Skolelinux - Architekturbeschreibung

Petter Reinholdtsen

pere@hungry.com

Skolelinux - Architekturbeschreibung

by Petter Reinholdtsen

Published v0.1, 2002-12-07

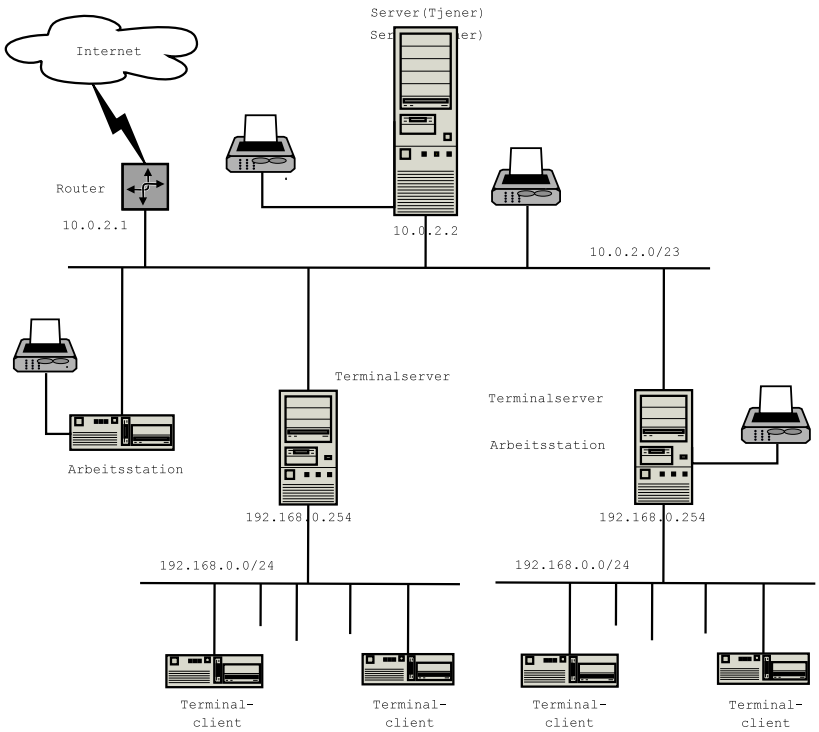
Skolelinux ist eine *Debian* (http://www.debian.org)-basierende Linux-Distribution fr den Einsatz im Lehrbetrieb mit Schlern im Alter von 6-16 Jahren[Initiiert wurde diese Projekt in Norwegen, wo dieses System schon im Einsatz ist. A.d.ï¿½. Dieses Dokument beschreibt die Architektur des Netzwerkes, und geht auf die Funktionalitï¿½ der Netzwerkdienste ein.

Revision History

Revision 0.1 2002-12-07 Revised by: pere

Table of Contents

Chapter 1. Netzwerk



Network architecture

Das Schaubild zeigt die Architektur des Netzwerkes. In der Standardkonfiguration des Skolelinux Netzwerkes ist ein Server und ein bis mehrere Arbeitsstationen und Terminalserver vorgesehen. Optional sind Clients vorhanden, die auf einen der Terminalserver zurckgreifen.

In einem Netzwerk darf es nie mehr als eine DHCP Server geben. Das ist auch der Grund dafr, das es nur einen Server in der Skolelinux Instalation gibt. Natrlich kï¿½nen die verschiedenen Netzwerkdienste auf andere Maschienen verteilt werden. Dafr ist aber das Setup umzustellen und es muss dafr gesorgt sein das der DNS Dienst entsprechend aktualisiert wird. Auf diese Weise kï¿½nen die Arbeitsstationen und die Terminalclients die Dienste auf den richtigen Maschinen ansprechen.

Fr die Verbindung zum Internet ist ein eigenstï¿½diger Router vorgesehen. Die Voraussetzung wurde aus Grnden der Vereinfachung der Skolelinux Installation und Konfiguration definiert. Natrlich ist es mï¿½lich, den Server oder eine andere Maschine via Modem, ISDN oder DSL an das Internet anzuschlieï¿½n, aber die

Installation und Konfiguration wird nicht von der Skolelinux Installation abgedeckt. Diese Installation und Konfiguration muss gesondert durchgefhrt und dokumentiert werden. Da die Skolelinux Debian-basierend ist, kï¿½nen die Debian Standardwerkzeuge dafr verwendet werden.

Chapter 2. Dienste

Alle Dienste werden ausschlieï¿½ich ber IPv4 angeboten. Alle Dienste werden zentral auf einer Maschine installiert(Server). Die Ausnahme sind die Terminalserver Dienste fr die Terminalclients, da hier sonst mit Leistungseinbuï¿½n auf dem Server zu rechnen ist. Alle Dienste sind unter einem eindeutigen DNS Namen ansprechbar. Auf diese Weise ist eine Verteilung von Diensten auf verschiedenen Maschinen einfach durchfhrbar.

Passwï¿½ter werden niemals im Klartext ber das Netzwerk gesendet. Alle Verbindungen die Passwï¿½ter im Netzwerk versenden, sollen Verschlsselungstechniken verwenden.

Folgende Dienste stehen zur Verfgung [DNS Name in eckigen Klammern]

- Zentraler Logginserver [syslog]
- Domain Name Service (Bind?) [domain]
- Automatische IP Adressvergabe und Netzwerkkonfiguration (DHCP)[bootps]
- Zeitsynchonisierung (NTP) [ntp]
- Heimatverzeichnisse via Netzwerkdateisystem (SMB/NFS/Appletalk) [homes]
- Mailserver [postoffice]
- Verzeichnisdienst (OpenLDAP) [ldap]
- Webservice (Apache/PHP/eZ) [www]
- SQL Server (PostgreSQL) [database]
- Zentrale Datensicherung (?) [backup]
- Webproxy / Webfilter (Squid) [webcache]
- Zentraler Druckservice (CUPS) [ipp]
- Fernwartungszugang (OpenSSH) [ssh]
- Zentrale automatische Konfiguration [cfengine]
- Terminalserver fr Thinclients (LTSP) [ltsp-server-\#]
- Maschinen- und Dienstberwachung mit Fehlerbenachrichtigung. Der Status und die Historie sind via Web erreichbar. Fehler werden per Mail gemeldet.

Der Terminalserver holt sich die Dateisysteme ber das Netzwerk und bietet so allen Arbeitsplï¿½zen Heimatverzeichnisse. Wir nutzen NFS fr Unix Clients, SMB fr

Windows Clients und Appletalk fr MacIntosh Clients. Alle Benutzerdaten werden in den jeweiligen Heimatverzeichnissen gespeichert. Auf diese Weise haben die Benutzer Zugriff auf ihre Dateien unabhï¿½gig auf welcher Maschine sie arbeiten.

Ein interner Mailservice ist so konfiguriert, der Mail nur lokal ausliefert und den Zugriff via POP und IMAP zur Verfgung stellt. Der Mailservice kann fr die Internet Nutzung umgestellt werden, wenn das notwendig erscheint. Innerhalb des lokalen Mailservices ist auf der Basis der Benutzerdatenbank eine Mailingliste fr jede Schulklasse eingerichtet, sodaï¿½jede Klasse ber ihre eigene Mailingliste verfgt. Alle Clients sind so konfiguriert, das sie Mails zu diesem Mailserver senden(z.B.“smarthost”).

Eine zentrale Benutzerdatenbank ist fr die Authentifizierung und Authorisierung konfiguriert, sodaï¿½die Anmeldedaten fr alle Dienste und Server gleich sind.

Der Webzugriff auf Internetresourcen ist ausschlieï¿½ich ber den Webproxy und Webfilter erlaubt. Der Webproxy ermï¿½licht das lokale Zwischenspeichern der Webobjekte, was ï¿½ertragungszeit und -kosten spart. Diese Konfiguration ermï¿½lich die genauer Kontrolle, wer wann auf welche Internetresourcen zugreifen darf. Wenn der verwendete Internetrouter nur Verbindungen vom Webproxy erlaubt, ist eine Durchsetzung der Benutzerrichtlinen einfach mï¿½lich.

Die IP Adressen der Arbeitsplï¿½ze werden dynamisch mit DHCP vergeben. Wir haben dafr ein privates Netzwerk gewï¿½lt, aus dem die IP Adressen verwendet werden. Das gewï¿½lte Netzwerk ist 10.0.2.0/23. Die IP Adressen der Thinclients werden aus einem seperaten Subnetz 192.168.0.0/24 vergeben. Jeder Terminalserver verwendet fr die Thinclients das gleiche Subnetz.

Das Logging sï¿½tlicher Maschinen ist so eingerichtet, das alle syslog-Meldungen zum zentralen Server gesendet werden. Der syslog Dienst auf dem Server ist so eingerichte, dass er nur syslog-Meldungen vom lokalen Netzwerk(10.0.2.0/23) entgegen nimmt.

Der Server ist als Domain Name Server nur fr die interne Domain *.intern. eingerichet. Einer Einrichtung einer offiziellen (“externen”) Domain steht nichts im Wege. Zusï¿½zlich ist der DNS Dienst als “caching DNS Server” eingerichtet. Alle Clients sollten diesen DNS Server als ihren Haupt DNS Server verwenden.

Ein Webserver fr die interne Verï¿½fentlichung ist fr die Nutzung durch Schler und

Lehrer freigeschaltet. Das Webserversystem wird einen Anmeldemechanismus zur Verfgung stellen, mit dem die Zugriffsbeschrï¿½kung auf einzelen Seiten und ganze Verzeichnisse auf Benutzer- und Gruppenbasis geregelt werden kï¿½nen. Der Webserver wird die Mï¿½lichkeit der serverseitigen dynamischen Seitenerzeugung bieten.

Ein zentraler Verzeichnisdienst ist fr die einfache und transparente Pflege der Benutzer- und Maschinendaten vorgesehen. Da alle Maschinen im Netzwerk auf die Daten in diesem zentralen Verzeichnisdienst zugreifen, werden ï¿½derungen sofort auf allen Maschinen wirksam. Der Verzeichnisdienst enthï¿½t die Informationen ber die Benutzer, Benutzergruppen, Maschinen und Netzwerkbenutzergruppen. Fr Benutzer die keine Unterschiede zwischen Benutzergruppen, Mailinglisten und Maschinen und keine Verstï¿½dnisprobleme haben mï¿½hten, welchen Typ von Gruppe der Benutzer angehï¿½t, wird den gleichen Namensraum fr Benutzergruppen, Mailinglisten und Netzwerkbenutzergruppen nutzen.

Die Administration der Dienste und Benutzer wird in weiten Teilen via Webinterface mï¿½lich sein. Dabei werden etablierte Benutzerstandards eingehalten, die einwandfrei mit den vorinstallierten Webbrowsern funktionieren. Die Administrationsoberflï¿½he bietet die Mï¿½lichkeit der Delegation von verschiedenen Aufgaben an einzelne Benutzer oder Benutzergruppen.

Die Systemuhren sï¿½tlicher Maschinen werden sychron gehalten, um diversen Problemen(z.B. mit NFS) aus dem Weg zu gehen. Diese Zeitsychronisation wird ber den NTP Dienst auf dem Server ermï¿½licht. Alle Arbeitsplï¿½ze und Terminalserver sychronisieren ihre internen Uhren ber den NTP Dienst des Servers. Der Server sollte bei der Verfgbarkeit einer Internetverbindung gegen einen offiziellen Zeitserver sychronisieren, um dem gesamten Netzwerk die korrekte Zeit zur Verfgung zu stellen.

Drucker werden per Netzwerk angebunden oder direkt an den Server, einer der Terminalserver und/oder einer Arbeitsstation zur Verfgung gestellt. Die Drucker haben eine konfigurierbare Druckmengenbegrenzung und Zugriffkontrolle. Den einzelnen Benutzern wird der Zugriff auf die Drucker ber die Gruppen gewï¿½rt denen er angehï¿½t.

2.1. Terminalserver Dienst

Die Konfiguration der Terminalserverclients(Thinclients) basiert auf dem Linux

Terminal Server Project (http://www.ltsp.org) (LTSP). Das LTSP System ermï¿½licht den Betrieb eines PC's als grafisches X-Terminal. Das ermï¿½licht den Betrieb des PC's ohne lokale Festplatte, wobei das PC-System mit einer Bootdiskette oder einem Netzwerkboot gestartet wird.

Der Terminalserver Dienst nutzt DHCP und TFTP um die Verbindung zum Netzwerk und das Starten vom Netzwerk zu ermï¿½lichen. Anschlieï¿½nd wird das notwendige Dateisystem per NFS vom Terminalserver eingebunden, umd dann die grafische Oberflï¿½he zu laden die per XDMCP die grafische Verbindung zum Terminalserver aufbaut.

Der Terminalserver ist dafr konfiguriert die Systemmeldungen der Thinclient via syslog zu erhalten, die anschlieï¿½nd an deren zentralen Syslog-Server weitergeleitet werden. [1]

Notes

1. Oops, die Thinclients haben keine eindeutigen Namen ber alle Terminalserver. Wie kï¿½nen wir die verschiedene Thinclients unterscheiden, wenn diese sich bei den Diensten auf dem zentralen Server anmelden?

Chapter 3. Administration

Alle installierten Linuxmaschinen, die mit der Skolelinux CD Installation erstellt wurden, sind ber die zentrale Servermaschine administrierbar. Ausserdem ist es mï¿½lich per SSH auf allen Maschinen Fernwartung mit vollem Zugriff zu machen.

Wir nutzen cfengine um die Konfigurationsdateien zu bearbeiten. Die Dateien werden von Server auf den Clients aktualisiert. Um eine Clientkonfiguration zu ï¿½dern, reicht es diese auf dem Server vorzunehmen. Die automatische Verteilung sorgt fr die Aktivierung der ï¿½derung auf den Clients.

Alle Benutzerinformationen werden in einer SQL Datenbank vorgehalten. ï¿½derungen von Benutzerkonten werden immer gegen diese Datenbank gemacht. Diese ï¿½derungen werden dann in den LDAP Verzeichnisdienst exportiert, welcher von den Clients zur Benutzerauthentifizierung und -authorisierung genutzt wird.

Chapter 4. Installation

Die Installation ist sowohl von der CD als auch per Diskette vom Server mï¿½lich.

Das Ziel ist den Server von der CD zu installieren und alle weiteren Maschinen ber das lokale Netzwerk, indem das Booten vom Netzwerk genutz wird. Die Installation arbeitet ohne Verbindung zum Internet.

Die Installation sollte keine Fragen stellen, auï¿½r die nach der Landessprache(z.B. Norwegian Bokmï¿½, Nynorsk, Sami, Deustch, Franzï¿½isch etc) und dem Maschinenprofil (Server, Arbeitsplatz, Terminalserver etc). Alle weiteren Konfigurationen erfolgen automatisch mit sinnvollen Voreinstellungen. Die Konfiguration kann zentral auf dem Server nach dem eigenen Berfnissen angepasst werden.

Appendix A. Anhang 1: Dateisystem Zugriffskonfiguration

Jedes Skolelinux Benutzerkonto hat einen Bereich im Dateisystem des Servers. Dieser Bereich(Heimatverzeichnis, Homedirectory) enthï¿½t alle Benutzerkonfigurationsdateien, Dokumente, Mails und Webseiten. Einige dieser Dateien sind bei den Zugriffsrechten so eingestellt, dass andere Benutzer darauf lesend zugreifen drfen. Einige sollten fr jeden lesbar sein, damit diese vom Webserver ausgeliefert werden kï¿½nen.

Um sicherzustellen, das alle Platten, die fr Heimatverzeichnisse genutzt werden, in der Skolelinux Installation eindeutig identifizierbar sind, kï¿½nen diese als `/skole/`*`host/directory/`* gemounted werden. Anfï¿½glich werden im Verzeichniss `/skole/tjener/home0/` auf dem Dateiserver alle Heimatverzeichnisse erzeugt. Weitere Verzeichnisse kï¿½nen nach Bedarf erzeugt werden um besondere Benutzergruppen oder Arbeitsstrukturen abzubilden.

Um die verteilte Zugriffskontrolle der Dateien zu ermï¿½lichen, sind Dateigruppen zu nutzen. Jeder Benutzer ist Mitglied einer Hauptgruppe in der kein weiterer Benutzer eingetragen ist. Der Name der privaten Gruppe entspricht dem Benutzernamen. [1] Dieses Vorgehen erlaubt das alle neu erzeugten Dateien vom Benutzer volle Zugruiffsrechte fr die Dateigruppe ermï¿½licht. Im Zusammenhang mit dem set-gid Bit bei Verzeichnissen und der Vererbung von Zugriffsrechten erï¿½fnet das den kontrollierten Zugriff zwischen den Mitgliedern einer Dateigruppe. Dafr muss umask auf 00X gesetzt sein. [2].

Die Standardzugriffsrechte fr neu erzeugte Dateien ist eine Frage der Schulvorgabe. Diese kann entweder Leserechte fr jeden vergeben, was vom Benutzer nachtrï¿½lich entfernt werden kann, oder es wird kein Zugriff gewï¿½rt, was vom Benutzter nachtrï¿½lich freigegeben werden kann. Der erste Ansatz fï¿½dert das Teilen von Wissen und macht das System transparenter. Der zweite Ansatz reduziert die Mï¿½lichkeit geschtzte Daten preiszugeben. Das Problem mit den ersten Ansatz ist, das die Benutzer sehr leicht vergessen, daï¿½alle neuen Dateien lesbar sind fr den Rest der Welt. Das kann nur durch durch Inspektion anderer Benutzerverzeichnisse erkannt werden. Das Problem mit dem zweiten Ansatz ist, das nur wenige Benutzer ihre neuen Daten fr den Zugriff durch andere freigeben, auch wenn keine sensiblen Daten enthalten sind. Der Inhalt von Benutzerdateien kann fr andere ntzlich sein, um zu lernen wie ein Anderer das Problem XY gelï¿½t hat(typischerweise Konfigurationsdateien).

Vorschlag: Die Dateien werden mit den Zugriffsrechten erzeugt, das diese lesbar sind fr alle. Aber einige Verzeichnisse sind mit Zugriffsrechten ausgestattet, die den freien Zugriff unterbinden. Das vereinfacht die Handhabung und Entscheidung ob die neue Dateien ï¿½fentlich verfgbar sein sollen oder nicht. Konkret bedeutet das, dass die umask 002 gesetzt wird, und das Verzeichnis `~/` wird mit den Zugriffsrechten 0775 erzeugt. Das Verzeichnis `~/priv/` wird mit den Zugriffsrechten 0750, und das Verzeichnis `~/pub/` wird mit den Zugriffsrechten 0775 erzeugt. Dateien mit schtzenswertem Inhalt werden unter `~/priv/` abgelegt und ï¿½fentlich zugï¿½gliche Dateien unter `~/pub/`. Die anderen Dateien sind standardmï¿½ig fr andere lesbar, was jedoch einfach vom Benutzer geï¿½dert werden kann.

Eine Voraussetzung von SSH ist es, das das Heimatverzeichnis des Benutzers nur vom Benutzer selbst schreibbar sein darf. Daher drfen die Zugriffsrechte fr das Verzeichnis `~/` maximal 755 sein.

- Zugriff auf Heimatverzeichnisse (*~/.)? Heimatverzeichnisse - ï¿½fentliche Verzeichnisse?

Notes

1. *Weiteren Informationen zu privaten Gruppen* (http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-users-groups-private-groups.html) sind von Redhat verfgbar(english).
2. Wenn alle Benutzer die neu erzeugten Dateien lesen drfen, ist X=2. Wenn nur entsprechende Gruppen Zugriff darauf erhalten sollen, ist X=7.

Appendix B. Anmerkungen

Da sind noch einige Anmerkungen die in dieses Dokument einflieï¿½n sollten.

- Eine zentrale Benutzerdatenbank mit Benuztzergruppen und der Mï¿½lichkeit, welche Gruppen auf welcher Maschine Zugriff haben.
- Gruppieren von Machinen und die Mï¿½lichkeit der Zugriffskontrolle zu Netzwerkdiensten fr diese Gruppen(Internetzugangskontrolle per Webproxy).