentro da seção [global](de forma que o log inclua os acessos e as alterações feitas em todos os compartilhamentos) quanto ser incluída apenas na configuração de um compartilhamento específico.

Com isso, o Samba vai passar a gerar os eventos referentes aos acessos. Falta agora configurar o sysklogd (o serviço responsável pela geração dos logs do sistema), para logar os eventos, gerando o arquivo de log que poderá ser consultado. Para isso, abra o arquivo “**/etc/syslog.conf**” e adicione a linha abaixo:

**local5.notice /var/log/samba-full\_audit.log**

Note que o “local5.notice” corresponde aos valores informados nas opções “full\_audit:facility” e “full\_audit:priority”, enquanto o “/var/log/samba-full\_audit.log” é o arquivo de log que será gerado.

Depois de concluída a configuração, reinicie os serviços e o log passará a ser gerado imediatamente:

# /etc/init.d/samba restart  
# /etc/init.d/sysklogd restart

Dentro do arquivo, você verá entradas contendo a data e hora, o nome da máquina, o usuário, o IP da máquina, o nome do compartilhamento, a operação realizada e o nome do arquivo ou pasta onde ela foi realizada, como em:

Nov 18 15:21:15 m5 smbd\_audit: joao|192.168.1.23|arquivos|opendir|ok|.  
Nov 18 15:21:29 m5 smbd\_audit: joao|192.168.1.23|arquivos|open|ok|r|addr.txt  
Nov 18 15:21:34 m5 smbd\_audit: joao|192.168.1.23|arquivos|mkdir|ok|trabalho  
Nov 18 15:21:36 m5 smbd\_audit: joao|192.168.1.23|arquivos|opendir|ok|trabalho  
Nov 18 15:21:43 m5 smbd\_audit: joao|192.168.1.23|arquivos|open|ok|w|trabalho/Samba.sxw  
Nov 18 15:21:44 m5 smbd\_audit: joao|192.168.1.23|arquivos|open|ok|w|trabalho/foto.jpg

O log conterá entradas referentes a todos os usuários e máquinas, mas é fácil ver apenas as entradas referentes a um determinado usuário, compartilhamento, endereço IP ou outro parâmetro qualquer ao listar o arquivo pelo terminal usando o grep, que permite mostrar apenas as linhas contendo determinados trechos de texto, como em:

# cat /var/log/samba-full\_audit.log | grep “joao|192.168.1.23”

(mostra os acessos provenientes do usuário joao, feitos a partir do endereço 192.168.1.23)

# cat /var/log/samba-full\_audit.log | grep “|arquivos|”

(acessos feitos ao compartilhamento “arquivos”, por parte de qualquer usuário)

… e assim por diante. Você pode também direcionar a saída para um novo arquivo (ao invés de tentar lê-la pelo próprio terminal), como em:

# cat /var/log/samba-full\_audit.log | grep “|arquivos|” > arquivos.log