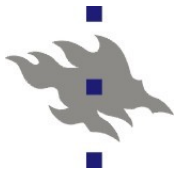
HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Linux-ylläpito: Verkkopalvelut

4. Kalvosetti

Jani Jaakkola
jjaakkol@cs.helsinki.fi
http://www.cs.helsinki.fi/u/jjaakkol/lyp2010



Kerberos

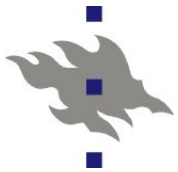
- Kryptografinen autentikointiprotokolla
  - Mahdollistaa käyttäjien ja palveluiden identiteetin luotettavan tunnistuksen ei luotetussa verkossa
  - Verkossa on luotettu 3. osapuoli, autentikointipalvelin
    - AS, Authentication Server
  - Protokolla käyttää AS:n ja autentikoitavan osapuolen välillä jaettuja salaisuuksia
    - Julkisen avaimen kryptografiaa ei käytetä lainkaan
- Kerberos tiketti:
  - Kerberos autentiprosessin tuloksena syntynyt salainen avain, jolla pääsee käsiksi varsinaisiin palveluihin
  - Tiketillä on rajallinen elinaika, jonka jälkeen se täytyy uusia
  - Mahdollistaa single sign on -verkon toteutuksen
    - TGS (Ticket Granting Service) tiketti luodaan kirjautuessa verkkoon sisään ja sillä hankitaan tiketit verkon muihin palveluihin

Kerberos ..

- GSSAPI
  - Generic Security Services Application Program Interface
  - Standardoitu API Kerberos-tikettien välittämiseen (verkossa)
  - Openssh kerberos-autentikointi ja tikettien välitys on toteutettu GSSAPI:lla
- Linux-toteutukset:
  - MIT kerberos, Heimdal kerberos, Javan kerberos
- Kerberoksen heikkouksia
  - Autentikointipalvelimella talletetut jaetut salaisuudet kelpaavat sellaisenaan sisäänkirjautumiseen
  - Protokolla on altis sanakirjahyökkäyksille
- KDC: Key Distribution Center
  - Palvelin, jonne on talletettu salaiset avaimet
- TGS: Ticket Granting Service
  - Palvelin, joka luo Kerberos tiketit
- Käytännössä aina sama palvelin

MIT Kerberos konfigurointi

- Konfiguroidaan master KDC
  - Asennetaan paketit krb5-server, krb5-libs, krb5-workstation
  - Valitaan valtakunta (CS.HELSINKI.FI)
  - Kerberos asiakkaan konfiguraatio: */etc/krb5.conf*
  - */var/kerberos/krb5kdc/kdc.conf*
  - Alustetaan tietokanta
    - */usr/kerberos/sbin/kdb5_util create -s -r CS.HELSINKI.FI*
  - Admin oikeuksien antaminen tunnuksille
    - */var/kerberos/krb5kdc/kadm5.acl*
  - Luodaan admin-tunnus (ja muitakin tunnuksia)
    - */usr/kerberos/sbin/kadmin.local*
  - Käynnistetään KDC
    - */sbin/service krb5kdc start*
    - */sbin/service kadmin start*



Kerberos-palvelin jatkoa..

- Tässä vaiheessa konfiguroitaisiin replikointipalvelimet (Slave KDC)
- Tunnusten (principal) luonti
  - Etähallinta kadmin-komennolla
    - */usr/kerberos/sbin/kadmin -p root/admin@CS.HELSINKI.FI*
  - Konetunnuksen luonti ja salaisen avaimen talletus
    - *addprinc -randkey host/wow-2.cs.helsinki.fi*
    - *ktadd host/wow-2.cs.helsinki.fi@CS.HELSINKI.FI*
  - Käyttäjätunnusten luonti
    - *addprinc tkt_test*
  - Tunnuksen attribuuttien listaus
    - *get_principal tkt_test*
- Testataan
  - *kinit tkt_test*
    - Jos kaikki meni hyvin syntyi tiedosto */tmp/krb5cc_<uid>*

Kerberos-asiakas

- */etc/krb5.conf*
  - Asiakkaan konfigurointi
- Openssh
  - Asiakas autentikointi GSSAPI:n välittämillä kerberos-tiketeillä:
    - *GSSAPIAuthentication*
    - *GSSAPIDelegateCredentials*
  - Kerberos autentikointi serverillä käyttöön:

    KerberosAuthentication yes

    KerberosOrLocalPasswd yes

    KerberosTicketCleanup yes
  - *Openssh GSSAPI-patch*
    - http://www.sxw.org.uk/computing/patches/openssh.html
    - Myös ssh-palvelinten autentikointi kerberoksella
- *pam_krb5:* PAM-autentikointimoduli

Kerberos komentoriviltä

- */usr/kerberos/bin/kinit <principal>*
  - Autentikoituminen AS:lle ja Ticket Granting Tiketin pyytäminen
- */usr/kerberos/bin/klist <principal>*
  - Voimassa olevien tikettien listaus
- */usr/kerberos/bin/kdestroy*
  - Tikettien poistaminen
- Tiedosto */tmp/krb5cc_<uid>*
  - Käyttäjän tiketit

Windows: ADS

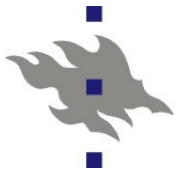
- Active Directory Service
  - W2K:n julkaisun myötä Windows-mikroverkossa otettu käyttöön LDAP ja Kerberos
    - Linux:in LDAP-asiakkailla voi kysellä ja päivittää ADS-palvelinten LDAP-tietokantaa
    - Laitoksen Windows-salasanojen vaihto tapahtuu LDAP:in yli
  - Keskitetyn PDC:n sijasta ADS:n avulla voi rakentaa käyttäjätunnuspalvelimista hierarkioita
  - Kerberoksella korvattu vanha NTLM challenge response autentikointi
    - MS Kerberos-toteutus ei aikoinaan ollut yhteensopiva MIT-kerberoksen kanssa, mutta ongelmat on nyt korjattu
  - AD tukee myös keskitettyä Windows-mikroverkon konfigurointia ja päivityksiä

Linux NFSv4 ja kerberos

- http://www.citi.umich.edu/projects/nfsv4/linux/
- Linuxin NFSv4 tuki on nykyään tuotantokelpoinen
  - Uusiin mikroverkkoihin siis NFSv4
  - Mountd eliminoitu: mountd:n listaamien exporttien sijaan näkyy virtuaalihakemisto, jossa exportatut fs:t ovat alihakemistoja
    - Tämä virtuaalihakemisto täytyy olla olemassa serverillä!
      - */etc/exports* -tiedoston *fsid=0* vipu
  - Kerberos-toteutus
    - *rpc.idmap* – kerberos-käyttäjien kuvaaminen uid:ksi
    - *rpc.gssd* – kerberos tikettien siirto kernelin NFS-asiakkaalle gssapi:n avulla
      - Hakee tiketit suoraan */tmp* hakemistosta
    - *rpc.svcgssd* – kerberos tikettien validointi NFS-serverillä
  - Fedorassa */etc/sysconfig/nfs* tiedostoon *SECURE_NFS=yes*

Linux NFSv4 ja kerberos

- Palvelimella:
  - NFS tunnuksen luonti *kadmin*-komennolla
    - *addprinc -randkey nfs/hallikari.cs.helsinki.fi*
    - *ktadd -e des-cbc-crc:normal nfs/hallikari.cs.helsinki.fi*
  - */etc/rc.d/init.d/rpcsvcgssd start*
  - /etc/rc.d/init.d/rpcidmapd start
  - */etc/exports* tiedoston muokkaus
    - rpc/krb5: pelkkä autentikointi
    - rpc/krb5i: integriteetin tarkastus (tietoa ei voi muuttaa)
    - rpc/krb5p: privacy (tieto on kryptattu)
- Asiakkaalla
  - NFS tunnuksen luonti vastaavasti kuin palvelimella
  - */etc/rc.d/init.d/rpcidmapd restart*
  - */etc/rc.d/init.d/rpcgssd start*
  - */etc/fstab*-rivi:
    - hallikari:/ /linux-kurssi-krb nfs4 sec=krb5p,noauto 0 0
    -

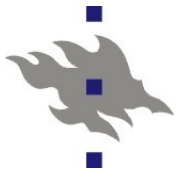


Samba

- CIFS-protokollan toteutus
  - CIFS on oikeasti SMB uudelleen nimettynä
  - Protokolla peräisin muinaisesta DOS:in NETBIOS-toteutuksesta
  - Windowseissa CIFS/SMB tarkoittaa käytännössä kaikkea Windows-mikroverkon liikennettä
    - Autentikointi
    - Tiedostonjako
    - Tulostus
    - Etähallinta
    - Nimipalvelu ja palveluiden saatavuuden mainostaminen
  - SMB Suurimmaksi osaksi dokumentoimaton
  - Sambaa kehitetään pitkälti reverse engineering menetelmällä (tosin kehittäjät kutsuvat sitä toisella nimellä)

Politiikkapäätöksiä

- MS on hylännyt perinteiset selväkieliset salasanat SMB-protokollassa
  - Registry-säädöllä ne voisi saada käyttöön jollain tasolla
  - Käytännössä kannattaa suosiolla unohtaa kryptaamattomat salasanat
- Autentikointimekanismin valinta
  - Share-level security – autentikointi salasanalla
  - User-level security – autentikointi käyttäjätunnuksella ja salasanalla, ei domainia
    - Salasanatietokannan valinta: smbpasswd, tdbsam, LDAP
  - Domain security – Samba on osa NT-domainia
  - ADS security – Samba osa ADS-domainia
- Samba ei osaa toimia (luotettavasti) ADS-domainin toteuttavana palvelimena
  - Toimi luotettavasti vain historiallisen NT-domain protokollan yhteydessä
  - Samba 4.x saattaa korjata tämän

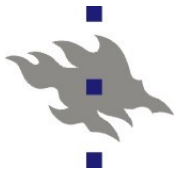


Samba-3.x

- MS:n ADS (Active Directory) tuki
  - Samban voi liittää osaksi ADS-domainia
  - Osaa Windowsien LDAP/Kerberos autentikoinnin
- *net* – työkalu
  - Tarkoituksena vastata Windows:ien *net*-komennon toimintaa
- Windows-printteriajurit ja printterin konfiguraatio samba-tulostuspalvelimelta
- Työkalut NT-domainin siirtämiseen kokonaan samban alle
  - Autentikointidatan ja palvelun siirtäminen vanhasta NT:stä Linuxille
- LDAP-tuki
  - Samban omat tietokannat voivat sijaita LDAP-serverillä

Samba ja Linux?

- Samban avulla Linux palvelinta voi käyttää Windows-verkon
  - Tiedostopalvelimena
  - Tulostuspalvelimena
  - Wins (ennen NBNS)-nimipalvelimena
- Linux-asiakas voi Samban avulla
  - Käyttää Windows-verkon tunnuksia sellaisenaan
  - Käyttää Windows-verkon tiedosto- ja tulostuspalveluja komentoriviltä käsin
    - Eri asia kuin Linux-kernelin sisäinen CIFS-ajuri
  - Tehdä yksinkertaista Windows-verkon hallintaa Samban mukana tulevan *net* komentorivityökalun avulla
  - *Smbtar* -työkalun avulla tehdä windows-työasemista varmistuskopioita



Samban konfigurointi

- Konfiguraatiotiedosto *smb.conf*
  - *.ini-tiedostosyntaksi*
  - Aluksi globaalit asetukset
  - Tiedostojakoon tai printteriin riittyvät asetukset kulmasulkeissa annetun jaon nimen jälkeen

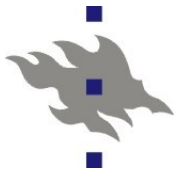
```
[global]
workgroup = WKG
netbios name = MYNAME
security = user
[share1]
path = /tmp
[share2]
path = /my_shared_folder
comment = Some random files
```

Tiedostojakojen konfigurointi

- Huomioon otettavaa:
  - Unix-puolella isoilla ja pienillä kirjaimilla on väliä, windows-puolella ei
  - Symboliset linkit näkyvät Windows-puolella aitoina tiedostoina tai hakemistoina
    - Näytä symbolisia linkkejä voi tehdä samba-jaon yli
- Konfigurointiparametreja
  - *Path*
    - Polku samballa jaettuun hakemistoon
  - *Force group, force user*
    - Pakotetaan tiedostoille annettu Linux-käyttäjä
  - *Admin users*
    - Rootin oikeuksin windowsista käsin toimivat käyttäjät
  - *Read list, write list, valid users*
    - Lista sallituista käyttäjistä
  - *Create mask, force create mode, force directory mode*
    - Unix-oikeuksien pakotus tehdyille tiedostoille

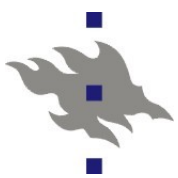
Printterijakojen konfigurointi

- Autentikointi kuten tiedostojakojen kanssa
  - Anonyymit tulostukset myös mahdollisia
- Toteutus
  - Samba vain vastaanottaa valmiita tulostustöitä Windows-asiakkailta. Linuxin oma tulostuspalvelu pitää olla jo valmiiksi konfiguroitu
- AD-domainissa tulostusajurit sijaitsevat Windows-asiakkaissa
  - Tulostusajurit voi domain-konfiguraatiossa tallettaa samba-palvelimelle keskitetysti
    - *[printers]* jako sisältää kaikille tulostimille yhteiset asetukset
    - *[print$]* jako sisältää asennetut ajurit
    - Windows-asiakkaat automaattisesti hakevat ja asentavat ajurin
  - CUPS-postscript tulostusajurit voivat kokonaan korvata tavalliset printterivalmistajien tulostusajurit



Samba 4.x

- Ei ole valmis, testiversioita julkaistu
- Uusi Samban sisäinen VFS-malli
  - Virtuaalitiedostojärjestelmät
- ADS-palvelimen toteutus
  - KDC
  - LDAP
  - Registry
  - ACL:t



Samba Linux-mikroverkon tiedostopalvelimena

- Samba-palvelin ja kernelin SMB-ajuri toteuttavat laajennokset, jolla symlinkit ja muut unix-tiedostojärjestelmien erikoisuudet toimivat
- Samba-tiedostojärjestelmän mounttaamiseen tarvitaan aina autentikointi
  - Kerberos + AD tai salana
- *pam_mount* PAM-moduli mahdollisesti toteuttaa tiedostojärjestelmän mounttauksen login-prosessin aikana