Skolelinux - Opzet

Petter Reinholdtsen

pere@hungry.com

Skolelinux - Opzet

by Petter Reinholdtsen

Published v0.1, 2002-12-07

Skolelinux is een op Debian gebaseerde linux distributie die zich richt op schoolnetwerken. (In Noorwegen, richt men zich voornamelijk op scholen met leeftijdsgroep 6-16). Dit document beschrijft hoe het schoolnetwerk door Skolelinux wordt opgebouwd, en welke diensten er door het netwerk aangeboden worden.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

Table of Contents

Chapter 1. Netwerk

Nettverks-skisse

Netwerk architectuur
Deze figuur geeft een schematisch overzicht van de vooropgestelde netwerkstructuur. In de default setup is er één hoodserver, één of meerdere werkstations, één meer thin client servers (LTSP). Elke thin client server bedient een apart netwerk van thin clients, dit om te voorkomen dat het netwerkverkeer tussen the thin clients en de thin client server andere netwerkdiensten hindert.

Een netwerk kan slechts een DHCP server bevatten. Dit is de reden waarom er nooit meer dan een hoofd server is. De door de hoofdserver aangeboden diensten kunnen desgewenst naar een andere computer verplaatsd worden, hiertoe hoeft u enkele de dienst met instellingen te verhuizen, en daarna de DNS instellingen aanpassen zodat die naar de nieuwe locatie verwijst.

Het netwerk vereist dat de Internet verbinding via een aparte router verloopt. Deze vereiste word gesteld om de standaard Skolelinux setup te vereenvoudigen. Modem of ISDN verbindingen zijn mogelijk, maar er zijn tot nog toe geen pogingen ondernomen om dit in de standaard setup te ondersteunen. Dat soort setups vergt aanpassingen, en moet apart gedocumenteerd worden.

Chapter 2. Netwerk diensten

De aangeboden netwerk diensten verlopen allen via IPv4. Initieel worden, afgezien van de thin-client controle, alle diensten op een centrale computer voorzien (de Skolelinux server). De thin-clients worden door aparte computers verzorgt omwille van performantie. Alle netwerk diensten zijn voorzien van een standaard DNS naam, waardoor het makkelijk wordt om diensten te verplaatsen naar andere servers (hiertoe dient men de dienst te stoppen, en the DNS verwijzing aan te passen zodat die naar de nieuwe dienstverlenende computer wijst).

Wachtwoorden worden nooit als gewone tekst verzonden. Alle wachtwoord-gebruikende verbindingen verlopen over een beveiligde verbinding.

De volgende netwerk diensten zijn standaard aanwezig [de DNS naam van de dienst staat tussen vierkante haken]. The DNS naam van de netwerkdiensten komt waar mogelijk overeen met de dienst naam in /etc/services. Waar dit niet mogelijk is, word de gewone naam van de dienst gebruikt als DNS naam. Alle configuratie files dienen, indien zulks ondersteund, naar de diensten te verwijzen bij naam, en niet door middel van de domein naam. Dit om het makkelijk te maken om het domein en IP adres te veranderen.

- Gecentralizeerde logbestanden [syslog]
- DNS(Bind?) [domain]
- Automatische netwerk configuratie (DHCP)[bootps]
- Gesynchronizeerde klok (NTP)[ntp]
- Netwerk toegankelijke thuismappen (SMB/NFS/Appletalk)[homes]
- Electronische post (Limacute) [postoffice]
- Directoryservice (OpenLDAP)[ldap]
- Webserver (Apache/PHP/eZ)[www]
- SQL server (PostgreSQL)[database]
- Centrale backup (?) [backup]
- Web-cache / proxy (Squid) [webcache]
- Printen (CUPS) [ipp]
- Vanop afstand aanmelden (OpenSSH) [ssh]
- Automatische configuratie [cfengine]
- Thin-client servers (LTSP) [ltsp-server-\#]

- Bewaking van machines en diensten, met rapporten, status en geschiedenis op het web, en foutmeldingen via mail.

De server maakt bestandsystemen beschikbaar over het netwerk, waardoor de thuismappen vanop alle werkstationnen beschikbaar zijn. Hiervoor gebruiken we NFS voor Unix clients, SMB for Windows clients en Appletalk voor Macintosh clients. Alle persoonlijke bestanden worden opgeslagen in de thuismap waardoor de gebruikers toegang hebben tot deze bestanden vanop eender welke machine.

De electronische post is ingesteld met lokale verzorging en toegang via POP en IMAP. Indien de school een vaste verbinding heeft kan er post naar Internet verstuurt worden. Er worden emaillijsten opgesteld volgens de gebruikers database zodanig dat iedere klas zijn eigen email lijst heeft. Alle clients verzenden mail via de server (i.e. maken gebruik van “smarthost”.

Een centrale gebruikersdatabase is aanwezig voor authenticatie en authorizatie. Hierdoor hoeft elke gebruiker slechts één gebruikersnaam en wachtwoord te onthouden, waarmee hij van alle diensten kan gebruik maken.

Toegang tot het WWW verloopt via een web proxy (Squid),met locale caching van bestanden. Dit verhoogd de performantie op regelmatig opgevraagde sites. Samen met het blokeren van web verkeer in de router, voorziet deze opzet in toegangscontrole voor het web op individuele machines.

Clients krijgen een ip adres toegewezen via DHCP. We gebruiken hiervoor een private IP range, onze keuze is gevallen op het 10.0.2.0/23 subnet. Thin-clients zijn met hun LTSP server verbonden via een apart subnet 192.168.0.0/24.

Om de logbestanden centraal te kunnen bijhouden zijn alle machines ingesteld om hun syslog berichten naar de server te versturen. De syslog dienst is ingesteld zodat enkel van het locale netwerk berichten worden aanvaard.

De DNS dienst van de server is in eerste instantie enkel ingesteld voor intern gebruik (*.intern.), dit totdat een extern DNS domein opgezet kan worden. Verder is de DNS dienst ingesteld als een caching DNS, zodat alle machines op het netwerk de DNS dienst als hun hoofd-DNS server kunnen gebruiken.

Leerlingen en leerkrachten hebben de mogelijkheid om webpagina’s te publiceren. Het is hierbij mogelijk om bezoekers te authenticeren, en zodoende de toegang tot

bepaalde webpagina’s te beperken. Aan de serverkant is de mogelijkheid voor dynamische webpagina’s voorzien.

Een centrale directoryserver is aanwezig, zodat informatie over gebruikers en machines op een centrale plaats aangepast kan worden. Aanpasssingen zijn vervolgens toegankelijk vanop alle computers in het netwerk. De directoryserver bevat informatie over gebruikers, gebruikersgroepen, machines, en machinegroepen. Teneinde verwarring te voorkomen zullen er voor de gebruikers geen merkbare verschillen zijn tussen bestandsgroepen, emaillijsten, en netwerkgroepen. Dit houd in dat groepen van machines dezelfde namen hebben als gebruikers groepen en emaillijsten.

Het beheer van diensten en gebruikers zal grotendeels via het web, en gebruikmakend van gevestigde standaarden plaatsvinden. Belangrijke vereiste hierbij is dat dit beheer vlot verloopt in de browsers die deel uitmaken van Skolelinux. Het delegeren van bepaalde taken naar individuele gebruikers zal met dit systeem mogelijk zijn.

Een gesynchronizeerde klok op alle machines is noodzakelijk om problemen te voorkomen wanneer NFS gebruikt wordt. Ook wordt het hierdoor makkelijker om sommige problemen te debuggen. Om de klokken gesynchronizeerd te kunnen houden wordt gebruik gemaakt van het Network Time Protocol. Alle machines in het netwerk zijn ingesteld om hun klok te synchronizeren met de server. De server synchronizeerd zijn klok via NTP met servers op het Internet teneinde de juiste tijd te hebben.

Printers worden aangesloten waar dit het best uitkomt. Dit kan direct op het netwerk zijn, verbonden met de server,of verbonden met een werkstation. Printers zullen voorzien zijn van quota’s en toeganscontrole, waarbij gebruikers toegang krijgen afhankelijk van tot welke groepen ze behoren.

2.1. Thin-client setup

The thin-client setup is gebazeerd op het werk van het Linux Terminal Server Project (LTSP). Dit is een systeem dat het mogelijk maakt om een PC te gebruiken als een X terminal. Deze X terminals worden geboot vanaf een diskette of via het netwerk, hierbij wordt geen gebruik gemaakt van de locale harde schijf.

De thin-clients maken gebruik van DHCP en TFTP om van het netwerk te booten. Vervolgens word het netwerk bestandssysteem geladen via NFS en wordt een grafische login met de LTSP server verbonden via XDMCP. Het resultaat is een werkstation dat alle programma's op de LTSP server draait.

De thin-client server is ingesteld om de syslog berichten die door de clients gegenereerd worden door te spelen naar de centrale logbestanden. [1]

Notes

1. Oops, de thin clients hebben geen unieke namen gezien over verscheidene LTSP servers. Hoe kunnen we op de centrale server nagaan welke client waar zit?

Chapter 3. Beheer

Alle machines die geinstalleerd zijn door middel van de Skolelinux CD zijn vanaf de centrale machine, meestal de server, te beheren. Via ssh kan men op alle machines inloggen, en daar zonder beperkingen werken.

We maken gebruik van cfengine om configuratie bestanden te veranderen. Deze bestanden worden op de clients geupdate door de erver. Om de client configuratie te veranderen volstaat het om op de server de configuratie aan te passen, veranderingen worden automatisch doorgestuurd naar de clients.

Alle gebruikers informatie wordt bijgehouden in een SQL database. Aanpassen van gebruiker accounts wordt via de database geregeld. De gebruikersinformatie wordt geexporteerd naar een LDAP-directory die door de clients gebruikt wordt voor gebruikers authenticatie.

Chapter 4. Installatie

Installatie is mogelijk via CD of, met behulp van een diskette, vanaf de server.

De bedoeling is om een server te installeren vanop de CD, en om clients te installeren over het netwerk door deze via het netwerk te booten. Voor deze installatie is geen Internet toegang vereist.

De enige vragen die door de installatie gesteld worden, zijn de gewenste taal (e.g. Nederlands (België), of Nederlands (Nederland)), en het gewenste profiel (server, werkstation, thin-client server). Alle verdere configuratie moet automatisch van redelijke defaults voorzien worden. De beheerder kan de configuratie na de installatie vanop de server centraal bijstellen.

Appendix A. Toegangsconfiguratie van het bestandsysteem

Aan elke Skolelinux gebruikersaccount is een map toegewezen via het bestandsysteem van de bestandsserver. Deze map (de thuismap) is de plaats waar de gebruiker zijn documenten, email, webpagina's, en persoonlijke configuratiebestanden opslaat. Het is wenselijk dat de gebruiker de mogelijkheid heeft om de toegangsrechten voor de verschillende bestanden te variëren, somige bestanden dienen enkel voor de gebruiker toegankelijk te zijn, andere voor een bepaalde groep van gebruikers, en weer andere wil men op Internet beschikbaar maken.

Alle alle gedeelde mappen en alle thuismappen dienen een, over alle computers unieke, naam te hebben. Om die reden worden ze aangekoppelt als `/skole/`*`computer/map/`*. Standaard is enkel `/skole/tjener/home0/` beschikbaar, dit is de map waarin al de thuismappen staan. Extra mappen kunnen, wanneer nodig, toegevoegd worden (e.g om bepaalde groepen en/of, gebruikspatronen te accomoderen).

Om bestanden op een gecontroleerde manier te kunnen delen, geven we elke gebruiker een hoofdgroep waarvan hij het enigste lid is. Om overzichtelijkheid te behouden maken we de naam van deze private groep gelijk aan de gebruikersnaam. [1] Deze aanpak laat toe om de bestandgroep volledige rechten toe te kennen op geven op door de gebruiker aangemaakte bestanden. In combinatie met de set-gid bit van mappen, en overerving van rechten laat dit toe om op een gecontroleerde manier bestanden te delen tussen leden van een bestandsgroep. Hiertoe stellen we het umask van gebruikers in als 00X. [2].

De initiële toegangsrechten op nieuwe bestanden zijn een kwestie van beleid. Ofwel heeft iedereen standaard leesrechten, die eventueel door een expliciete gebruikersactie verwijdert kunnen worden. Ofwel heeft iedereen standaard geen rechten, en is het aan de gebruiker om via expleciete acties mensen rechten te geven. De eerste aanpak moedigt het delen van kennis aan, en maakt het systeem meer open. Terwijl de tweede aanpak vermijd dat gevoelige informatie per ongeluk door anderen in te kijken is. Het probleem van de eerste aanpak is dat het voor gebruikers niet duidelijk is dat hun documenten door anderen gelezen kunnen worden, dit merken ze alleen wanneer ze de mappen van andere gebruikers proberen nakijken, waardoor ze merken dat documenten inkijkbaar zijn. Het probleem van de tweede oplossing is dat weinig mensen de moeite zullen doen om hun bestanden

beschikbaar te stellen, hoewel vele bestanden geen gevoelige informatie bevatten, en mogelijks andere gebruikers, die het wiel niet willen heruitvinden (bijvoorbeeld wat betreft software configuratie), vooruit kunnen helpen.

Onze voorgestelde opzet: Er is een speciale map voor bestanden met gevoelige informatie, alle bestanden buiten die map zijn standaard door iedereen in te kijken. Meer concreet stellen we het umask in op 002. Daarnaast geven we `~/` en `~/pub/` rechten 0775, en `~/priv/` rechten 0750. Bestanden met gevoelige informatie dienen in `~/priv/` opgeslagen te worden en bestanden die voor publieke consumptie bedoeld zijn in `~/pub/`. De overige bestanden zijn initiëel toegankelijk, hoewel dit naar believen veranderd kan worden.

ssh vereist dat thuismap waarnaar enkel de eigenaar kan schrijven. Om die reden is de maximale toegang voor `~/` 755.

- toegang tot thuismappen (*~/.)? - thuismappen - gedeelde mappen?

Notes

1. Via Redhat is er *meer informatie over private groepen* (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-users-groups-private-groups.html) beschikbaar.
2. Waarbij X=2 indien men wil dat nieuwe bestanden standaard door alle gebruikers te lezen zijn, en X=7 indien men nieuwe bestanden enkel door leden van de bestandsgroep wil laten inkijken.

Appendix B. Sleutelwoorden

Dit zijn een aantal opmerkingen aangaande dingen die nog verder bekeken dienen te worden.

- Gecentralizeerde gebruikers database met groepering en de mogelijkheid aan te geven welke groepen toegang hebben tot welke machines.
- Groeperen van machines en de mogelijkheid om toegang tot de netwerkdiensten te controleren voor deze groepen (blokkeren van Internet toegang via squid)