Jadir Marra da Silva

Uso do SAMBA como PDC em uma rede mista criando políticas de uso e autenticação

Monografia de Pós-Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em Administração de Redes Linux.

Orientador
Prof. Joaquim Quinteiro Uchoa

Lavras
Minas Gerais - Brasil
2003

Jadir Marra da Silva

Uso do SAMBA como PDC em uma rede mista criando políticas de uso e autenticação

Monografia de Pós-Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em Administração de Redes Linux.

Aprovada em *25 de Abril de 2004*

Prof. Fernando Cortez Sica

Prof. Ricardo Martins de Abreu Silva

Prof. Joaquim Quinteiro Uchoa
(Orientador)

Lavras
Minas Gerais - Brasil

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Códigos e Listagens

A Deus e a minha família.

Agradecimentos

A Joaquim Quinteiro Uchoa pela classe uflamon.cls que me ajudou muito na confecção deste trabalho.

Resumo

Para integrar redes *Windows*(c) e Linux tem sido bastante utilizado o *Samba*[Eckstein (1999)] disponível em `http://www.samba.org`, que permite a convivência pacífica de clientes de rede que utilizam ambos os sistemas operacionais. Este trabalho visa mostrar o uso do *Samba* agindo como controlador primário de domínio(PDC) provendo não apenas os serviços de autenticação e compartilhamento mas também os mecanismos básicos para implantar uma política de uso dos recursos computacionais através do uso de mecanismos de policiamento do usuário encontrados nos sistemas operacionais da família *Win9x*.

Capítulo 1

Introdução

Um grande problema na vida dos administradores de redes é o uso inadequado dos computadores que compõem a rede. São usuários que transformam os computadores em verdadeiros laboratórios de testes para *software* inúteis do ponto de vista produtivo, mas muito eficazes no consumo de recursos da máquina. Não raramente acabam comprometendo a segurança de toda uma rede.

O que se espera de usuários de computadores em seu ambiente de trabalho é que esses utilizem seus PC's exclusivamente para suas tarefas profissionais. Invariavelmente esses PC's são adquiridos tendo em mente finalidades práticas como processamento de textos, uso de planilhas ou aplicativos específicos ao ramo de atuação da empresa.

Esse comportamento do usuário acaba sobrecarregando de trabalho os profissionais responsáveis pela manutenção do parque de máquinas da empresa, pois esses PC's , após sucessivas instalações de *software* e mudanças em suas configurações, acabam perdendo a sua performance. Deve-se lembrar também que permitir ao usuário executar qualquer aplicativo em seu PC significa também permitir a execução de vírus e *trojans*.

Para contornar essa situação o ideal seria que cada usuário tivesse suas ações limitadas àquelas citadas na Tabela 1.1:

Tabela 1.1: Ações permitidas ao usuário de um PDC

Executar um número limitado de aplicativos
Não pode mudar as confi gurações de seu PC
É obrigado a logar na rede antes utilizar qualquer recurso do PC

Tudo isso poderia ser feito acrescentando a essa rede um controlador primário de domínio(PDC) NT e utilizando o *software poledit.exe* citado em [Microsoft (1997)]. O que o *poledit.exe* faz é definir o que cada usuário pode fazer em seu computador. Quais aplicativos ele tem permissão de uso, se ele pode modificar as configurações

de seu *desktop* ou não. O problema dessa solução é que o seu custo seria tão elevado quando maior fosse o número de PC's ligados à rede. O alto custo se deve ao fato de que para cada máquina conectada ao PDC seria necessária uma licença de uso. Uma alternativa seria o uso de um *software* livre no lugar do servidor NT. Esse software existe e seu nome é Samba. Nas páginas a seguir será mostrado como implementar um PDC para redes *Windows*(c) baseado no *Samba* que implemente tudo isso.

O Capítulo 2 descreve como modificar as configurações do *Samba* , o uso de diretivas de configuração que farão com que o servidor *Samba* execute algumas ações antes do *logon* do usuário.

O Capítulo 3 aborda a aplicação de restrições em um computador executando *Windows*(c) e de como implementar essas restrições via registro.

O Capítulo 4 mostra como implementar o uso de restrições para os usuários de um determinado grupo e finalmente, no Capítulo 5, as considerações finais e conclusões.

Capítulo 2

O *Samba* como PDC

O *Samba* é uma implementação *open source* do protocolo *CIFS* [Hertel (2003)] , antigamente conhecido como *NETBIOS* [Evans (2002)]. Ele foi criado para permitir que sistemas *Unix like*, entre eles o Linux, consigam interagir com computadores *Windows*(c) em uma rede. A criação de um PDC *Samba* , muito bem detalhada em [Eckstein (1999)], é um tarefa relativamente simples. Para esse trabalho serão feitas algumas pequenas alterações na configuração de um PDC *Samba*.

2.1 Alterando o `/etc/smb.conf`.

Será citado então alguns exemplos das modificações feitas no arquivo `/etc/smb.conf` necessárias para esse trabalho. Nesse trabalho é desejável que para cada usuário do PDC seja criado um *script* de *logon* específico. Na Listagem 2.1 pode-se ver um fragmento do arquivo `/etc/smb.conf` com as modificações necessárias.

Listagem 2.1: Configurações para os scripts de logon

```
1 # script de logon especifico para cada usuario
2 # o nome do script de logoné o nome do áusurio
3 # que áest logando
4 logon script = \%U.bat\\
5 #caminho onde o cliente ira procurar pelos scripts de logon
6 logon path = \\%L\netlogon\\
7 logon drive = h:
8 logon home = \\%L\%U\winprofile\\
```

A Listagem 2.1 faz uso de algumas variáveis internas do *Samba* como `%U nome` do usuário da seção, `%L nome` *NETBIOS* do servidor (caso ele possua outros nomes). Uma descrição mais detalhada dessas variáveis pode ser vista na Tabela 2.1.

Seria desejável também que o conteúdo de cada *script* de *logon* fosse diferenciado para cada usuário de acordo com o seu grupo de trabalho no servidor Linux, o seu nome, a máquina que ele está usando, o nome do servidor e o endereço IP de

Tabela 2.1: Variáveis internas do *Samba*

%S	o nome do serviço atual, se houver
%P	o diretório home do serviço atual, se houver
%u	o nome do usuário do serviço atual, se houver
%g	o nome do grupo primário do %u
%U	o nome do usuário da sessão
%G	nome do grupo principal de %U
%H	o diretório home do usuário fornecido por %u
%v	A versão do samba
%h	Nome do host na internet onde o Samba está sendo executado
%m	Nome NetBIOS da máquina cliente (muito útil)
%L	o nome NetBIOS do servidor. Isso permite a você mudar a confi guração baseado na forma como o cliente te chama Seu servidor pode ter uma dupla personalidade. Note que esse parâmetro não está disponível quando o Samba escuta a porta 445, como o cliente não envia mais essa informação
%M	o nome internet da máquina cliente
%N	o nome do seu servidor de diretórios NIS.Isto é obtido de sua entrada no auto.map NIS. Se você não compilou o Samba com a opção –with-automount então este valor será o mesmo de %L
%p	o caminho do diretório home do serviço, obtido de sua entrada no auto.map NIS. A entrada no auto.map NIS é expandida como "%N:%p"
%R	o nível do protocolo selecionado após negociação de protocolos. Ele pode ser um destes CORE, COREPLUS, LANMAN1, LANMAN2 ou NT1
%d	o id do processo relacionado ao processo do servidor atual
%a	a arquitetura da máquina remota. Apenas algumas são reconhecidas, e estas podem não ser 100% confi áveis. Atualmente são reconhecidas corretamente Samba, WfWg, Win95, WinNT e Win2k. Qualquer coisa diferente será recolhecida como "UNKNOWN". Se ele reconhecer errado então enviar um log nível 3 para `samba@samba.org` deve permitir que seja reparado
%I	o endereço IP da máquina cliente
%T	a data e hora atuais
%$(envvar)	o valor da variável de ambiente envar

sua estação de trabalho. Para isso foi alterada a seção [netlogon] como mostrado na Listagem 2.2.

Listagem 2.2: Confi guração da seção netlogon.

```
1 [netlogon]
2 path = /home/netlogon/%g
3 root preexec = /usr/sbin/smblogin.sh %U %g %m %L %I
4 root postexec = /usr/sbin/smblogout.sh %U %g %m %L %I
5 browseable = No
```

Na Listagem 2.2 pode-se ver o uso da diretiva *root preexec* e *root postexec*. São essas diretivas que tornam possíveis a criação de *scripts* de *logon* personalizáveis. De acordo com [Samba (2004)] essas diretivas servem para executar comandos antes que uma conexão ao serviço seja efetuada, especificamente *root preexec*, e também quando a conexão é encerrada, *root postexec*. Um detalhe interessante é que os comandos executados dessa forma serão executados com as permissões do superusuário.

2.2 Personalizando os *scripts* de *logon*

Os *scripts* citados na Listagem 2.2 é que são os responsáveis pela geração dos *scripts* de *logon* que serão executados pela máquina cliente no momento do *logon*. A seguir será dado uma descrição do que cada um faz.

2.2.1 O *script smblogin.sh*

Esse *script* irá gerar os *scripts* de *logon* para a máquina cliente. Um fato importante a ser considerado é que o *script* de *logon* gerado deverá ter o caractere de final de linha, código hexadecimal *0xa*, trocado pela sequência em hexadecimal *0xd0xa*, caso contrário os *scripts* de *logon* (arquivos bat) não serão executados pela máquina cliente, tomando esse cuidado será produzida uma saída na tela do usuário parecida com a da Figura 2.1.

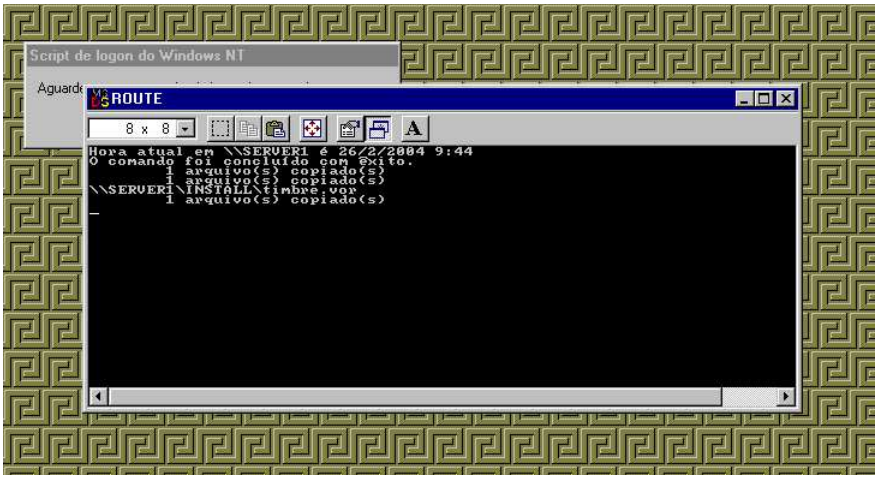

Figura 2.1: Exemplo de saída de um *script* de *logon*

De acordo com as configurações citadas na Listagem 2.2 para a diretiva *root preexec* esse *script* receberá do *Samba* 5 parâmetros. O significado desses parâmetros pode ser vista na Tabela 2.2:

Tabela 2.2: parâmetros passados pelo *Samba* para o *script smblogin.sh*

$1	nome do usuario da sessão
$2	grupo ao qual pertence o usuário no Linux
$3	nome da máquina de onde o usuário esta logando
$4	nome(*NetBIOS*) do servidor *Samba* caso o servidor possua vários nomes
$5	endereco IP da estação que esta logando no *Samba*

Com essas informações já é possível montar um *script* básico para a diretiva *root preexec* do *Samba*. A Listagem 2.3 mostra um *shell script* simples baseado nessas informações.

Listagem 2.3: *Script* a ser executado pelo *Samba* pela diretiva *root preexec*.

```
1  #!/bin/sh
2  # configura as variaveis utilizadas pelo script
3  export USUARIO=$1
4  export GRUPO=$2
5  export HOST_NAME=$3
6  export SERVER_NAME=$4
7  export HOST_IP=$5
8  export LOGONBAT=/home/netlogon/$GRUPO/$USUARIO.bat
9  export CONF_DIR=/etc/smblogon
10 export LOG_CMD='logger -t SMB-PDC'
11 $LOG_CMD "Login started => $USUARIO@$HOST_NAME"
12 # manter os relogios das estacoes sincronizados com o relogio do servidor
13 printf "%s%s%s\x0d\x0a" 'net time \\' $SERVER_NAME ' /set /yes' >> $LOGONBAT
```

O *script* da Listagem 2.3 irá criar um arquivo de comandos em lote, arquivo bat, no diretório de *logon* do usuário com o seguinte conteúdo:

```
net time \\servidorx /set /yes
```

Como se vê esse arquivo bat apenas ajusta o relógio da estação de trabalho com o relógio do servidor *Samba*. Mais adiante serão dadas mais funcionalidades para esse arquivo de comandos em lote.

2.2.2 O *script smblogout.sh*

Esse *script* tem a finalidade de executar algumas tarefas antes que o usuário desconecte do serviço de *logon*. Essa desconexão ocorre logo após a autenticação do usuário pelo PDC. Os mesmos parâmetros passados para o *script* da Listagem 2.3 são passados agora para o *script smblogout.sh* da Listagem 2.4.

Listagem 2.4: *Script* a ser executado pelo *Samba* pela diretiva *root postexec*.

```
1  #!/bin/sh
2  export USUARIO=$1
3  export GRUPO=$2
4  export HOST_NAME=$3
5  export SERVER_NAME=$4
6  export HOST_IP=$5
7  # apaga o script de logon antigo
8  rm /home/netlogon/$GRUPO/$USUARIO*.bat
```

Assim como o *script* da Listagem 2.3 o *script smblogout.sh* citado acima não faz muita coisa. Apesar de básico este *script* pode ser alterado para realizar as tarefas de faxina como apagar o *script* de *logon* após o seu uso, desconectar *drives* de rede, e liberar todos os recursos que não sejam mais necessários após o processo de *logon* do usuário.

Capítulo 3

As políticas de uso

Nesse trabalho, a política de uso dos computadores em uma rede será implementada através da aplicação de restrições para cada máquina que compõe a rede levando em consideração que os usuários de um determinado grupo de trabalho realizam tarefas semelhantes logo necessitam de permissões semelhantes. Doravante, toda vez que for falado em grupo de trabalho, entenda-se como o grupo de trabalho ao qual o usuário pertence no servidor Linux e não como o grupo de trabalho especificado no *Windows*(c).

O esforço realizado no capítulo anterior será agora melhorado e os exemplos citados anteriormentes serão agora incrementados para incorporarem novas funcionalidades.

Os *scripts* citados na Listagem 2.3 e na Listagem 2.4 serão agora modificados e se tornarão mais úteis.

Com o intuito de especificar as permissões e restrições que serão impostas a cada grupo de trabalho será feito um estudo das chaves de registro do *Windows*(c) responsáveis pelo policiamento do computador e que seriam modificadas pelo aplicativo *poledit.exe*.

3.1 Aplicando as restrições

O modo mais fácil de aplicar restrições ao *Windows*(c) é utilizando o *poledit.exe*, Figura 3.1.

Mas ao invés de utilizar o *poledit.exe*, será feito o mesmo trabalho importando as chaves de registro, que seriam modificadas pelo *poledit.exe*, do servidor *Samba*. O policiamento de um *desktop Windows*(c) pode ser aplicado nos seguintes elementos da Tabela 3.1.

Qualquer tentativa de burlar o policiamento aplicado aos itens citados na Tabela 3.1 resultará em uma advertência como a da Figura 3.2.

A seguir será dado as explicações a cerca de cada um deles.

Figura 3.1: Janela principal do *poledit.exe*

Tabela 3.1: Itens do *Windows*(c) passíveis de policiamento

1	*Windows Explorer*
2	Painel de Controle
3	Confi gurações de Rede
4	Aplicativos do MS-DOS

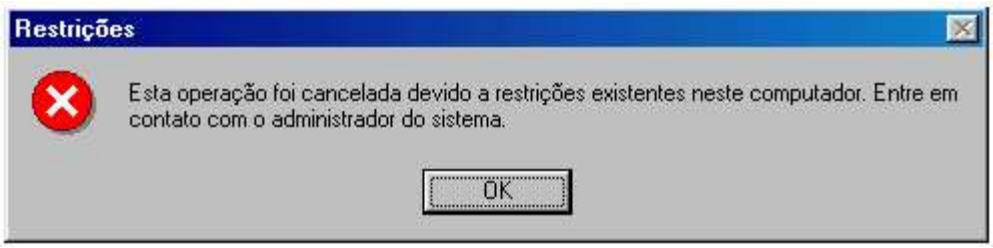

Figura 3.2: Advertência emitida após uma tentativa de operação não permitida.

3.1.1 Alterando o comportamento do *Windows Explorer*

O *Windows Explorer* é o *shell* padrão do sistema operacional *Windows*(c) e não apenas um gerenciador de arquivos.Para alterar o seu comportamento e aplicar restrições nele é necessário modificar as opções da seguinte chave:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
```

Antes de continuar será mostrado como criar um arquivo com as configurações de registro. Um arquivo de registro se parece com o fragmento de arquivo da Listagem 3.1

Listagem 3.1: Arquivo com configurações do registro do Windows

```
1  REGEDIT4
2  ; um comentario
3  [HKEY_LOCAL_MACHINE\Network\Logon]
4  ;forca o usuario a logar na rede
5  "MustBeValidated"=dword:00000001
6  ;configura ou nao os perfis de usuario
7  "UserProfiles"=dword:00000000
```

Na Linha 1 tem-se a versão do editor de registro e na Linha 2 um comentário. Palavras entre [e] indicam uma chave, Linha 3. As *strings* subsequentes indicam as possíveis opções para cada chave seguidas de seus valores que podem ou não ser precedidos por um indicador de tipo(*dword, hex*). Nesse trabalho todos os valores do tipo *dword* indicam uma opção com apenas 2 valores possíveis 1(habilitado) ou 0(desabilitado).

As restrições mostradas na Listagem 3.2 podem ser aplicadas ao *Windows Explorer*:

Listagem 3.2: Chaves que modificam o comportamento do *Windows Explorer*

```
1  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
2  ;disabilita o autorun
3  "NoDriveTypeAutoRun"=hex:95,00,00,00
4  ;esconde drives no windows explorer
5  "NoDrives"=hex:00,00,00,00
6  ;esconde o menu executar
7  "NoRun"=dword:00000000
8  ;nao permite ao usuario excluir impressoras
9  "NoDeletePrinter"=dword:00000001
10 ;nao permite ao usuario adicionar impressoras
11 "NoAddPrinter"=dword:00000001
12 ;esconde o menu de configuracoes do painel de controle,
13 ;impressoras e rede do menu iniciar. Se a barra de tarefas
14 ;for removida o menu configuracoes sera removido
15 "NoSetFolders"=dword:00000001
16 ;esconde todos os icones do desktop
17 "NoDesktop"=dword:00000001
18 ;esconde o menu arquivo do explorer
19 "NoFileMenu"=dword:00000000
20 ;nao permite ao usuario mapear drives de rede
21 "NoNetConnectDisconnect"=dword:00000001
22 ;desabilita o ambiente de rede
23 "NoNetHood"=dword:00000000
24 ;remove as configuracoes da barra de tarefas do menu configuracoes
25 "NoSetTaskbar"=dword:00000001 ;
26 ;permite a execucao apenas dos aplicativos selecedionado pelo administrador
27 "RestrictRun"=dword:000000001 ;
28 ;desabilitar o active desktop
29 "NoActiveDesktop"=dword:00000001
```

3.1.2 Alterando o comportamento do Painel de Controle

É através do painel de controle que a maioria das configurações do *Windows*(c) é feita. Impedir seu acesso ao usuário comum pode poupar bastante trabalho ao administrador da rede. As restrições que podem ser aplicadas nesse item vão desde a negação total de acesso ao painel de controle até o acesso a itens específicos. Os itens que podem ser controlados ficam abaixo da chave

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
```

Uma relação mais detalhada e comentada pode ser vista na Listagem 3.3.

Listagem 3.3: Chaves que modificam o comportamento do Painel de Controle

```
30 "NoDispCPL"=dword:00000001 ;esconde o painel de controle
31 "NoDispBackgroundPage"=dword:00000001 ;nao permite mudar o papel de parede
32 "NoDispScrSavPage"=dword:00000001 ;nao permite mudar/configurar o screensaver
33 "NoDispAppearancePage"=dword:00000001 ;nao permite mudar a aparencia do windows
34 "NoDispSettingsPage"=dword:00000000 ;nao permite mudar as configuracoes de video
35 "NoAdminPage"=dword:00000001 ;nao permite alterar as configuracoes de administracao remota
36 "NoProfilePage"=dword:00000001 ;nao permite acessar as configuracoes de perfis de usuario
37 ;nao permite acessar a paleta de configuracoes de hardware do painel de controle
38 "NoConfigPage"=dword:00000001
39 "NoDevMgrPage"=dword:00000001 ;nao permite acessar o gerenciador de dispositivos
40 "NoFileSysPage"=dword:00000001 ;nao permite mudar as configuracoes do sistema de arquivos
41 "NoVirtMemPage"=dword:00000001 ;nao permite mudar as configuracoes da memoria virtual
```

3.1.3 Restringindo as modificações na configuração da rede

Uma outra área sensível de um *desktop Windows*(c) é justamente a sua configuração de rede. Seu acesso deve ser definitivamente proibido para o usuário. Os itens e valores que definem as restrições para as configurações de rede se encontram abaixo da chave

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
```

Na Listagem 3.4 pode-se ver o que pode ser configurado para este item.

Listagem 3.4: Chaves que restringem as modificações nas configurações de rede

```
42 ; nao permite ao usuario mudar o compartilhamento de user para share
43 "NoNetSetupSecurityPage"=dword:00000001
44 "NoNetSetup"=dword:00000000 ; Disable the Network Control Panel
45 "NoNetSetupIDPage"=dword:00000000 ;Hide Identification Page
46 "NoFileSharingControl"=dword:00000000 ; desabilita os controles de compartilhamento de arquivos
47 "NoPrintSharing"=dword:00000000; desabilita os controles de compartilhamento de impressoras
```

3.1.4 Restringindo as execução de aplicativos para MS-DOS

Nesse item pode-se modificar o modo como o *Windows*(c) tratará os aplicativos feitos para serem executados sobre o MS-DOS. Os itens que podem ser controlados encontram-se abaixo da chave

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\ Policies\WinOldApp]
```

Na Listagem 3.5 pode-se ver as possíveis opções de policiamento para aplicativos MS-DOS.

Listagem 3.5: Chaves que restringem o uso de aplicativos MS-DOS

```
1 ;disabilita a execucao de aplicativos MS-DOS
2 Disabled=dword:00000001
3 ;disabilita a execucao de aplicativos de modo real.
4 NoRealMode=dword:00000001
```

Nas listagens anteriores foram citadas algumas modificações que podem ser feitas no registro do *Windows*(c) para limitar as ações do usuário sem penalizar a sua produtividade. Uma listagem mais completa de todas as opções de policiamento pode ser encontrada em [Winguides (2004)] e em [Microsoft (1997)]. Em

[Winguides (2004)] encontra-se uma relação maior de opções para aplicativos expecíficos como o pacote *Office, o netmeting, internet explorer,* etc.

Capítulo 4

Criando as Restrições por Grupo de Trabalho

Serão criados agora os mecanismos para restringir o uso dos computadores, baseado no grupo de trabalho do usuário. Imagine uma empresa onde existam os seguintes departamentos: Contabilidade, administração e recursos humanos. Deverá existir então, para cada departamento, um grupo de usuários no servidor Linux, conforme a Tabela 4.1.

Tabela 4.1: Grupos de usuários no servidor Linux

Grupo	Departamento
admin	Administração
rh	Recursos Humanos
contab	Contabilidade

De posse dessas informações deverão ser feitas algumas mudanças no *script* citado na Listagem 2.3.

4.1 De volta ao *smblogin.sh*

Como foi visto na Tabela 2.2 o segundo parâmetro recebido pelo *script smblogin.sh* é justamento o nome do grupo de trabalho do usuário que está logando. Com base nisso, o *script* fica assim:

Listagem 4.1: primeira modificação em *smblogin.sh*.

```
1  #!/bin/sh
2  # configura as variaveis utilizadas pelo script
3  export USUARIO=$1
4  export GRUPO=$2
5  export HOST_NAME=$3
6  export SERVER_NAME=$4
7  export HOST_IP=$5
8  export LOGONBAT=/home/netlogon/$GRUPO/$USUARIO.bat
9  export CONF_DIR=/etc/smblogon
10 export LOG_CMD='logger -t SMB-PDC'
11 $LOG_CMD "Login started => $USUARIO@$HOST_NAME"
12 # manter os relogios das estacoes sincronizados com o relogio do servidor
13 printf "%s%s%s\x0d\x0a" 'net time \\' $SERVER_NAME ' /set /yes' >> $LOGONBAT
14 case "$2" in
15   rh)
16     config_rh $1 $4
17     ;;
18   contab)
19     config_contab $1 $4
20     ;;
21   admin)
22     config_admin $1 $4
23     ;;
24 esac
```

Como se pode ver na Linha 14 da Listagem 4.1 foi acrescentado um teste condicional *case* para verificar a qual dos grupos, citados na Tabela 4.1, pertence o usuário e a partir disso executar uma rotina expecífica para o seu grupo. Na Listagem 4.1 as rotinas *config_rh*, *config_contab* , *config_admin* são responsáveis pela configuração dos computadores toda vez que um usuário pertencente a um dos grupos da Tabela 4.1 logar na rede. O grupo *contab* será usado, como exemplo, para desenvolvimento de uma configuração específica para um grupo específico.

4.2 Configurando um grupo de trabalho

Ao se configurar um grupo de trabalho em um PDC deve-se fazê-lo de forma que não se penalize o desempenho profissional de seus componentes. Como serão criadas várias restrições de uso do computador via registro do *Windows*(c) deve-se ter o cuidado de não exagerar nas restrições. Um exemplo simples de exagero pode ser visto na Listagem 4.2 logo abaixo.

Listagem 4.2: Configuração paranóica de restrições.

```
1 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
2 "NoRun"=dword:00000001 ;esconde o menu executar
3 ;esconde o menu de configuracoes do painel de controle,
4 ;impressoras e rede do menu iniciar. Se a barra de tarefas
5 ;for removida o menu configuracoes sera removido
6 "NoSetFolders"=dword:00000001
7 "NoDesktop"=dword:00000001 ;esconde todos os icones do desktop
8 "NoFileMenu"=dword:00000001 ;esconde o menu arquivo do explorer
9 "NoSetTaskbar"=dword:00000001 ;remove as configuracoes da barra de tarefas do menu configuracoes
```

Como se pode ver na Listagem 4.2 foram desabilitados o menu "Executar"(linha 2), o painel de controle(linhas 6 e 9), foram escondidos todos os ícones da área de trabalho(linha 7) e o menu "Arquivo"do *Windows Explorer* e do *Internet Explorer*.

4.2.1 Definições básicas para todos os grupos

Algumas configurações foram definidas como básicas tendo em mente que todos os usuários do PDC são simplesmente usuários de tecnologia. Na Tabela 1.1 na página 1 pode-se ver que uma das características desejáveis em um ambiente de rede é que cada usuário da rede se identifique antes de começar a utilizar seu computador, ou seja, ele deve obrigatoriamente logar na rede. Segundo [Winguides (2004)] isso pode ser implementado alterando-se uma chave do registro onde pode-se configurar alguns parâmetros do processo de *logon*, Tabela 4.2.

Tabela 4.2: Chave em `[HKEY\LOCAL\MACHINE\Network\Logon]`

Opção	Tipo	Habilitado	Desabilitado	Signifi cado
"MustBeValidated"	dword	00000001	00000001	Força o login na rede
"UserProfi les"	dword	00000001	00000001	Habilita/Desabilitado os perfi s de usuários ambulantes

Então essas serão as primeiras entradas em nosso arquivo de registro. A opção *"MustBeValidated"* irá forçar o usuário a logar na rede, caso ele clique no botão cancelar será exibida uma mensagem semelhante à da figura 4.1.

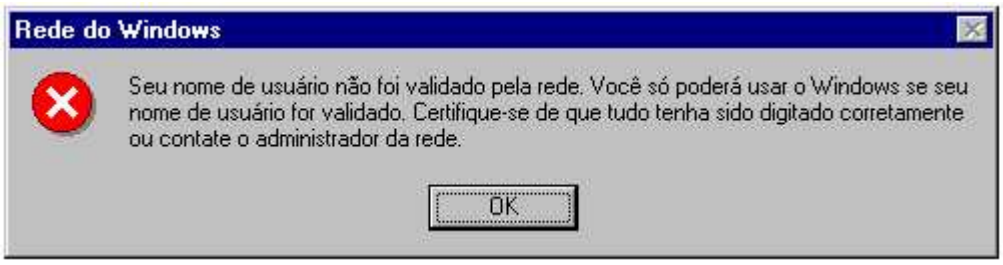

Figura 4.1: Mensagem exibida após o *clique* no botão cancelar da janela de *login*.

Também poderia ser criado um ambiente homogêneo com o mesmo papel de parede em todos os *desktops* e novamente em [Winguides (2004)] encontra-se uma solução interessante para isso, ver Tabela 4.3.

Opção	Tipo	Valor	Signifi cado
"WallpaperStyle"	string	"0"	Força o login na rede
"Pattern"	string		Padrão de fundo
"Wallpaper"	string	"egito.bmp"	;arquivo a ser usado como papel de parede
"TileWallpaper"	string	"1"	confi gura ou nao o mozaico para papeis de parede pequenos

Tabela 4.3: Chave em `[HKEY_CURRENT_USER\ControlPanel\Desktop]` para personalizar o *desktop*.

E por último seria interessante avisar ao usuário que ele está em um ambiente de rede controlado e alertá-lo sobre as possíveis conseqüências dos seus atos. Em

[Microsoft (1997)] pode-se ver na página 66 a chave de registro [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon] que serve exatamente para exibir uma mensagem antes do *logon* do usuário, recorrendo a [Winguides (2004)] encontra-se uma chave semelhante, porém para outras versões do *Windows*(c), como esse trabalho foca o uso de um PDC *Samba* com clientes *Win9x* será usada essa última. Na Tabela 4.4 encontram-se as opções para essa chave.

Opção	Valor
"LegalNoticeCaption"	"Aviso ao Usuário"
"LegalNoticeText"	"Não tente utilizar este computador se você não for um usuário autorizado. As suas ações podem ser monitoradas a qualquer momento. Use este computador com responsabilidade. Se você não concordar com estes termos não prossiga, ao prosseguir você estará manifestando a sua concordância.Qualquer dúvida contacte o administrador da rede."

Tabela 4.4: Chave em `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]` para exibir mensagens antes do *logon*.

As opções listadas na Tabela 4.4 são do tipo *string*. A opção *"LegalNoticeText"* apesar de estar listada em várias linhas deverá ser informada no arquivo de registro em apenas uma linha, caso contrário não será exibida corretamente. Na Figura 4.2 percebe-se o resultado dessa configuração na tela do usuário.

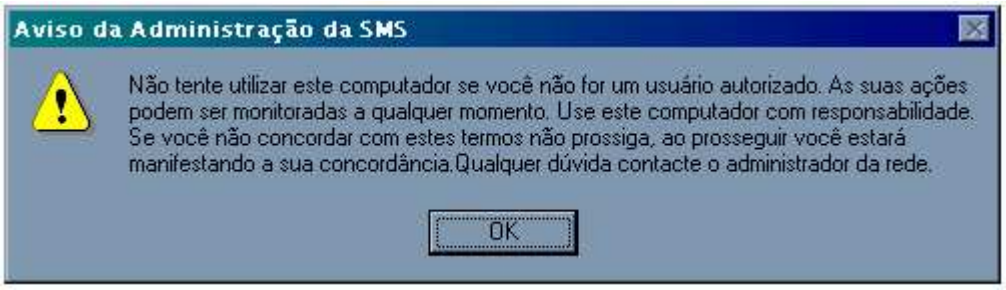

Figura 4.2: Alerta exibido ao usuário antes do processo de *logon*

Terminadas as configurações básicas é hora de passar às configurações específicas de cada grupo.

4.2.2 Configurações específicas de um grupo

Como foi definido que seria configurado um grupo de trabalho para os usuários do grupo *contab*, deve-se expecificar então o que é permitido aos membros desse grupo. Neste departamento fictício, contabilidade, os usuários necessitam de todos os software listados na tabela 4.5.

Programa	Nome do executável
Tabajara Contabil XP	tbjcontabilxp.exe
ReceitaNet	receitanet.exe
Pacote MS Offi ce	winword.exe, excel.exe, powerpnt.exe, access.exe
Emulador NetTerm	netterm.exe
Calculadora	calc.exe
Acrobat Reader	acrord32.exe
Internet Explorer	iexplorer.exe
Outlook Express	msimn.exe
Bloco de Notas	notepad.exe

Tabela 4.5: Programas de computador permitidos para o grupo contab.

Deve-se criar agora um arquivo de registro que contenha as configurações padrão para todos os grupos e as configurações específicas do grupo *contab*. Ao criar esse arquivo deve-se respeitar as seguintes condições:

- criar um diretório dentro do diretório correspondente ao compartilhamento *netlogon* cujo nome corresponda ao nome do grupo de trabalho em questão;
- criar/mover ou copiar o arquivo de registro dentro do diretório citado no item anterior.

Nesse caso deve-se criar o diretório `/home/netlogon/contab` e colocar nele o arquivo de registro que será importado pelos usuários do grupo *contab* durante o processo de *logon*. As restrições quanto a permissão de execução de aplicativos são configuradas na chave de registro:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun]
```

Deverão ser acrescentados pares de valores do tipo string ordenados seqüencialmente a partir do número 1 contendo os nomes dos aplicativos permitidos, ver Tabela 4.5. O arquivo de registro para o grupo *contab* ficará então como mostrado na Listagem 4.3.

Listagem 4.3: Arquivo de registro para o grupo *contab*

```
1  REGEDIT4
2  ; =
3  ; ==================== CONFIGURACAO PADRAO PARA TODOS ========================
4  ; =
5  [HKEY_LOCAL_MACHINE\Network\Logon]
6  "MustBeValidated"=dword:00000001 ;forca o usuario a logar na rede
7  "UserProfiles"=dword:00000000 ;configura ou nao os perfis de usuario
8
9  ; esta configuracao tem efeito apenas psicologico. Faz o usuario
10 ; saber que ele nao esta em uma terra de ninguem e que pode fazer
11 ; o que quiser em sua estacao de trabalho. Esta modificacao so
12 ; tera efeito apos o segundo login na mesma ámquina.
13 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]
14 "LegalNoticeCaption"="Aviso da Administracao da SMS"
15 "LegalNoticeText"="Nao tente utilizar este computador se voce nao for um usuario autorizado.
16 As suas acoes podem ser monitoradas a qualquer momento. Use este computador com responsabi—
17 lidade. Se voce nao concordar com estes termos nao prossiga, ao prosseguir voce estara mani—
18 festando a sua concordancia.Qualquer duvida contacte o administrador da rede."
19
20 ; a configuracoes abaixo nao sao relacionadas a seguranca
```

```
; mas a padronizacao dos desktops em um ambiente corporativo
[HKEY_CURRENT_USER\Control Panel\Desktop]
"WallpaperStyle"="0" ;
"Pattern"=""
"Wallpaper"="egito.bmp" ;arquivo a ser usado como papel de parede
"TileWallpaper"="1" ;configura ou nao o mozaico para papeis de parede pequenos

; =
; ============== CONFIGURACOES ESPECIFICAS DE CADA GRUPO DE TRABALHO ===========
; =
; sistema de policiamento
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
; nao permitir ao usuario alterar as configuracoes de rede de sua
; estacao de trabalho poupa tempo dos responsaveis pelo suporte de
; rede.
"NoNetSetup"=dword:00000001
; esta configuracoes abaixo ajudam a prevenir possiveis estragos feitos
; por aquele usuario leitor assiduo da "PC-Expert"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"NoDispCPL"=dword:00000001 ;esconde o painel de controle de video
"NoDispBackgroundPage"=dword:00000001 ;nao permite mudar o papel de parede
"NoDispScrSavPage"=dword:00000001 ;nao permite mudar/configurar o screensaver
"NoDispAppearancePage"=dword:00000001 ;nao permite mudar a aparencia do windows
"NoDispSettingsPage"=dword:00000001 ;nao permite mudar as configuracoes de video
"NoAdminPage"=dword:00000001 ;nao permite a administracao remota
"NoProfilePage"=dword:00000001 ;nao permite acessar as configuracoes de perfis de usuario
"NoConfigPage"=dword:00000001 ;nao permite acessar a paleta de configuracoes de hardware
"NoDevMgrPage"=dword:00000001 ;nao permite acessar o gerenciador de dispositivos
"NoFileSysPage"=dword:00000001 ;nao permite mudar as configuracoes do sistema de arquivos
"NoVirtMemPage"=dword:00000001 ;nao permite mudar as configuracoes da memoria virtual

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoRun"=dword:00000001 ;esconde o menu executar
"NoDeletePrinter"=dword:00000001 ;nao permite ao usuario excluir impressoras
"NoAddPrinter"=dword:00000000 ;nao permite ao usuario adicionar impressoras
"NoSetFolders"=dword:00000000 ;esconde o menu de configuracoes
"NoDesktop"=dword:00000000 ;esconde os icones do desktop e desabilita o menu popup do desktop
"NoFileMenu"=dword:00000000 ;esconde o menu arquivo do explorer
"NoNetConnectDisconnect"=dword:00000001 ;nao permite ao usuario mapear drives de rede
"NoNetHood"=dword:00000001 ;desabilita o ambiente de rede
"NoSetTaskbar"=dword:00000000 ;remove o item de menu "Barra de tarefas e menu iniciar"
"RestrictRun"=dword:000000001 ;habilita/desabilita a execucao de aplicativos
"NoActiveDesktop"=dword:00000001 ;desabilitar o active desktop

; daqui para baixo estao listados todos os softwares com ãpermisso de
; execucao na ámquina do usuario. A numeracao deve ser sempre crescente
; e unica. Com excecao de alguns aplicativos do windows tudo o que nao
; estiver explicitamente liberado áser bloqueado.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun]
"1"="regedit.exe"
"2"="explorer.exe"
"3"="iexplore.exe"
"4"="notepad.exe"
"5"="msimn.exe"
"6"="winhelp.exe"
"7"="acrord32.exe"
"8"="tbjcontabilxp.exe"
"9"="receitanet.exe"
"10"="winword.exe"
"11"="excel.exe"
"12"="powerpnt.exe"
"13"="access.exe"
"14"="netterm.exe"
"15"="calc.exe"
```

Com o arquivo de registro no lugar correto é necessário garantir que ele seja importado durante o *logon* do usuário. Precisa-se agora implementar a rotina *config_contab* , Listagem 4.1, para que essa importação seja feita. Após a criação da rotina *config_contab* o *script smblogin.sh*, Listagem 4.1, sofrerá mais uma modificação e ficará como mostrado na Listagem 4.4.

Listagem 4.4: última modificação em *smblogin.sh*.

```
1  #!/bin/sh
2  # configura as variaveis utilizadas pelo script
3  export USUARIO=$1
4  export GRUPO=$2
5  export HOST_NAME=$3
6  export SERVER_NAME=$4
7  export HOST_IP=$5
8  export LOGONBAT=/home/netlogon/$GRUPO/$USUARIO.bat
9  export CONF_DIR=/etc/smblogon
10 export LOG_CMD='logger -t SMB-PDC'
11 $LOG_CMD "Login started => $USUARIO@$HOST_NAME"
12
13 #
14 # tarefas especificas do grupo contab
15 #
16 config_contab() {
17         printf "%s%s%s\x0d\x0a" 'regedit /s \\' $2 '\NETLOGON\GERAL.REG' >> $LOGONBAT
18         printf "%s\x0d\x0a" 'del C:\windows\temp\*.*' >> $LOGONBAT
19 }
20
21 config_rh(){}
22 config_admin(){}
23
24 # manter os relogios das estacoes sincronizados com o relogio do servidor
25 printf "%s%s%s\x0d\x0a" 'net time \\' $SERVER_NAME ' /set /yes' >> $LOGONBAT
26 case "$2" in
27   rh)
28     config_rh $1 $4
29     ;;
30   contab)
31     config_contab $1 $4
32     ;;
33   admin)
34     config_admin $1 $4
35     ;;
36 esac
```

Como se pode ver na linha 16 da Listagem 4.4 a implementação da rotina *config_contab* adiciona ao *script de logon* dos usuários do grupo *contab* o comando necessário para importar o arquivo de registro com as configurações do grupo de trabalho.

4.3 Configurando os clientes Win9x.

As configurações de rede dos clientes Win9x deverão ser alteradas para que estes façam o *logon* no domínio do NT. Dessa forma a autenticação dos usuários será realizada pelo PDC *Samba*. Na figura 4.3 está descrito como proceder essas configurações.

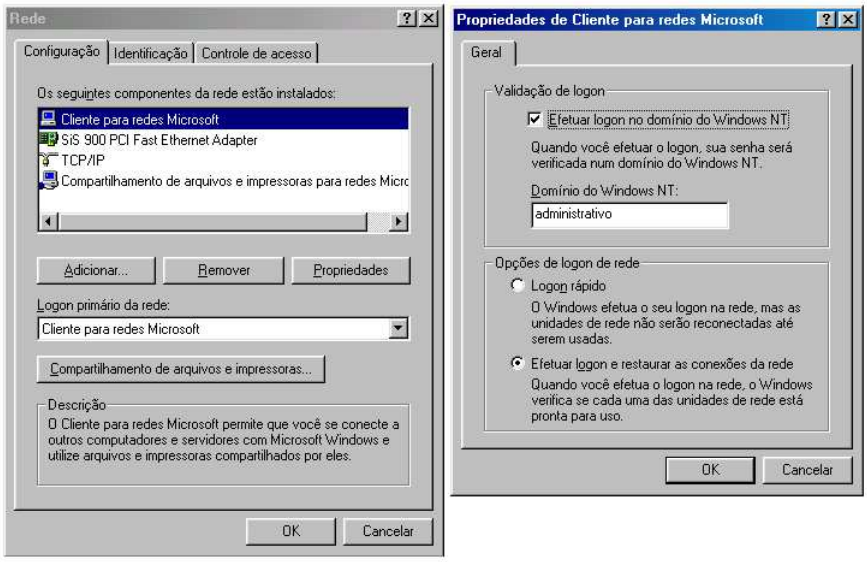

Figura 4.3: Confi guração de um cliente Win9x para *logon* no domínio do NT.

Para configurar cada cliente Win9x deve-se clicar com o botão direito do *mouse* em "Ambiente de Rede"e em seguida no ítem de menu "Propriedades". Então será aberta uma janela como a da Figura 4.3 onde se clicará em "Cliente para redes Microsoft"e depois no botão "Propriedades". Aparecerá então uma segunda janela onde deverá ser marcada a opção "Efetuar logon no domínio do Windows NT". Na caixa de texto "Domínio do Windows NT"deve ser digitado o nome do grupo de trabalho especificado no arquivo de configuração do *Samba*. Basta agora reiniciar o computador cliente para que o mesmo efetue o *logon* no PDC Samba. Esse procedimento deverá ser repetido para todos os computadores da rede.

Terminam aqui todos os procedimentos para configuração do PDC, a partir de agora todos os computadores utilizados pelos usuários do grupo *contab* serão reconfigurados quando os usuários efetuarem o *logon* no *Samba*.

Capítulo 5

Considerações Finais

A criação de um ambiente de rede mais seguro e estável não é uma das tarefas mais simples que existe, sempre existirão usuários que burlarão as regras e aprenderão a contornar as restrições impostas pelos administradores de redes.

Nesse trabalho foi mostrado como tornar uma rede baseada em computadores Win9x menos propensa a falhas decorrentes do uso inadequado. Embora o foco aqui fosse a criação de um ambiente controlado por meio de restrições no lado cliente nada impede que os princípios aqui explicados sejam usados para aplicar restrições do lado servidor.O mesmo *script* da Listagem 4.4 na página 19 poderia ser utilizado para criar regras de firewall baseadas no usuário não importando em qual máquina ele estivesse. Em redes onde o *Samba* é utilizado como servidor de arquivos a localização da pasta "Meus Documentos"de todos os usuários da rede poderia ser mudada para uma pasta no servidor *Samba* o que simplificaria muito o processo de *backup*.

O que se pretendeu com este trabalho foi mostrar de forma simples e clara que o *Samba* pode substituir muito bem um servidor NT. O único limite é a criatividade e a habilidade do administrador.

Referências Bibliográficas

[Eckstein (1999)] Eckstein,Robert. *Using Samba*, 1999. Disponível em ftp://ftp.ora.com/examples/misc/samba/sambapdf.zip última verificação em 28/01/2004.

[Samba (2004)] Auer,Karl. *Samba(7)*[on-line]. Disponível na internet via www. url: http://us1.samba.org/samba/docs/man/samba.7.html. Arquivo capturado em 06 de fevereiro de 2004.

[Evans (2002)] Evans, Timothy D. *NetBios, NetBEUI, NBF, SMB, CIFS Networking* [on-line]. Disponível na internet via www. url: http://ourworld.compuserve.com/homepages/timothydevans/contents.htm. Arquivo capturado em 06 de fevereiro de 2004.

[Microsoft (1997)] *Guide to Microsoft Windows NT 4.0 Profiles and Policies*. [on-line]. Disponível na internet via www. url: http://www.microsoft.com/ntserver/docs/prof_policies.doc. Arquivo capturado em 04 de fevereiro de 2004.

[Winguides (2004)] *The Registry Guide for Windows*. [on-line]. Disponível na internet via www. url: http://www.winguides.com/registry/. Arquivo capturado em 04 de fevereiro de 2004.

[Hertel (2003)] Hertel, Christopher R. *Implementing CIFS: The Common Internet File System*. [on-line]. Disponível na internet via www. url: http://www.ubiqx.org/cifs/. Arquivo capturado em 06 de fevereiro de 2004.