



Autenticando o SQUID no Active Directory via NTLM

Versão 2.0 - 09/06/2007

Sumário

Sumário	2
Objetivo	3
Pré-Requisitos.....	3
Introdução	3
Preparação do Ambiente	4
Instalação do Kerberos	5
Instalação do SAMBA/Winbind	7
Instalação do SQUID	9
Testes.....	12
Monitoração.....	12
Documentos Adicionais	12
Agradecimentos	12

Objetivo

O objetivo deste documento é configurar o SQUID (Proxy Open Source que roda em cima do Sistema Operacional LINUX) para efetuar a autenticação de usuários automaticamente através do login da estação de trabalho (NTLM).

Não vou entrar no mérito de qual o melhor proxy. (Se SQUID é melhor que ISA Server ou se o Isa Server é melhor que o SQUID). Há espaço suficiente para os dois no mercado atual. Em alguns casos é melhor utilizar o SQUID e em outros o MS Isa Server.

Pré-Requisitos

Conhecimento básico de Active Directory, Kerberos, Linux e Squid, conhecimento avançado de Samba/Winbind.

Introdução

Ultimamente, tenho visto diversas solicitações de usuários, tanto da comunidade MCPdx como de outras comunidades para saber como seria possível configurar o SQUID para integrar-se ao Active Directory (AD) e utilizar o login automaticamente, sem que seja solicitada a digitação no Internet Explorer.

Esta configuração é possível, desde que o SQUID esteja configurado para utilizar o SAMBA e o Winbind, que é o módulo que conversa com o AD via KERBEROS e utiliza a lista de usuários e senhas do AD. Desta forma, é possível utilizar dois tipos de autenticação: NTLM e BASIC.

A autenticação NTLM é automática, ou seja, o Internet Explorer detecta o usuário logado na estação de trabalho e utiliza para liberar a navegação no Proxy, que neste caso é o SQUID.

A autenticação BASIC é feita solicitando a digitação do usuário e senha ao tentar efetuar a navegação no Internet Explorer e após a digitação do usuário/senha é liberado o acesso.

A vantagem da utilização da autenticação via NTLM é que o usuário não é importunado para que fique digitando usuário e senha toda hora e quando não for possível utilizar NTLM, será solicitada a autenticação BASIC.

Preparação do Ambiente

Será necessário um servidor Windows 2000 ou 2003 atuando como Domain Controller e um servidor Linux para Proxy.

Neste caso específico, o servidor Linux está rodando Debian Sarge 3.1, mas o tutorial também pode ser utilizado com outras versões de Linux. Também sei que é possível utilizar o SQUID_NT que roda sobre o Windows, mas nunca utilizei.

Domain Controller:
Windows 2000 Adv. Server
FQDN: DC01.LAB.VIRTUAL
IP: 192.168.88.100

Proxy:
Debian Sarge 4.0 RC0
FQDN: PROXY.LAB.VIRTUAL
IP: 192.168.88.130

Obs.: É obrigatório que exista um SERVIDOR WINS na REDE!

Vamos instalar as dependências para dar seqüência ao tutorial:

Primeiro, edite o arquivo /etc/hosts colocando o nome e o ip do seu Domain Controller:

```
# vi /etc/hosts
```

```
192.168.88.100 dc01.lab.virtual      dc01
127.0.0.1      localhost.localdomain localhost prx
```

Em seguida, vamos instalar o NTPDATE para efetuar o sincronismo de horário entre o Servidor Linux e um NTP Server:

```
# apt-get install ntpdate
```

Instalação do Kerberos

- Kerberos p/ Linux

```
# apt-get install krb5-kdc krb5-config krb5-clients libpam-krb5 krb5-user
```

Caso apareça uma tela azul solicitando o Nome do Domínio e o IP do Servidor, coloque o FQDN do seu domínio (Neste caso, LAB.VIRTUAL) e o IP (Neste caso, 192.168.88.100).

Após a instalação dos pacotes acima, é necessário alterar o arquivo /etc/krb5.conf.

```
[libdefaults]
    default_realm = LAB.VIRTUAL

    krb4_config = /etc/krb.conf
    krb4_realms = /etc/krb.realms
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

v4_instance_resolve = false
v4_name_convert = {
    host = {
        rcmd = host
        ftp = ftp
    }
    plain = {
        something = something-else
    }
}
fcc-mit-ticketflags = true

[realms]
    LAB.VIRTUAL = {
        kdc = 192.168.88.100
        admin_server = 192.168.88.100:749
        default_domain = 192.168.88.100
    }

[domain_realm]
    .lab.virtual = LAB.VIRTUAL
    lab.virtual = LAB.VIRTUAL

[login]
    krb4_convert = true
    krb4_get_tickets = false

[logging]
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmin.log
    default = FILE:/var/log/krb5lib.log
```

Vamos editar alguns dos arquivos de configuração e efetuar a comunicação entre o Proxy e o Domain Controller via Kerberos.

Autor : Guilherme Kaneto

Primeiro, é necessário que o horário do servidor Linux e do Servidor Windows estejam sincronizados. Para isto, iremos utilizar um servidor NTP, seguindo os seguintes passos:

- Servidor Linux

```
# ntpdate ntp.cais.rnp.br
```

- Servidor Windows

```
C:\Winnt> net time /setsntp:ntp.cais.rnp.br  
C:\Winnt> net stop w32time & net start w32time
```

Em seguida, vamos iniciar a comunicação entre o Linux e o Domain Controller utilizando Kerberos. (Lembrando que o domínio utilizado neste tutorial chama LAB.VIRTUAL)

```
# kinit administrator@LAB.VIRTUAL
```

Será solicitada a senha do usuário "administrator". Se tudo correu bem, você irá rodar o comando "klist" e o retorno será semelhante ao que obtivemos, conforme abaixo:

```
# kinit administrator@LAB.VIRTUAL  
Password for administrator@LAB.VIRTUAL:  
# klist  
Ticket cache: FILE:/tmp/krb5cc_0  
Default principal: administrator@LAB.VIRTUAL  
  
Valid starting Expires Service principal  
02/22/07 14:25:47 02/23/07 00:25:47 krbtgt/LAB.VIRTUAL@LAB.VIRTUAL  
  
Kerberos 4 ticket cache: /tmp/tkt0  
klist: You have no tickets cached
```

Em seguida, vamos editar o arquivo nsswitch.conf

```
# vi /etc/nsswitch.conf
```

E alterar as linhas:

DE:

```
passwd: compat  
group: compat
```

PARA:

```
passwd: compat winbind  
group: compat winbind
```

Pronto! O ambiente está preparado para receber o SAMBA/Winbind e o SQUID.

Autor : Guilherme Kaneto

Instalação do SAMBA/Winbind

A instalação do SAMBA/Winbind é simples e pode ser feita via apt-get. Então, vamos por a mão na massa:

```
# apt-get install samba winbind
```

Após rodarmos o comando acima, será aberta uma tela de configuração, onde é solicitado o nome do domínio, o uso de senhas encriptadas, que OBRIGATORIAMENTE tem que ser SIM e também é necessário que o samba crie o arquivo de senhas.

Agora é necessário configurar o samba. Para isso, vamos fazer backup do arquivo original e depois vamos criar o nosso arquivo de configuração.

```
# mv /etc/samba/smb.conf /etc/samba/smb.original  
# vi /etc/samba/smb.conf
```

O arquivo smb.conf deve conter OBRIGATORIAMENTE as linhas abaixo. Outras configurações podem ser feitas de acordo com a necessidade.

```
[global]  
workgroup = LAB  
netbios name = PROXY  
server string = PROXY SERVER  
load printers = no  
log file = /var/log/samba/log.%m  
max log size = 500  
realm = LAB.VIRTUAL  
security = ads  
auth methods = winbind  
password server = dc01.lab.virtual  
winbind separator = +  
encrypt passwords = yes  
winbind cache time = 15  
winbind enum users = yes  
winbind enum groups = yes  
winbind use default domain = yes  
idmap uid = 10000-20000  
idmap gid = 10000-20000  
local master = no  
os level = 233  
domain master = no  
preferred master = no  
domain logons = no  
wins server = 192.168.88.100  
dns proxy = no  
ldap ssl = no
```

Autor : Guilherme Kaneto

Criado o arquivo de configuração, vamos reiniciar os serviços do Samba e do Winbind.

```
# /etc/init.d/samba stop
# /etc/init.d/winbind stop
# /etc/init.d/samba start
# /etc/init.d/winbind start
```

Obs.: Não esqueça de verificar os logs para saber se tudo iniciou corretamente.

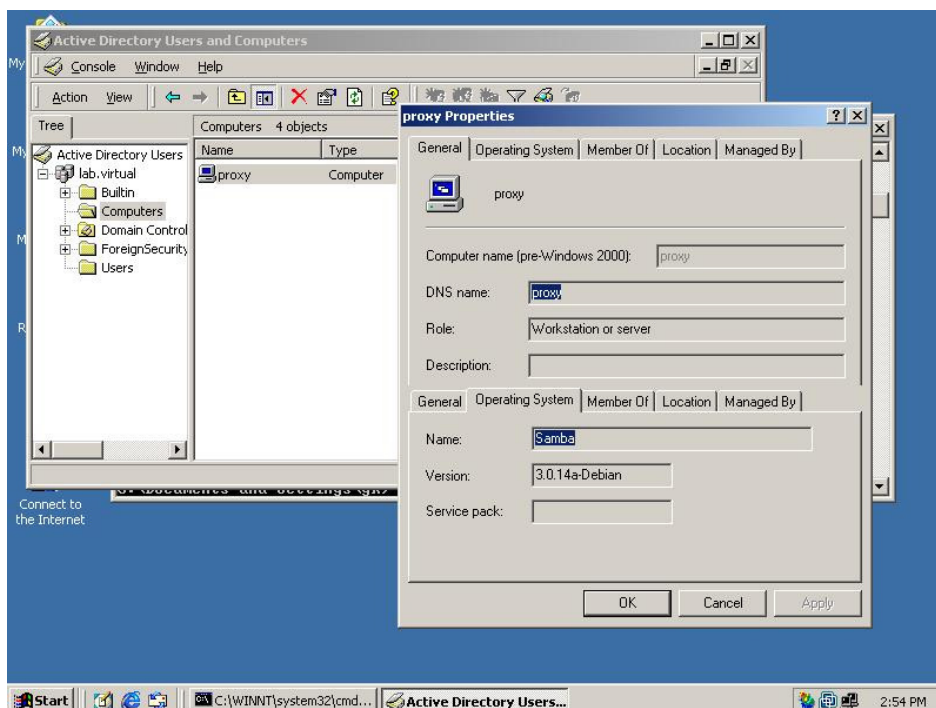
Agora vamos colocar a máquina linux no domínio Windows.

```
# net ads join -U administrator -S LAB.VIRTUAL
```

Após digitar a senha, que será solicitada, o retorno deve ser semelhante ao retornado abaixo:

```
# net ads join -U administrator -S LAB.VIRTUAL
administrator's password:
Using short domain name -- LAB
Joined 'PROXY' to realm 'LAB.VIRTUAL'
```

Pronto! A máquina que está rodando o LINUX já faz parte do Domínio Microsoft e pode ser vista no Active Directory Users and Computers:



Agora vamos definir o usuário que irá ser utilizado pelo winbind e verificar se podemos listar usuários e grupos do AD (Recomendo a criação de uma conta de serviço específica com as permissões necessárias.)

```
# wbinfo --set-auth-user=svr-winbind
- Reiniciando os serviços
```

Autor : Guilherme Kaneto

```
# /etc/init.d/samba stop && /etc/init.d/samba start  
# /etc/init.d/winbind stop && /etc/init.d/winbind start
```

- Verificando se o Winbind está comunicando com o RPC Server

```
# wbinfo -t  
Retorno Esperado: checking the trust secret via RPC calls succeeded
```

- Listando Usuários do AD

```
# wbinfo -u
```

- Listando os Grupos do AD

```
# wbinfo -g
```

Ótimo! Tudo ok, podemos dar seqüência na instalação do Squid!

Instalação do SQUID

O squid deve ser instalado pelo source, pois usaremos algumas opções específicas que não são utilizadas ao usar o apt-get. (Recomendo a utilização da versão 2.5, pois quando utilizei a 2.6-STABLE não funcionou de acordo, mas não testei as versões mais novas.)

Vamos ao que interessa:

- Entrando no diretório de sources

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

- Efetuando o Download do pacote estável.

```
# wget http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE14.tar.gz
```

- Descompactando

```
# tar zxvf squid-2.5.STABLE14.tar.gz
```

- Acessando o Diretório do Squid/Source

```
# cd squid-2.5.STABLE14
```

- Compilando com as opções necessárias

```
# ./configure --prefix=/usr --exec_prefix=/usr --bindir=/usr/sbin --sbindir=/usr/sbin --  
libexecdir=/usr/lib/squid --sysconfdir=/etc/squid --localstatedir=/var/spool/squid --  
datadir=/usr/share/squid --enable-auth="ntlm,basic" --enable-basic-auth-helpers="winbind" -  
-enable-ntlm-auth-helpers="winbind" --enable-external-acl-  
helpers="winbind_group,wbinfo_group" --enable-delay-pools --enable-removal-policies --  
enable-underscores --enable-cache-digests --disable-ident-lookups --enable-truncate --enable-  
arp-acl --with-winbind-auth-challenge
```

- Instalando

```
# Make && make install
```

- Criando o Grupo para utilizar o Squid

```
# groupadd proxy
```

- Criando o Usuário e colocando-o no grupo do Squid

```
# useradd proxy -g proxy
```

Autor : Guilherme Kaneto

- Dando permissão para o diretório do SQUID

```
# chown -R proxy.proxy /usr/share/squid  
# chown -R proxy.proxy /var/spool/squid
```

- Efetuando bkp do arquivo de configuração original

```
# cd /etc/squid/etc  
# mv squid.conf squid.original
```

- Limpando todas as linhas comentadas do squid.original e gerando o squid.conf

```
# egrep -v "^#|^$" squid.original > squid.conf
```

- Gerando o diretório de logs e liberando as permissões

```
# mkdir /var/log/squid  
# chown -R proxy.proxy /var/log/squid
```

- Liberando a permissão no arquivo do Winbind

```
# chown root.proxy /var/run/samba/winbindd_privileged
```

- Reiniciando o Winbind

```
# /etc/init.d/winbind stop & /etc/init.d/winbind start
```

Editando o arquivo squid.conf e colocando as linhas abaixo (As linhas em vermelho são as linhas utilizadas pela autenticação NTLM):

```
# vi /etc/squid/squid.conf
```

```
http_port 3128  
cache_effective_user proxy  
cache_effective_group proxy  
cache_log /var/log/squid/cache.log  
cache_access_log /var/log/squid/access.log  
cache_store_log /var/log/squid/store.log  
hierarchy_stoplist cgi-bin ?  
acl QUERY urlpath_regex cgi-bin \?  
no_cache deny QUERY  
auth_param ntlm program /usr/bin/ntlm_auth LAB/DC01 --helper-protocol=squid-2.5-ntlmssp  
auth_param ntlm use_ntlm_negotiate off  
auth_param ntlm children 10  
auth_param ntlm max_challenge_reuses 0  
auth_param ntlm max_challenge_lifetime 5 minutes  
auth_param basic program /usr/bin/ntlm_auth LAB/DC01 --helper-protocol=squid-2.5-basic  
auth_param basic children 5  
auth_param basic realm Digite o LOGIN/SENHA  
auth_param basic credentialsttl 2 hours  
auth_param basic casesensitive off  
refresh_pattern ^ftp: 1440 20% 10080  
refresh_pattern ^gopher: 1440 0% 1440  
refresh_pattern . 0 20% 4320  
acl all src 192.168.88.0/255.255.255.0  
acl manager proto cache_object  
acl localhost src 127.0.0.1/255.255.255.255
```

Autor : Guilherme Kaneto

```
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT
acl acesso proxy_auth REQUIRED # Solicitando a autenticação
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow acesso # Liberando usuários autenticados
http_access allow all
http_reply_access allow all
icp_access allow all
coredump_dir /usr/local/squid/var/cache
```

- Criando o cache e iniciando o squid.

```
# squid -z
# squid &
```

- Para utilizar as regras baseadas em Grupos do Active Directory, utilize as seguintes linhas no seu squid.conf

```
external_acl_type nt_group %LOGIN /usr/lib/squid/wbinfo_group.pl
acl AllowedWindowsGroups external nt_group GrupodoAD
http_access allow AllowedWindowsGroups
```

Depois de editar o seu squid.conf, não esqueça de recarregá-lo:

```
# squid -k reconfigure
```

Testes

Efetue a configuração do PROXY no navegador (192.168.88.130:3128) e tente acessar algum website.

Monitoração

Monitorando o arquivo de log de acessos do squid com o commando tail -f e vemos que o acesso foi liberado utilizando o usuário GK, que é o usuário logado na estação de trabalho.

```
# tail -f /var/log/squid/access.log
```

```
1172165029.325          756   192.168.88.100   TCP_MISS/200   9646   GET  
http://home.img.uol.com.br/0702/d/festa22.jpg gk DIRECT/200.221.7.37 text/plain
```

Documentos Adicionais

<http://pt.wikipedia.org/wiki/Kerberos>
<http://en.wikipedia.org/wiki/NTLM>
<http://davenport.sourceforge.net/ntlm.html>
<http://www.linuxman.pro.br/squid/>

Agradecimentos

Primeiramente a minha Noiva, por me agüentar durante 8 anos, a Comunidade MCPdx, principalmente aos Owners pela força, Rodrigo Barros Lopes, Mauro Palomaro, Felipe Sammarco e Maurício Bonami (Autor do tutorial Integrando Postfix com Active Directory)

Quaisquer críticas, dúvidas e/ou sugestões, estou as ordens.

Guilherme Kaneto

guikaneto at gmail dot com
MCSA 2003
MCSA Messaging

Moderador do Grupo MCPdx
Portal MCPdx: <http://portal.mcpdx.eti.br>