# Skolelinux - Arquitetura

**Petter Reinholdtsen**

**pere@hungry.com**

**Skolelinux - Arquitetura**

by Petter Reinholdtsen

Published v0.1, 2002-12-07



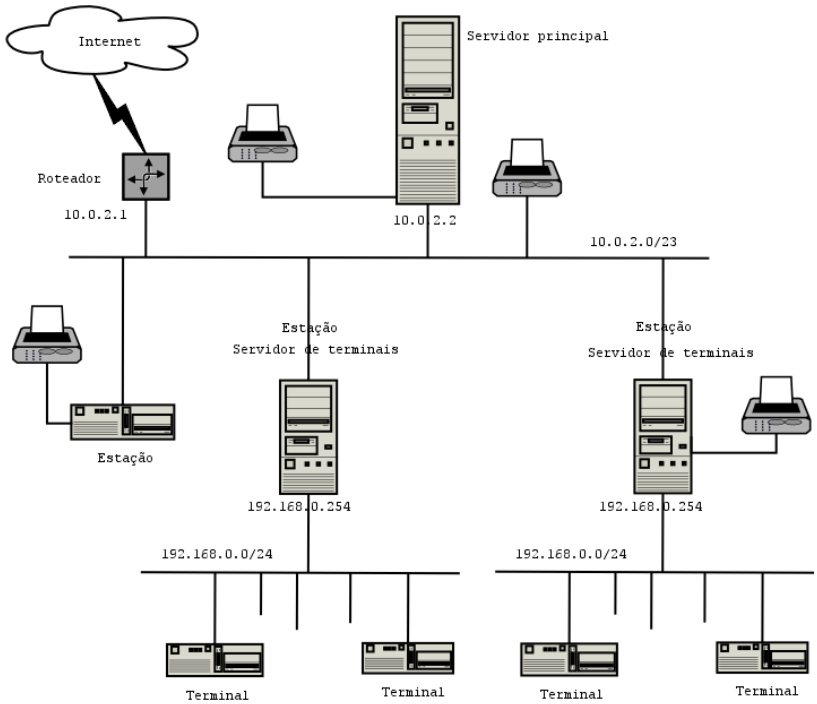
A Skolelinux é a Distribuição Debian Personalizada (Custom Debian Distribution - CDD) (http://wiki.debian.net/index.cgi?CustomDebian) em desenvolvimento do projeto Debian-edu. Isso significa que a Skolelinux é a versão da Debian cujo ambente pré-formatado oferece uma rede escolar completamente configurada (na Noruega, onde o projeto começou, o alvo principal eram as escolas que atendiam a faixa etária de 6 a 16 anos). Esta documentação descreve a arquitetura da rede e os serviços oferecidos pela instalação Skolelinux.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

# Table of Contents

# Chapter 1. Rede




Network architecture
A figura é um rascunho de uma topologia de suposta rede. A configuração padrão do Skolelinux pressupõe que existe um (e somente um) servidor principal, permitindo a inclusão tanto de estações de trabalho normais quanto servidores de terminais (com os seus terminais associados). O número de estações pode ser do tamanho que você desejar (indo de um a muitos). O mesmo vale para os servidores de terminais, cada um em uma rede separada, de forma que o tráfego entre os terminais e o servidor de terminais não afete o resto dos serviços da rede.

O motivo pelo qual pode existir somente um servidor principal em cada rede na escola é que esse servidor provê o DHCP e só pode ter uma máquina fazendo isso na rede. É possível mover os serviços do servidor principal para outras máquinas configurando-os nesses computadores e, subseqüentemente, atualizando a configuração do DNS de forma que ele aponte para aquele serviço no computador correto.

Com o objetivo de simplificar a configuração padrão da Skolelinux, a conexão com a Internet funciona em um roteador separado. É possível configurar a Debian para conexões tanto com via modem ou ISDN, entretanto, nenhuma tentativa foi feita para que isso funcione automaticamente no Skolelinux (os ajustes necessários para mudar a configuração padrão para essa serão documentados separadamente).

# Chapter 2. Serviços

Com exceção do controle dos terminais, todos os serviços são inicialmente configurados em um computador central (o servidor principal). Por questões ligadas à performance, o servidore de terminais deverá ser uma máquina separada (apesar de ser possível instalar os perfis tanto do servidor principal quanto do servidor de terminais na mesma máquina). Todos os serviços estão alocados a um nome de DNS dedicado e são oferecidos exclusivamente sobre IPv4. A alocação de nomes de DNS torna mais simples mover serviços individuais do servidor principal para outra máquina, simplesmente parando o serviço e mudando a configuração do DNS para apontar para a sua nova localização (que, obviamente, deve estar previamente configurado na máquina de destino).

Para garantir a segurança, todas as conexões nas quais ocorre transmissão de senha pela rede são criptografadas. Assim, nenhuma senha transita pela rede na forma de texto plano.

A lista dos serviços configurados como padrão na rede Skolelinux encontra-se abaixo, com o nome de DNS de cada serviço dentro de colchetes. Sempre que possível o nome DNS corresponderá ao nome do serviço no diretório `/etc/services`. Quando isso não for possível, será usado o nome comum do serviço. Todos os arquivos de configuração irão, se possível, se referir ao serviço pelo nome (sem o nome de domínio). Dessa forma, fica fácil para as escolas mudarem tanto o seu domínio (se elas tiverem o seu próprio domínio DNS) quanto o seu endereço IP.

- Centralização dos registros de atividades (logs) [syslog]
- DNS(Bind?)[domain]
- Configuração automática da rede nas máquinas (DHCP) [bootps]
- Sincronização do relógio (NTP) [ntp]
- Home directories via network file system (SMB/NFS)[homes]
- Correio eletrônico (Limacute) [postoffice]
- Serviço de diretórios (OpenLDAP) [ldap]
- Servidor de páginas Web (Apache/PHP/eZ) [www]
- Servidor de SQL (PostgreSQL) [database]
- Backup centralizado (?) [backup]
- Cache/proxy Web (Squid) [webcache]
- Impressão (CUPS) [ipp]
- Acesso remoto (OpenSSH) [ssh]
- Configuração automática [cfengine]
- Servidor de terminais (LTSP) [ltsp-server-\#]
- Levantamento das máquinas e serviços com relatório de erros, situação e histórico via Web. Relatório de erros por e-mail.

Each user stores his personal files in his home folder which is made availble by the server. Home folders are accessible from all machines, giving users access to the same files regardless of which machine they are using. The server is operating system agnostic in offering access using NFS for Unix Clients, SMB for Windows and Macintosh clients.

Por padrão, o correio eletrônico está configurado somente para entregas locias (isto é, dentro da rede da escola). Entretanto, a entrega de e-mails pode ser extendida para toda a Internet, caso a escola possua uma conexão fixa com Internet. Listas de discussão são configuradas baseadas no banco de dados do usuário, oferecendo a cada classe a sua lista. Os clientes são configurados para remeter os e-mails para o servidor (usando "smarthost") e os usuários podem acessar sua caixa postal pessoal tanto via POP3 quanto IMAP.

Todos os serviços são acessados com os mesmos nome de usuário e senha, graças ao banco de dados de usuários central para autenticação e autorização.

Para aumentar a performance no acesso aos sites visitados freqüentemente, é usado um proxy de web que armazena os arquivos localmente (Squid). Juntamente com o bloqueio do tráfego da web no roteador, isso também permite controlar o acesso à Internet para cada máquina individualmente.

A configuração da rede é feita automaticamente nos clientes, através do DHCP. Aos clientes normais são alocados endereços IP na sub-rede privada 10.0.2.0/23, enquanto que os terminais estão conectados ao servidor de terminais correspondente través da sub-rede 192.168.0.0/24 separada (isso para garantir que o tráfego dos terminais não interfira com o resto dos serviços da rede).

O registro de eventos é centralizado, o que faz com que todas as máquinas enviem as suas mensagens do syslog para o servidor. O serviço syslog está configurado de forma a aceitar somente mensagens provenientes da rede local.

Como padrão, o servidor de DNS é configurado para um domínio de uso interno somente, até que um domínio DNS real ("externo") possa ser configurado. Esse servidor funciona também como um servidor de cache de DNS. Dessa forma, todas as máquinas da rede podem usar este como o seu servidor de DNS principal.

Alunos e professores tem a possibilidade de publicar sítios de Internet. O servidor de Web oferece mecanismos para autenticação de usuários e para limitar a acesso a páginas e diretórios individuais a grupos e usuários específicos. Os usuários terão a possibilidade de criar páginas Web dinâmicas, uma vez que o servidor será programável para permitir tal recurso.

As informações dos usuários e das máquinas podem ser modificadas em um computador central e disponibilizadas para todos os computadores da rede automaticamente. Para permitir isso, configura-se um servidor de diretórios centralizado. O diretório terá informações sobre os usuários, grupos de usuários, máquinas e grupos de máquinas. Para evitar confusão por parte do usuário, não existirá nenhuma diferença entre os grupos de arquivos, listas de discussão e grupos de rede. Isso implica que os

grupos de máquinas que têm que ser grupos de rede possuem o mesmo espaço de nome dos grupos de usuário e listas de discussão.

A administração dos serviços e usuários é feita via web e segue padrões estabelecidos, funcionando muito bem nos navegadores web que fazem parte da Skolelinux. O sistema de administração baseado em web permite delegar certas tarefas para determinados usuários ou grupos de usuários.

À fim de evitar certos problemas com o NFS e tornar mais simples a verificação de problemas, os relógios das diferentes máquinas devem estar sincronizados. Para realizar isso, o servidor Skolelinux está configurado como um servidor de Network Time Protocol (NTP) local e todas as estações e terminais estão configurados para sincronizar os seus relógios com o servidor. O próprio servidor deve sincronizar o seu relógio via NTP com os servidores oficiais na Internet, garatindo, assim, que toda a rede estará com a hora correta.

As impressoras podem ser conectadas onde for mais conveniente, seja diretamente na rede, no servidor, em uma estação ou no servidor de terminais. O acesso às impressoras pode ser controlado para cada um dos usuários individuais, de acordo com o grupo ao qual eles pertençam. Isto é realizado através do uso de controles de cotas e de acesso às impressoras.

## 2.1. Serviços para terminais

A configuração de um terminal torna possível a utilização de um PC comum como um terminal (ou mesmo um terminal gráfico). Isso significa que essa máquina inicializa a partir de um disquete ou diretamente do servidor usando uma placa de rede com EPROM, sem usar o disco rígido local. A configuração de terminais utilizada é a do Linux Terminal Server Project (LTSP).

Terminais são uma boa maneira de se fazer uso de máquinas mais antigas e menos potentes, uma vez que todos os programas serão executados no servidor de terminais. Isso funciona da seguinte maneira: o serviço usa oDHCP e o TFTP para se conectar e inicializar a partir da rede. Depois o sistema é montado via NFS a partir do servidor LTSP e, por fim, o X11 é iniciado e conectado ao mesmo servidor LTSP através do XDMCP, garantindo, dessa forma, que todos os programas sejam executados no servidor LTSP.

O servidor de terminais é configurado para receber relatórios do sistema (syslog) dos terminais e encaminhar essas mensagens para o receptor central de syslogs. [1]

# Notes

1. Peraí, os terminais não possuem nomes únicos junto aos servidores LTSP. Como nós podemos identificar qual cliente está conectado aonde, a partir do servidor central?

# Chapter 3. Administração

Todas as máquinas Linux que são instaladas usando o CD Skolelinux são administráveis a partir de um computador central, geralmente o servidor. É possível se conectar em qualquer das máquinas da rede usando ssh, passando a ter, dessa forma, acesso total a essas máquinas.

Nós usamos cfengine para editar os arquivos de configuração. Esses arquivos são atualizados do servidor para os clientes. Caso queria mudar a configuração do cliente, basta editar a configuração no servidor e deixar que as alterações sejam distribuídas automaticamente

Todas as informações dos usuários são mantidas em um banco de dados SQL. Atualizações nas contas dos usuários são feitas nesse banco de dados. As informações são exportadas para um diretório LDAP, que é usado pelos clientes para efetuar a autenticação dos usuários.

# Chapter 4. Instalação

Installation is possible either from a CD or by a diskette from server.

O nosso objetivo possibilitar que o servidor seja instalado a partir do CD e os clientes a partir da própria rede interna. A instalação deve funcionar sem nenhum acesso à Internet.

A instalação não deve fazer somente as setuintes perguntas: o idioma desejado (por ex. português, norueguês, inglês) e o perfil da máquina (servidor, estação, terminal). Todas as outras configurações devem ser efetuadas automaticamente, com valores razoáveis, para serem mudadas a partir de uma administração centralizada, subseqüente à instalação.

# Appendix A. Configuração de acesso ao sistema de arquivos

Cada conta de usuário do Skolelinux está associada a uma seção do sistema de arquivos no servidor de arquivos. Esta seção (diretório home) contém os arquivos de configuração do usuário, documentos, e-mails e páginas web. Alguns arquivos devem ser configurados para permitir acesso de leitura para outros usuários no sistema, alguns devem ser legíveis para todos na Internet e alguns não devem ser acessíveis para mais ninguém, exceto o usuário.

Para garantir que todos os discos que forem utilizados para diretórios compartilhados ou de usuários tenham um nome único entre todos os computadores da instalação, eles podem ser montados da seguinte forma: `/skole/`*`host`*`/`*`diretório`*`/`. Inicialmente um diretório é criado no servidor de arquivos, `/skole/servidor/home0/`, no qual todas as contas de usuário são criadas. Outros diretórios podem, então, ser criados quando necessário, para acomodar grupos de usuários ou padrões de uso próprios.

Para habilitar o controle de acesso ao compartilhamento de arquivos usando os grupos de arquivos, cada usuário deve estar associado a um grupo primário sem nenhum outro membro. O nome desse grupo privado deve ser idêntico ao seu nome de usuário. [1] Isto permite que todos os novos arquivos criados pelo usuário sejam configurados para permitir acesso total ao grupo daquele arquivo. Juntamente com a configuração do gid nos diretórios e a herança de direitos, isto permite um compartilhamento de arquivos entre os membros de um grupo de arquivos de forma controlada. Para isso, a configuração umask dos usuários deve ser 00X. [2].

As configurações iniciais de acesso aos novos arquivos fazem parte da política de uso da rede . Elas tanto podem permitir o acesso de leitura para todos - o que pode ser alterado posteriormente através de uma ação explícita do usuário -, quanto podem bloquear totalmente o acesso, sendo necessária uma ação do usuário para torná-los acessíveis. A primeira postura estimula o compartilhamento do conhecimento e torna o sistema mais transparente, enquanto que o segundo método diminui o risco de disseminação indesejada de informações restritas. O problema com a primeira política é que não é muito aparente aos usuários que o material que eles criam será acessível para todos os outros. Isto é percebido somente quando se inspeciona os diretórios dos outros usuários, onde então se descobre que os arquivos são passíveis de leitura. O problema com a segunda alternativa é que poucas pessoas tendem a deixar seus arquivos acessíveis, mesmo que eles não contenham informações restritas e que o conteúdo possa servir de ajuda para usuários curiosos que desejem aprender como os outros resolveram problemas particulares (geralmente questões de configuração).

Sugestão: Os arquivos são inicialmente configurados para permitir acesso de leitura para todos, mas criam-se diretórios particulares nos quais o conteúdo é inicialmente bloqueado. Isso simplifica o processo de decidir se o arquivo deve ser legível para outros ou não. Na prática, deve-se configurar umask para 002 e criar o diretório `~/` com privilégio 0775, um `~/priv/` com 0750 e um `~/pub/` com 0775. Arquivos que não deve ser acessados por outros devem ser colocados em `~/priv/` e os arquivos públicos em `~/pub/`. Outros arquivos serão inicialmente acessíveis, mas podem ser bloqueados de acordo com a necessidade.

O ssh exige que o diretório home tenha permissão de escrita somente para o seu proprietário, por isso, o privilégio de acesso máximo para ~/ tem que ser 755.

- acesso aos diretórios home (*~/.)? - diretórios home - diretórios compartilhados?

# Notes

1. *Mais informações acerca de grupos privados* (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-users-groups-private-groups.html) estão disponíveis no site da RedHat.
2. Se, inicialmente, for permitida para todos os usuários a leitura dos novos arquivos criados, então X=2. Se esse acesso inicial de leitura for apenas para um grupo restrito, então X=7.

# Appendix B. Palavras-chave

Estas são notas aleatórias acerca de coisas que deveriam ser incluídas neste documento.

- Banco de dados de usuário centralizado com agrupamento e a capacidade de controlar quais grupos têm acesso a quais máquinas.
- Agrupamento de máquinas e a capacidade de controlar o acesso aos serviços da rede para esses grupos (bloqueio de acesso à Internet através do squid)
- Should consider using a DNS name from RFC 2606.