

Integração Windows e Linux com Samba

Rubens Queiroz de Almeida
queiroz@unicamp.br

UNICAMP
CENTRO DE COMPUTAÇÃO

O que é o samba

- Servidor UNIX de arquivos e de impressão em redes baseado no protocolo SMB
- Sistemas Windows em geral e OS/2 utilizam o protocolo SMB nativamente para realizar compartilhamento de arquivos e impressão em rede. Foi desenvolvido originalmente pelas empresas 3Com e Microsoft.
- O protocolo SMB foi recentemente rebatizado com o nome CIFS (Common Internet File System)
- O enfoque adotado pelo Samba é que é muito mais fácil fazer o sistema UNIX entender o protocolo utilizado por PCs do que o contrário.
- Utilizado por milhares de empresas por todo o mundo

Origens

- Desenvolvido originalmente por Andrew Tridgell, à época estudante de doutorado na Austrália
- Mantido no momento por uma equipe de programadores de várias partes do mundo, que se comunicam através da Internet
- De forma semelhante ao Linux, o Samba pode ser distribuído livremente sem ônus. Sua distribuição é regida pela licença GPL, da GNU
- Qualquer pessoa ou empresa pode utilizar o código como bem entender mas não pode restringir o acesso ao código fonte original e derivado

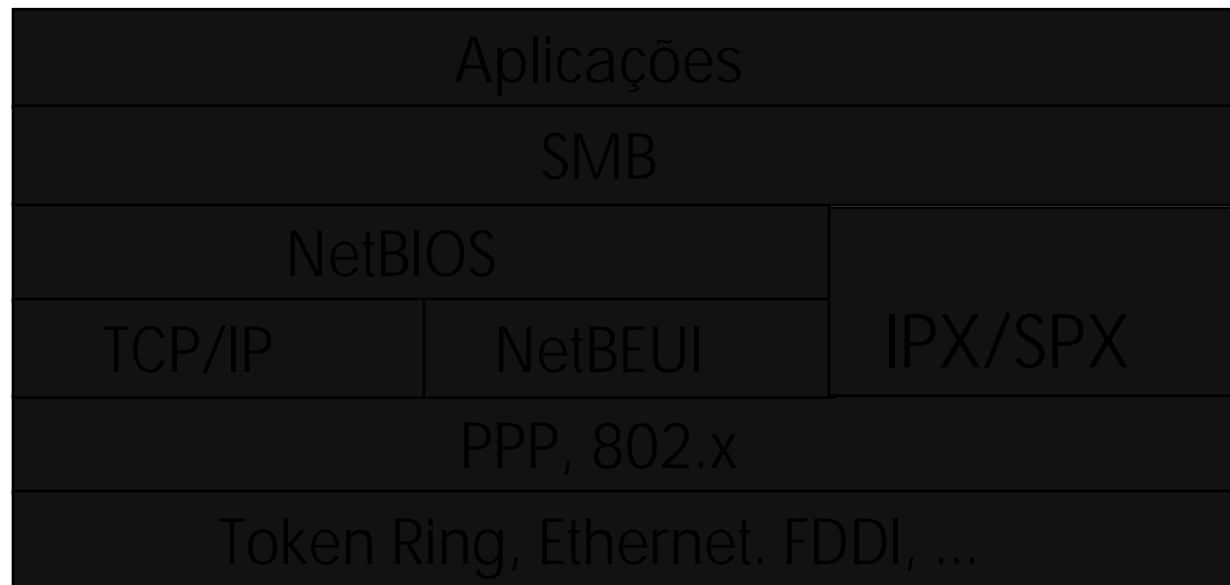
O protocolo SMB/CIFS (1)

- O protocolo SMB é bastante complexo e foi extensivamente modificado pela Microsoft nos últimos anos para atender às suas necessidades
- Especificado pela organização X/Open porém não completamente. A maior parte dos documentos descritivos do protocolo foram disponibilizados na Internet pela Microsoft. Alguns documentos cruciais descritivos de certos componentes do Windows NT continuam sob sigilo
- SMB ou “Server Message Block” é o protocolo utilizado em computadores baseados nos sistemas Windows para comunicação e compartilhamento de recursos via rede

O Protocolo SMB/CIFS (2)

- O Samba implementa o protocolo SMB sobre TCP para compartilhamento de arquivos e UDP para browsing. SMB pode também ser executado sobre outros protocolos de transporte como por exemplo IPX e NetBEUI.
- A estratégia da Microsoft é abandonar estes protocolos de transporte e concentrar-se no TCP/IP

O Protocolo SMB



SMB - Componentes

- Três tipos de pacotes são usados no protocolo SMB sobre TCP/IP:
 - UDP/137 (resolução de nomes e registro de tráfego)
 - UDP/138 (browsing e anúncio de tráfego)
 - TCP/139 (compartilhamento de arquivos).

Terminologia (1)

- CIFS - Common Internet File System (SMB)
- NBT - NetBIOS over TCP
- WINS - versão não broadcast do protocolo UDP/137 NBT
- Local Browse Master (LBM) - computador em cada subrede que coleta anúncios de hosts e os combina em uma lista
- Domain Master Browser (DBM) - máquina do domínio que combina as listas de computadores enviadas pelos LBMs

Terminologia (2)

- Workgroup - conjunto de máquinas que compartilham uma lista de recursos comum
- Domain - um grupo de trabalho que inclui um servidor central de autenticação
- Domain Controller - a máquina no domínio que sedia o banco de dados de autenticação

Terminologia (3)

- Domain Logon - processo através do qual as máquinas clientes autenticam seus usuários por meio de acesso a um servidor remoto
- Logon Server - máquina que aceita pedidos de logon no domínio

SMB/CIFS

Características Avançadas (1)

- O protocolo SMB possui algumas características muito avançadas (chaining, oplocks) adicionadas para torná-lo mais rápido do que o NFS (embora não seja tão seguro para compartilhamento de arquivos).
- Sua principal característica é o chamado “opportunistic locking” (conhecidos como op-locks)
- Op-locks permitem que um cliente receba uma ficha (token) que lhe garante uso exclusivo de um arquivo. O servidor notifica quando alterações no arquivo são feitas requerendo a quebra do oplock (lock oportunista)

SMB/CIFS

Características Avançadas (2)

- Permite que os clientes realizem o cache de arquivos inteiros localmente - clientes Microsoft utilizam-se desta característica extensivamente
- Perigo de perda de dados se o cliente abortar por alguma razão
- As versões do Samba a partir de 1.9.18 implementam op-locks resultando numa melhora substancial de desempenho

O Protocolo NBT (1)

- NBT (NetBIOS over TCP) é o protocolo utilizado para encapsular o antigo protocolo NetBIOS no TCP
- Também utilizado para implementar o registro e resolução de nomes. Especificado pelas RFC's 1001 e 1002.
- A resolução de nomes pode ser divulgada por meio de broadcasts ou ponto a ponto para um servidor WINS
- O samba pode também desempenhar o papel de um servidor WINS mas não faz a replicação de dados com um servidor WINS da Microsoft - a Microsoft ainda não tornou público este protocolo.

O Protocolo NBT (2)

- O espaço de nomes NBT, ao contrário do DNS, é plano e não se adequa às necessidades de comunicação via Internet
- A Microsoft começou a usar nomes DNS mas isto requer uma alteração nos clientes (hack) para permitir que os clientes contactem os servidores (uso do nome "SMBSERVER")
- Somente funciona com Windows NT 4.0 e superiores
- Não existe segurança no registro dos nomes, o que pode ser muito perigoso.

Samba - Segurança (1)

- O Samba foi escrito com atenção especial para a segurança. Oferece muito mais opções de segurança que outros pacotes para compartilhamento de arquivos
- As versões anteriores a 1.9.17p2 são inseguras. Não as utilize
- Provê suporte a senhas SMB criptografadas ou senhas UNIX.
- Pode utilizar os serviços de um servidor NT para verificação de usuários

Samba - Segurança (2)

- Todas as operações em arquivos são realizadas apenas para usuários autenticados. Por default não é definido o usuário guest
- NUNCA se sobrepõe aos mecanismos de segurança do UNIX
- Possui um mecanismo nativo de segurança semelhante ao oferecido pelo TCP/WRAPPER

Samba - Segurança (3)

O modelo SMB define dois tipos de segurança:

- Compartilhamento em nível de recursos (share level)
 - Cada recurso compartilhado possui uma senha e o cliente necessita apenas desta senha para acessar tais os recursos . Este foi o primeiro modelo de segurança oferecido pelo SMB
- Compartilhamento em nível de usuários
 - Acesso é controlado baseado nos privilégios garantidos a cada usuário. O usuário precisa se identificar previamente junto ao servidor

Portabilidade

- O Samba foi escrito para ser portátil e não requer alterações no kernel
- Já foi portado para plataformas não UNIX como OS/2, Novell Netware, VMS e AmigaOS
- Em algumas empresas roda em supercomputadores Cray e Convex
- O maior empecilho à portabilidade é lock de arquivos. Aplicações Windows usam rotinas complexas para lock de arquivos utilizando IPC (Inter-Process Communication). O Samba lida com este problema implementando um mecanismo de lock sobre os mecanismos nativos do UNIX.

Escalabilidade

- O Samba cria um processo UNIX para cada usuário conectado
- Cada usuário requer por volta de 600 a 800 k de memória dependendo do tipo de utilização feito
- Empresas comerciais têm utilizado Samba em larga escala com mais de 500 usuários concorrentes
- O Samba pode ser executado como um processo residente (stand-alone daemon) ou acionado através do servidor inetd
- Recomenda-se o uso do Samba como processo residente (daemon) para obter-se um melhor desempenho

Componentes Principais (1)

- `smbd`
 - Este processo escuta a porta TCP/139 e se replica para cada solicitação recebida por clientes. Realiza todas as tarefas de impressão e compartilhamento de arquivos
- `nmbd`
 - Atende a todo o tráfego das portas UDP/137 e UDP/138 para serviço de nomes, registro e browsing

Componentes Principais (2)

- smbclient
 - cliente útil para teste do samba e operações batch. Apresenta uma interface semelhante à do FTP
- nmblookup
 - utilitário para consultar nomes NBT
- testparm
 - utilitário para verificação da sintaxe do arquivo smb.conf

Outros utilitários (1)

- `smbmount` (Linux)
 - acesso a sistemas de arquivos Windows a partir de máquinas Linux
- `smbpasswd`
 - troca de senhas em ambiente SMB
- `smbstatus`
 - informa a situação atual das conexões Samba.

Outros utilitários (2)

- `smbtar`
 - Backups de compartilhamentos SMB/CIFS em fitas magnéticas sob o Unix.
- `pwdump`
 - <http://us1.samba.org/samba/ftp/pwdump/>
- `nt2passwd`
 - http://sunsite.auc.dk/samba/ntdom_faq/nt2passwd

Instalação (1)

- Simples e descomplicada
- Versão atual 2.05a
- Compatível com um grande número de sistemas Unix
 - Como root:
gzip -dc samba.tar.gz | tar xvf -
cd samba/source
./configure
make
make install
- Conectiva Linux
 - Opção de ativação no processo de instalação do sistema
 - Através do RPM (Red Hat Package Manager)
 - rpm -ivh samba-2.0.4b-10cl.i386.rpm

Instalação (2)

- Configure seu sistema para ativar automaticamente durante o processo de boot os daemons `/usr/sbin/smbd` e `/usr/sbin/nmbd`
- Para inicializar os servidores automaticamente quando todo o sistema for iniciado, acione o programa `ntsysv` e torne a opção `smb` ativa.
- Alterações no arquivo de configuração (`smb.conf`) devem ser sinalizadas ao SMB:

```
/etc/rc.d/init.d/smb stop  
/etc/rc.d/init.d/smb start  
ou ainda  
/etc/rc.d/init.d/smb restart
```

Configuração - smb.conf

- Toda a configuração do Samba é feita a partir do arquivo smb.conf
- Formato similar ao arquivo WINDOWS.INI
- Uma enorme quantidade de opções muito bem documentadas. A documentação do arquivo smb.conf possui 75 páginas. A maioria das opções não precisam ser alteradas visto que as definições padrão funcionam perfeitamente.
- A configuração do arquivo smb.conf requer a alteração de pouquíssimos parâmetros

smb.conf - Exemplo (1)

[global]

security=user

workgroup = ccuec

encrypt passwords = yes

hosts allow = 143.106. 127. EXCEPT 143.106.10.2

include = /usr/local/samba/lib/smb.conf.%m

[homes]

browseable = no

guest ok = no

read only = no

create mask = 0755

smb.conf - Exemplo (2)

[printers]

guest ok = no

path = /var/spool/smbprint

print ok = yes

[cdrom]

comment = CDROM Compartilhado

path = /mnt/cdrom

read only = yes

locking = no

Servidor Wins, logons, DMB (1)

[global]

workgroup = samba
server string = Samba Server
hosts allow = 143.106. 127.
printcap name = /etc/printcap
load printers = yes
log file = /var/log/samba/log.%m
max log size = 50
security = user
smb passwd file = /etc/smbpasswd
os level = 33
domain master = yes
preferred master = yes
domain logons = yes
wins support = yes

Servidor Wins, logons, DMB (2)

[netlogon]

comment = Network Logon Service

path = /home/netlogon

guest ok = yes

writable = no

share modes = no

Autenticação com PDC/NT

```
[global]
workgroup = SAMBA
server string = Samba Server
hosts allow = 143.106. 127.
printcap name = /etc/printcap
load printers = yes
log file = /var/log/samba/log.%m
max log size = 50
security = server
password server = 143.106.80.6
encrypt passwords = yes
```

Configuração Samba

Interfaces Gráficas

- Diversas opções disponíveis. Listagem completa em <http://us1.samba.org/samba/GUI/>
- **SWAT - Samba Web Administration Tool**
 - Distribuído juntamente com o Samba
 - Utiliza um browser Web
 - Requer a senha do superusuário. Pode ser inseguro se acessado a partir da rede
 - Criação e modificação do arquivo smb.conf
 - Ativação e desativação do serviço
- **Linuxconf**

Ambiente de Rede -> Tarefas de Servidor -> Samba

SWAT

Netscape: Samba Web Administration Tool

File Edit View Go Communicator Help

HOME GLOBALS SHARES PRINTERS STATUS VIEW PASSWORD

Global Variables

Reset Values **Advanced View**

Base Options

Help	workgroup	<input type="text" value="GRUPO LINUX"/>	<input type="button" value="Set Default"/>
Help	netbios name	<input type="text" value="LINUX"/>	<input type="button" value="Set Default"/>
Help	server string	<input type="text" value="Servidor Samba"/>	<input type="button" value="Set Default"/>
Help	interfaces	<input type="text" value="I"/>	<input type="button" value="Set Default"/>

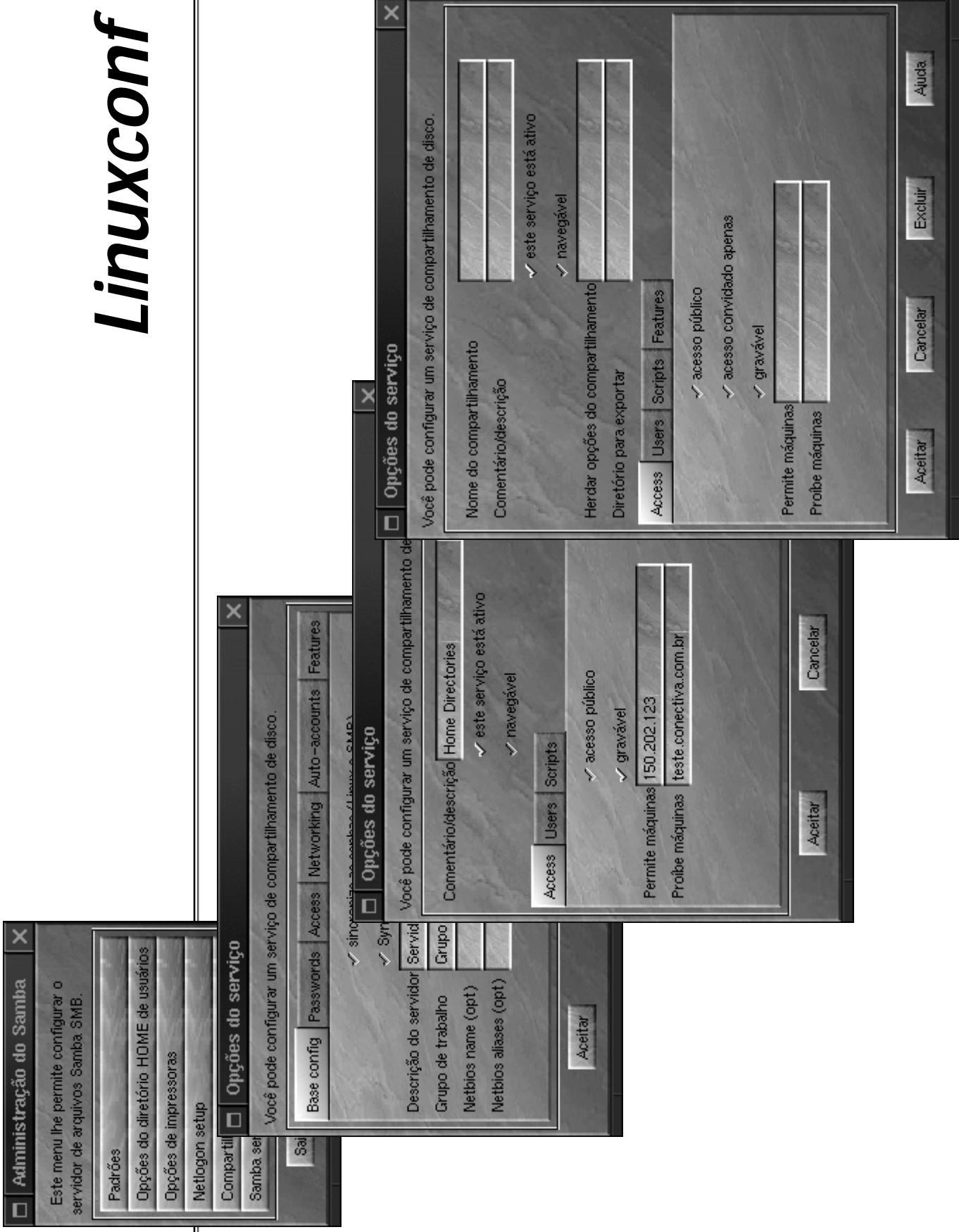
Security Options

Help	security	<input type="text" value="USER"/>	<input type="button" value="Set Default"/>
Help	encrypt passwords	<input type="text" value="No"/>	<input type="button" value="Set Default"/>

SWAT - Configuração

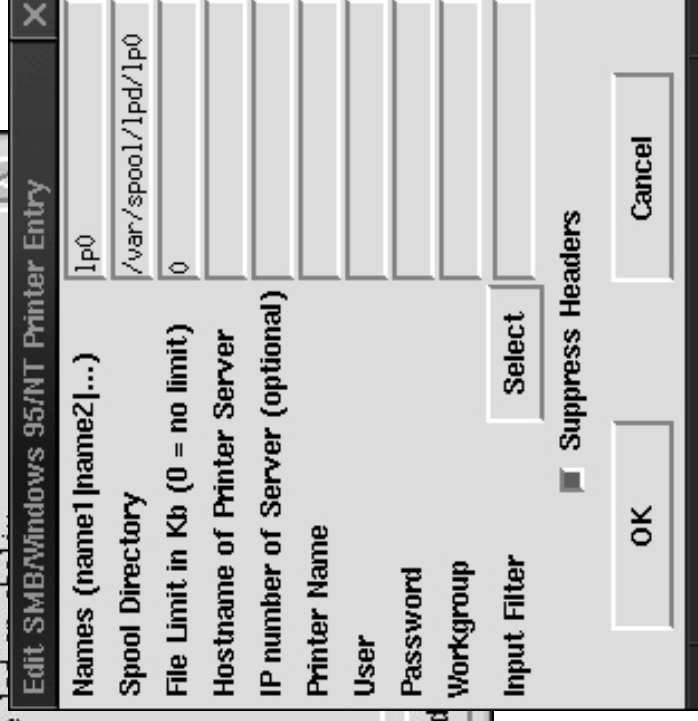
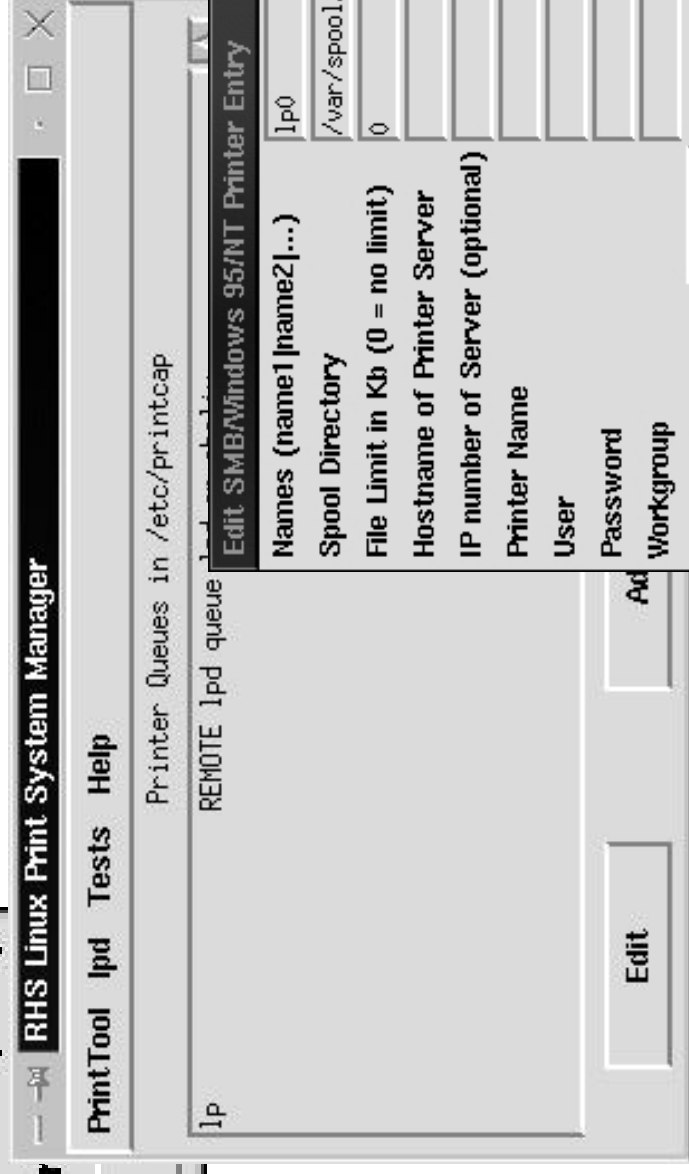
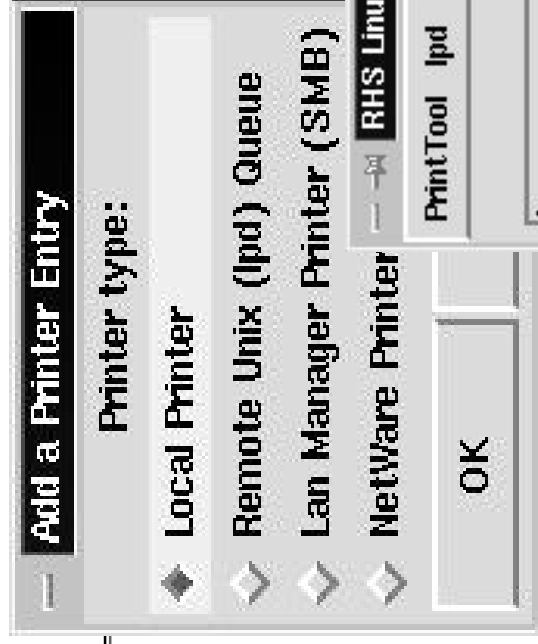
- **/etc/services**
 - swat 901/tcp
Selecionar um número não utilizado inferior a 1024 (portas reservadas)
- **/etc/inetd.conf**
swat stream tcp nowait.400 root /usr/local/samba/bin/swat swat
- **Reiniciar processo inetd**
 - kill -1 [pid inetd]
- **Acesso**
 - <http://localhost:901>

Linuxconf



Configuração de Impressoras

Linux: Printtool



Browsing (1)

- Os protocolos de browsing permitem que a “Network Neighborhood” ou “Toda a Rede” vejam todos os servidores disponíveis
- Os protocolos de browsing são complexos e envolvem um sistema de eleição para decidir o “browse master” que é a máquina responsável por manter a lista de servidores visível (“Network Neighborhood”)
- Utiliza principalmente a porta UDP/138

Browsing (2)

- O browsing daemon do Samba foi completamente reescrito e agora provê suporte para computadores com mais de uma interface de rede (*multi-homed hosts*)
- As versões do Samba superiores a 1.9.17 suportam browsing corretamente em subredes
- Servidores Samba podem também atuar como servidores WINS

Samba e Domínios (1)

- O sistema de domínios do Windows NT é o coração do modelo de comunicação em redes de sistemas NT
- Desempenha a mesma função do NIS/NIS+ em sistemas UNIX sendo entretanto consideravelmente mais complexo - utiliza DCE-RPC.
- Sistemas Windows 95 apenas participam
- O Samba suporta logons do Windows 95 e scripts de logon
- A Microsoft liberou os detalhes destes protocolos apenas após o código do Samba ter sido liberado
- Se uma instalação possuir apenas clientes baseados em Windows 95 o Samba pode substituir completamente servidores Windows NT

Samba e Domínios (2)

- Os protocolos de domínio do Windows NT ainda não foram documentados e a Microsoft não tenciona divulgá-los. O protocolo de logon do Windows NT foi publicado em agosto de 1997 no newsgroup comp.protocols.smb
- A maior vantagem dos protocolos de domínio é a replicação de contas permitindo um login único
- O utilitário pwdump permite descarregar o arquivo de senhas do Windows NT em formato compatível para uso em um servidor Samba
- Servidores Samba podem atuar como PDC (Primary Domain Controller) de um domínio NT

Perspectivas do protocolo SMB/CIFS

- A Microsoft está tentando limpar o protocolo CIFS eliminando chamadas redundantes
- O modelo de segurança do Windows NT 5.0 será o Kerberos 5 (já disponível em sistemas Unix)
- A Microsoft anunciou que sua implementação do Kerberos será compatível com a do UNIX (RFC 1510)
- A autenticação CIFS se moverá para o modelo de tokens do Kerberos. Várias modificações serão necessárias. Ainda não existe documentação sobre estas mudanças

Bibliografia

Esta apresentação foi baseada em grande parte em material obtido a partir da Web Page do Projeto Samba nos seguintes endereços:

<http://www.samba.org>

<http://us1.samba.org/samba/ftp/slides>

<http://us1.samba.org/samba/docs/>

Referências (1)

Conectiva Linux em Redes Windows

<http://www.conectiva.com.br/artigos/samba.html>

Samba - Aspectos Avançados

<http://www.conectiva.com.br/artigos/samba2.html>

Referências (2)

An Introduction to Samba

<http://us1.samba.org/samba/docs/SambaIntro.html>

File sharing made easy

<http://www.linuxworld.com/linuxworld/lw-1999-03/lw-03-thereandback.html>

Getting Linux And Windows Together With Samba

<http://www.performancecomputing.com/unixintegration/9807/9807f1.htm>

Integrating NT Into A UNIX Network

<http://www.performancecomputing.com/unixintegration/9706/9706u1.htm>

Referências (3)

Integrating UNIX and NT Environments

<http://www.linuxworld.com/linuxworld/expo/lw-wednesday-enviornments.html>

Linux on the LAN

<http://www.linuxworld.com/linuxworld/lw-1999-02/lw-02-netware.html>

Networking Facilities In Windows 95 And NT

<http://www.performancecomputing.com/unixintegration/9711/9711f2.htm>

Sharing With Samba

<http://www.performancecomputing.com/unixintegration/9801/9801n1.htm>

Sharing a printer between Linux and NT

<http://www.linuxworld.com/linuxworld/lw-1999-02/lw-02-thereandback.html>

Referências (4)

Samba NT domain FAQ

http://us1.samba.org/samba/docs/ntdom_faq/samba_ntdom_faq.htm

Share And Share Alike

<http://www.performancecomputing.com/unixintegration/9704/9704n2.htm>

Samba Windows-Unix tool is updated

<http://www.linuxworld.com/linuxworld/lw-1999-01/lw-01-samba.html>

The Samba FAQ

<http://us1.samba.org/samba/docs/FAQ/>

What is CIFS?

<http://anu.samba.org/cifs/>