Skolelinux - Arkitekturbeskrivelse

Petter Reinholdtsen

pere@hungry.com

Skolelinux - Arkitekturbeskrivelse

by Petter Reinholdtsen

Published v0.1, 2002-12-07

Skolelinux er en Debian-baseret Linux-distribution målrettet til elevnetværk i grundskolen (6-16 år). Dette dokument beskriver hvordan netværket struktureres, og hvordan tjenesterne i netværket kommer til at fungere.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

Table of Contents

Chapter 1. Netværk

Nettverks-skisse

Netværksarkitektur
Figuren viser en skitse over antaget netværkstopologi. Når et Skolelinux-netværk sættes op i standard-opsætningen, antages der at være een tjener, en eller flere arbejdsstationer og LTSP-tjenere, og ingen eller flere LTSP-klienter. LTSP-klienterne er på separate netværk, for at undgå at trafikken mellem LTSP-tjener og klienter påvirker andre tjenester på netværket.

Et netværk kan kun have een DHCP-tjener. Dette er årsagen til at der aldrig må være mere end een tjener på samme netværk. Tjenester på tjeneren kan flyttes til andre maskiner ved at flytte konfiguration og tjeneste, og derefter opdatere DNS-opsætningen så DNS-henvisningen peger på den rigtige maskine.

Det forventes at forbindelsen ud på Internet går via en separat router. Denne forudsætning er for at forenkle den standardiserede opsætning af Skolelinux. Det er muligt at sætte Debian op både med modem og ISDN-forbindelse, men der gøres ikke forsøg på at få dette til at fungere automatisk med Skolelinux. En sådan opsætning skal tilpasses hver enkelt installation, og dokumenteres separat.

Chapter 2. Tjenester

Vi tilbyder kun tjenester via IPv4. Alle tjenester sættes som udgangspunkt op på en central maskine (skolelinux-tjeneren), med undtagelse af styring af tynde klienter som anbefales spredt til andre maskiner af ydelses-hensyn. Alle tjenesterne får tildelt eget DNS-navn, så enkelt-tjenester kan flyttes fra hovedtjeneren til andre maskiner ved blot at stoppe tjenesten på skolelinux-tjeneren og ændre i DNS-opsætningen så den peger på den nye maskine.

Der må aldrig sendes adgangskoder i klartekst over netværket. Alle forbindelser hvor der sendes adgangskoder over netværket skal være krypterede.

Følgende tjenester settes op [med DNS-navnet i lodrette klammer]. DNS-navnet skal stemme overens med tjenestenavnet i /etc/services. Da dette mangler bruges det alment brugte navn på tjenesten som DNS-navn. Alle opsætningsfiler skal såvidt muligt referere til tjenesterne ved navn, og uden domænenavn, sådet er enklere at ændre domænenavn på de skoler som har eget DNS-domæne, og enklere at ændre IP-nummer på de skoler som ønsker det.

- Central indlogning [syslog]
- DNS (Bind?) [domain]
- Automatisk netværksopsætning af maskiner (DHCP) [bootps]
- Tidssynkronisering (NTP) [ntp]
- Hjemmeområder via netværksfilsystem (SMB/NFS/Appletalk) [homes]
- Elektronisk postkontor (Limacute) [postoffice]
- Katalogtjeneste (OpenLDAP) [ldap]
- webtjener (Apache/PHP/eZ) [www]
- SQL tjener (PostgreSQL) [database]
- Central backup (?) [backup]
- web-cache / proxy (Squid) [webcache]
- Udskrift (CUPS) [ipp]
- Fjern-indlogning (OpenSSH) [ssh]
- Automatiseret opsætningsstyring [cfengine]
- Tjenere for tynde klienter (LTSP) [ltsp-server-\#]

- Maskin- og tjenesteovervågning med fejlrapportering, + statusoversigt og historik på web. Fejlrapportering via mail.

Tjeneren uddeler filsystem over netværket, og tilbyder brugernes hjemmeområder til alle arbejdsstationer. Vi bruger NFS til Unix-klienter, SMB til Windows-klienter og Appletalk til Macintosh-klienter. Alle personlige filer skal gemmes på hjemmeområdet, så der er tilgang til de samme filer uanset hvilken maskine der arbejdes på.

Intern postkontor-tjeneste sættes op, med lokal levering og tilgang til personlig mail vha. POP og IMAP. Mail kan sættes op til at levere til Internet hvis skolen har fast linje til netværket. Vi opsætter mailinglister baseret på brugerdatabasen, såd hver klasse har tilgang til egne mailinglister. Alle klienter indstilles til at levere mail til tjeneren (dvs bruger “smarthost”).

Der opsættes en central brugerdatabase til godkendelse og tildeling af adgangsrettigheder, så brugeren har samme brugernavn og adgangskode ved alle tjenester som kræver indlogning.

Tilgang til WWW sættes op til at gå via en web-proxy (Squid), med lokal mellemlagring af filer. Dette øger ydelsen på ofte brugte sider, og muliggør sammen med spærring af web-trafik i router adgangskontrol til Internet pr. maskine.

IP-nummer til klienterne tildeles via DHCP. Vi vælger et privat IP-net, og tildeler IP i dette net. Vi har valgt at bruge subnet 10.0.2.0/23. Tynde klienter kobles til LTSP-tjeneren via et separat subnet 192.168.0.0/24 tilkoblet hver enkelt LTSP-tjener.

Central logning sættes op så alle maskinerne sender sine syslog-meldinger til tjeneren. syslog-tjenesten sættes op så den kun accepterer indkommende meldinger fra lokalnettet.

Tjeneren sættes op som DNS-tjener for et DNS-domæne som kun bruges internt (*.intern.), og frem til hvor et officielt (“eksternt”) DNS-domæne kan sættes op. Denne DNS-tjener fungerer desuden som mellemlagrende DNS-tjener, så alle maskiner på netværket kan sættes op til at have denne som sin hoved-DNS-tjener.

Der opsættes en webtjener med publiceringsløsning til brug af elever og lærere. Websystemet skal have mekanismer til at kunne godkende brugerne, og til at

begrænse adgangen til enkeltsider og underkataloger til enkeltbrugere og grupper af brugere. Websystemet skal være programmérbart på tjenersiden, så brugerne kan gemme dynamiske websider.

Der opsættes en central katalogtjener så information om brugere og maskiner kan ændres på eet centralt sted, og automatisk gøres tilgængeligt på alle maskinerne på netværket. Kataloget skal indeholde information om brugere, brugergrupper, maskiner og maskingrupper. For brugere skal der ikke skelnes mellem arkivgrupper, mailinglister og netværksgrupper, for at undgå forvirring om hvilken gruppetype en bruger er lagt ind under. Dette indebærer, at maskingrupper som skal være netværksgrupper har samme navnerum som brugergrupper og mailinglister.

Administrationen af tjenester og brugere skal stort set være webbaseret, og følge etablerede standarder og fungere med de netlæsere som følger med Skolelinux. Det webbaserede administrationssystem skal kunne håndtere uddelegering af enkelte opgaver til enkeltbrugere eller grupper af brugere.

Ens tid på alle maskiner er en nødvendighed for at undgå en del problemer når der bruges NFS, og gør det enklere at fejlsøge en række problemer. For at holde urene synkroniseret på tværs af maskiner opsættes Skolelinux-tjeneren som en lokal Network Time Protocol-tjener. Alle arbejdsstationer og klienter sættes op til at synkronisere sin tid med tjeneren. Tjeneren bør sættes op til at synkronisere sit ur via NTP op imod maskiner på Internet med korrekt tid, så hele netværket får korrekt tid.

Printere kobles op hvor det passer bedst, enten direkte på netværket, tilkoblet tjener, arbejdsstationer eller LTSP-tjenere. Printere skal have kvotestyring og adgangskontrol, hvor enkeltbrugere gives forskellig adgang alt efter hvilke grupper de tilhører.

2.1. Tjenester for tynde klienter

Opsætningen til tynde klienter er baseret på The Linux Terminal Server Project (LTSP). Dette er et system som lader en PC fungere som X-terminal. Det lader maskiner starte fra diskette eller netkort-PROM og indlæser system direkte fra en tjenermaskine uden at bruge klientens lokale harddisk.

Tjenesten bruger DHCP og TFTP til at forbinde til netværket og starte op fra

netværket. Derefter monteres filsystem via NFS fra en LTSP-tjener og X11 startes op og kobles til samme LTSP-tjener vha XDMCP. Resultatet er en arbejdsstation hvor alle programmer kører på en LTSP-tjener.

Tjeneren til tynde klienter sættes op til at modtage syslog fra de tynde kliente, og til at videreformidle disse meldinger til den centrale syslog-modtager. [1]

Notes

1. Hm, de tynde klienter har ikke unikke navne på tværs af LTSP-tjenerne. Hvordan identificerer vi hvilken tynd klient er indlogget hvad på den centrale tjener?

Chapter 3. Drift

Alle linux-maskiner installeret ved hjælp af Skolelinux-CD'en skal lade sig administrere fra en central maskine, fortrinsvis tjenermaskinen. Der skal kunne logges ind på alle maskinerne vha. ssh, og dermed være fuld tilgang til maskinerne.

Vi bruger cfengine til at redigere opsætningsfiler. Disse filer opdateres fra tjeneren til klienterne. For at ændre opsætning på klienterne er det nok at ændre opsætningen på tjeneren og lade automatikken sprede ændringerne.

Information om alle brugere ligger i en SQL-database. Opdatering af brugere sker op imod denne database. Informationen eksporteres til et LDAP-katalog som bruges af klienterne til brugergodkendelse.

Chapter 4. Installation

Installation skal kunne foregå enten fra CD, eller vha. diskette fra tjener.

Målet er at kunne installere en tjener fra CD, og resten af klienterne over netværket ved at opstarte alle de andre maskiner fra netværket. Installatioon skal fungere helt uden tilgang til Internet.

Installationen skal ikke stille spørgsmål, undtagen spørsmål om sprog (dansk, bokmål, nynorsk osv.) og maskinprofil (tjener, arbejdsstation, tjener til tynde klienter). Al øvrig opsætning skal vi sætte automatisk til rimelige værdier, og lade systemadministrator ændre fra centralt hold efter installationen.

Appendix A. File system access configuration

Each Skolelinux user account is assigned a section of the file system on the file server. This section (home directory) contains the user's configuration files, documents, email and web pages. Some of the files should be set to have read access for other users on the system, some should be readable by everyone on the internet, and some should not be accessible for reading by anyone but the user.

To ensure that all disks that are used for user directories or shared directories can be uniquely named across all the computers in the installation, they can be mounted as `/skole/`*`host/directory/`*. Initially, one directory is created on the file server, `/skole/tjener/home0/`, in which all the user accounts are created. More directories may then be created when needed, to accomodate particular user groups or particular patterns of usage.

To enable shared file access control using the file groups, each user must be assigned a primary group with no other members. The name of this private group should be identical to the username. [1] This allows for all new files created by the user to be set with full access for the file's group. Together with set-gid bit on directories and inheritance of rights, this enables controlled file sharing between the members of a file group. Therefore, the users' umask should be 00X. [2].

The initial access settings for newly created files is a matter of policy. They may either be set to give read access to everybody, which can later be removed by explicit user action, or they may be initially blocked, necessiating user action to make them accessible. The first approach encourages knowledge sharing, and makes the system more transparent, whereas the second method decreases the risk of unwanted spreading of sensitive information. The problem with the first solution is that it is not apparent to the users that the material they create will be accessible to all other users. This is detectable only upon inspection of other users' directories, where one can see that the files are readable. The problem with the second solution is that few people are likely to make their files accessible, even if they do not contain sensitive information and the content would be helpful to inquisitive users who want to learn how others have solved particular problems (typically configuration issues).

Suggestion: The files are initially set to be readable by all, but particular directories are created in which the content is initially blocked. This will simplify deciding

whether the file should be made readable or not. Concretely, umask should be set to 002, and `~/` created with priviliges 0775, `~/priv/` given 0750,and `~/pub/` given 0775. Files that should not be readable by others should be put in `~/priv/`, whereas public files will be put in `~/pub/`. Other files will initially be accessible, but may be blocked as needed.

ssh requires that the home directory can only be written to by the owner, thus the maximum access privilege for `~/` is 755.

- access to home directories (*~/.)? - home directories - shared directories?

Notes

1. *More info on private groups* (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-users-groups-private-groups.html) is available from Redhat.
2. If all users initially should be able to read newly created files, then X=2. If only the relevant group should be given initial read access then X=7.

Appendix B. Stikkord

Dette er tilfældige noter over ting som skal ind i resten af dokumentet

- central brugerdatabase med gruppering og mulighed for at styre hvilke grupper som har adgang til (indlogge på) hvilke maskiner.
- gruppering af maskiner og mulighed for at regulere tilgangen til netværkstjenester for disse grupper (blokere tilgang til Internet via squid)