



Versão 1.41

Alceu Rodrigues de Freitas Junior

São Paulo

2003

Agradecimentos

Gostaria de agradecer o time de desenvolvimento do Squid, por ter escrito um excelente software e torná-lo livremente disponível, oferecendo uma alternativa, muitas vezes superior, a produtos comerciais existentes.

Gostaria e agradecer também **Aurélio Marinho Vargas**, por ter escrito o Guia de Expressões Regulares e torná-lo disponível gratuitamente na Internet, me ajudando a criar expressões regulares não só para o Squid mas também para diversos outros fins.

Meu muito obrigado também ao autor do artigo “Autorização baseada em grupos de um domínio NT/2000 no Squid, utilizando o Samba/winbind” **André Moraes** (andrelmoraes@terra.com.br) e seu colaborador **Glaúcio Rocha** (garocha@terra.com.br), por terem permitido incluir o mesmo neste manual.

Índice

Introdução.....	1
Sobre as versões desse manual.....	1
Capítulo 1 - Requisitos básicos.....	2
Capítulo 2 - O feijão com arroz.....	3
2.1 - Instalação.....	3
2.2 - Configuração.....	3
Capítulo 3 - Controlando os usuários.....	5
3.1 - Exemplos de configuração.....	7
Capítulo 4 - Autenticação.....	10
4.1 - Módulo NCSA de autenticação.....	10
4.2 - Módulo SMB de autenticação.....	11
4.3 - Problemas à vista.....	11
4.4 - Módulo de autenticação Winbind.....	12
4.4.1 - Instalação e configuração do Samba com suporte ao winbind.....	12
Opções de Compilação.....	12
Compilação e instalação.....	12
Configuração.....	13
Testes.....	15
Scripts de inicialização automática.....	16
4.4.2 - Instalação e configuração do Squid.....	17
Download e descompactação do código-fonte.....	17
Opções de Compilação.....	17
Compilação e instalação.....	18
Configuração.....	18
Testes.....	19
Script de inicialização automática.....	22
4.4.3 - Manutenção.....	22
Capítulo 5 - Gerenciamento de cache.....	24
Capítulo 6 - Recursos na Internet.....	25
Bibliografia.....	26
Licença de uso.....	27

Introdução

Resolvi escrever esse manual principalmente porque ninguém o havia feito antes. Dentre todos os inúmeros documentos sobre Linux e software livre em <http://www.linuxdoc.org> não havia nenhum que falasse sobre Squid, mesmo em inglês, quem diria em português.

Você poderá encontrar maiores informações sobre o Squid no seu *website* (<http://www.squid-cache.org>) e ainda poderá recorrer a FAQs e a lista de discussão para dúvidas.

Squidnomicon significa manual do Squid. Eu achei divertido fazer graça com relação ao Necronomicon (Livro dos Mortos). Mas não espere encontrar nenhuma outra semelhança além desta. Talvez eu use um desenho do grande Cthullu como logo do manual, mas tenho receio dos direitos autorais.

Este manual é livre e está sobre a licença *Free GNU Documentation*. Qualquer ajuda (dicas, comentários) e/ou modificações são muito bem-vindas. Você pode escrever para o email glasswalk3r@yahoo.com.br nesses casos.

Esse manual foi criado à partir do uso do Open Office, versão 1.1. Nenhum byte foi ferido durante o processo.

Sobre as versões desse manual

Eu resolvi adotar um critério bem simples para numerar as versões do manual. O primeiro número indica a versão do manual. Os últimos dois indicam os *releases* ou novas versões. O segundo número indica que algo novo foi incluído no manual, como descrições de recursos não apresentados em versões anteriores.

O terceiro número mostra correções em relação ao manuais anteriores.

Capítulo 1 - Requisitos básicos

Para utilizar o Squid, você terá que ter:

- ➔ um UNIX: o tutorial tem seu foco em Linux, mas com algum esforço você pode utilizar o mesmo tutorial em FreeBSD, SUN Solaris, etc. **Existe** versões do Squid para MS Windows, mas esse manual não cobre a utilização desse proxy nesta plataforma de sistema operacional.
- ➔ o pacote/fonte do Squid;
- ➔ um computador: para testes qualquer um serve, mas para entrar em operação você terá que ter pelo menos um Pentium 2 com 128MB e um HD de 4 Gb. Isto é aproximado, e pode variar muito conforme o número de usuários versus requisições. Basta saber que os requisitos de hardware de um servidor proxy são muito maiores em relação à quantidade de memória e velocidade do disco do que para um firewall, principalmente devido ao cache; velocidade de processamento também influirá na performance do proxy.
- ➔ conhecimento básico sobre protocolo TCP-IP e Internet;
- ➔ conhecer o UNIX no qual você quer instalar o Squid!

Capítulo 2 - O feijão com arroz

O Squid é um webproxy que suporta proxying para DNS e FTP, além do tradicional HTTP/HTTPS. Ele permite também a criação de árvores de cache via HTCP, load balance para servidores HTTP (vide `http_accelerator`) e diversos modos de autenticação de usuário, o que também inclui a possibilidade de criação de listas de sites e/ou palavras proibidas para acesso.

Neste capítulo irei mostrar apenas o básico para você ter o Squid rodando. Com essas configurações, você irá ter o Squid como proxy e efetuando cache das páginas visitadas.

2.1 - Instalação

A instalação poderá depender de qual distribuição você estiver usando. Normalmente você encontrará o Squid nos CDROM de distribuição em formatos RPM, DEB ou TGZ. Você também pode usar o fonte do Squid e compilar os binários usando somente as funções que você precisar.

Para distribuições que trabalham com pacotes a instalação é muito simples:

```
rpm -ivh squid-versao.rpm
```

para distribuições baseadas em RPM ou

```
apt-get install squid
```

para o Debian

O Conectiva (à partir da versão 6 e posteriores) também podem usar as mesmas facilidades do `apt-get`. O Red Hat também possui o comando `up2date` e as distribuições do SuSe, Mandrake e Slackware possui seus comandos similares.

Para instalar a partir do fonte, faça o download do Squid em <http://www.squid-cache.org> na seção de downloads. Depois execute:

```
tar -xzf squid-versao.tar.gz
cd /diretorio_criado
./configure
make
make install
```

Ler o arquivo README que acompanha o arquivo fonte também é essencial para obter os detalhes.

A versão termina em números pares (para versões estáveis) e ímpares (para versões de teste) então escolha a ultima de acordo com seus interesses. Procure sempre pelos arquivos RELEASE inclusos.

2.2 - Configuração

Depois de instalado você provavelmente (espero!) terá os binários e arquivos de configuração, muitos deles comentados e precedidos de comentários sobre as funções que exercem.

O arquivo de configuração do Squid fica em `/etc/squid.conf`.

Inicialmente você deve configurar apenas 3 parâmetros para que tenha o Squid ao menos respondendo a requisições e criando cache das páginas requisitadas:

```
http_port 3128
cache_mem 8Mb
http_access allow all
```

Com exceção do ultimo parâmetro (que deve ser inserido) esses parâmetros estão apenas comentados (com um sinal "#"). Depois disso você pode iniciar o Squid usando o script de inicialização que fica dentro do diretório */etc/rc.d/init.d* (ou */etc/init.d* para o Debian):

```
# cd /etc/rc.d/init.d
# ./squid start
```

Na maioria das distribuições o cache é criado quando o Squid é iniciado pela primeira vez (pelo menos para sistemas Linux). Você ainda pode forçar a criação de cache digitando:

```
# squid -z
```

Ainda é possível fazer com que o Squid interprete novos parâmetros no arquivo de configuração sem interromper os processos atuais:

```
# squid -k reconfigure
```

O Squid já está rodando e aceitando conexões. Agora vamos explicar melhor os parâmetros utilizados:

```
http_port 3128
```

Este parâmetro indica em que porta o Squid estará aceitando requisições de páginas Web. Várias portas diferentes podem ser listadas simultaneamente, desde que estejam livres.

```
cache_mem 8Mb
```

Este parâmetro especifica a quantidade ideal de memória a ser usada pelo Squid, mas isso não significa um limite. O Squid irá ultrapassar o valor estipulado se assim for necessário.

```
http_access allow all
```

Inicialmente o Squid estará recusando o serviço de proxy para qualquer requisição que não tenha sido feita a partir do localhost (127.0.0.1). Essa diretriz, pelo contrário, esta permitindo que qualquer um requisite qualquer página.

O Squid permite uma grande flexibilidade sobre o que é permitido ou não que o cliente requisite (conforme você poderá acompanhar mais à frente). Agora você pode fazer um teste com um navegador qualquer, como o Netscape ou o Internet Explorer. Para isso, configure (na parte referente a servidor proxy) o endereço IP do proxy Squid sem esquecer de indicar a porta 3128.

As solicitações agora serão atendidas pelo Squid, que irá fazer cache das requisições, como páginas html e figuras, o que aumenta consideravelmente a rapidez de navegação e diminui a ocupação de banda do link.

Capítulo 3 - Controlando os usuários

Usuários costumam dar dores de cabeça horríveis a um administrador de redes, mas também sem eles como você justificaria seu salário?

O Squid fornece meios de evitar que você tenha (muitos) problemas com seus usuários acessando a Internet para fins não muito ortodoxos. Você pode bloquear acesso a algum tipo de recurso ou a um site inteiro.

No arquivo */etc/squid.conf* existem definições de listas de controle (ACL em inglês) e como é feito o acesso a recursos definidos nestas listas.

Antes de mostrar como a lista é feita, procure ter antes em mente a seguinte idéia:

1 - As regras são interpretadas na ordem que aparecem: quando você define regras, a primeira é interpretada. Se a regra descrita não combinar com a requisição a mesma será comparada com a próxima regra, e assim por diante.

2 - Sempre, **SEMPRE** coloque como última regra uma ACL que bloqueie tudo. Se você não fizer isso, seu controle vai para o espaço.

3 - Não crie regras demais e desnecessárias! Procure evitar redundâncias e regras de controle que exijam resolução de nomes. Isso pode atrasar muita a resposta do Squid para requisições.

4 - Se você precisa criar muitas regras e precisa de maior flexibilidade para criá-las, procure utilizar o software **Squidguard**: o pobre Squid começa a engasgar se você o entope de regras. Ele trabalha em conjunto com o Squid e permite utilizar um número de regras **muito** maior (e com maior flexibilidade) sem perda de performance. O Squidguard pode ser encontrado em: <http://www.squidguard.org>

Existem diversos critérios/tipos de listas. Acompanhe abaixo:

SCR

A lista é baseada no endereço IP do cliente (requisitante).

DST

A lista é baseada no endereço IP do servidor (que será requisitado).

SCRDOMAIN

O domínio da máquina cliente. O domínio serão obtido por resolução reversa de IP o que pode causar atrasos para a requisição ter resposta.

DSTDOMAIN

Método de controle sobre um domínio específico.

SRCDOM_REGEX

Expressão regular que é avaliada para tentar marcar um domínio requisitante; esse parâmetro pode causar atrasos por usar resolução reversa de endereço IP.

DSTDOM_REGEX

O mesmo que srcdom_regex só que para o domínio de destino.

TIME

Dia da semana e hora da semana.

URL_REGEX

Essa ACL irá procura em na URL uma expressa regular que você especificar.

URLPATH_REGEX

Semelhante ao url_regex só que ira procurar a expressão na url toda exceto no nome do protocolo e domínio. Isso irá tentar combinar com o nome do diretório ao longo da url.

PORT

O acesso pode ser controlado pela porta do endereço do servidor requisitado.

PROTO

Especifica o protocolo de transferência.

METHOD

Especifica o tipo de método da requisição (GET ou POST).

BROWSER

Expressão regular cujo padrão tentará combinar com o contido no cabeçalho HTTP de requisição do cliente. Isso é útil se você quiser bloquear o acesso a sites do Windows Update, por exemplo, pelo Internet Explorer.

IDENT

Seqüência de caracteres que combinam com o nome do usuário. Requer um servidor Ident rodando na máquina do cliente, o que pode ser uma dor de cabeça caso seus clientes sejam sistemas não-UNIX (apesar de existirem clientes IDENT para outros sistemas operacionais). O IDENT seria utilizado para identificar qual usuário está fazendo a requisição da página, mas esse é um método **muito** pouco confiável, considerando que o usuário pode simplesmente parar o servidor ident e sair navegando por aí livremente. Se você quer identificar usuários, **use autenticação**.

IDENT_REGEX

O mesmo que ident, mas utilizando-se de uma expressão regular.

PROXY_AUTH

Permite a autenticação de usuários através do envio de usuário/senha. Requer um programa externo para realizar essa autenticação. Veja no próximo capítulo como usar um.

PROXY_AUTH_REGEX

O mesmo que proxy_auth, só que ira tentar combinar o nome do usuário fornecido pelo programa de autenticação através de uma expressão regular.

SNMP_COMMUNITY

Seqüência de caracteres que tentarão combinar com o nome da comunidade SNMP.

REQ_MIME_TYPE

Expressão regular que tentará combinar com o tipo de conteúdo contido no cabeçalho de requisição.

ARP

Tenta combinar o MAC ADDRESS da máquina requisitante.

Como você pode ter notado, existe uma quantidade bem grande de facilidades com as quais você pode construir uma ACL, até mais do que você provavelmente ira precisar (eu me pergunto se alguém

usa ident).

Depois de definir as listas de controle você precisa definir para cada linha da acl o que ela poderá ter como permitido (ou negado). A lista de regras já é um pouco menor.

HTTP_ACCESS

sintaxe: `http_access allow | deny [!] acl`

Descrição: permite ou nega acesso ao serviço http baseado na lista de acesso (acl) definida. O uso de "!" indica inversão (diferente de).

Eu coloquei uma observação um pouco acima de que você sempre tem de ter como última regra uma regra de bloqueie tudo, a fim de evitar brechas no conjunto de acl's que você tenha criado. Você pode usar o `http_access` para bloquear acesso a http dessa forma:

```
acl all src 0.0.0.0/0
http_access deny all
```

Isso diz ao Squid "qualquer requisitante". No final das contas, se um requisitante não tiver seu pedido encaixado em alguma acl anterior, ele terá seu pedido negado.

ICP_ACCESS

sintaxe: `icp_access allow | deny [!] acl`

descrição: use para forçar seus vizinhos a usarem você como um “filho” ao invés de “pai”. Isso é utilizado quando se trabalha com árvores de cache.

MISS_ACCESS

sintaxe: `miss_access allow | deny [!] acl`

descrição: limita os domínios que podem fazer requisições ao cache do servidor utilizando os recursos acl.

PROXY_AUTH_REALM

sintaxe: `proxy_auth_realm seqüência de caracteres`

descrição: na realidade esse comando não exerce nenhum tipo de controle, apenas informa ao cliente (através da seqüência de caracteres) aonde ele esta realizando o logon. Não é essencial, mas o padrão aparece como "Squid proxy" e você pode mudar isso sem problemas.

IDENT_LOOKUP_ACCESS

sintaxe: `ident_lookup_access allow | deny acl`

descrição: se a acl combinar com a requisição do cliente, este cliente será autenticado por uma procura ident.

3.1 - Exemplos de configuração

Agora que todos os itens foram discutidos vou mostrar alguns exemplos práticos de configuração para controle de acesso.

1 - Permitir `http_access` para apenas uma máquina com MAC address igual a 00:08:c7:9f:34:41 :

```
acl all src 0.0.0.0
acl pl800_arp arp 00:08:c7:9f:34:41
http_access allow pl800_arp
http_access deny all
```

2 - Para restringir acesso nas horas de trabalho (9 horas - 17 horas, de segunda sexta) da faixa de IP 192.168.2.0 máscara 255.255.255.0 :

```
acl all src 0.0.0.0
acl ip_acl src 192.168.2.0/24
acl time_acl time M T W H F 9:00-17:00
http_access allow ip_acl time_acl
http_access deny all
```

3 - Usar uma lista de controle com multiplos horários para diferentes usuários:

Se você pensou em algo assim:

```
acl carlos src 192.168.10.1
acl davi src 192.168.10.2
acl cleusa src 192.168.10.3
acl manhã time 06:00-11:00
acl tarde time 14:00-14:30
acl noite time 16:25-23:59
http_access allow carlos manhã almoço
http_access allow davi manhã almoço
http_access allow cleusa noite
```

você errou!

O Squid interpreta regras desta forma:

http_access REGRA definição1 E definição 2 E definição3
OU

http_access AÇÃO definição1 E definição 2 E definição3

Atenção porque esses E e OU são operadores lógicos! Portanto a acl:

```
http_access allow carlos manhã almoco
```

nunca irá funcionar porque *manhã* E *almoço* serão sempre falsos, uma vez que nunca serão verdadeiros na mesma hora. Como é falso (de acordo com a lógica booleana):

0/1 E 1 = 0 (falso)

```
http_access allow carlos E manhã OU
http_access allow carlos almoço
```

O uso de “E” e “OU” é apenas ilustrativo: não vá inseri-los no arquivo de configuração!

4 - Criar uma acl para bloquear sites com a palavra sexo pois meus funcionários ficam baixando filmes em Divx de pornografia:

```
acl porno url_regex sexo
http_access deny porno
```

Isso tem algumas consequências¹. Primeiro que essa regra deve encabeçar a lista para você não correr o risco de liberar o acesso antes de bloqueá-lo. Segundo que um site

¹ Como tudo na vida, afinal das contas.

<http://www.sexoesaude.com.br> estaria encaixado na lista de bloqueio, apesar do conteúdo não ser o mesmo.

5 - A idéia acima é ótima, mas eu tenho uma lista de palavras para fazer o mesmo. Terei que repetir esse comando várias vezes?

De forma alguma:

```
acl porno url_regex "/etc/squid/porno.txt"
http_access deny porno
```

No arquivo texto, inclua uma palavra sobre a outra, como uma coluna.

6 - Ainda existem sites que escapam a esse controle. Gostaria de bloqueá-los diretamente.

```
acl porno2amissao dstdomain playboy.com
```

ou

```
acl porno2amissao dstdomain "/etc/squid/pornosites.txt"
http_access deny porno2
```

7 - Meu diretor reclama que agora não consegue mais ler as entrevistas no site da Playboy.

Chefe é chefe. Antes que ele deixe de pagar seu salário, inclua no arquivo */etc/squid.conf*:

```
acl entrevistas urlpath_regex entrevistas
http_access allow entrevistas
```

Essa regra deve vir ANTES do bloqueio do site da Playboy.

8 - E uma lista de diretórios?

Insira esse conteúdo dentro de um arquivo texto:

```
batepapo$
batepapo/$
sexo/$
fofoca/$
chat/$
```

O símbolo de \$ indica que o Squid deve combinar as ocorrências quando estas palavras aparecerem no final da URL. O símbolo é usado em expressões regulares e pode ajudar a marcar casos bem específicos.

A essa altura você já sabe como proceder em seguida.

Capítulo 4 - Autenticação

É muito vantajoso usar autenticação de usuários no Squid: praticamente não vejo motivos em não fazê-lo. Primeiro, você impede que usuários não autorizados usem a Internet. Segundo, os que são autorizados serão melhor monitorados, pois você poderá gerar relatórios individuais do que cada usuário acessou, independente de que máquina tenham feito o acesso. Talvez eles reclamem por ter que digitar login e senha além do tradicional login na rede/máquina: mas fazer o que, são ossos do ofício (você já leu BOFH²?) e com o tempo eles acostumam.

O Squid não providencia nenhum método de autenticação, **exceto** pelo uso de programas externos, normalmente contribuições da comunidade. A seguinte diretriz:

```
authenticate_program
```

permite que você insira o pathname completo de onde está localizado o programa de autenticação a ser usado. Isso é útil, porque o Squid criará processo filhos para atender as requisições de autenticação, ao invés de respondê-las ele mesmo: isso evita demoras no atendimento de requisições, tanto de autenticação quanto de arquivos da Internet.

Quando o Squid é iniciado, ele cria uma quantidade X de processos-filhos que ficarão esperando requisições. O número de processos-filhos que serão criados na inicialização do Squid é definida pela diretriz:

```
authenticate_children 5
```

O número inicial padrão é 5. Se você tiver muitos usuários querendo acessar a Internet, procure aumentar esse número até obter um valor ótimo de processos-filhos versus usuários.

Eu vou mostrar dois módulos de autenticação aqui, ambos distribuídos normalmente junto com o Squid. Vamos à eles:

4.1 - Módulo NCSA de autenticação

Sendo muito sincero: eu vou mostrar esse módulo apenas com o intuito de não parecer (muito) preguiçoso. Se você possui mais de 10 usuários na sua intranet, e espera implementar uma política de expiração de senhas, você vai ter dores cabeça.

Inclua a diretriz abaixo no *squid.conf*:

```
authenticate_program /usr/local/squid/bin/ncsa_auth /  
usr/local/squid/etc/passwd  
acl auth_users proxy_auth REQUIRED  
http_access allow auth_users
```

Sem muitas dores de cabeça, o pathname do programa e o pathname do arquivo de senhas. Não é simples?

Esse programa usa o mesmo método que o Apache usa para fazer autenticação básica de usuários. Você vai precisar usar o programa *htpasswd* (que vem junto com o Apache) ou qualquer outro programa qualquer que implemente criptografia via o método *crypt* do UNIX. Infelizmente o módulo NCSA não permite o uso de criptografia via MD5, que é o método utilizado em senhas *shadow*, muito mais seguro por sinal. Você pode simplesmente copiar o programa do Apache para fazer administração de usuários. O comando

² *Bastard Operator from Hell*, um operador de sistemas UNIX sádico, sarcástico, malvado e uma porção de outros adjetivos ruins à mais. A única coisa boa dele é que ele é extremamente engraçado e apronta coisas que eu e você já tivemos vontade de fazer.

`man htpasswd`

lhe fornecerá as informações necessárias.

4.2 - Módulo SMB de autenticação

Esse módulo é um pouco superior ao NCSA porque usa base de dados de usuários do Samba (ou Windows NT) para fazer autenticação. Isso é bom porque você evita duplicar o esforço de manter duas bases de dados e o esforço complicado de manter as senhas sincronizadas. Você também leva vantagem por poder usar as ferramentas de administração de usuários do Samba, bem superiores ao do NCSA, como os programas `smbpasswd`, `SWAT`, `Webmin` ou `FAUS` (no caso de utilizar o Samba).

Para usar o módulo SMB, você precisará:

1. De um servidor Samba ou Microsoft NT que realize autenticação de usuários como PDC;
2. Do programa `smbclient`, disponível na distribuição do Samba; você não precisa de um servidor Samba rodando no mesmo computador que o Squid, apenas desse programa.

Esse módulo funciona da seguinte maneira: é criado um arquivo no servidor Samba (ou Windows NT) chamado *proxyauth*. Se o programa `smb_auth` conseguir ler o arquivo com as credenciais (login/senha) fornecidas pelo usuário, o usuário é permitido a utilizar o proxy.

Para configurar isso tudo no servidor PDC:

1. No compartilhamento *netlogon*, crie o arquivo *proxyauth* e insira dentro dele a palavra *allow*. Se você usa BDC dentro de sua rede, garanta a replicação desse arquivo. Você também pode alterar a localização desse arquivo usando a opção “-S” do programa `smb_auth`.
2. Garanta acesso de leitura ao arquivo *proxyauth* para todos os usuários ou grupos que você quer que tenha acesso ao proxy.

Agora configurando isso no arquivo *squid.conf*:

```
authenticate_program /usr/local/bin/smb_auth -W MEDIA@VANTAGE
acl auth_users proxy_auth REQUIRED
http_access allow auth_users
```

O programa `smb_auth` possui diversas opções de linha de comando. Acima por exemplo, está sendo usando uma. Vamos à elas:

4.3 - Problemas à vista

Ambos os módulos possuem um problema sério de segurança: os pares login/senha trafegam sem criptografia pela rede. Aparentemente, o módulo `smb_auth` parece comprometer sua rede, já que a senha utilizada para autenticação é a mesma utilizada para autenticar no computador/rede.

Na realidade, isso não faz muita diferença, já que você não tem como garantir que um usuário não use a mesma senha que usa para acessar o computador e/ou a rede para se autenticar no Squid se você usar o módulo NCSA.

A versão 2.5 do Squid trabalha com autenticação via *digest mode*, o que impede que a senha trafegue livremente pela rede: ela sequer faz isso. Infelizmente até a data de alteração do Squidnomicon, não havia documentação disponível no site oficial do Squid sobre como usar esse método.

4. 4 - Módulo de autenticação Winbind³

O texto a seguir apresenta as configurações necessárias para que o Squid autentique e autorize um usuário de um domínio NT/2000 a ter acesso à sites Web a partir do grupo a que este usuário pertence. Para que isto seja possível é necessário utilizar o Samba com suporte ao winbind para recuperar os usuários e grupos do domínio NT/2000 e ativar módulos auxiliares do Squid para autenticar e autorizar a partir do winbind. As configurações permitem que o usuário seja autenticado com base em suas credenciais de logon (autenticação NTLM, que funciona apenas para o Internet Explorer 4.x ou superior; novas versões do Mozilla parecem estar sendo capazes de realizar esse tipo de autenticação: por favor, cheque a página oficial do Mozilla para maiores informações) ou com base na informação de usuário e senha (autenticação básica).

4.4.1 - Instalação e configuração do Samba com suporte ao winbind

O Samba pode ser instalado a partir do código-fonte ou de pacote pré-compilado para a sua distribuição. A preferência pelo código-fonte deriva da possibilidade de configurar o software apenas com as opções necessárias para suportar a solução desejada.

O Samba pode ser baixado a partir de <http://www.samba.org> . A versão utilizada neste artigo é a 2.2.7a. Versões diferentes podem apresentar comportamentos diferentes dos descritos a seguir.

Após o download, descompacte os fontes no diretório de sua preferência (neste caso, os fontes serão instalados em `/usr/local/src`), com o comando:

```
[root@r2d2 src]# tar -zxvf samba-2.2.7a.tar.gz
```

Opções de Compilação

Após a descompactação do código-fonte, é necessário compilar o Samba com as opções que habilitam a autenticação com o winbind. Para verificar todas as opções de compilação disponíveis, execute o comando `configure --help` no diretório `/usr/local/src/samba-2.2.7a/source/`.

No caso deste artigo, o Samba será compilado com as seguintes opções:

`--with-configdir=/etc/samba:` define o diretório de configuração do samba para `/etc/samba`;

`--with-winbind:` compila o winbind, permitindo o uso de autenticação básica (com trânsito de senha pela rede);

`--with-winbind-auth-challenge:` habilita a capacidade de utilizar a interface desafio-resposta do NTLM;

Compilação e instalação

Para compilar o Samba, vá para `/usr/local/src/samba-2.2.7a/source/`.

As opções descritas sobre compilação do Samba serão utilizadas com o comando `configure`. Se esta não for a primeira compilação realizada para esta versão do Samba, limpe todos arquivos de saída e configurações com o comando `make clean`.

Caso não seja necessário, ou após utilizar, o comando `make clean`, rode o script `configure` com as opções de compilação, conforme abaixo:

³ Este texto foi originalmente escrito por André Moraes. Veja o capítulo sobre agradecimentos para maiores detalhes.

```
[root@r2d2 source]# ./configure --with-winbind --with-winbind-auth-challenge --with-configdir=/etc/samba
```

O script **configure** verifica as dependências e edita o Makefile para incluir as opções de compilação desejadas. Se a verificação não exibir nenhuma mensagem de erro, execute o comando:

```
[root@r2d2 source]# make
```

para compilar e montar os binários do Samba. A compilação deve seguir sem qualquer erro. Após a compilação com sucesso, execute o comando:

```
[root@r2d2 source]# make install
```

para instalar os binários, manpages e outros componentes do Samba 2.2.7a no diretório **/usr/local/samba/**.

Para completar a instalação, é necessário copiar o arquivo **/usr/local/src/samba-2.2.7a/source/nsswitch/libnss_winbind.so** para **/lib**, criar um link simbólico para **libnss_winbind.so.2**, no mesmo diretório.

Configuração

Para fazer com que o Samba e o winbind funcionem corretamente é necessário realizar uma série de configurações referentes ao próprio Samba e ao Name Service Switch (NSS), que permite que uma estação Linux/Unix recupere informações de sistema a partir de diversas fontes. **Antes de qualquer configuração, salve uma cópia do arquivo original.**

Entre as informações de sistema que o NSS permite pesquisar estão a relação de usuários (entrada **passwd**) e de grupos (entrada **group**) válidos para o host. Para permitir que o usuário de um domínio NT/2000 seja reconhecido como usuário válido através do winbind, é necessário alterar as linhas **passwd** e **group** do arquivo **/etc/nsswitch.conf** para o seguinte:

```
passwd: files winbind
group: files winbind
```

Após a configuração do NSS, é necessário configurar o Samba através do arquivo **/etc/samba/smb.conf**. Todas as configurações a seguir serão parte da seção **[global]** do arquivo.

Os parâmetros referentes ao Samba são descritos na manpage do arquivo **smb.conf**. A lista abaixo está na forma **parâmetro=valor** e deve ser adequada ao seu domínio. Os valores mostrados abaixo foram utilizados em laboratório para testar o funcionamento da autenticação e autorização:

```
workgroup = NWTRADERS
server string = Servidor Samba
hosts allow = 192.168.1
netbios name = R2D2
log file = /var/log/samba/%m.log
max log size = 0
security = domain
password server = LONDON
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
encrypt passwords = yes
wins server = 192.168.1.2
```

Importante: se sua rede não possuir um servidor WINS, é necessário criar um arquivo **lmhosts** para que o Samba localize o domínio NT/2000. Por default, o arquivo é armazenado em **/etc/samba/lmhosts** e deve conter, ao menos, uma entrada para o domínio ao qual o servidor é

ligado, listando o IP do PDC e o nome Netbios do domínio, como abaixo:

```
192.168.1.2 NWTRADERS
```

Os demais parâmetros do Samba podem ser utilizados com seus valores padrão.

Os parâmetros referentes à configuração do winbind também são parte da seção `[global]` do arquivo `smb.conf` e estão descritas na manpage do winbind.

```
winbind separator = "\"
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
template homedir = /dev/null
template shell = /dev/null
winbind use default domain = yes
```

Os demais parâmetros referentes ao winbind podem ser usados com seus valores default.

Após modificar o arquivo `smb.conf`, o passo seguinte é a inclusão do servidor Samba no domínio NT/2000. Para fazer isso é necessário criar a conta de máquina do servidor no domínio e usar o programa `smbpasswd` para associar o servidor Samba à conta recém-criada. O processo de criação de contas de máquina no domínio NT/2000 está fora do escopo deste artigo. O comando `smbpasswd` deve ser utilizado com os serviços smb e winbind desativados e com a seguinte sintaxe (utilizando o domínio fictício **NWTRADERS**):

```
[root@r2d2 root]# smbpasswd -j NWTRADERS -r LONDON -U Administrator
```

Em seguida você deve receber a mensagem:

```
Joined domain NWTRADERS.
```

A execução deste comando solicitará a senha do usuário e deverá informar que o servidor Samba foi incluído no domínio NT/2000 de acordo com a mensagem acima.

Com isso, o Samba e o winbind estão configurados e prontos para serem testados. Em caso de erro, verifique se o domínio está acessível e se a conta do servidor Samba foi criada.

Testes

Para realizar os testes de validação do Samba/winbind é necessário inicializar os serviços `smbd`, `nmbd` e `winbindd`, através dos comandos:

```
[root@r2d2 root]# /usr/local/samba/bin/smbd -D
[root@r2d2 root]# /usr/local/samba/bin/nmbd -D
[root@r2d2 root]# /usr/local/samba/bin/winbindd
```

Verifique se os serviços estão executando. É possível que os serviços não inicializem corretamente devido a erros de digitação nos arquivos de configuração. Após a revisão dos arquivos, inicialize os serviços.

Com os daemons do Samba e do winbind executando, o comando `wbinfo` será utilizado para testar a configuração. Apenas alguns parâmetros são necessários para verificar o funcionamento dos serviços. Para maiores informações, utilize a opção `--help` do comando.

O primeiro teste a ser realizado é a verificação da senha da conta de máquina do servidor Samba no domínio NT/2000, através do comando:

```
[root@r2d2 root]# wbinfo -t
```

Você deve receber a mensagem:

```
Secret is good
```

Se o servidor foi incluído no domínio sem problemas, a opção **-t** deve retornar a mensagem acima, indicando que a senha compartilhada é correta. Caso exista algum erro, o comando retorna a mensagem: i) **Could not check secret**, que ocorre quando algum dos serviços não está executando; ou ii) **Secret is bad**, quando a conta de máquina não foi registrada no domínio NT/2000 com sucesso.

Em seguida, deve ser realizado o teste de autenticação, usando a opção **-a**, e um nome de usuário válido do domínio, com sua senha. O separador **** deve ser utilizado duas vezes, a primeira como caractere de escape. No exemplo a seguir, a conta utilizada é **NWTRADERS\amoraes**, com a senha **teste01**:

```
[root@r2d2 root]# wbinfo -a NWTRADERS\\amoraes%teste01
```

Você deve receber a mensagem:

```
plaintext password authentication succeeded  
challenge/response password authentication succeeded
```

Em caso de erro em algum dos processos, verifique se o Samba foi compilado com as opções corretas. Se os dois processos falharem, certifique-se de que o nome de usuário e a senha utilizada para o teste são válidos.

Os últimos dois testes utilizando o comando **wbinfo** servem para verificar o acesso ao domínio NT/2000, retornando os usuários e grupos existentes. Para isso, utilize as opções **-u** (lista de usuários) e **-g** (lista de grupos), conforme mostrado a seguir:

```
[root@r2d2 root]# wbinfo -u
```

Você deve receber a mensagem:

```
NWTRADERS\Administrator  
NWTRADERS\amoraes (...)  
[root@r2d2 root]# wbinfo -g
```

Você deve receber a mensagem:

```
NWTRADERS\Domains Admins  
NWTRADERS\Domain Users (...)
```

Se o domínio NT/2000 estiver bloqueando conexões anônimas, os comandos acima devem retornar o erro **0xc0000022**. Para resolver este problema, é necessário registrar um usuário e senha que o winbind usará para contactar o PDC. Este usuário precisa ter privilégios administrativos mínimos, o que representa um risco à segurança (num domínio Windows 2000, o usuário deve pertencer ao grupo Account Operators). O usuário é registrado com o comando **wbinfo**:

```
[root@r2d2 root]# wbinfo -A NWTRADERS\\winbind%senha01
```

Após registrar o usuário, teste novamente os comandos **wbinfo -u** e **wbinfo -g**. A saída deverá ser similar à mostrada anteriormente.

Até aqui é possível mostrar que o Samba e o winbind estão funcionando corretamente. A última verificação a ser realizada diz respeito ao Name Service Switch e será realizada com o comando **getent**, usando as opções **group** e **passwd**, que se referem às entradas do arquivo **/etc/nsswitch.conf**.

```
[root@r2d2 root]# getent passwd
```

Você deve receber a mensagem:

```
root:x:0:0:root:/root:/bin/bash
```

```
...
```

```
NWTRADERS\Administrator:x:10001:10002:Admin:/dev/null:/dev/null
```

```
NWTRADERS\amoraes:x:10002:10003:André Moraes:/dev/null:/dev/null
```

```
[root@r2d2 root]# getent group
```

Você deve receber a mensagem:

```
root:x:0:0:root
```

```
...
```

```
NWTRADERS\Domain Admins:x:10002:NWTRADERS\Administrator
```

```
NWTRADERS\Domains Users:x:10003:NWTRADERS\amoraes
```

A saída destes comandos deve ser diferente em função do domínio utilizado. O funcionamento destes comandos é crucial para o processo de autenticação do Squid.

Scripts de inicialização automática

Os scripts utilizados para inicializar os serviços **smbd**, **nmbd** e **winbindd** foram modificados a partir dos arquivos **smb.init** e **winbind.init** que acompanham o código-fonte do Samba, localizados no diretório **/usr/local/src/samba-2.2.7a/packaging/RedHat**. As modificações necessárias são a inclusão do caminho correto dos binários do Samba para a execução dos daemons e a alteração da ordem de inicialização do winbind, para que este seja iniciado depois do **smb**, alterando a linha **chkconfig** do arquivo **winbind.init** para:

```
# chkconfig: 345 95 45
```

Após as modificações, é necessário copiar os arquivos **smb.init** e **winbind.init** para o diretório de inicialização. No caso do Redhat, o diretório é **/etc/init.d/**:

```
[root@r2d2 RedHat]# cp smb.init /etc/init.d/smb
```

```
[root@r2d2 RedHat]# cp winbind.init /etc/init.d/winbind
```

Em seguida, modifique as permissões dos arquivos **smb** e **winbind** para **775** e adicione os dois scripts aos níveis de execução definidos nos arquivos através do comando **chkconfig**:

```
[root@r2d2 init.d]# chkconfig --add smb
```

```
[root@r2d2 init.d]# chkconfig --add winbind
```

Para iniciar, parar, reiniciar ou verificar o status dos serviços, utilize o comando **service** seguido do nome do serviço (**smb** ou **winbind**) e siga as instruções na linha de comando.

Este procedimento conclui a instalação e configuração do Samba/winbind. O próximo passo é compilar, configurar e testar o Squid com suporte à autenticação/autorização baseada em winbind.

4.4.2 - Instalação e configuração do Squid

Download e descompactação do código-fonte

Da mesma forma que o Samba, o Squid pode ser instalado tanto a partir de binários pré-compilados para a sua distribuição quanto através do código-fonte. Utilizaremos a segunda opção.

O código-fonte do Squid pode ser baixado de <http://www.squid->

cache.org/Versions/v2/2.5/. A versão utilizada neste artigo é a 2.5.STABLE1. Versões diferentes podem apresentar comportamentos diferentes dos descritos a seguir.

Após o download, descompacte os fontes no diretório de sua preferência (neste caso, os fontes serão instalados em `/usr/local/src`), com o comando:

```
[root@r2d2 src]# tar -zxvf squid-2.5.STABLE1.tar.gz
```

Opções de Compilação

O Squid realiza a autenticação e autorização a partir de módulos externos cujo suporte depende de uma série de opções de compilação. A lista a seguir mostra as opções de compilação necessárias para o funcionamento desejado. Para conhecer todas as opções disponíveis, execute o comando `./configure --help` no diretório `/usr/local/src/squid-2.5.STABLE1/`.

Para o escopo deste artigo, o Squid será compilado com as seguintes opções:

```
--enable-auth="ntlm,basic": habilita a autenticação básica (texto aberto) e NTLM para o squid;
```

```
--enable-basic-auth-helpers="winbind": habilita o winbind como módulo auxiliar de autenticação básica para o squid (wb_auth);
```

```
--enable-ntlm-auth-helpers="winbind": habilita o winbind como modulo auxiliar de autenticação NTLM para o squid (wb_ntlmauth);
```

```
--enable-external-acl-helpers="winbind_group": habilita o modulo wb_group como módulo auxiliar para autorização baseada em grupos (wb_group);
```

Compilação e instalação

Para compilar o Squid, vá para o diretório `/usr/local/src/squid-2.5.STABLE1/`.

Devido a modificações na interface do winbindd, os *headers* `winbind_nss.h` presentes no código-fonte do Squid 2.5 não funcionam corretamente com o Samba 2.2 (versão 2.2.6 e superiores), causando problemas com a autenticação com winbind. Para sanar esse problema, é necessário copiar o arquivo `winbindd_nss.h` presente em `/usr/local/src/samba/source/nsswitch/` para os diretórios:

```
helpers/basic_auth/winbind/  
helpers/ntlm_auth/winbind/  
helpers/external_acl/winbind_group/
```

As opções descritas no item anterior serão utilizadas com o comando `configure`, que verifica as dependências e edita o Makefile, habilitando a compilação com as opções de compilação. Se esta não for a primeira compilação realizada para esta versão do Squid, limpe todos arquivos de saída e configurações com o comando `make clean`.

Caso não seja necessário, ou após, executar o comando `make clean`, execute o script de configuração conforme abaixo:

```
[root@r2d2 squid-2.5.STABLE1]# ./configure --enable-auth="ntlm,basic" --enable-basic-auth-helpers="winbind" --enable-ntlm-auth-helpers="winbind" --enable-external-acl-helpers="winbind_group"
```

Repare que não há quebras de linha no comando acima: as linhas foram quebradas apenas para exposição.

Se a configuração não apresentar nenhum erro, execute o comando:

```
[root@r2d2 squid-2.5.STABLE1]# make
```

para compilar e montar os binários do Squid. Se a compilação ocorrer sem erros, execute o comando

```
[root@r2d2 squid-2.5.STABLE1]# make install
```

para instalar os binários e outros componentes do Squid no diretório `/usr/local/squid`.

Configuração

A maior parte da configuração do Squid é feita sobre o arquivo `/usr/local/squid/etc/squid.conf`. Por razões de segurança, o Squid executará como usuário `nobody` do grupo `nobody`. Para isso, após a instalação, é necessário mudar o proprietário do diretório `/usr/local/squid/var` e de todos os seus subdiretórios para o usuário e grupo `nobody`.

Atenção: o nome de grupo a ser informado na `acl` baseada no módulo `wb_group` (`AcessoPermitido`, na configuração mostrada a seguir) não pode conter espaços devido a uma limitação da versão 2.5.STABLE1 do Squid.

A configuração básica do Squid está além do escopo deste artigo. As definições a seguir serão adicionadas ao arquivo `squid.conf` e pressupõem que as demais configurações necessárias foram realizadas pelo administrador. Para maiores informações sobre as opções, consulte a documentação do Squid:

```
cache_effective_user nobody
cache_effective_group nobody
# Autenticação NTLM
auth_param ntlm program /usr/local/squid/libexec/wb_ntlmauth
auth_param ntlm children 5
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 2 minutes
# Autenticação Básica
auth_param basic program /usr/local/squid/libexec/wb_auth
auth_param basic children 5
auth_param basic realm Dominio nwtraders
auth_param basic credentialsttl 2 hours
# Carrega o módulo auxiliar wb_group
external_acl_type NT_global_group %LOGIN \
/usr/local/squid/libexec/wb_group
acl UsuariosAutenticados proxy_auth REQUIRED
# ACL que monta a lista de usuários do grupo Permitido
acl AcessoPermitido external NT_global_group Permitido
http_access allow AcessoPermitido
http_access deny all
```

A configuração acima permite que o usuário navegue sem informar `username` e senha (utilizando o Internet Explorer, através do módulo `wb_ntlmauth`), ou informando - no formato `domínio\nome` e `senha` - na caixa de diálogo que aparecerá ao tentar navegar através de um browser que realize apenas autenticação básica (p. ex. Mozilla, através do módulo `wb_auth`).

Testes

Todos os testes a seguir assumem que o Squid foi compilado sem alterar nenhum dos diretórios default.

Para testar a configuração do Squid é necessário testar, separadamente, os módulos de autenticação

(**wb_auth** e **wb_group**), a configuração do proxy e a interação entre o browser Internet Explorer e o Squid, verificando se a autenticação foi realizada e se o proxy está autorizando com base no grupo ao qual o usuário pertence. Os testes devem ser feitos com os serviços **smb** e **winbind** executando. Os programas estão localizados em **/usr/local/squid/libexec/**.

Para verificar a autenticação do usuário com o comando **wb_auth**, este deve ser executado no modo debug, com a opção **-d**. Este comando recebe a informação de usuário e senha e devolve **OK**, quando o usuário é autenticado ou **ERR** caso contrário. O nome de usuário e senha deve ser informado no formato **DOMINIO\usuário senha**. O resultado do teste deve ser similar ao seguinte:

```
[root@r2d2 root]# /usr/local/squid/libexec/wb_auth -d /wb_auth
[30236] (wb_basic_auth.c:167): basic winbindd auth helper build Feb
14 2003, 14:22:42 starting up...
```

Você deve receber a mensagem:

```
NWTRADERS\amoraes teste01
/wb_auth[30236] (wb_basic_auth.c:129): Got 'NWTRADERS\amoraes
teste01' from squid (length: 22).
/wb_auth[30236] (wb_basic_auth.c:55): winbindd result: 1
/wb_auth[30236] (wb_basic_auth.c:58): sending 'OK' to squid
OK
```

Em caso de erro, verifique se a conta e a senha informada estão corretas.

Para verificar se um usuário pertence à determinado grupo, será utilizado o comando **wb_group**, com a opção **-d**. Este comando recebe o nome de usuário e um nome grupo contra o qual o login será testado. Se o usuário pertence ao grupo, **wb_group** retorna **OK**, caso contrário, retorna **ERR**. O nome de usuário e o grupo devem ser informados no formato **usuário grupo**. O teste deve apresentar resultado similar a este:

```
[root@r2d2 root]# /usr/local/squid/libexec/wb_group -d /wb_group
[30248] (wb_check_group.c:265): External ACL winbindd group helper
build Feb 14 2003, 14:22:56 starting up...
amoraes "Domain Users"
/wb_group[30248] (wb_check_group.c:285): Got 'amoraes Domain Users'
from Squid (length: 8192).
/wb_group[30248] (wb_check_group.c:187): SID: S-1-5-21-1390067357-
1078145449-1060284298-2758
/wb_group[30248] (wb_check_group.c:153): Windows group: Permitido,
Squid group: Domain Users
/wb_group[30248] (wb_check_group.c:187): SID: S-1-5-21-1390067357-
1078145449-1060284298-513
/wb_group[30248] (wb_check_group.c:153): Windows group: Domain
Users, Squid group: Domain Users
OK
```

Os testes acima confirmam o funcionamento básico da autenticação de usuários e da verificação de grupos.

Os módulos de autenticação são necessários para identificar o usuário e preencher a variável **LOGIN** utilizada pelo módulo **wb_group**, conforme a configuração do Squid.

A próxima verificação a ser feita é a da configuração do Squid. Para isso, é necessário inicializar o Squid através do comando:

```
[root@r2d2 root]# /usr/local/squid/sbin/squid
```

Com o Squid executando, verifique o log do cache em `/usr/local/squid/var/logs/cache.log`, que deve apresentar, entre outras linhas, as seguintes:

```
[root@r2d2 root]# tail -f /usr/local/squid/var/logs/cache.log
```

Você deve receber a mensagem:

```
2003/02/20 15:02:23| helperOpenServers: Starting 5 'wb_group'
processes
...
2003/02/20 15:02:23| Ready to serve requests.
```

Se o arquivo `cache.log` apresentar algum erro, verifique se as alterações aplicadas ao arquivo `squid.conf` foram digitadas corretamente.

A primeira linha da saída mostrada acima indica que Squid disparou as cópias do `wb_group` para realizar a verificação de usuários. Como não foi informado nenhum número de processos para o módulo, o Squid dispara cinco processos, que é o valor default. O mesmo vale para os módulos `wb_auth` e `wb_ntlmauth`.

Para concluir a verificação das configurações do proxy, observe se todos os processos associados ao Squid estão executando. A lista de processos executando no servidor sob o usuário `nobody` deve incluir os seguintes:

```
[root@r2d2 root]# ps -U nobody
PID TTY TIME CMD
30311 ? 00:00:03 squid
30312 ? 00:00:00 wb_ntlmauth
30313 ? 00:00:00 wb_ntlmauth
30314 ? 00:00:00 wb_ntlmauth
30315 ? 00:00:00 wb_ntlmauth
30316 ? 00:00:00 wb_ntlmauth
30317 ? 00:00:00 wb_auth
30318 ? 00:00:00 wb_auth
30319 ? 00:00:00 wb_auth
30320 ? 00:00:00 wb_auth
30321 ? 00:00:00 wb_mauth
30322 ? 00:00:00 wb_group
30323 ? 00:00:00 wb_group
30324 ? 00:00:00 wb_group
30325 ? 00:00:00 wb_group
30326 ? 00:00:00 wb_group
30327 ? 00:00:00 unlinkd
```

Com todos os processos rodando, é hora de testar a conexão autenticada através do navegador, para o que serão necessárias quatro etapas:

- ➔ Configurar o navegador de sua escolha para acesso através de servidor Proxy, informando o endereço do servidor Squid e a porta 3128;
- ➔ Adicionar usuários ao grupo que você deseja que tenha acesso através do Squid, no caso deste artigo, o grupo Permitido. Para este teste, o usuário `NWTRADERS\amoraes` será adicionado ao grupo;
- ➔ Efetuar login como um usuário do grupo que tenha acesso à sites externos e tentar navegar;

→ Efetuar login como um usuário de qualquer outro grupo para verificar o bloqueio;

Com todas as configurações e testes realizados com sucesso, o usuário pertencente ao grupo que possui acesso deve estar navegando autenticado e autorizado. Usuários dos demais grupos devem ter sido bloqueados.

Para verificar se o acesso está sendo permitido através da autorização, verifique o arquivo `/usr/local/squid/var/logs/access.log`. Tanto os usuários liberados quanto os bloqueados devem apresentar a informação `domínio\usuário` como parte do log de acesso, conforme o excerto abaixo:

```
[root@r2d2 root]# tail -f /usr/local/squid/var/logs/accesss.log
1045768398.423 4 192.168.1.81 TCP_DENIED/407 1621 CONNECT
simg.bol.com.br:443 - NONE/- text/html
1045768398.437 5 192.168.1.81 TCP_DENIED/407 1687 CONNECT
simg.bol.com.br:443 - NONE/- text/html
1045768398.705 519 192.168.1.81 TCP_MISS/200 1107 GET
http://img.bol.com.br/premium/vantagens.gif nwtraders\amoraes
DIRECT/200.221.7.120 image/gif
1045768398.806 571 192.168.1.81 TCP_MISS/200 2469 GET
http://img.bol.com.br/premium/ico_planos.gif nwtraders\amoraes
DIRECT/200.221.7.122 image/gif
```

A informação `TCP_DENIED/407` indica que o Squid está solicitando a autenticação ao navegador. Os nomes de domínio e de usuário indicam que o acesso foi feito após a autorização.

Com este último passo, temos o Squid configurado para autenticação e autorização baseada em grupos de um domínio NT/2000 para controlar o acesso à sites web, através das interfaces proporcionadas pelo Samba/winbind.

Script de inicialização automática

O script de inicialização utilizado para o Squid é derivado do script padrão fornecido pelo RedHat 7.3 para o binário pré-compilado.

Após a modificação do conteúdo da variável `PATH` para `/usr/local/squid/sbin/`, altere as permissões do arquivo `squid` para 775, com o comando e adicione o script aos níveis de execução definidos no script, através do comando `chkconfig`:

```
[root@r2d2 init.d]# chkconfig --add squid
```

Para iniciar, parar, reiniciar ou verificar o status dos serviços, utilize os comandos abaixo sem parâmetros e siga as instruções na linha de comando:

```
[root@r2d2 init.d]# service squid
```

Este procedimento conclui a instalação e configuração do Squid para autenticação e autorização baseadas em grupos.

4.4.3 - Manutenção

A manutenção do conjunto Samba/winbind/Squid é extremamente simples, demandando pouco trabalho por parte do administrador. Entretanto, alguns problemas foram encontrados durante o uso em produção e estão listados abaixo:

1. Durante a operação, a autorização de usuários incluídos (ou removidos) recentemente no(s) grupo(s) que deve(m) ter acesso liberado através do Squid não é realizada de imediato devido ao cache do winbind. Para resolver este problema é necessário reiniciar os serviços `smb`, `winbind` e `squid` para

que os novos usuários sejam liberados ou bloqueados imediatamente;

2. O comando **wbinfo -g** retorna todos os grupos do domínio NT/2000, mas o **wbinfo -u** retorna apenas alguns usuários. Este problema ocorre para domínios com restrição de conexão anônima e cuja conta de acesso do winbind não possua privilégios mínimos para acessar as contas de usuários. Os passos abaixo descrevem a solução para este problema:
 - a) parar os serviços **winbind** e **smb** e verificar se alguma instância continua rodando;
 - b) remover o arquivo **/etc/samba/secrets.tdb**;
 - c) incluir o servidor Samba novamente no domínio, com o comando **smbpasswd**;
 - d) executar o comando **wbinfo -A**, registrando uma conta com privilégios administrativos adequados;
3. Quando existe uma política de bloqueio de conta depois de um certo número de tentativas erradas de efetuar logon, o processo de autenticação do squid, utilizando o winbind, causa o bloqueio de contas (**contribuição de Mauricio Steinert**). Este problema foi verificado, num domínio Windows 2000, para política de bloqueio após uma tentativa de logon errada. Neste caso, as contas começam a ser bloqueadas assim que os usuários tentam acessar páginas através do Squid. A solução para este problema é o aumento do número de tentativas de logon erradas permitidas antes do bloqueio. Durante o teste, verificou-se que a partir da permissão de duas tentativas erradas de logon, a autenticação do squid não bloqueou a conta do usuário.

Capítulo 5 - Gerenciamento de cache

O gerenciamento de como o Squid irá armazenar os dados é que fará a diferença entre ter um proxy com bom desempenho ou mal desempenho e o tamanho que o cache em disco irá ocupar.

Vamos começar por definir o que será gravado no disco do proxy. Por exemplo, a diretiva

```
maximum_object_size
```

define qual o tamanho máximo de um objeto que será salvo no disco. Entenda como objeto um arquivo qualquer, como um documento HTML ou uma figura GIF. Padrão para esse parâmetro é 4096Kb, mas você pode aumentá-lo para quanto desejar se deseja salvar parte do consumo de banda. Veja BYTES hit ratio.

Capítulo 6 - Recursos na Internet

O site do Squid possui muito mais documentação que esse pequeno tutorial e é ponto obrigatório de passagem se você entende inglês: <http://www.squid-cache.org>

Outro site interessante é o ORSO (<http://web.onda.com.br/orso/index.html>) pois contem um bom conteúdo sobre o Squid, incluindo o SARG, um programa para gerar páginas html dos arquivos de log do Squid. No site você também encontrará listas de palavras para bloqueios de sites pornográficos.

Você poderá encontrar versões novas desse manual no website <http://www.imortais.cjb.net/linux/>

Bibliografia

Site oficial do Samba: <http://www.samba.org>

Site oficial do Squid: <http://www.squid-cache.org>

Name Service Switch: http://www.gnu.org/manual/glibc-2.2.5/html_node/Name-Service-Switch.html

Squid FAQ - Authentication: <http://www.squid-cache.org/Doc/FAQ/FAQ-23.html>

Unified logons between Windows NT and Unix using Winbind:
<http://info.ccone.at/INFO/Samba/winbind.html>

Como sempre, o Google™ é seu amigo: <http://www.google.com.br>

Licença de uso

GNU Free Documentation License

Version 1.1, March 2000

Copyright (C) 2002 Alceu Rodrigues de Freitas Junior
glasswalk3r@yahoo.com.br

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says

that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition.

Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text

and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number.

Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate.

Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4.

Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number.

If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.