Skolelinux - Arkitekturbeskrivelse

Petter Reinholdtsen

pere@hungry.com

Skolelinux - Arkitekturbeskrivelse

by Petter Reinholdtsen

Published v0.1, 2002-12-07

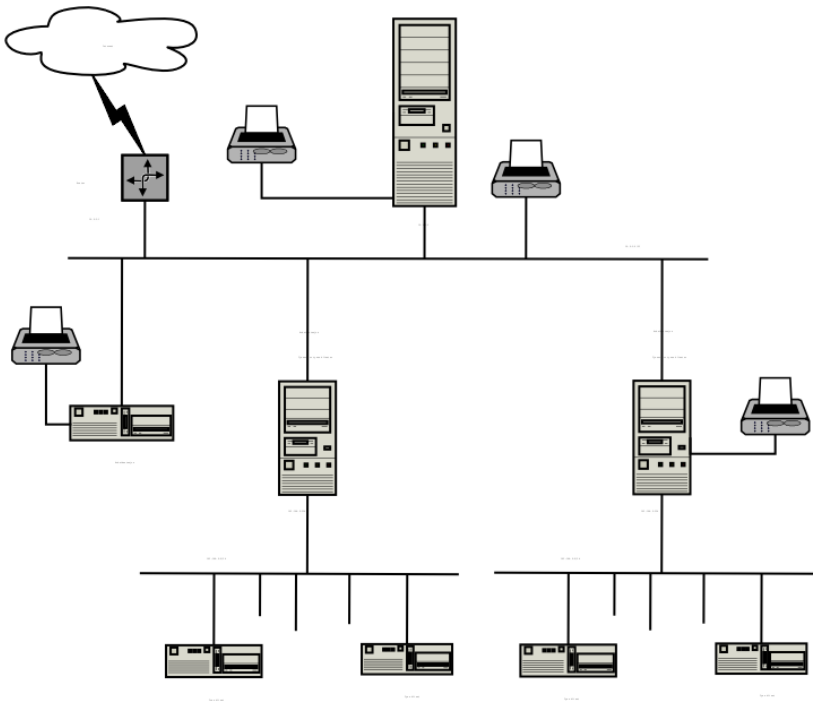
Skolelinux er en Debian-basert Linux-distribusjon beregnet på elevnettverket i grunnskolen (6-16 år). Dette dokumentet beskriver hvordan dette nettverket skal bygget opp, og hvordan tjenestene i dette nettverket skal fungere.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

Table of Contents

Chapter 1. Nettverk



Nettverksarkitektur

Figuren viser en skisse over antatt nettverkstopologi. Når et Skolelinux-nettverk settes opp med default-oppsett, så antas det å være kun en tjener, en eller flere arbeidsstasjoner og LTSP-tjenere, og ingen eller flere LTSP-klienter. LTSP-klientene er på separate nettverk, for å unngå at trafikken mellom LTSP-tjener og klienter påvirker andre tjenester i nettverket.

Et nettverk kan kun ha en DHCP-tjener. Dette er årsaken til at det aldri må være mer enn en tjener på samme nettverk. Tjenestene på tjeneren kan flyttes til andre maskiner ved å flytte oppsett og tjeneste, og deretter oppdatere DNS-oppsettet slik at DNS-aliaset peker til riktig maskin.

Det forventes av forbindelsen ut på Internet går via en separat router. Denne forutsetningen gjøres for å forenkle det standardiserte oppsettet i Skolelinux. Det er mulig å sette opp Debian både med modem og ISDN-forbindelsen, men det gjøres ikke forsøk på å få dette til å fungere ut av boksen med Skolelinux. Slik oppsett må tilpasses hver enkelt installasjon, og dokumenteres separat.

Chapter 2. Tjenester

Vi tilbyr kun tjenester via IPv4. Alle tjenester settes i utgangspunktet opp på en sentral maskin (skolelinux-tjeneren), med unntak av styring av tynne klienter som anbefales spredt til andre maskiner av ytelses-hensyn. Alle tjenestene får tildelt et eget DNS-navn, slik at en kan flytte enkelt-tjenester fra hovedtjeneren og til andre maskiner ved å stoppe tjenesten på skolelinux-tjeneren og endre i DNS-oppsettet til å peke på den nye maskinen.

Det skal aldri sendes passord i klartekst over nettet. Alle forbindelser der det sendes passord over nettet skal være kryptert.

Følgende tjenester settes opp [med DNS-navnet i hakeparentes]. DNS-navnet skal stemme over ens med tjenestenavnet i /etc/services. Der dette mangler brukes det allment brukte navnet på tjenesten som DNS-navn. Alle oppsettfiler skal så sant det er mulig referere til tjenestene ved navn, og uten domenenavn, slik at det er enklere å endre domenenavn på de skolene som har eget DNS-domene, og enklere å endre IP-nummer på de skolene som ønsker det.

- Sentralisert logging [syslog]
- DNS (Bind?) [domain]
- Automatisk nettverksoppsett av maskiner (DHCP)[bootps]
- Klokkesynkronisering (NTP) [ntp]
- Hjemmeområder via nettverksfilsystem (SMB/NFS/Appletalk) [homes]
- Elektronisk postkontor [postoffice]
- Katalogtjeneste (OpenLDAP) [ldap]
- webtjener (Apache/PHP/eZ) [www]
- SQL tjener (PostgreSQL) [database]
- Sentral backup (?) [backup]
- web-cache / proxy (Squid) [webcache]
- Utskrift (CUPS) [ipp]
- Fjerninnlogging (OpenSSH) [ssh]
- Automatisert oppsettstyring [cfengine]
- Tjenere for tynne klienter (LTSP) [ltsp-server-\#]

- Maskin- og tjenesteovervåkning med feilrapportering, + statusoversikt og historikk på web. Feilrapportering via mail.

Tjeneren deler ut filsystem over nettet, og tilbyr brukernes hjemmeområder til alle arbeidsstasjoner. Vi bruker NFS mot Unix-klienter, SMB mot Windows-klienter og Appletalk mot Macintosh-klienter. Alle personlige filer skal lages på hjemmeområdet, slik at brukere har tilgang til de samme filene uansett hvilken maskin de jobber mot.

Intern postkontor-tjeneste settes opp, med lokal levering og tilgang til personlig mail vha. POP og IMAP. Mail kan settes opp til å levere til Internet hvis skolen har fastlinje til nettet. Vi setter opp mailinglister basert på brukerdatabasen, slik at hver klasse har tilgang til egne mailinglister. Alle klienter settes om til å levere mail til tjeneren (dvs bruker “smarthost”).

Det settes opp en sentral brukerdatabase for autentisering og autorisering, slik at en har samme brukernavn og passord på alle tjenester som krever innlogging.

Tilgang til WWW settes opp til å gå via en web-proxy (Squid), med lokal mellomlagring av filer. Dette øker ytelsen på ofte brukte sider, og muliggjør sammen med sperring av web-trafikk i router tilgangskontroll til Internet pr. maskin.

IP-nummer til klientene deles ut via DHCP. Vi velger et privat IP-nett, og deler ut IP i dette nettet. Vi har valgt å bruke subnett 10.0.2.0/23. Tynne klienter kobles til LTSP-tjeneren via et separat subnett 192.168.0.0/24 tilkoblet hver enkelt LTSP-tjener.

Sentralisert logging settes opp slik at alle maskinene sender sine syslog-meldinger til tjeneren. syslog-tjenesten settes opp slik at den kun aksepterer innkommende meldinger fra lokalnettet.

Tjeneren settes opp som DNS-tjener for et DNS-domene som kun brukes internt (*.intern.), og fram til et virkelig (“eksternt”) DNS-domene kan settes opp. Denne DNS-tjeneren fungerer i tillegg som cachene DNS-tjener, slik at alle maskiner på nettet kan settes opp til å ha denne som sin hoved-DNS-tjener.

Det settes opp en webtjener med publiseringsløsning for bruk av elever og lærere. Websystemet skal ha mekanismer for å kunne autentisere brukerne, og å begrense tilgangen til enkeltsider og underkataloger til enkeltbrukere og grupper av brukere.

Websystemet skal være programmerbart på tjenersiden, slik at brukerne kan lage dynamiske websider.

Det settes opp en sentralisert katalogtjener slik at informasjon om brukere og maskiner kan endres på et sentralt sted, og automatisk gjøres tilgjengelig på alle maskinene på nettverket. Katalogen skal inneholde informasjon om brukere, brukergrupper, maskiner og maskingrupper. For brukere skal det ikke være skille mellom filgrupper, mailinglister og nettgrupper, for å unngå forvirring om hvilken gruppetype en bruker er lagt inn i. Dette innebærer at maskingrupper som må være nettgrupper, har samme navnerom som brukergrupper og mailinglister.

Administrasjonen av tjenester og brukere skal stort sett være webbasert, og følge etablerte standarder og fungere med de nettleserne som følger med Skolelinux. Det webbaserte administrasjonssystemet skal håndtere delegering av enkelte oppgaver til enkeltbrukere eller grupper av brukere.

Lik klokke på alle maskiner er en nødvendighet for å unngå endel problemer når en bruker NFS og gjør det enklere å feilsøke endelproblemer. For å holde klokkene synkronisert på tvers av maskinene, så settes Skolelinux-tjeneren opp som en lokal Network Time Protocol-tjener. Alle arbeidsstasjoner og klienter settes opp til å synkronisere sin klokke med tjeneren. Tjeneren bør settes opp til a synkronisere sin klokke via NTP mot maskiner på Internet med riktig klokke, slik at hele nettverket får riktig klokke.

Skrivere kobles opp der det passer best, enten direkte på nettet, tilkoblet tjener, arbeidsstasjoner eller LTSP-tjenere. Skrivere skal ha kvotestyring og adgangskontroll, der enkeltbrukere gis differensiert adgang etter hvilke grupper de tilhører.

2.1. Tjenester for tynne klienter

Oppsettet for tynne klienter er basert på The Linux Terminal Server Project (LTSP). Dette er et system som lar en PC fungere som X-terminal. Det lar maskiner boote fra disket eller nettkort-PROM direkte fra en tjenermaskin uten å brukeklientens lokale harddisk.

Tjenesten bruker DHCP og TFTP for å komme på nett og å for å boote fra nettet. Deretter monteres filsystem via NFS fra en LTSP-tjener og X11 startes opp og

kobles til samme LTSP-tjeneren vha XDMCP. Resultatet er en arbeidsstasjon der alle programmene kjører på en LTSP-tjener.

Tynnklient-tjeneren settes opp til å motta syslog fra tynnklientene, og til å videreformidle disse meldingene til det sentrale syslog-mottaket. [1]

Notes

1. Hm, tynnklientene har ikke unike navn på tvers av LTSP-tjenerne. Hvordan identifiserer vi hvilket tynnklient som logget hva til den sentrale maskinen?

Chapter 3. Drift

Alle linux-maskinene som installeres ved hjelp av Skolelinux-CDen skal la seg administrere fra en sentral maskin, fortrinnsvis tjenermaskinen. En skal kunne logge inn på alle maskinene vha ssh, og dermed ha full tilgang til maskinene.

Vi bruker cfengine til å redigere oppsettfiler. Disse filene oppdateres fra tjeneren til klientene. For å endre oppsett på klientene så er det nok å endre på oppsettet på tjeneren og la automatikken spre endringene.

Informasjon om alle brukerne ligger i SQL-database. Oppdatering av brukere skjer mot denne databasen. Informasjonen eksporteres til en LDAP-katalog som brukes av klientene for brukerautentisering.

Chapter 4. Installasjon

Installasjon skal kunne foregå enten fra CD, eller vha. diskett fra tjener.

Målet er at en skal kunne installere en tjener fra CD, og resten av klientene over nettet ved å boote alle de andre maskinene fra nettet. Installasjon må fungere helt uten tilgang til Internet.

Installasjonen skal ikke stille spørsmål, med unntak av spørsmål om språkform (bokmål, nynorsk, samisk) og maskinprofil (tjener, arbeidsstasjon, tjener for tynne klienter). Alt annet oppsett skal vi sette automatisk til rimelige verdier, og la systemadministrator endre fra sentralt sted etter installasjonen.

Appendix A. Kontooppsett på filsystemet

En brukerkonto i Skolelinux har et område på filsystemet til filtjeneren tilknyttet seg. Dette området inneholder brukerens oppsettfiler, dokumenter, email og websider. Noen av filene skal være lesbare for andre brukere, noen skal være lesbare for alle på web, og noen av filene skal ikke være lesbare for andre enn brukeren selv.

For å sikre at alle disker som brukes til brukerområder eller fellesområder kan navngis unikt på tvers av alle maskinene i en installasjon, så kan disse monteres som `/skole/`*`maskin/område/`*. I utgangspunktet opprettes et område på filtjeneren, `/skole/tjener/home0/`, der alle brukerkontoer opprettes. Ved behov kan det opprettes flere områder, enten for bestemte brukergrupper, eller for bestemte bruksmønstre.

For å muliggjøre tilgangskontroll av fildeling ved bruk av filgruppene, så må hver bruker ha som sin primærgruppe en gruppe der ingen andre brukere er medlem. Denne private gruppen skal ha samme navn som brukeren den tilhører [1] . Denne private gruppen muliggjør at alle nye filer som brukeren oppretter opprettes med full tilgang til filens gruppe. Sammen med set-gid bit på kataloger og arv av rettigheter muliggjør dette kontrollert fildeling mellom medlemmene i en filgruppe. Brukernes umask skal derfor være 00X [2]

Det er et politisk spørsmål hvordan tilgangen til nyopprettede filer på brukerens område skal være. De kan enten være lesbare for alle og sperres med en aktiv handling fra brukeren, eller de kan være sperret i utgangspunktet og må gjøres tilgjengelig for alle ved en aktiv handling. Den første tilnærmingen legger opp til kunnskapsdeling og gjør systemet mer gjennomsiktig. Den andre gjør det mindre sannsynlig at informasjon kommer på avveie. Problemet med den første løsningen er at det er lite synlig for brukerne at det de lagrer er tilgjengelig for alle de andre brukerne. Dette oppdages først når en forsøker å se i de andre brukernes områder, og en ser at filene der er lesbare. Problemet med den andre løsningen er at de færreste vil gjøre sine filer tilgjengelig, selv om de ikke inneholder følsom informasjon og at innholdet ville hjulpet nysgjerrige brukere som vil lære hvordan andre brukere har løst sine problemer (typisk oppsettfiler).

Forslag: Filene er i utgangspunktet lesbare for alle, men det opprettes kataloger der innholdet vil være skjult for alle for å gjøre det enklere å velge om filene skal være tilgjengelige eller ikke. Konkret da at umask settes til 002, og at det opprettes `~/` med rettigheter 0775, `~/priv/` med 0750 og `~/pub/` med 0775. Filer som skal

være skjult legges i priv, filer som skal være offentlige legges i `~/pub/`. De andre er i utgangspunktet tilgjengelige, men kan sperres ved behov.

ssh krever at hjemmeområdet ikke skal være skrivbart for andre eier. Det gir max 755 som rettighet på ~/

- tilgang til hjemmeområder (~/.)? - hjemmeområder - fellesområder?

Notes

1. *Mer info om private grupper* (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-users-groups-private-groups.html) er tilgjengelig fra RedHat
2. X=2 hvis alle brukere i utgangspunktet skal få lese nyopprettede filer og X=7 hvis kun relevant gruppe i utgangspunktet skal få lese nyopprettede filer.

Appendix B. Stikkord

Dette er tilfeldige notater over ting som skal inn i resten av dokumentet

- sentralisert brukerdatabase med gruppering og mulighet for å styre hvilke grupper som får bruke (logge inn på) hvilke maskiner.
- gruppering av maskiner og mulighet for å regulere tilgangen til nettverkstjenester for disse gruppene (blokkere tilgang til Internet via squid?)