

Documentação Sacix (Tamanduá)

Documentação da versão servidor, para
implementação por terceiros e referência

(rascunho atual, ainda em progresso de criação,
gerado em 02 de fevereiro de 2004)

Sumário

1. Introdução.....	4
1.1 Motivação.....	4
1.2 Sacix (Tamanduá).....	4
1.3 Onde Obter.....	5
1.4 Características.....	5
1.5 Problemas conhecidos.....	5
1.6 Para Fazer.....	6
1.7 Autores.....	6
1.8 Direitos Autorais.....	7
2. Visão Geral.....	8
2.1 Objetivo.....	8
2.2 Distribuição.....	8
2.3 Programas Utilizados.....	9
2.4 Conhecimento Mínimo Necessário.....	10
2.5 Teoria.....	10
2.6 Processo de Inicialização do Terminal.....	10
3. Instalação do Sacix (Tamanduá).....	12
3.1 Características do Instalador.....	12
3.1.1 Instalação Automática:.....	12
3.1.2 Instalação Passo-a-Passo:.....	12
3.1.3 Registro de Atividades (logs):.....	13
3.1.4 Acesso a shells:.....	13
3.2 Instalação Automática.....	13
3.3 Instalação Passo-a-Passo.....	14
4. Configuração do Cliente.....	15
4.1 Kernel do cliente.....	15
4.2 Mini-Distro.....	15
4.2.1 Inicialização da Mini-Distro.....	15
4.2.2 Modificação da Mini-Distro em NFS.....	16
4.2.3 Modificação da Mini-Distro em RAM.....	16
4.3 Initrd do cliente.....	17
4.4 XFree86 da Mini-Distro.....	17
5. Configuração do servidor.....	18
5.1 Initrd.....	18
5.2 DHCP.....	18
5.3 TFTP.....	18
5.4 NFS.....	18
5.5 SSH.....	19
5.6 Proxy.....	19
5.7 Web/BD.....	19
5.8 Rede.....	19
5.8.1 Topologia com uma placa de rede.....	20
5.8.2 Topologia com duas placas de rede.....	20
6. Configurações de Usuário.....	21

6.1 Guia rápido de personalização.....	22
6.2 Lidando com o Pacote Gnome-Telecentro.....	23
6.3 Administração via GConf.....	24
6.4 Ajustes específicos de programas.....	25
7. Configuração adicional.....	26
7.1 Disquete Remoto.....	26
7.2 Programa de gerenciamento.....	26
8. Segurança Básica.....	27
8.1 Senhas do LILO e BIOS.....	27
8.2 Permissões.....	27
8.3 Alteração de Senha.....	27
8.4 Limite de Processos.....	27
8.5 TCP Wrappers.....	28
9. Replicação de Servidores.....	29
9.1 Gerando as Imagens.....	29
9.2 Restaurando as Imagens.....	30

1. Introdução

Este documento é, acima de tudo, a marca de uma grande vitória alcançada pela Prefeitura do Município de São Paulo, através do Governo Eletrônico e da comunidade de Software Livre.

A Prefeitura Municipal de São Paulo, desde 2001, tem construído Telecentros para executar o Plano de Inclusão Digital, que se propõe a tratar o acesso às tecnologias de informação como política pública. Para tanto, a Prefeitura vem implantando Telecentros nas áreas mais carentes da cidade de São Paulo, escolhidas de acordo com o Índice de Desenvolvimento Humano (IDH). Os locais são geralmente bairros distantes do centro da cidade, em que poucas pessoas têm acesso a essas tecnologias. Os dois primeiros Telecentros, por exemplo, foram inaugurados na Cidade Tiradentes (Zona Leste) e na Brasilândia (Zona Norte).

Um Telecentro possui entre 10 e 20 computadores com acesso em banda larga à Internet, provendo uso livre dos softwares instalados para a população. Além dos funcionários do Governo Eletrônico, também é monitorado por funcionários públicos que auxiliam e instruem a população. Aliado a metodologias de uso, de instrução, de envolvimento e de organização da comunidade, inclusive em projetos, o Telecentro pode ser utilizado como instrumento para a Inclusão Digital.

Sacix é o nome da customização do Debian para uso nos Telecentros. E-cidadania é o nome dado pela Prefeitura de São Paulo ao Projeto como um todo.

1.1 Motivação

O Projeto e-cidadania tem diversas ramificações. Na área de informática, vai desde a implantação da rede física dos Telecentros até a manutenção dos softwares instalados de forma remota. Assim, a documentação de como é feita a instalação do servidor do Telecentro torna-se indispensável.

Mas é importante ressaltar que a solução cliente-servidor dos Telecentros é genérica, e pode ser utilizada para outras aplicações, inclusive em ambiente de trabalho, com manutenção centralizada e reaproveitamento de computadores antigos ou obsoletos.

Dentro deste contexto de uso diversificado, esta documentação foca principalmente no conceito de Telecentro Livre, ou seja, um Telecentro utilizando exclusivamente Software Livres.

1.2 Sacix (Tamanduá)

Esta versão do servidor Sacix (Tamanduá) foi desenvolvida e é mantida pela equipe de desenvolvimento GNU/Linux da Coordenadoria do Governo Eletrônico da Prefeitura de São Paulo, que é composta por:

Kung Te (kte@prefeitura.sp.gov.br)

Lucas S. Santos (lucass@prefeitura.sp.gov.br)

Caio Begotti (cbegotti@prefeitura.sp.gov.br)

Francisco Silva (ediltonsilva@prefeitura.sp.gov.br)

Eduardo Lisboa (elisboa@prefeitura.sp.gov.br)

Luiz F. Capitulino (lcapitulino@terra.com.br)

O Sacix (Tamanduá) é um sistema cliente-servidor, baseado em GNU/Linux 100% Livre, utilizando terminais sem disco rígido. O Servidor é o computador responsável por rodar os programas e disponibilizá-los para um conjunto de terminais (clientes).

Após configurados, os terminais poderão ter acesso à Internet, aos dispositivos locais de disquete e som, além de ter à disposição centenas de programas para as mais diversas tarefas: pacotes de escritório,

navegadores, programas de desenho, ferramentas de programação, jogos etc.

1.3 Onde Obter

Para obter o Sacix (Tamanduá) basta acessar o endereço abaixo:

<http://sl.prefeitura.sp.gov.br/download/sacix/tamandua/>

1.4 Características

- Kernel 2.6.7
- Gnome 2.6, OpenOffice.org 1.1.2 e Mozilla 1.7.2
- Plugins de Java, Flash, Filmes e outros
- Suporte a RAID, LVM na instalação
- Hardware dos clientes são auto-detectados (hotplug, discovery)
- Suporte a disquete remoto (sftp)
- A Mini-Distro pode rodar via NFS ou em RAM
- Personalização nas configurações de usuários via Gconf
- Suporte a som remoto

1.5 Problemas conhecidos

- Disquete não está desmontando automaticamente. Foi utilizado um script que desmonta o disquete a cada 1 segundo.
- TFTP demora para responder. Prioridades ajudam, mas não resolvem.
- Mensagem de erro do XKB após a autenticação do usuário no ambiente gráfico. O módulo do XKB foi desabilitado na configuração do servidor gráfico.

1.6 Para Fazer

Esta é a nossa lista de tarefas, pretensões e coisas ainda pendentes, ou seja, nossa lista de objetivos para as próximas versões do servidor.

- Otimizações de sistema:
 - Wrapper para inicialização mais rápida de determinados programas
 - Compilação de programas buscando otimizações próprias
 - Prelink, se aplicável, em poucos programas (OpenOffice.org, por exemplo)
 - Seleção de bibliotecas (restringir carregamento de bibliotecas diversas)
 - Balanceamento de CPU e recursos para garantir justiça na divisão entre os usuários (fairscheduler ou algo semelhante que seja aplicável)
- Ferramenta para atualização automática da imagem em ramdisk
- Suporte USB nos clientes (para uso de pen drive, câmeras digitais e outros dispositivos)
- Acessibilidade e melhor usabilidade do ambiente gráfico
- Ferramenta de administração (scripting e front-end gráfico)
- Jogos e programas educativos para reduzir uso de Flash e Java.

1.7 Autores

Este documento foi escrito por um grande número de pessoas, referenciadas na última listagem de autores e é atualmente mantido pela equipe de desenvolvimento GNU/Linux do Governo Eletrônico de SP, mencionada na seção 1.2 deste texto. A última versão deste documento, depreciada em relação a esta, foi mantida por:

Frederico Câmara (fcamara@prefeitura.sp.gov.br)

Luiz Fernando N. Capitulino (lcapitulino@prefeitura.sp.gov.br)

Outras pessoas também trabalharam no arquivo original (versão antiga) deste documento e contribuíram de formas diversas, com testes e reportes de erros:

Adriana Tosta

Aparecido Quesada

Simone Leal dos Santos

Thyago Akira de Moraes Ribeiro

Yuri Robinsom de Souza

Márcio Leonardi

Frederico Câmara

A Coordenadoria do Governo Eletrônico de São Paulo é composta por:

Coordenação Geral:

Beatriz Tibiriçá (beatrizt@prefeitura.sp.gov.br)

Comunicação/Imprensa:

Jorge Cordeiro (jhcordeiro@prefeitura.sp.gov.br)

Marden David Barbosa (mdavid@prefeitura.sp.gov.br)

Software Livre:

Frederico Câmara (fcamara@prefeitura.sp.gov.br)

Administração:

Wilken Sanches (wdsanches@prefeitura.sp.gov.br)

Rogéria Massula (rsouza@prefeitura.sp.gov.br)

Mila Azevedo (milaazevedo@prefeitura.sp.gov.br)

Implantação dos Telecentros:

Kiminoshim Yoshida (yoshidak@prefeitura.sp.gov.br)

Michelle Gancz (mgancz@prefeitura.sp.gov.br)

O projeto e-cidadania não seria possível sem a participação de muitas outras pessoas, em especial as listadas abaixo, que contribuíram para o nascimento do projeto:

Sérgio Amadeu da Silveira

Ricardo Bimbo

Luiz F. N. Capitulino

Alex Camacho Castilho

Para mais informações visite a página do projeto na Internet, em <http://www.telecentros.sp.gov.br>

1.8 Direitos Autorais

Direitos Autorais - Copyright © 2003, 2004 Governo Eletrônico da Prefeitura de São Paulo.

Este trabalho está sob a licença Creative Commons Attribution-ShareAlike License. Para ver uma cópia desta licença, visite <http://creativecommons.org/licenses/by-sa/2.0/> ou envie uma carta para Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

2. Visão Geral

Este capítulo oferece uma visão geral do objetivo a ser atingido e dos programas necessários para a implementação do sistema.

2.1 Objetivo

O objetivo desse documento é auxiliar o leitor na instalação de um servidor semelhante ao dos Telecentros (da Prefeitura de São Paulo) através do instalador Sacix - versão Tamanduá. Esse sistema é um sistema baseado no modelo cliente-servidor em GNU/Linux, que utiliza terminais sem disco rígido.

Após a instalação e configuração, os terminais poderão ter acesso à Internet, aos dispositivos locais de disquete e som, além de ter a sua disposição centenas de programas para as mais diversas tarefas: pacotes de escritório, navegadores, programas de desenho, ferramentas de programação, jogos etc.

2.2 Distribuição

A distribuição utilizada inicialmente no projeto E-cidadania é o Debian GNU/Linux estável, com o Gnome 2.0. O Debian é uma distribuição GNU/Linux em que os pacotes tem um ciclo de produção instável -> teste -> estável. Como o ciclo de produção de uma nova versão de um pacote pode durar muito tempo, um pacote Debian estável pode ser muito antigo.

A grande questão na utilização do Debian é “Como utilizar versões atuais dos pacotes sem comprometer a estabilidade?”. Nós resolvemos essa questão criando uma ramificação própria do projeto Debian. Para isso, simplesmente selecionamos pacotes do estável, do instável e do teste, construímos o servidor e fazemos testes por vários dias. Quando não há problemas, ele se torna nossa versão estável. O resultado é a instalação do Debian estável com alguns pacotes do instável.

Este documento vai detalhar esse processo. Mas iremos, na medida do possível, tornar a explicação independente de distribuição. Dessa maneira o leitor é livre para escolher qualquer outra distribuição, além de qualquer gerenciador de janelas, e adaptar quando julgar necessário.

2.3 Programas Utilizados

NECESSÁRIOS

Aplicação	Programa	Pacotes Debian
Distribuição GNU/Linux	Debian http://www.debian.org	----
Mini Distribuição	Mini-Distro	----
Servidor DHCP	ISC 3 DHCP Server http://www.isc.org./products/DHCP	dhcp3-server
Servidor TFTP	Pacote Netkit http://www.hcs.harvard.edu/dholland/computers/netkit.html	atftpd
Servidor NFS	The LINUX Kernel-Space NFS Server	nfs-kernel-server
Servidor gráfico	Xfree86 http://www.xfree86.org	vários

RECOMENDADOS

Aplicação	Programa	Pacote Debian
Proxy	Squid http://www.squid-cache.org	squid
Servidor Web	Apache http://www.apache.org	apache

OPCIONAIS

Aplicação	Programa	Pacote Debian
Banco de dados	MySQL http://www.mysql.com	mysql-server
Linguagem Web	PHP http://www.php.net	php4
Ferramenta SQL	PHPMYAdmin http://www.phpmyadmin.net	phpmyadmin
Gerenciamento	Gerenciamento http://sl.prefeitura.sp.gov.br/download/	----

2.4 Conhecimento Mínimo Necessário

É possível que uma pessoa com conhecimentos mínimos em GNU/Linux e redes tenha sucesso na configuração do Telecentro Livre. Para isso, basta seguir os passos deste manual. Em qualquer caso, quanto maior o conhecimento, maior será a facilidade do leitor na configuração.

2.5 Teoria

A teoria do funcionamento do Sacix (Tamanduá) teve como base a teoria apresentada originalmente pelo projeto LTSP (Linux Terminal Server Project). Como descrito em sua documentação, o LTSP é um projeto para a utilização de terminais de baixo custo, como terminais de texto ou gráficos de um servidor GNU/Linux.

A teoria de funcionamento é, em sua essência, comum aos vários projetos de terminais em GNU/Linux, como o PXES e o Xterminal. O que varia é a implementação e escopo de cada projeto. O Telecentro Livre teve influência do LTSP, do qual incorpora alguns scripts modificados, além de idéias e contribuições de outras pessoas ao redor do mundo.

2.6 Processo de Inicialização do Terminal

A melhor maneira de entender a teoria é acompanhar o processo de inicialização do terminal. Este processo é apresentado a seguir:

- Ao ligar o cliente, ele passa pelo processo de auto-teste (Power On Self Test - POST).
- Durante o auto-teste, a BIOS procura por ROMs de expansão e encontra a placa de rede.
- Terminado o POST, a execução passa para o código PXE em ROM que detecta a placa de rede e envia um broadcast com a tag PXEClient. O broadcast é um pedido enviado para a rede, respondido pelos serviços que a monitoram, de acordo com a tag.
- O serviço DHCP do servidor identifica a tag e responde, de acordo com a configuração do MAC address, informando como a placa de rede deve se configurar e o nome do arquivo (Network Bootstrap Program) que deve ser carregado através do protocolo TFTP (Trivial File Transfer Protocol).
- O Network Bootstrap Program, baseado no syslinux, carrega o kernel e executa o initrd, onde detecta a placa de rede do terminal e envia outra requisição para o DHCP.
- O script do initrd verifica parâmetro de inicialização (`use_ramdisk_image`), que indica como a raiz do sistema deve ser montado, em RAMDISK ou NFS.
- Se o parâmetro indicar para NFS, o kernel monta a raiz do sistema por NFS (Network File System), ou seja, a raiz do terminal é exportado pela rede a partir do servidor. A exportação é feita no modo somente-leitura.
- Caso contrário, o servidor envia uma imagem da Mini-Distro através do TFTP. Ela monta a raiz do sistema na própria RAMDISK do cliente e os diretórios `usr` e `lib` são montados por NFS.
- O terminal agora executa o INIT, que continua o processo de inicialização, de acordo com as configurações em `/etc/inittab`.

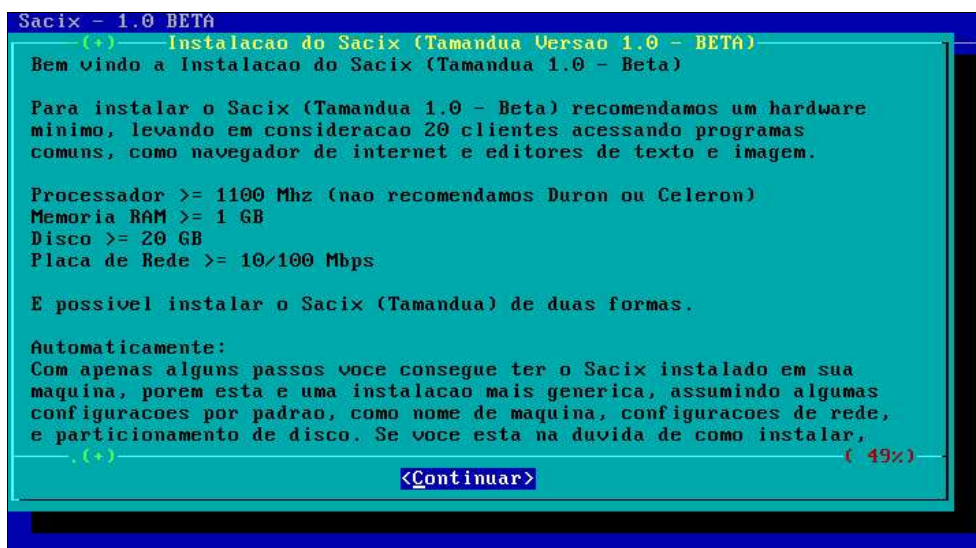
- O script principal, `/etc/rc.sysinit`, é executado pelo INIT. Esse script cria um disco em memória RAM (RAMDISC), o qual é montado para leitura e gravação em `/tmp`. Alguns arquivos do terminal são links simbólicos apontando para este diretório. Desta forma, o diretório `/tmp` é o único que pode ser alterado no sistema de arquivos do terminal.
- `/etc/rc.sysinit` monta o sistema de arquivos virtual `/proc` e cria vários diretórios e arquivos de configuração, preenchendo os links simbólicos. (`/tmp/compiled`, `/tmp/var`, `/tmp/var/run`, `/tmp/var/log`, `/tmp/var/lock`, `/tmp/var/lock/subsys`)
- `/etc/rc.sysinit` chama outro script para configurar o sistema de janela X.
- `/etc/rc.local` finalmente chama o script `start_ws` que inicia o servidor X no terminal.
- O servidor X no terminal faz uma requisição XDMCP para o gerenciador de vídeo no Servidor da rede (login).
- Neste momento, quando o usuário logar, ele vai estar no servidor.

3. Instalação do Sacix (Tamanduá)

Para instalar o Sacix (Tamanduá) é necessário ter a mídia do servidor no drive e configurar o computador para inicializar pelo CD-rom. Assim que o CD-rom inicializar, pressione <Enter> ou <F2> para mais opções. Com o CD você tem 4 opções:

- Aperte <Enter> e ele inicializará com o kernel ide.i
- Escolher o kernel scsi.i (é só escrever scsi.i), caso necessite de suporte SCSI
- Escolha um dos kernels e passe parâmetros. Exemplo: ide.i root=/dev/hdax init=/sbin/init
- Iniciar com o kernel padrão e usá-lo para reparar alguma instalação anterior

Assim que o CD inicializar, o instalador aparecerá:



```
Sacix - 1.0 BETA
(+)----- Instalacao do Sacix (Tamandua Versao 1.0 - BETA)
 Bem vindo a Instalacao do Sacix (Tamandua 1.0 - Beta)

 Para instalar o Sacix (Tamandua 1.0 - Beta) recomendamos um hardware
 minimo, levando em consideracao 20 clientes acessando programas
 comuns, como navegador de internet e editores de texto e imagem.

 Processador >= 1100 Mhz (nao recomendamos Duron ou Celeron)
 Memoria RAM >= 1 GB
 Disco >= 20 GB
 Placa de Rede >= 10/100 Mbps

 E possivel instalar o Sacix (Tamandua) de duas formas.

 Automaticamente:
 Com apenas alguns passos voce consegue ter o Sacix instalado em sua
 maquina, porem esta e uma instalacao mais generica, assumindo algumas
 configuracoes por padrao, como nome de maquina, configuracoes de rede,
 e particionamento de disco. Se voce esta na duvida de como instalar,
 .(+)----- ( 49% )
 <Continuar>
```

Considerando que o servidor suportará 20 clientes acessando programas comuns, como navegador da Internet e editores de texto e imagem, recomendamos a seguinte configuração mínima para a instalação do Sacix (Tamanduá 1.0):

- Pelo menos 1GB de memória RAM
- Disco com capacidade de pelo menos 20 GB
- Placa de Rede de 10/100 mbps
- Processador com clock igual ou maior 1100mhz (Obs*: Não recomendamos processadores **Duron** ou **Celeron**)

3.1 Características do Instalador

3.1.1 Instalação Automática:

Com apenas alguns passos é possível ter o Sacix instalado em sua máquina, porém esta é uma instalação mais genérica, assumindo algumas configurações por padrão, como nome de máquina, configurações de rede, e particionamento de disco. Caso tenha dúvidas de como instalar, escolha esta opção.

3.1.2 Instalação Passo-a-Passo:

Para pessoas que possuem um grande conhecimento do sistema GNU/Linux e como instalar o GNU/Linux, permite uma maior flexibilidade no particionamento do disco (cfdisk/fdisk), criação de RAID e LVM, escolha de nome da máquina, configurações de rede, lilo etc.

3.1.3 Registro de Atividades (logs):

Caso estiver tendo problemas durante a instalação, todas as saídas padrões dos programas estarão sendo direcionadas para /dev/tty4, e as mensagens de erro estão sendo enviadas para /dev/tty5. Você pode acessá-las usando <Alt>+<F4> e <Alt>+<F5>.

3.1.4 Acesso a shells:

Se houver necessidade de usar um console (bash), o /dev/tty2 e /dev/tty3 estarão habilitados (<Alt>+<F2> ou <Alt>+<F3>). Lembre-se que neste modo você estará por sua conta e risco.

3.2 Instalação Automática

A instalação automática pedirá uma confirmação antes de prosseguir.

ATENÇÃO: TODOS OS SEUS DADOS DO PRIMEIRO DISCO ENCONTRADO SERÃO APAGADOS.

A instalação automática procura o primeiro Disco do computador e faz um particionamento básico (caso o seu disco possua menos de 10GB a instalação será abortada):

- Partição SWAP com 200 MB
- Partição REISER com a raiz (/)

Caso a sua partição (antes da instalação) faça parte de um RAID, será necessário reiniciar o computador. Com o disco particionado, a partição SWAP é ativada e é criado o sistema de arquivos na partição principal, que dependendo do tamanho do seu disco pode demorar alguns minutos. A partição é montada após a criação do sistema de arquivos.

O instalador irá procurar pelo seu CD-rom. Caso não ache CD-rom no seu computador será pedido para entrar manualmente com o dispositivo do CD-rom (exemplo: /dev/sda). O instalador só procura por CD-rom IDE. Caso o CD-rom e a partição raiz tenham sido montados com sucesso, a imagem do Sacix(Tamanduá) será transferida para o computador (pode demorar um tempo, dependendo do seu computador).

Então será configurada algumas permissões, transferida a imagem do kernel escolhido na inicialização. Será configurado também o setor de inicialização para inicializar pelo Sacix.

Escolha a senha do root (Administrador do sistema) e está finalizada a instalação. O sistema irá desmontar todas as partições que foram montadas durante a instalação e reiniciar o servidor.

3.3 Instalação Passo-a-Passo

PARTICIONAR: Dentro desta opção é possível selecionar entre `fdisk` e `fdisk` para particionar seus discos. Se for utilizado LVM ou RAID, não esqueça de criar as partições do tipo `raid (fd)` ou `lvm (8e)`. Caso exista alguma partição que já fizesse parte de um RAID é necessário parar o RAID. Para isso, entre no menu RAID, escolha "Remover", selecione o RAID desejado e remova. Volte para o menu e comece novamente.

RAID: Dentro desta opção você pode gerar seus raids, nível 0, 1, 5 e 6. Existe uma documentação (caso você prefira criar o RAID manualmente) de ajuda dentro da opção. Só use se souber o que está fazendo. Muito cuidado ao escolher partições marcadas como RAID.

LVM: Dentro desta opção você pode instalar o sistema usando LVM. Com o `lvm` é possível redimensionar os volumes, acrescentar novos discos e utilizar vários discos como um único volume, facilitando a administração dos discos.

DESTINO: Nesta opção você deve definir qual será sua raiz, o ponto de montagem das suas partições e o sistema de arquivo que irá utilizar. Serão detectados RAID ou LVM, caso você esteja usando-os. Depois de selecionado as partições, o sistema de arquivo e o ponto de montagem, estes são montados para que o próximo passo possa instalar o sistema. Muito cuidado ao escolher partições marcadas como ocupadas.

INSTALAR: Procure pelo CD-rom com as imagens, que ficam dentro do diretório `/telecentro`, e comece a instalação do sistema. Caso não ache CD-rom no seu computador, será pedido para entrar manualmente com o dispositivo do CD-rom (ex. `/dev/sda`).

CONFIGURAR: Será perguntado o nome do computador e em seguida se o sistema possui acesso a Internet. Após a configuração da Internet será configurada a rede local. Caso possua apenas uma placa de rede coloque `eth0` para a Internet e `eth0:0` para a rede local. Nesse passo ele irá gerar todos os arquivos de configuração com as informações que foram passadas. Após as configurações de rede será alterada a senha do root. Logo em seguida, deve-se escolher um kernel: IDE ou SCSI. Recomendamos que escolha SCSI apenas se tiver um dispositivo SCSI. Para encerrar a configuração vamos ao lilo, você pode usar o padrão, que é mostrado na tela, ou alterá-lo para atender melhor as suas necessidades. Caso a sua Internet seja GIRO ou PPPOE, ela não será habilitada na inicialização.

FINALIZAR: Automaticamente são desmontadas as partições, é desativada a `lvm` (se necessário), é sincronizado o sistema. Terminado, o sistema sai do instalador. Depois deste ponto aparecerá uma mensagem para apertar `<Ctrl>+<Alt>+`.

4. Configuração do Cliente

4.1 Kernel do cliente

A ser escrito.

4.2 Mini-Distro

4.2.1 Inicialização da Mini-Distro

Na versão Tamanduá do servidor Sacix existem duas Mini-Distros possíveis de se utilizar: uma que roda a raiz do sistema em RAM e a outra que roda a raiz via NFS. Por padrão usamos via NFS, pois para se usar a raiz em RAM recomendamos que o terminal tenha no mínimo 64MB de memória RAM.

Para selecionar em qual Mini-Distro o cliente vai iniciar, é necessário editar e mudar um parâmetro em: `/opt/tc_livre/boot/2.6-pxe/pxelinux.cfg/default`

Este arquivo deve estar da seguinte forma (note que a barra invertida indica continuação da linha, não uma quebra de linha):

```
prompt=0
label linux
    kernel bzImage-2.6.7
    append init=/linuxrc rw root=/dev/ram0 initrd=initrd-2.6.7.gz \
    ramdisk_size=20480 use_ram_image=no
```

Neste caso, as opções significam:

kernel

Indica qual o nome da imagem do kernel a ser utilizada. Esta imagem fica no diretório: `/opt/tc_livre/boot/2.6-pxe`.

init

Indica qual programa deve ser chamado após o kernel.

rw

Indica que a raiz do sistema deve ser montada com modo de leitura e escrita.

root

Indica a raiz do sistema.

initrd

A raiz deve ser carregada antes de montá-la. Ela é sempre executada em RAM.

ramdisk_size

Espaço em bytes que deve ser alocado para o initrd.

use_ram_image

Indica se deve ser usado a Mini-Distro com a raiz em RAM (yes), ou NFS (no).

Para maiores detalhes de configuração deste arquivo, consulte o arquivo de documentação chamado README.pxe, no diretório /opt/tc_livre/boot/2.6-pxe.

4.2.2 Modificação da Mini-Distro em NFS

A ser escrito.

4.2.3 Modificação da Mini-Distro em RAM

Durante o desenvolvimento do Sacix (Tamanduá), surgiu a necessidade de desenvolvermos uma base da Mini-Distro que é armazenada na memória RAM dos clientes durante a execução. A base desta Mini-Distro está no diretório /home do usuário admin (/home/admin/micro-distro/mini-distro/ram/ram-img). A maioria dos binários que estão nesta base foram copiados dos servidor e alguns foram herdados do LTSP. Como todo binário que é compilado para usar bibliotecas dinâmicas precisa delas para ser executado, as bibliotecas também foram copiadas. Para descobirmos quais bibliotecas precisavam ser copiadas, foi usado o comando ldd, que mostra quais bibliotecas o programa usa. Sendo assim, toda vez que for preciso adicionar algum programa dentro desta base é necessário que suas bibliotecas sejam copiadas, se estas ainda não estiverem na base da Mini-Distro.

Esta forma de manter a Mini-Distro em RAM é um tanto complicada, por isso ainda estamos estudando uma forma de melhorar este desenvolvimento.

Depois de alterada a base da Mini-Distro é necessário criar uma imagem (iso compactada), que será lida com o cloop. O cloop é um módulo do kernel bastante utilizado por distribuições live-cd (para saber mais sobre o cloop na Mini-Distro, veja a documentação do kernel da Mini-Distro). Esta imagem também precisa ser colocado no local certo para que o terminal copie-a para sua memória durante sua inicialização.

Para criar a imagem, no formato cloop, foi criado um script (cria.sh), que está em /home/admin/micro-distro/mini-distro/ram. Este script pede uma senha para ser executado, esta senha é a mesma do usuário root. Depois de digitar a senha corretamente, o script chama o binário create_compressed_fs, que está no mesmo diretório, e cria dois novos arquivos (ram.img e ram.img.md5):

ram.img

É a imagem da Mini-Distro em RAM. Este arquivo deve ser copiado para:
/opt/tc_livre/boot/ram.img.

ram.img.md5C

Contém a verificação (md5sum) da integridade do arquivo ram.img. Este arquivo deve ser copiado para /opt/tc_livre/boot/ram.img.md5.

4.3 Initrtd do cliente

O arquivo `initrtd-2.6.7.gz`, que está no diretório `/opt/tc_livre/boot/2.6-pxe/`, é uma das partes mais importantes da inicialização do terminal. Todos os binários que estão em `/bin` e `/sbin` são links simbólicos para o `busybox`, e a biblioteca usada para compilar estes programas foi a `uClibc-0.9.26`. Dentro deste arquivo existe um `linuxrc` que faz a detecção da placa de rede (PCI), a requisição DHCP e verifica se a Mini-Distro vai ser via RAM ou NFS.

4.4 XFree86 da Mini-Distro

A Mini-Distro atual tenta detectar o seus hardware, incluindo placa de vídeo. Para atingirmos este nível de automatismo, nós precisamos integrar uma série de ferramentas, como `discover`, `kudzu`, `scan_pci` (veio do LTSP) e `hotplug`. Ainda não é possível detectar mouse e teclado.

O processo de criação do arquivo de configuração do arquivo `/etc/X11/XF86Config-4` começa logo após o término do `rc.sysinit` (`rc.sysinit` é o principal script de inicialização. Veja o `/etc/inittab` para maiores detalhes). Então ao invés do sistema chamar o processo de login em um terminal é chamado o script `screen_session`.

Em `screen_session` é verificado qual script de `/etc/screen.d/` deve ser executado (`rdesktop`, `shell`, `startx`, `telnet`). O padrão é `"startx"`. Dentro de `"startx"` o `discover` é chamado para detectar qual o driver de vídeo deve ser usado para a placa de vídeo do terminal. Este driver com mais alguns argumentos é passado para o script `/etc/build_x4_cfg`, e este é responsável por montar o arquivo de configuração `/etc/X11/XF86Config-4`. De dentro do `/etc/build_x4_cfg` é usado o comando `ddcxinfo`, do pacote `kudzu`, para detectar a frequência do monitor.

Depois que o `/etc/build_x4_cfg` criar o `/etc/X11/XF86Config-4`, o controle volta para o `"startx"`, que então chama o binário do X11 (`/usr/X11R6/bin/X`), com alguns parâmetros, para então iniciar uma sessão do ambiente gráfico. A partir deste ponto o controle é do GDM (gerenciador gráfico de login), que está rodando no servidor.

5. Configuração do servidor

5.1 Initrd

A ser escrito.

5.2 DHCP

O DHCP (Dynamic Host Configuration Protocol) é um protocolo utilizado para configurar o ambiente de rede das máquinas, de forma remota. O servidor DHCP, no Sacix, é responsável por determinar a configuração TCP/IP dos terminais, bem como quais os arquivos que devem ser transferidos por TFTP. O servidor DHCP está configurado por padrão para usar a rede 192.168.0.0/255.255.255.0 e aceitar qualquer máquina da rede, sem restrições de MAC address.

Dois parâmetros especiais são passados ao terminal durante a inicialização: root-path e filename.

A linha root-path, seguido do caminho padrão 192.168.0.1:/opt/tc_livre/root, informa ao terminal onde montar a raiz do sistema, via NFS, durante a inicialização.

O parâmetro filename diz qual será o kernel oferecido. O padrão da versão 1.0 do Sacix é o 2.6.7.

O sistema de inicialização utilizado é o syslinux.

5.3 TFTP

O TFTP (Trivial File Transfer Protocol) é um protocolo simples, baseado no FTP (File Transfer Protocol), para transferência de arquivos. Ele é geralmente usado para transferir arquivos de inicialização para terminais sem disco. Utilizamos um servidor TFTP para enviar o kernel ou uma imagem de inicialização para os terminais. Sua configuração é feita na linha "tftp" do arquivo de configuração /etc/inetd.conf.

O servidor TFTP instalado no Sacix é o atftpd, versão 0.6.3. Este servidor atua através do inetd para oferecer o kernel ao terminal.

5.4 NFS

O NFS (Network File System) é uma aplicação cliente/servidor utilizada para exportar diretórios através da rede. No Sacix, utilizamos o NFS para disponibilizar ao terminal uma área do disco do servidor como sistema de arquivos. Esta área está configurada como somente-leitura e contém a Mini-Distro. No Sacix, utilizamos o servidor NFS no espaço do kernel.

5.5 SSH

O servidor SSH está configurado para não aceitar login do usuário root. Para se tornar root, deve-se entrar como o usuário admin (senha padrão: admin) e usar o comando su. A senha padrão do usuário root é sacix. No terminal também há um servidor SSH. Ele é responsável por permitir o acesso ao leitor de disquetes do mesmo, bem como qualquer outra mídia, removível ou não, que se queira configurar.

5.6 Proxy

O Proxy de Internet é um serviço que armazena páginas, figuras e outros dados baixados da Internet, de forma que uma mesma página, por exemplo, não precise ser baixada da Internet toda vez que um usuário estiver visitando-a, somente quando modificada. No Sacix utilizamos o Squid como proxy de Internet. Outras vantagens de se utilizar um proxy no Sacix (Tamanduá) são: restringir o acesso a sites determinados e centralização das configurações da Internet. Por exemplo, a sua conexão com a Internet pode ser trocada entre conexão direta, através de um outro proxy ou através de outra interface de rede, bastando alterar as configurações do proxy, em vez da configuração de cada navegador. O servidor proxy está configurado para aceitar conexões em sua porta padrão (3128). Uma ACL (Access Control List - Lista de Controle de Acesso) bloqueando sites está configurada. O arquivo com os sites bloqueados é o `/etc/squid/porn`.

5.7 Web/BD

Existe a possibilidade de se utilizar um Servidor Web no Sacix. Isso ajuda nas oficinas de criação de site, disponibilizando páginas web. Também pode ser utilizado durante a clonagem de servidores, disponibilizando as imagens dos HDs. O servidor Apache está disponível para uso, e por padrão está com o Programa de Gerenciamento Off-line de Usuários ativado, em: `http://127.0.0.1/gerenciamento`. O usuário padrão para login é gerencia, cuja senha de acesso é gerencia.

O MySQL é um servidor de Banco de Dados SQL. Nos Telecentros pode ser utilizado para ensinar noções de banco de dados e programação voltada a bancos de dados. Ele também é utilizado pelo Programa de Gerenciamento de Usuários. A base de dados padrão se chama gerenciamento.

5.8 Rede

O Sacix (Tamanduá) é baseado no projeto Sacix dos Telecentros da Cidade de São Paulo, que é dimensionado para funcionar com um servidor e vinte clientes. Duas topologias de rede são possíveis: uma envolvendo apenas uma placa de rede, e outra envolvendo duas placas de rede no servidor. As duas topologias são apresentadas a seguir:

5.8.1 Topologia com uma placa de rede

A placa de rede do servidor trabalha com dois endereços IPs, um em eth0 e outro em eth0:0, que é um alias (apelido) para a mesma placa de rede. O acesso à Internet é feito por um IP (válido na Internet) e os terminais se comunicam num endereço de rede local (intranet). O servidor, os terminais e o dispositivo de acesso à Internet são todos ligados a um switch:

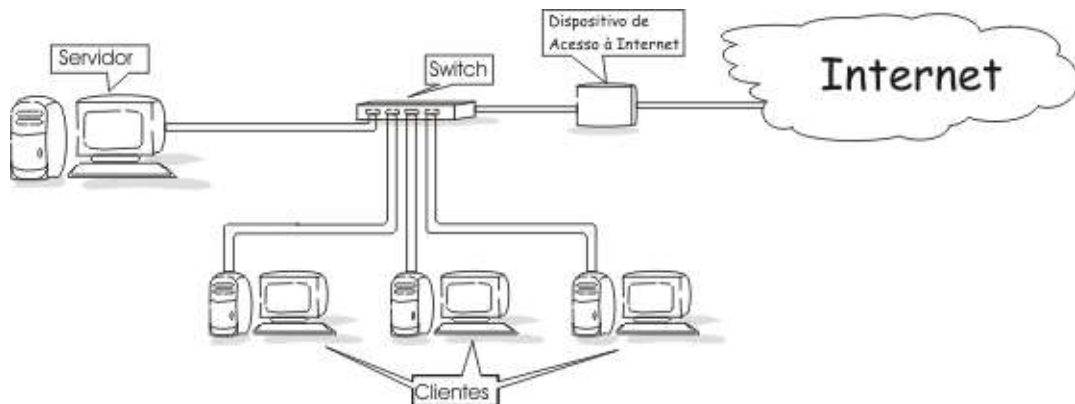


Ilustração Silvio Viana

5.8.2 Topologia com duas placas de rede

Uma placa de rede é configurada para acesso exclusivo à Internet com o IP válido, e a outra é configurada para acessar a rede local. A primeira é ligada ao dispositivo de acesso à Internet a segunda é ligada ao switch, junto com todos os clientes:

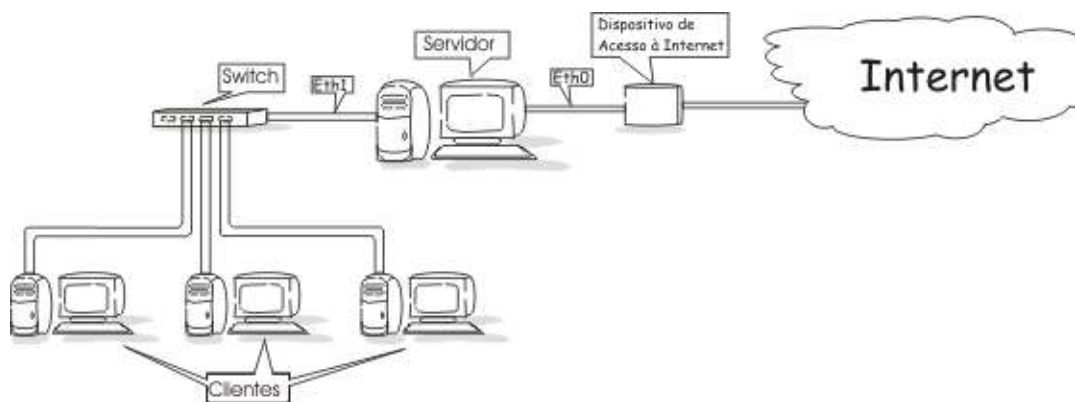
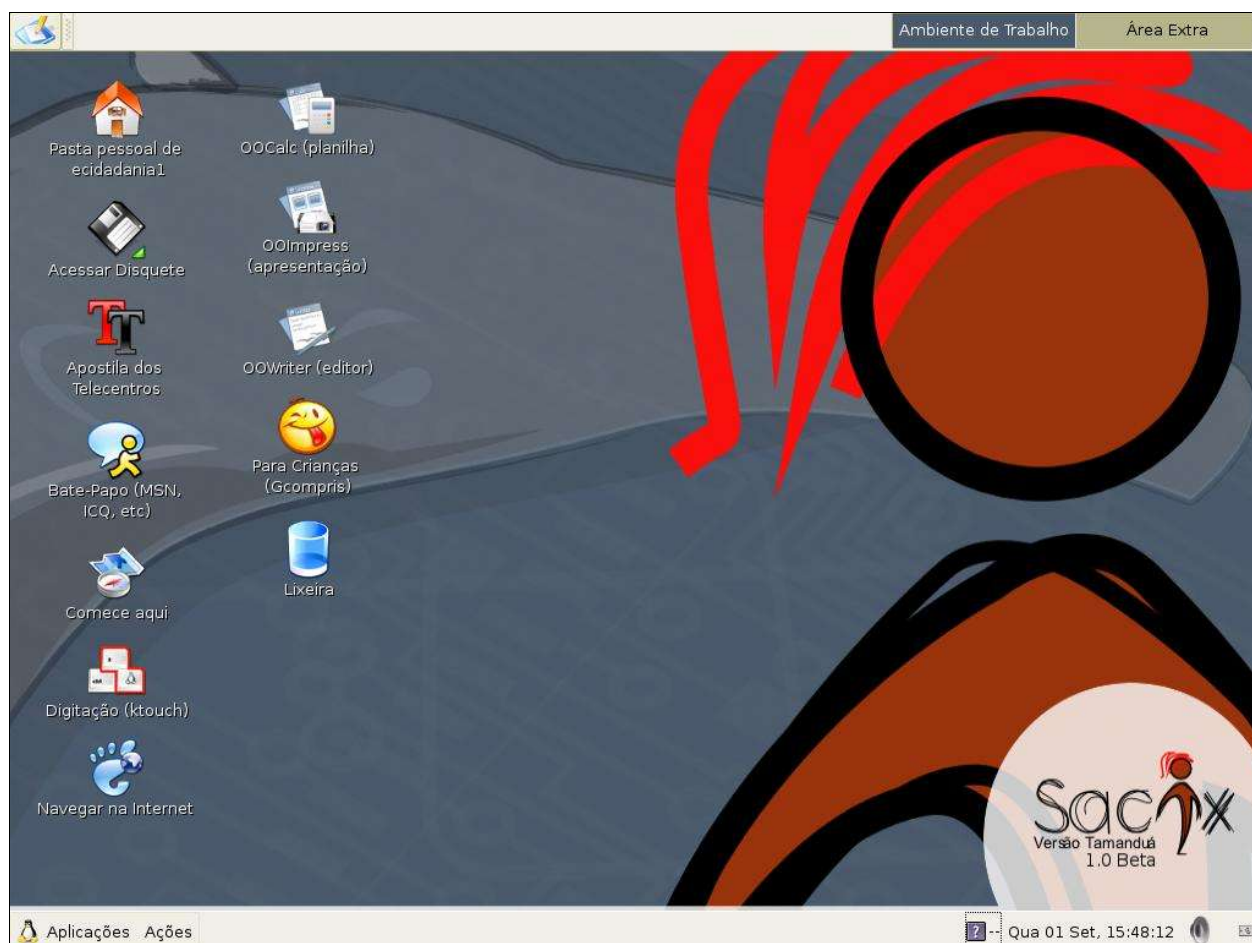


Ilustração Silvio Viana

6. Configurações de Usuário

Todas as configurações de programas e scripts de usuário desta nova versão do servidor Sacix Tamanduá se baseiam na idéia de que o diretório pessoal de cada usuário deve estar vazio, ou no mínimo reduzido ao limite, e que todas as configurações possíveis devem ser globais e padrão. Sendo assim, foi criado um pacote .deb simples (instalável em qualquer distribuição compatível com o Debian) que ajuda nessa tarefa.



6.1 Guia rápido de personalização

Abaixo estão listados alguns arquivos importantes deste pacote e que provavelmente serão alvo freqüente de modificações, caso você precise personalizar o sistema (instruções de como montar seu próprio pacote com as modificações serão explicadas posteriormente).

Pelo modo de autenticação (login) dos usuários ter de ser gráfico, foi adotado o GDM como gerenciador padrão de login e algumas modificações foram feitas no tema padrão:

- `/usr/share/gdm/themes/telecentro/wallpaper.png`
Papel-de-parede usado no login
- `/usr/share/gdm/themes/telecentro/telecentro.xml`
Arquivo XML (editável) simples com configurações do tema
- `/usr/share/gdm/themes/telecentro/GdmGreeterTheme.desktop`
Arquivo que indica os dois primeiros e forma o tema

Quando o usuário consegue entrar no sistema, é iniciado o ambiente de trabalho do mesmo. Uma tela de apresentação é exibida e então um fundo de tela amigável que identifica a versão do servidor é configurado (note que existe referências a esses caminhos de arquivos no arquivo XML do Gconf mais abaixo). Caso altere a splash ou o papel de parede, sobrescreva os arquivos mesmo ou use links simbólicos (mais inteligente):

- `/usr/share/images/desktop-base/telecentro_splash.png`
Tela de apresentação do Sacix Tamanduá
- `/usr/share/images/desktop-base/telecentro_wallpaper.png`
Papel-de-parede, um PNG semi-transparente

Existe um diretório de documentos do pacote `gnome-telecentro` que podem ser encontrados um changelog (registro de alterações) do pacote, uma lista de tarefas pendentes (TODO) e uns arquivos com créditos. Todos devem ser atualizados, caso você os edite, para manter a consistência do pacote. E também existe lá o arquivo:

- `/usr/share/doc/gnome-telecentro/apostila.pdf`
Apostila em PDF usada nos telecentros e acessível no desktop

Outros arquivos e diretórios importantes que identificam a solução são:

- `/usr/share/gnome-telecentro/gtkrc`
Tema de cores dos programas em GTK2
- `/usr/share/gnome-telecentro/bookmarks.html`
Conjunto padrão de marcadores usados nos telecentros
- `/usr/share/icons/telecentro/`
Diretório que contém os ícones Crystal, usados no GNOME

Caso seja necessário adicionar, remover ou editar algum item de ícone da área de trabalho do usuário, primeiro deve-se verificar o diretório abaixo:

- `/usr/share/gnome-telecentro/gnome-desktop/`
Todos os arquivos ".desktop" ficam aqui

Alguns outros arquivos no pacote possuem funções específicas que podem ser interessantes, dependendo do nível de personalização que se deseja conseguir:

- `/usr/share/gnome-telecentro/mimeTypes.rdf`
Tipos MIME de arquivos para o navegador lidar (streaming .pls, .psd etc)

- /usr/lib/mozilla/defaults/profile/US/user.js
Configurações do navegador de Internet Mozilla
- /usr/local/bin/tele_msg.sh
Script usado para exibir mensagens para o usuário
- /etc/X11/cursors/telecentro.theme
Tema de ícones usados como cursores do mouse
- /etc/gconf/telecentro_gconf_defaults.xml
Arquivo XML do GConf que engloba a maior parte das configurações do ambiente do usuário dentro do GNOME (possui capítulo próprio nesta documentação)
- /etc/gdm/PostLogin/Default
Script executado após cada login de usuário, antes do ambiente ser iniciado para o uso (é chamado pelo GDM, e muito importante, descrito ao longo da documentação)

6.2 Lidando com o Pacote Gnome-Telecentro

Como dito, todas as configurações de usuários e alguns ajustes de programas ficam armazenadas em um pacote .deb, padrão Debian, para facilitar a manutenção das mesmas. Caso exista a necessidade de personalização do pacote, deve-se usar as informações abaixo.

Para saber se o pacote está instalado corretamente, digite `dpkg -l | grep telecentro` (onde `dpkg` é o gerenciador de pacotes, `-l` pede a listagem dos pacotes e `grep telecentro` filtra a lista procurando pelo pacote usado nos telecentros).

Para ver o conteúdo do pacote já instalado, use o comando `dpkg -L gnome-telecentro`, mas note que a letra “L” agora é maiúscula, e listará o caminho de cada arquivo que existe no pacote, caso você precise localizar algum específico.

Você já o tem ele instalado, sabe onde está o arquivo que deseja modificar mas precisa abrir o pacote e reempacotá-lo. Primeiro, crie um diretório `gnome-telecentro` no `/tmp` e copie para lá o arquivo `gnome-telecentro_0.4-3_all.deb`, que deve ser a versão mais recente do mesmo, localizada no diretório do usuário `admin` em `/home/admin/outros/`. Para “explodir” o pacote, use o comando `ar -x nome-telecentro_0.4-3_all.deb`, e então descompacte o arquivo recém-criado `data.tar.gz`. Depois descompacte o outro recém-criado `control.tar.gz` em um diretório chamado `DEBIAN`, em maiúsculo mesmo.

Após isso, você deverá ter uma listagem parecida com esta:

```
/tmp/gnome-telecentro: ls
DEBIAN etc usr
```

e dentro do diretório `DEBIAN`:

```
/tmp/gnome-telecentro: ls DEBIAN/
control debian-binary md5sums postinst postrm prerm
```

Faça as modificações necessárias onde desejar ou for preciso. Para reempacotar o pacote basta voltar ao diretório pai, `/tmp`, e digitar `dpkg-deb -b gnome-telecentro nome_do_pacote.deb`. Mas é extremamente necessário lembrar que esse é o método mais rápido e sem detalhes de como lidar com um pacote .deb simples. Por favor, consulte alguns manuais sobre o assunto caso algo dê errado, pois essas instruções são básicas.

Se for necessário remover o pacote `gnome-telecentro`, use `apt-get --purge remove gnome-telecentro` em uma linha de comando (o comando equivalente do `dpkg` também pode ser usado, de qualquer forma).

Para instalar o pacote novamente, basta digitar na linha de comando a instrução `dpkg -i nome_do_pacote.deb`. Caso o pacote já esteja instalado e a versão do pacote reempacotado esteja

corretamente configurada para exigir uma atualização, o dpkg irá remover naturalmente a versão antiga instalada para configurar a sua nova no sistema.

Vale notar que no diretório DEBIAN acima estão alguns scripts usado pelo dpkg e pelo próprio pacote para ajustar algumas coisas no sistema. Os scripts podem ser alterados se necessário, mas deve-se ter cuidado com isso. Eles são: postinst, postrm e prepm.

6.3 Administração via GConf

O GConf é o sistema de configurações globais usado no ambiente desktop Gnome atual. Ele é capaz de centralizar todas as configurações e ajustes de programas que os usuários venham a usar. Ele possui um repositório de configurações XML, um serviço chamado gconfd-2 e uma ferramenta de configuração gconftool-2. Existe também uma segunda ferramenta, gráfica, chamada gconf-editor, que serve para editar os valores das chaves de configuração do GConf de uma forma mais amigável e rápida.

Com o GConf é possível especificar valores preferenciais para certos tipos de propriedades dos programas, especificar valores padrões (mas que podem ser sobrepostos pelos usuários em uma sessão do ambiente) e valores genéricos para cada usuário que podem ser alterados e salvos por eles. Abaixo, os diretórios onde ficam cada tipo de configuração dos programas, como mencionado acima:

`/etc/gconf/gconf.xml.defaults/` - Valores padrões, mas alteráveis pelos usuários.

`/etc/gconf/gconf.xml.mandatory/` - Valores obrigatórios e não-alteráveis por ninguém.

No diretório `/etc/gconf/` existe um arquivo chamado `telecentro_gconf_defaults.xml` que contém todas as configurações atuais do Sacix (Tamanduá) em formato XML, codificação UTF-8. Pode-se alterar o arquivo diretamente para especificar valores personalizados das configurações dos programas. No entanto, se for preciso fazer isso em vários programas e de forma detalhada, recomenda-se usar a ferramenta gráfica `gconf-editor` e depois exportar a árvore de arquivos gerada por ele para recriar outro `telecentro_gconf_defaults.xml`. Nos scripts de instalação e remoção já mencionados, existem chamadas que lidam com esse arquivo e podem ser úteis caso queira realizar testes. A seguir, uma lista com as principais ações das ferramentas mencionadas no começo da sessão, usadas para aplicar e remover o arquivo XML dito, e outras configurações no repositório do GConf, entre outras coisas:

gconfd-2

Serviço (daemon) responsável por intermediar as requisições feitas pelos programas do Gnome para que os mesmos usem conjuntos de configurações específicas. Ele é iniciado para cada usuário autenticado no ambiente e caso deseje-se alterar algo na base de configurações, deve-se primeiro interromper sua execução (veja o próximo item).

gconftool-2

Ferramenta que acompanha o pacote `gconfd-2` no caso do Debian. É a que deve ser usada para lidar com a base de configurações e com o próprio GConf, caso necessário. Algumas opções da mesma podem ser interessantes para a criação de scripts ou gerenciamento manual das configurações:

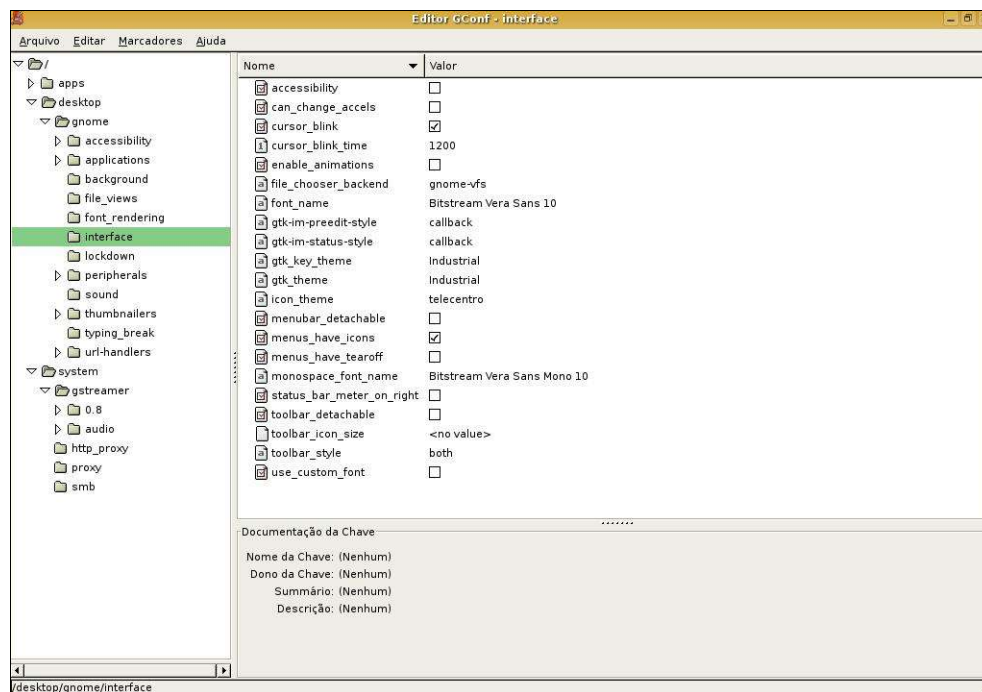
- `--dump` Serve para exportar toda uma árvore de configurações, útil para criar backups.
- `--load` Reverso da anterior, serve para carregar um arquivo de configurações em uma base.
- `--R` Lista recursivamente o conteúdo da árvore de configurações ou diretório específico.
- `--ping` Checa se o serviço `gconfd2` está sendo executado ou não; retorna 0 se positivo.
- `--shutdown` Interrompe a execução do `gconfd2`, apesar de não ser recomendável.

Para mais detalhes sobre cada opção e muitas outras, basta digitar `gconftool-2 --help` em uma linha de

comando. Caso possua um sistema localizado em português, as descrições serão mais compreensíveis.

gconf-editor

Programa gráfico para edição de cada chave e valor das configurações dos programas do Gnome. Caso seja feita alguma alteração de grande porte na árvore de configurações, recomenda-se usar este programa estando autenticado como um usuário comum, configurar todo o ambiente via gconf-editor e então usar o programa gconftool-2 para exportar a árvore de configurações. Tela do gconf-editor:



6.4 Ajustes específicos de programas

A ser escrito.

7. Configuração adicional

7.1 Disquete Remoto

É interessante notar que o disquete é montado e desmontado automaticamente, via automount, cujo suporte foi compilado no kernel do terminal. O tempo do automount foi configurado para 1 segundo. O método de acesso aos disquetes dos terminais usado anteriormente era o NBD. Devido à sua instabilidade e complexidade, foi adotado um novo método: o SFTP.

O SFTP consiste em servir, via SSH, um acesso FTP a partir do terminal para que o servidor, que é onde o usuário está autenticado e de onde são executadas as aplicações, possa acessar seus dispositivos de armazenamento, tais como disquetes, CD-roms, HDs, chaveiros USB e até câmeras fotográficas. Entretanto, a configuração padrão desta versão suporta apenas o acesso a disquetes.

Como funciona:

- A chave pública do usuário root do servidor é copiada, na instalação, para o arquivo chamado `/opt/tc_livre/root/etc/ssh/root-ak`
- Durante a inicialização do terminal, o arquivo é copiado para `/tmp/authorized_keys`
- O arquivo `/tmp/authorized_keys` contém as chaves públicas dos usuários autorizados a acessarem o serviço SSH, oferecido pelo terminal usando o login do usuário root do mesmo. Portanto, o arquivo `/root/.ssh/authorized_keys` do terminal é um atalho para o arquivo `/tmp/authorized_keys`, lembrando que estes caminhos são relativos à Mini-Distro, cuja raiz está em `/opt/tc_livre/root`, montada via NFS a partir do servidor.
- Ao ser autenticado o usuário no GDM, o script `/etc/gdm/PreSession/Default` é executado. Nele, a chave pública do usuário em questão é gerada e copiada, via ssh, para o terminal de onde o usuário se autenticou. Agora, o arquivo `authorized_keys` do terminal permitirá, além do usuário root do servidor, o usuário autenticado a acessar o serviço SSH no terminal.

Ao carregar a área de trabalho, o usuário tem a sua disposição um ícone para acessar o leitor de disquetes de seu terminal, sem precisar montar ou desmontar a unidade do mesmo. O acesso é feito via protocolo `sftp://`. Pode-se perceber que o acesso é virtualizado apenas para programas que usam a biblioteca GTK. Para programas que não a utilizam, como o OpenOffice, é necessário copiar o arquivo do disquete para o diretório pessoal do usuário. Este bug afeta apenas usuários do Nautilus. Caso seja usado o Konqueror, o mesmo não ocorrerá, permitindo o acesso virtualizado a todos os programas.

7.2 Programa de gerenciamento

Este programa em PHP pode ser utilizado para gerenciar o uso do Sacix (Tamanduá). Ele faz parte dos Programas Desenvolvidos pelo Governo Eletrônico e tem uma página própria sobre instalação e download em <http://softwarelivre.prefeitura.sp.gov.br/wiki/AdminUsuario>.

8. Segurança Básica

Segurança é um assunto complexo. O nível de segurança de um sistema depende do que esse sistema está armazenando ou protegendo. Este capítulo apresenta uma visão geral de alguns aspectos relacionados com a segurança do servidor. Para uma visão mais abrangente, recomendamos a leitura do Security-HOWTO do projeto LDP.

8.1 Senhas do LILO e BIOS

Para evitar modificações no BIOS do sistema, é aconselhável protegê-lo com senha. Isso pode variar de acordo com a placa mãe. Consulte o manual do seu computador.

No caso de estar usando o LILO, para prevenir que qualquer pessoa tente acessar o sistema com uma configuração que não seja a especificada no arquivo `lilo.conf` (exemplo `linux single`), é possível configurar o LILO para que ele solicite uma senha quando tal ação for feita. Edite o arquivo `/etc/lilo.conf` e adicione as linhas abaixo:

```
password=SENHA
restricted
```

Em que `SENHA` é a senha do lilo. Salve e saia do seu editor e depois proteja o arquivo `/etc/lilo.conf` e execute o LILO:

```
# chmod 700 /etc/lilo.conf
# lilo -v
```

8.2 Permissões

Os Telecentros da Prefeitura de São Paulo recebem um grande número de usuários. Para que os usuários tenham acesso apenas aos seus próprios arquivos, as permissões abaixo devem ser utilizadas.

```
# chmod 700 /root /boot
# chmod 730 /home
# chgrp users /home
```

Atenção, novos usuários devem ser acrescentados ao grupo `users`.

8.3 Alteração de Senha

Dependendo do objetivo do Sacix (Tamanduá) pode não ser uma boa política de segurança permitir que usuários normais alterem suas senhas.

Então, para que apenas o super-usuário use o programa `passwd`, retire o SUID `root` e altere a permissão:

```
# chmod -s /usr/bin/passwd
# chmod 700 /usr/bin/passwd
```

8.4 Limite de Processos

Existe a possibilidade de limitar o número de processos por usuário. Em ambientes como o do Sacix (Tamanduá), um usuário poderia, maliciosamente, escrever um programa que cria processos infinitamente. O resultado seria o travamento do servidor.

Uma maneira de limitar o número de processos por usuário é configurar o módulo PAM Limits. Edite o arquivo `/etc/security/limits.conf` e adicione a linha:

```
@users hard nproc 2047
```

Salve as alterações e proteja alguns arquivos da seguinte forma:

```
# chmod o-rwx /etc/security/access.conf /etc/security/group.conf \
/etc/security/limits.conf /etc/security/pam_env.conf /etc/security/time.conf
```

A configuração feita vai limitar a 2047 processos os membros do grupo `users`. Isso significa que os usuários do Sacix (Tamanduá) têm que estar no grupo `users`.

8.5 TCP Wrappers

O TCP wrappers é um pacote para controle de acesso. Nesta seção vamos descrever uma configuração mínima de seus dois arquivos: `/etc/hosts.allow` e `/etc/hosts.deny`, para mais informações consulte a página de manual:

```
$ man host_access
```

A configuração apresentada a seguir libera todos os serviços para conexões vindas de `127.0.0.1` (localhost), e libera os serviços TFTP, PORTMAP e GDM apenas para endereços IPs da rede `192.168.0.0`. Edite `/etc/hosts.allow` e adicione as linhas:

```
# Permite loopback
ALL: 127.0.0.1
```

Edite `/etc/hosts.deny` e adicione as linhas:

```
# Servidor TFTP
in.tftpd: ALL EXCEPT 192.168.0.
```

```
# Portmap
portmap: ALL EXCEPT 192.168.0.
```

```
# GDM
gdm: ALL EXCEPT 192.168.0.
```

9. Replicação de Servidores

9.1 Gerando as Imagens

Visando atender as necessidades dos Telecentros, criamos um script para replicação de servidores.

Durante a instalação o script fica em /sbin/geraimg.sh. Mas o Script foi desenvolvido para os Telecentros da Prefeitura de São Paulo. Nos Telecentros usamos RAID0 e LVM, então o script parte desse princípio. Caso você queira fazer o seu próprio gerador de imagem, ou queira alterar o que já existe aqui vai umas dicas.

Nós aconselhamos gerar alguns pacotes com o uso do tar, com compressão gzip, e não esqueça do --preserve para manter as permissões. Por exemplo:

```
tar --preserve -czf nome_do_arquivo.tar.gz <arquivos_que_vao_para_o_pacote>
```

A nossa idéia de empacotamento se preocupou na organização dos arquivos, então aconselhamos 6 pacotes:

boot.tar.gz

Diretório boot do servidor

home.tar.gz

Diretório home do servidor

opt.tar.gz

Diretório opt do servidor

usr.tar.gz

Diretório usr do servidor

var.tar.gz

Diretório var do servidor

root.tar.gz

Raiz do servidor

Caso o servidor use um esquema de partição semelhante a esse, o trabalho fica muito mais fácil. Caso contrário pode complicar um pouco. Cuidado para não gerar pacotes duplicados (inúteis) por exemplo um root.tar.gz que contenha os mesmos arquivos do var.tar.gz .

Nós aconselhamos criar um pacote tar.gz por partição existente e a medida que os pacotes forem gerados, as partições devem ser desmontadas. Assim quando for gerar o pacote da raiz não haverá muitas dificuldades.

9.2 Restaurando as Imagens

Existem muitas maneiras de restaurar as imagens. Nós sugerimos gravar um CD com as imagens, o que não impede de usar um FTP, SCP, wget, imagens em disco etc.

Primeiro coloque o CD-rom do Sacix(Tamanduá) para o computador iniciar pelo CD-rom. Assim que a instalação começar, cancele a instalação. Ejete o CD-rom do Sacix e coloque o CD-rom com as imagens. Monte o CD-rom e a sua partição raiz no terminal e descompacte o pacote referente a raiz. Monte as partições restantes após ter descompactado o pacote da raiz, e descompacte as outra imagens. Não esqueça de fazer um chroot para a partição raiz, para rodar o lilo e instalar o setor de boot.

Caso prefira uma restauração via rede, inicie com o CD-rom do Sacix e configure sua placa de rede (algumas placas estão nativas no kernel, mas a maioria está como módulo). Com a rede configurada, use o scp para copiar as imagens para uma partição temporária e siga os passos da restauração via CD-rom para descompactar os pacotes.

Caso queira aproveitar o esquema de partição do servidor (ISSO SÓ FUNCIONA EM HDS SEMELHANTES) use o comando:

```
dd if=/dev/hdX of=<nome_do_arquivo> count=1 bs=512
```

De posse desse arquivo é só fazer o caminho de volta no novo servidor:

```
dd if=<nome_do_arquivo> of=/dev/hdX count=1 bs=512
```