# Skolelinux - Arquitetura

**Petter Reinholdtsen**

**pere@hungry.com**

**Skolelinux - Arquitetura**

by Petter Reinholdtsen

Published v0.1, 2002-12-07

A Skolelinux é uma distribuição Linux baseada na Debian, voltada para a utilização em redes de computadores nas escolas (na Noruega, o público-alvo principal são as escolas que possuem classes com alunos entre 6 e 16 anos de idade). Este documento descreve como essa rede poderia ser construída e como os serviços dessa rede poderiam funcionar.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

# Table of Contents

# Chapter 1. Rede

Nettverks-skisse

Network architecture
A figura é um rascunho de uma suposta topologia de rede. Quando uma rede Skolelinux usa a configuração padrão, pressupõe-se que existe um único servidor, uma ou mais estações de trabalho e servidores LTSP (Linux Terminal Server Project) e nenhum ou mais clientes LTSP. Os clientes LTSP estão em redes separadas, para evitar que o tráfego entre o servidor LTSP e os clientes afete outros serviços da rede.

Uma rede não pode ter mais do que um servidor de DHCP. Este é o motivo pelo qual nunca pode haver mais do que um servidor na mesma rede. Os serviços no servidor pode ser movidos para outras máquinas, mudando-se a configuração e o serviço e, subseqüentemente, atualizando-se a configuração do DNS para fazer com que a denominação no DNS aponte para o computador correto.

É esperado que a conexão com a Internet seja feita através de um roteador separado. Essa recomendação é feita com o objetivo de simplicar a configuração padrão no Skolelinux. É possível configurar o Debian tanto usando um modem como uma conexão ISDN, mas nenhuma tentativa tem sido feita para que isso funcione automaticamente no Skolelinux. Este tipo de configuração deve ser ajustada para atender a situações particulares e ser documentada separadamente.

# Chapter 2. Serviços

Os serviços são oferecidos esclusivamente sobre IPv4. Todos os serviços são configurados inicialmente em um computador central (o servidor Skolelinux), com exceção dos controles dos terminais, que é recomendável que sejam colocados em outra máquina, por questões de performance. Todos os serviços estão alocados a um DNS dedicado, à fim de facilitar a mudança de serviços individuais do servidor principal para outras máquinas através da interrupção do serviço no servidor skolelinux e mudando a configuração do DNS para que ela aponte para a nova máquina.

As senhas nunca são enviadas como texto simples através da rede. Todas as conexões onde transitem senhas deverão ser criptografadas.

Os seguintes serviços são configurados [o nome DNS está dentro de colchetes]. O nome DNS deverá corresponder ao nome do serviço em /etc/services. Onde isso não estiver disponível, o nome usual do serviço é usado como nome DNS. Todos os arquivos de configuração deverão, se possível, se referir ao serviço pelo nome e sem o nome do domínio, o que facilita a mudança do nome do domínio em escolas que já possuem o seu próprio domínio DNS, além de facilitar também a mudança do número IP nas escolas que assim o desejarem.

- Centralização dos registros de atividades (logs) [syslog]
- DNS(Bind?)[domain]
- Configuração automática da rede nas máquinas (DHCP) [bootps]
- Sincronização do relógio (NTP) [ntp]
- Diretório home através do sistema de arquivos de rede (SMB/NFS/Appletalk) [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.

O servidor aloca sistemas de arquivos ao longo da rede e oferece diretórios home para todas as estações. Nós usamos NFS para clientes Unix, SMB para clientes Windows e Appletalk para clientes Macintosh. Todos os arquivos pessoais ficam armazenados no diretório home, dessa forma os usuários tem acesso ao seus arquivos a partir de qualquer máquina da rede.

O serviço interno de correio eletrônico é configurado com entrega local e acesso ao e-mail pessoal através de POP e IMAP. O correio pode ser configurado para enviar mensagens através da Internet, se a escola possuir uma conexão fixa. Nós configuramos listas de discussão baseadas no banco de dados de usuários, dessa forma, cada classe tem acesso à sua própria lista de discussão. Todos os clientes são configurados para enviar mensagens para o servidor (usando “smarthost”).

Um banco de dados de usuários central é configurado para autenticação e autorização, assim o nome de usuário e a senha são os mesmos para todos os serviços que exigem autenticação.

O acesso à WWW é configurado para passar por um proxy web (Squid), com armazenamento via cache dos arquivos. Isso aumenta a performance dos sites acessados com maior freqüência e, juntamente com o bloqueio do tráfico web no roteador, permite controlar o acesso individual das máquinas à Internet.

Os números IP dos clientes são alocados via DHCP. Nós escolhemos uma rede IP privada e alocamos os IP’s nessa rede. Nós escolhemos o uso da subrede 10.0.2.0/23. Os terminais burros são conectados ao servidor LTSP através de uma subrede separada (192.168.0.0/24).

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.

O servidor é configurado como um servidor de DNS para um domínio DNS somente para uso interno (*.intern.). Entretanto pode-se configurar também um domínio DNS real (“externo”). Além disso, esse servidor funciona também como

um servidor de cache de DNS. Dessa forma, todas as máquinas da rede podem ser configuradas para usar este como o seu servidor de DNS principal.

Um servidor de páginas web com capacidade de publicação é configurado para uso pelos alunos e professores. O sistema web possui mecanismos para autenticação de usuários e para limitar o acesso a páginas individuais e subdiretórios de usuários e grupos. O sistema web está configurado com recursos para permitir a criação de páginas web dinâmicas.

Tem-se também configurado um servidor de diretórios centralizado. Dessa forma, as informações sobre os usuários e a as máquinas podem ser modificadas em um só lugar e tornam-se acessíveis para todos os computadores da rede. O diretório contém informações sobre os usuários, grupos de usuários, máquinas e grupos de máquinas. Para os usuários, não irá existir nenhuma diference entre grupos, listas de discussão e grupos de rede, para evitar confusão acerca de a qual tipo de grupo o usuário pertence. Isso implica em que grupos de máquinas que deverão ser grupos de rede tenham o mesmo espaço de nome que os grupos de usuário e as 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.

A sincronização dos relógios em todas as máquinas é necessária para evitar certos problemas quando o NFS estiver sendo utilizado, além de tornar mais simples a tarefa de descobrir certos problemas. À fim de manter os relógios das máquinas sincronizados, o servidor Skolelinux está configurado como um servidor local de Network Time Protocol (NTP). Todas as estações e clientes são configurados para sincronizar seus relógios com o servidor. É uma boa idéia configurar o servidor para que ele próprio também sincronize o seu relógio via NTP com algum servidor padrão na Internet, de forma que toda a rede esteja 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 LTSP. As impressoras possuem controle de cota e de acesso e o acesso dos usuários a elas depende do grupo ao qual eles pertencem.

# 2.1. Serviços para terminais

A configuração para os terminais é baseada no Linux Terminal Server Project (LTSP). Este é um sistema que permite a um PC funcionar como um terminal X. Isso habilita as máquinas a iniciarem a partir de um disquete ou através da rede, usando uma placa de rede com PROM de de boot remoto. Dessa forma, fica dispensado o uso de um disco rígido nesta máquina.

O serviço usa o DHCP e o TFTP (Trivial File Transfer Protocol) para se conectar à rede e efetuar o boot a partir dela. Então o sistema de arquivos é montado via NFS a partir do servidor LTSP e o X11 é iniciado e conectado ao mesmo servidor LTSP por meio do XDMCP (X Display Manager Control Protocol). O resultado é uma estação de trabalho onde todos os programas são executados em um servidor LTSP.

O servidor de terminais burros é configurado para receber syslog dos terminais e encaminhar essas mensagens para o receptor central de syslogs. [1]

# Notes

1. Peraí, os terminais burros 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 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

É possível efetuar a instalação tanto de um CD quanto de um disquete a partir do servidor.

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 nenhuma pergunta, com exceção do idioma desejado (por ex. português, norueguês, inglês) e o perfil da máquina (servidor, estação, terminal). Todas as outras configurações devem ser configuradas automaticamente com valores razoáveis, para serem mudadas a partir de uma administração centralizada, subseqüentemente 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-mail e páginas web. Alguns dos 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 de usuários ou compartilhados tenham um nome único entre todos os computadores na 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. 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 de o arquivos 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 escrito somente pelo 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)