Integration von Linux-Rechnern in eine Windows-Umgebung

Nach Zwangsumstellung auf eine Windows-Systemlandschaft sind bestehende Linux-basierte Lösungen zu erhalten und möglichst gut zu integrieren.

Agenda

- Augangspunkt Linux: NFS, Kerberos, OpenLDAP
- Migration nach ActiveDirectory
- Benutzerauthentifizierung und -authorisierung
- Single Sign On
- Fileservices
- Terminalserver

Augangspunkt

- Jahrelang gepflegte Linux-Systemlandschaft
  - Benutzerverwaltung im LDAP
  - Passwörter im Kerberos
  - NFS (und Samba)
  - Selbst entwickeltes ERP als Webanwendung
  - Linux-Terminalserver
  - Single-Sign-On

LDAP

- Verzeichnisdienst: users, groups, email, ...
- Server: openldap
- Verwaltungs-GUI: gosa
- Replikation eingebaut => Standorte
- Client: libnss-ldap und libpam-krb5
  - nsswitch, ldap.conf, pam, libnss-ldap.conf
  - nscd, Cache für passwd und group

Kerberos

- Sichere Authentifizierung, symm. Verschlüsselt
- MIT-Kerberos
- Replikation => Standorte
- Client: libkrb5, libpam-krb5
  - krb5.conf, pam

Linux-Clients

- 1..4 Terminalserver je Standort, 5..20 user
  - Pures X11 (kdm), später xrdp
  - Trinity-Desktop (kde3++)
  - Firefox
  - Thunderbird
  - LibreOffice
- Außendienst → Notebooks
- Standorte → OpenVPN

Linux-Server

- Ganeti-Cluster je Standort, kvm
- Fileserver je Standort (NFS, Samba)
- Zentrale ERP-DB Postgres + Host-Standby
- 1..3 RoR-ApplicationServer
- Vieles weitere:
  - DHCP, tftpboot, DNS, LDAP, ssh, ntp, ...

Single-Sign-On unter Linux

- Erfordert kerberisierte Dienste
- Dienst-Principal anlegen
- keytab exportieren
- Dienst für Kerberos konfigurieren
- Client konfigurieren

SSO-Beispiel

- Server: apache
  - libapache2_mod_auth_kerb
  - addprinc -randkey -pwexpire never HTTP/…
  - ktadd -k /tmp/httpserver.keytab HTTP/…
  - .htaccess
- Client: firefox
  - network.negotiate-auth.trusted-uris
  - Windows: network.auth.use-sspi auf false setzen

ActiveDirectory

- Von MicroSoft mit Windows-2000 eingeführt
- LDAP+Kerberos+DNS+proprietäre Erweiterungen
- Verwaltung mittels GUI
- AD-LDAP enthält Vieles:
  - Benutzer, Gruppen, Org-Struktur, Computer, …
  - Schema-Erweiterungen => z.B. Exchange

AD einrichten

- Neue Subdomain == neue Kerberos-Domain
- Manuelles Anlegen der Benutzer und Gruppen
  - Grund: gleichzeitig aufräumen
  - RFC2307-Attribute mit einpflegen:
    - uid=username
    - uidNumber
    - gid=gruppenname
    - gidNumber
    - loginShell
    - UnixHomeDirectory
  - Gruppenmitgliedschaft wiederherstellen/überarbeiten

Kerberos mit AD

- krb5.conf
  - Realm-Namen ändern
  - Mapping domain ↔ realm ändern/hinzufügen
  - Evtl. AES-Ciphers hinzu/voran, je nach Windows-Server-Version (2012R2 → aes256)
  - Alte Server → des-cbc-md5, unsicher!
- Test: kinit user@domain
  - Wir bekommen ein TGT

Benutzer/Gruppen aus AD

- Verschiedene Möglichkeiten:
  - Libnss-ldap beibehalten
    - Funktioniert nach Gefummel in /etc/libnss-ldap.conf
    - Schnarchlangsam, nscd hilft nur wenig
  - winbindd aus samba
    - Erfindet uid/gid und hält mapping konstant
    - Gut für wenige/neue Linux-Clients
    - Kein sync des mappings zwischen den Clients
  - sssd
    - Zentrale Mapping-Instanz, Lösung für große Umgebungen?
    - Nicht ausprobiert

libnss-ldapd

- Daemon nslcd
  - Bekommt Anfragen von nss
  - Wandelt diese in LDAP-Abfragen
  - Wandelt Ergebnis zurück
- Vorteile:
  - Klein
  - Überschaubare Konfiguration
  - Kein ldap-Abfrage-Monster in jedem Prozess, der mal ein getent macht
  - schnell

nslcd.conf

```
uid nslcd
gid nslcd
nss_min_uid 1000
uri ldap://10.92.89.95      # ein AD-Domain-Controller
base dc=ad1,dc=esda-rogo,dc=de  # allgemeine Suchbasis
base passwd OU=Benutzer,OU=Esda St. Egidien,DC=ad1,DC=esda-rogo,DC=de  # Benutzer in Org-Struktur
base passwd CN=Users,DC=ad1,DC=esda-rogo,DC=de                        # andere Benutzer
base group OU=Gruppen,OU=Esda St. Egidien,DC=ad1,DC=esda-rogo,DC=de    # Gruppen in Org-Struktur
base group CN=Users,DC=ad1,DC=esda-rogo,DC=de                         # andere Gruppen
binddn ldapreader@ad1.esda-rogo.de      # kein anonymes bind
bindpw geheim
scope sub
filter passwd (&(objectClass=user)(uid=*))    # nur Benutzer, die im AD eine uid bekommen haben
map passwd homeDirectory unixHomeDirectory
filter group (&(objectClass=group)(gidNumber=*))   # nur Gruppen, die im AD eine gidNumber haben
```

Kerberisierte Dienste mit AD

- Manueller Weg:
  - Computer im AD anlegen
  - Für jeden Service einen Pseudo-Benutzer im AD anlegen
  - Mapping principal-Name auf Pseudo-Benutzer verwalten
  - Mit Windows-Kommandozeile keytab erzeugen

Kerberisierte Dienste mit AD (2)

- Abkürzung: msktutil
  - Debian ab jessie „apt-get install msktutil“
  - http://wiki.bitbinary.com/index.php/Wheezy_msktutil
  - kinit Administrator@domain
  - msktutil -c --computer-name olts2
    - Erzeugt Computer-Konto im AD
    - Erzeugt Principal host/FQDN
    - Erzeugt keytab und legt diese lokal ab
  - Nach Anschalten GSSAPIAuthentication in sshd.conf geht jetzt schon mal ssh mit kerberos

Kerberisierte Dienste mit AD (3)

- Beispiel apache:
  - msktutil --user-creds-only \
    -k /etc/apache2/esdarp2.e.esda-rogo.de.keytab \
    -s HTTP -s HTTP/esdarp2 --update \
    --computer-name HTTP_esdarp2 \
    --dont-expire-password
  - Legt User HTTP_esdarp2 an
  - Geht auch mit password-expiry, siehe auto-update in man msktutil

Kerberisierte Dienste mit AD (4)

- /etc/apache/sites-enabled/…conf

```
<Location "/login_kerb">
    AuthType Kerberos
    AuthName "Kerberos Login"
    KrbAuthRealms AD1.ESDA-ROGO.DE
    Krb5Keytab /etc/apache2/esdarp2.e.esda-rogo.de.keytab
    KrbMethodK5Passwd off
    KrbMethodNegotiate on
    require valid-user
</Location>
```

Fileservices

- Wären wir bloß bei Linux geblieben!
- NFS mit Windows-Server:
  - Chaos, kaputte Rechte, Usermapping über AD funktionierte einfach nicht => aufgegeben
- CIFS
  - apt-get install cifs-utils
  - Erster Versuch: autofs, mit Option multiuser,sec=krb5
    - Geht eine Weile, dann irgendwann Zugriff mit falschem User => findet Kerberos-Cache nicht => Verbindung weg
    - Ursache unklar.
  - Jetzt: fstab-Eintrag mit credentials-File für einzelne Verzeichnisse
  - Bessere Lösung gesucht!

Terminalserver

- Terminalserver-Farm mit automatischer Verteilung der Benutzer
- Thinstation: altes rdesktop
  - Vorgeschalteter Passwort-Dialog, sonst doppeltes Anmelden
  - Mausschatten per GPO ausschalten
  - Numlock mit externem Tool numlock.exe erzwingen
- Neueres Linux: freerdp-x11
  - Deutlich besser, aber wieso diese Windows-Optionssyntax???
- Gesucht: RDP mit Kerberos
  - Örgs, geht auf Microsoft-Seite nicht!!!