

Öffentliche Linux-Arbeitsplätze

Konzept und Realisierung in der UB Duisburg-
Essen (Campus Duisburg)

Frank Döschner, UB Duisburg-Essen

Vorstellung beim Treffen des Arbeitskreis der
Systembetreuer der Uni Duisburg-Essen
am 16.11.2004

Anforderung

- Versorgung von ca. 75 PCs mit Internet-Browser, PDF-Viewer und ICA-Client
- Schutz vor Manipulation der Systeme und damit Sicherstellung der Verfügbarkeit
- Kontrolle der Zugriffsmöglichkeiten
- Export von Dokumenten und Recherchen
- Ausdruck von Dokumenten und Recherchen

Bisherige Loesung

- OS = Windows NT 4.0 Workstation
- Absicherung ueber Systemrichtlinien innerhalb der NT-Domäne
- Zugriffskontrolle via Squid-Proxy
- Export/Druck via „selfmade“ Druck-/Export-Station

Nachteile

- Kein zentrales OS-/Application-Rollout
- Manipulations-Schutz lückenhaft
- Zugriffs-Kontrolle lückenhaft
- Druckausgaben nur mit spezieller Druck-Karte
- OS mittlerweile „outdated“
- Lizenzkosten

Neue Loesung

- OS = SuSE Linux 8.x bzw. 9.x
- Booten über das Netz
- Absicherung via Firewall (IpCop und/oder SuSEFirewall2)
- Export von Dokumenten und Recherchen direkt vom Arbeitsplatz via Mail, Diskette und USB-Stick
- Ausdruck mit Standard Kopierkarte von jedem Arbeitsplatz

Vorteile

- OS-/Application-Rollout zentral vom Server
- Sehr guter Schutz vor Manipulationen
- Sehr gute Zugriffskontrolle via Squid und Ip-tables
- Aktuelles OS
- moderate Hardwareanforderungen
- Keine Lizenzkosten

Konfiguration I

- Server :
 - DHCP-Server
 - TFTP-Server
 - RSYNCD-Server
 - Web-Server
 - Squid Proxy-Server
 - 2. Netzwerkkarte oder externe Firewall

Konfiguration II

- Client :
 - Mind. 200 Mhz Pentium I
 - Mind. 64 MB RAM
 - Mind. 2 GB HDD
 - Netboot-fähige Netzwerkkarte

Interna

- Boot-Ablauf :
 - Bootrom macht DHCP-Request an den DHCP-Server und erhält Bootparameter.
 - Bei PXE und GRUB wird via PXE zunächst GRUB geladen.
 - Kernel- und Init-Ramdisk werden via TFTP geladen
 - Kernel- und Ramdisk werden dekomprimiert
 - Die Datei linuxrc in der Ramdisk wird gestartet

Interna II

- Boot-Ablauf (Fortsetzung):
 - Laden der Netzwerktreiber
 - Nochmal DHCP-Request um z.B. den IBA-WWW-Server zu erfahren, da Angaben aus dem Bootrom nicht mehr verfügbar sind
 - Meldung via HTTP-Request, das gebootet wird
 - Zweiten Teil der linuxrc (iba90linrc_part2) via TFTP nachladen, darin sind die folgenden Schritte festgelegt
 - HTTP-Request ob die Platte neu eingerichtet werden soll, z. B. beim ersten Boot am Tag:

Interna III

- Boot-Ablauf (Fortsetzung):
 - Jetzt muss unterschieden werden:
 - 1. Boot an diesem Tag: Platte vollständig initialisieren in ca. 5-15 Minuten
 - Partition 3 wird gemountet oder falls diese nicht existiert angelegt
 - HTTP-Request um RSYNC-Server zu erfahren
 - Via RSYNC werden alle Imagedateien auf die Partition 3 synchronisiert, es werden daher nur Änderungen übertragen.

Interna IV

- Boot-Ablauf (Fortsetzung):
 - Auspacken der Imagedateien aus der lokalen Partition 3
 - Meldung via HTTP-Request, das Platte frischgemacht wurde
 - Partition 3 dismounten
- x. Boot an diesem Tag:
 - Überspringen der Initialisierung

Interna V

- Boot-Ablauf (Fortsetzung):
 - DHCPClient killen, da dieser sonst später beim "normalen Boot" von der Festplatte nicht nochmals gestartet werden kann
 - Init-Ramdisk wieder freigeben und von der Festplatte weiterbooten
 - Jetzt wird beim weiteren normalen Startvorgang wiederum ein DHCP-Request durchgeführt und es läuft der normale Bootvorgang ab als ob das Betriebssystem lokal installiert worden wäre.

Links

- IBA-Dokumentation :
 - http://uboot.uni-paderborn.de/iba_doku/html/index.html

Zum Schluss ...

Vielen Dank für Ihre Aufmerksamkeit.