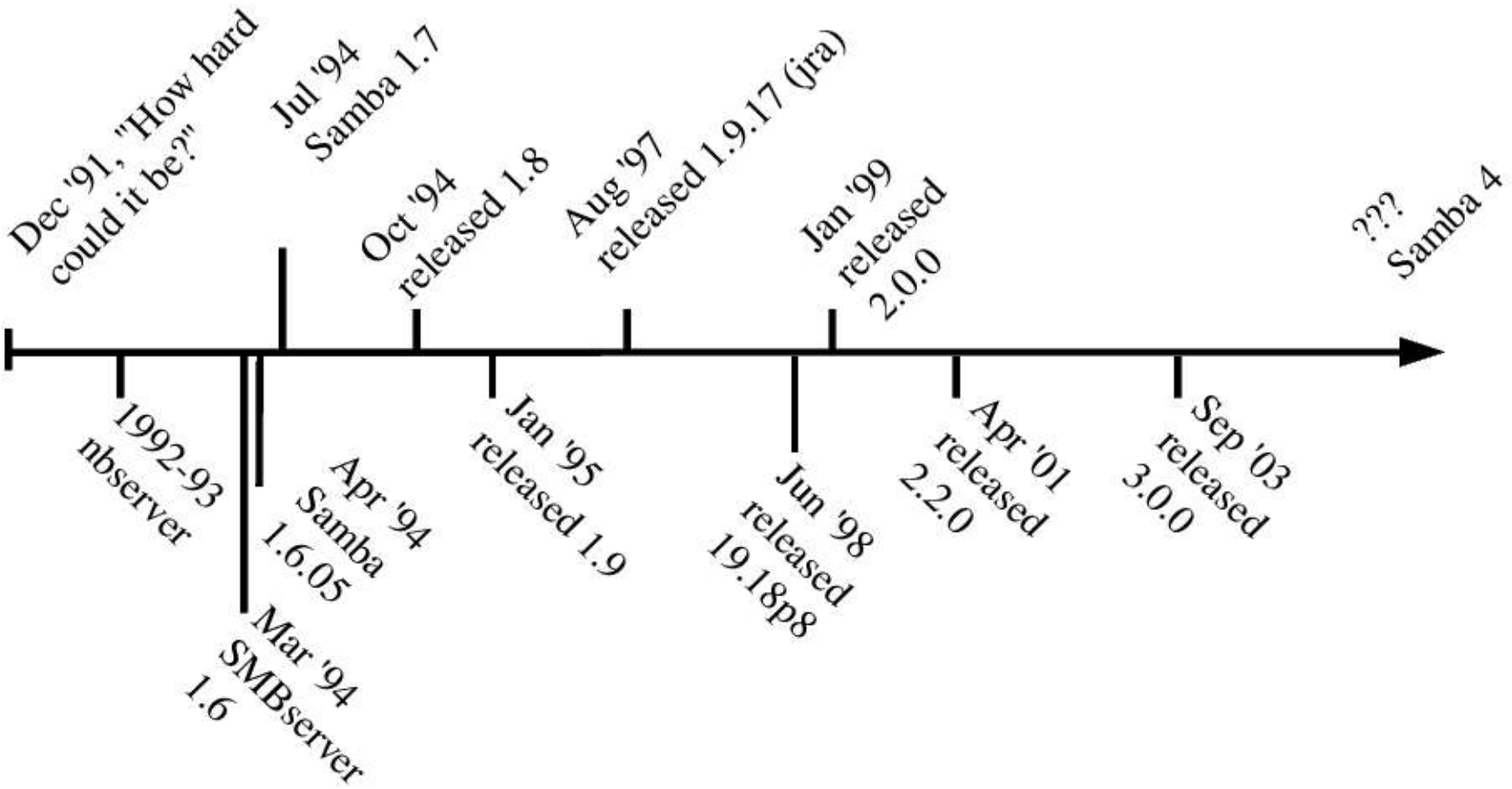
Samba 3
Integracija Unixa i Windowsa

Slobodan Milnović @srce.hr

Sadržaj

- Prošlost
- Što Samba 3 jest, a što nije?
- 5 minuta do uspjeha
- Za uspjeh ipak treba malo više
- Ispis pomoću sambe
- Migracije i nadogradnje
- Što ako...?
- Budućnost
- Pitanja

Prošlost


Dec '91, "How hard could it be?"
Jul '94 Samba 1.7
Oct '94 released 1.8
Aug '97 released 1.9.17 (jra)
Jan '99 released 2.0.0
??? Samba 4
1992-93 nbserver
Mar '94 SMBserver 1.6
Apr '94 Samba 1.6.05
Jan '95 released 1.9
Jun '98 released 19.18p8
Apr '01 released 2.2.0
Sep '03 released 3.0.0

Što samba 3 jest?

- Kerberos 5 i LDAP u sklopu Active Directory Domain
- UNICODE podrška
- Bolja podrška za MS-RPC ispis
- Migracija korisnika i grupa s WinNT4 domena

Što samba 3 jest?

- Slojeviti VFS (Virtual File System)
- Više mogućnosti autentifikacije i skladištenja korisničkih računa
- Poboljšani winbind
- Podrška za 32-bitne NT kodove stanja

Što samba 3 jest?

- Nedavno dodane mogućnosti
  - 3.0.3
    - Spremanje DOS atributa u EA (extended atributes)
    - EA podrška za OS/2 i Mac OS X
    - Podrška za zaključavanje lozinki na Samba DC
    - Podrška za podgrupe (Windows local groups)
  - 3.0.6
    - Povijest lozinki

Što samba 3 jest?

- Nedavno dodane mogućnosti
  - 3.0.11
    - Korisnička prava
    - Poboljšane winbind performanse
- Samba 3.0.x za x >= 11
  - Ispravke grešaka...

Što samba 3 nije?

- SAM replikacija s WinNT4 DC
  - Samba ne može biti BDC ako je PDC NT i obrnuto
  - Samba ne može replicirati korisničke podatke drugim MS BDC-ima
- Windows 200x/XP MMC
  - Nije moguće koristiti Computer Management Console za upravljanje sambom

Što samba 3 nije?

- Windows 2000 DC
  - Eksperimentalna podrška za Active Directory Domain Control
  - “Privatna” proširenja LDAP, DHCP i Kerberos protokola
  - Machine policy
  - Group Policy Objects
  - AD logon skripte
  - Dodjela pojedinih aplikacija pojedinim korisnicima i/ili grupama

5 minuta do uspjeha

- Instalacija
- Osnove samba postavki
  - Vrste servera i sigurnosnih postavki
  - Domain Controller i Backup Domain Controller
  - Član domene
  - Samostalni serveri
  - Postavljanje MS Windows mreže

Instalacija

- Source kod
  - http://www.samba.org
- Već gotovi CARNet debian paketi
  - apt-get install samba-cn
- Dodatni paketi
  - apt-get install openldap-cn
  - krb5 ili heimdal kerberos implementacija

Instalacija

- Anonimni read-only server

```
[global]
workgroup = MIDEARTH
netbios name = HOBBIT
security = share

[data]
comment = data
path = /export
read only = Yes
guest ok = Yes
```

Instalacija

- Anonimni print server

```
[global]
workgroup = MIDEARTH
netbios name = LUTHIEN
security = share
printcap name = cups
disable spoolss = Yes
show add printer wizard = No
printing = cups
[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = No
```

Vrste servera i sigurnosnih postavki

- Domain Controller
  - Primary Domain Controller
  - Backup Domain Controller
  - ADS Domain Controller
- Domain Member Server
  - Active Directory Domain Server
  - NT4 Domain Server
- Stand-alone Server

Vrste servera i sigurnosnih postavki

- Sigurnosna postavka *User*
  - *security = user*
  - *Autentikacija korisnika*
- Sigurnosna postavka *Share*
  - *security = share*
  - *Default user*
- Domain security mode
  - *security = domain*
  - *workgroup = MIDEARTH*

Vrste servera i sigurnosnih postavki

- ADS sigurnosna postavka
  - *realm = neki.kerberos.REALM*
  - *security = ADS*
  - *password server = neki.kerberos.server*
- *Server sigurnosna postavka (zastarjelo)*
  - *encrypt passwords = Yes*
  - *security = server*
  - *password server = "NetBIOS_ime_DCa"*

Domain Controller

- Domain Controller je SMB/CIFS server koji:
  - se registrira i javlja kao takav pomoću
    - NetBIOS broadcast ili
    - Mailslot Broadcast putem UDP broadcasta ili
    - WINS serveru putem UDP unicasta ili
    - DNS u sklopu Active Directory sustava
  - Nudi NETLOGON uslugu
  - Nudi share NETLOGON
- SSO - Single Sign On

Domain Controller

- Primary Domain Controller
- Backup Domain Controller
- Domain Member
- ADS Domain Controller

Domain Controller

- Nužni uvjeti za sambu 3 kao NT4 PDC za MS Windows NT4/200x/XP Professional klijente
  - Postavljeno osnovno TCP/IP i MS Win umrežavanje
  - Ispravno postavljanje uloge servera (*security = user)*
  - *Cjelovita i ispravna postavka Name Resolution sustava*
  - *Domain logon za Win NT4/200x/XP klijente*

Domain Controller

- Nužni uvjeti za sambu 3 kao NT4 PDC za MS Windows NT4/200x/XP Professional klijente (nastavak)
  - Postavljanje Roaming profila ili eksplicitna uporaba lokalnih profila
  - Postavljanje network/system policy
  - Dodavanje i upravljanje domenskim korisničkim računima
  - Postavljanje MS Win klijenata kao članove domene

Domain Controller

- Nužni uvjeti za sambu 3 kao NT4 PDC za MS Windows 9x/ME/XP Home klijente
  - Postavljeno osnovno TCP/IP i MS Win umrežavanje
  - Postavka uloge servera (*security = user)*
  - *Network logon – MS Win 9x/ME/XP home klijenti nisu u mogućnosti biti punopravni članovi domene*
  - *Postavljanje Roaming profila*

Domain Controller

- Nužni uvjeti za sambu 3 kao NT4 PDC za MS Windows 9x/ME/XP HOME klijente (nastavak)
  - Postavljanje rada sa System Policy
  - Instalacija mrežnog upravitelja *“Client for MS Windows Networks” i postavljanje spajanja na domenu*
  - *Postavljanje navedenih klijenata u User način sigurnosti*
  - *Dodavanje i upravljanje domenskim korisničkim računima*

Domain Controller

- Kako radna stanica nalazi DC?
  - NetBIOS putem TCP/IP omogućen (domena MIDEARTH)
    - NetBIOS upit za ime grupe MIDEARTH<#1c>
    - Svaki vraćeni rezultat je DC
    - Autentifikacija radne stanice i DC (kerberos)
    - Nakon uspješne autentifikacije, šalju se korisničko ime i lozinka radi autentifikacije korisnika

Domain Controller

- Kako radna stanica nalazi DC (nastavak)?
  - NetBIOS putem TCP/IP onemogućen (realm quenya.org)
    - Upit DNS serveru za zapis *_ldap._tcp.pdc._msdcs.quenya.org*

Backup Domain Controller

- Samo ako je password backend LDAP
  - PDC + BDC -> jedan centralni LDAP server
  - PDC -> LDAP master, BDC -> LDAP slave
  - PDC -> LDAP master + sekundarni LDAP slave
    BDC -> LDAP master + sekundarni LDAP slave
  - PDC -> LDAP master + sekundarni LDAP slave
    BDC -> LDAP slave + sekundarni LDAP master
- Samba 3 ne može biti BDC u MS Win 200x Active Directory domeni niti za NT4 PDC

Član domene

- Samba 3 može biti *native member server* u
  - MS Windows NT4 domeni
  - MS Windows Active Directory Domain
  - Samba Domain Control

Član domene

- Zašto biti član domene?
  - Korisnici MS Win radnih stanica imaju mogućnost SSO
  - Korisnička prava pristupa, vlasništvo i prava pristupa nad datotekama iz jedinstvene Domain Security Account Manager baze
  - Samo MS Win NT4/200x/XP Professional radne stanice koje su članovi domene mogu koristiti network logon mogućnosti

Član domene

- Zašto biti član domene (nastavak) ?
  - Lakše je upravljati radnim stanicama koje su članovi domene putem Policy datoteka (NTConfig.POL) i Desktop profila
  - Korištenjem logon skripti korisnici imaju transparentan pristup mrežnim aplikacijama pokretanim s aplikacijskih servera
  - Lakše upravljanje aplikacijama i korisnicima putem jedinstvene baze

Član domene

- Machine Trust Account
  - Autentificira klijent računalo (a ne korisnika), smije li računalo pristupiti domeni
  - MS Win NT4 ih sprema u registry
  - MS Win 200x ih sprema u AD

Član domene

- Machine Trust Account
  - Samba PDC ih sprema u dva dijela
    - Domain Security Account – passdb backend definiran u smb.conf
      - stariji – smbpasswd baza – Unix login ID, Unix user ID (UID), LanMan i NT kriptirane lozinke
      - noviji – tdbsam i ldapsam
    - Odgovarajući Unix korisnički račun, tipično u /etc/passwd, “prazna” i zaključana lozinka, ime računa je ime_klijent_računala$ - znak “$” je obavezan, ali na nekim implementacijama Unixa zahtjeva unos putem editora (npr. FreeBSD)

Član Domene

- Machine Trust Account – kreiranje
  - "Ručno"
    - *useradd -g machines -d /var/lib/nobody -c "nadimak \ računala" -s /bin/false ime_računala$*
    - *passwd -l ime_računala$*
  - *NT4 Server Manager*
    - *potrebna skripta za dodavanje računala*
    - *SRVTOOLS.EXE ili Nexus.exe*
  - *On-The-Fly (preporučeno)*
    - *[global]*
      add machine script = /usr/sbin/useradd -d /var/lib/nobody \ -g 100 -s /bin/false -M %u

Član Domene

- Autentifikacija putem Windows 200x kerberos DC-a
  - *realm = neki.kerberos.REALM*
    security = ADS
    encrypt passwords = yes
  - *U slučaju da samba ne uspije prepoznati kerberos DC*
    password server = neki.kerberos.server

Član Domene

- Spajanje računala u domenu
  - *net ads join -U Administrator%lozinka*
- *Spajanje računala u organizacijsku jedinicu*
  - *kinit Administrator@neki.kerberos.REALM*
    net ads join "organizacijska_jedinica"
- *Spajanje na kontainer "Servers" u sklopu organizacijskog direktorija "Computers\BusinessUnit\Department"*
  - *net ads join "Computers\BusinessUnit\Department\Servers"*

Stand-alone server

- Najčešće kao file i print serveri
- Nije potrebna kompleksna konfiguracija
- Nije potreban network logon

Za uspjeh ipak treba malo više

- Network browsing
- Baze podataka o korisnicima
- Rad s Windows i Unix grupama
- Identity Mapping – IDMAP
- Korisnička prava
- Pristup datotekama, mapama, shareovima
- Zaključavanje datoteka i zapisa
- Sigurnost

Za uspjeh ipak treba malo više

- Odnosi povjerenja među domenama
- MS DFS (Distributed File System)
- VFS (Virtual File System) moduli
- Winbind – korisnički računi u domeni
- System i account policy
- Desktop profile management
- Backup

Network browsing

- Što je browsing i kako izgleda?
- NetBIOS putem TCP/IP
- TCP/IP bez NetBIOS-a
- DNS i AD
- Workgroup browsing
  - Domain Master Browser
  - Local Master Browser

Network browsing

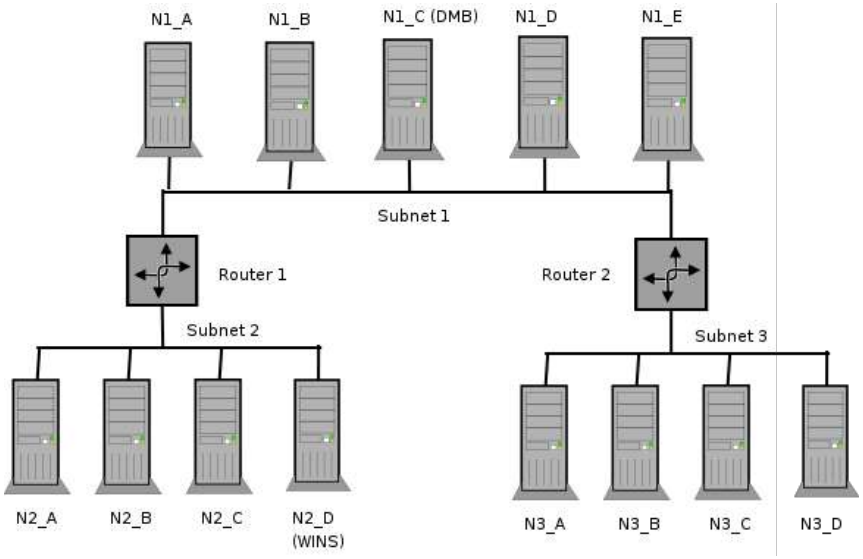
- Domain Master Browser
  - ***[global]***
    domain master = yes
    local master = yes
    preferred master = yes
    os level = 65
- ***Local Master Browser***
  - ***[global]***
    domain master = no
    local master = yes
    preferred master = yes
    os level = 65

Network browsing

- WINS server
  - *[global]*
    wins support = yes
- *Statički unos WINS elemenata*
  - */usr/local/samba/var/locks/wins.dat ili / var/run/samba/wins.dat*
    - *“IME#TIP” TTL ADRESA+ ZASTAVICE*
      - *Dinamički zapis*
        “PERO#03” 1055208278 192.168.1.2 66R
      - *Statički zapis*
        “PERO#03” 0 192.168.1.2. 66R

Network browsing

- Cross-subnet browsing

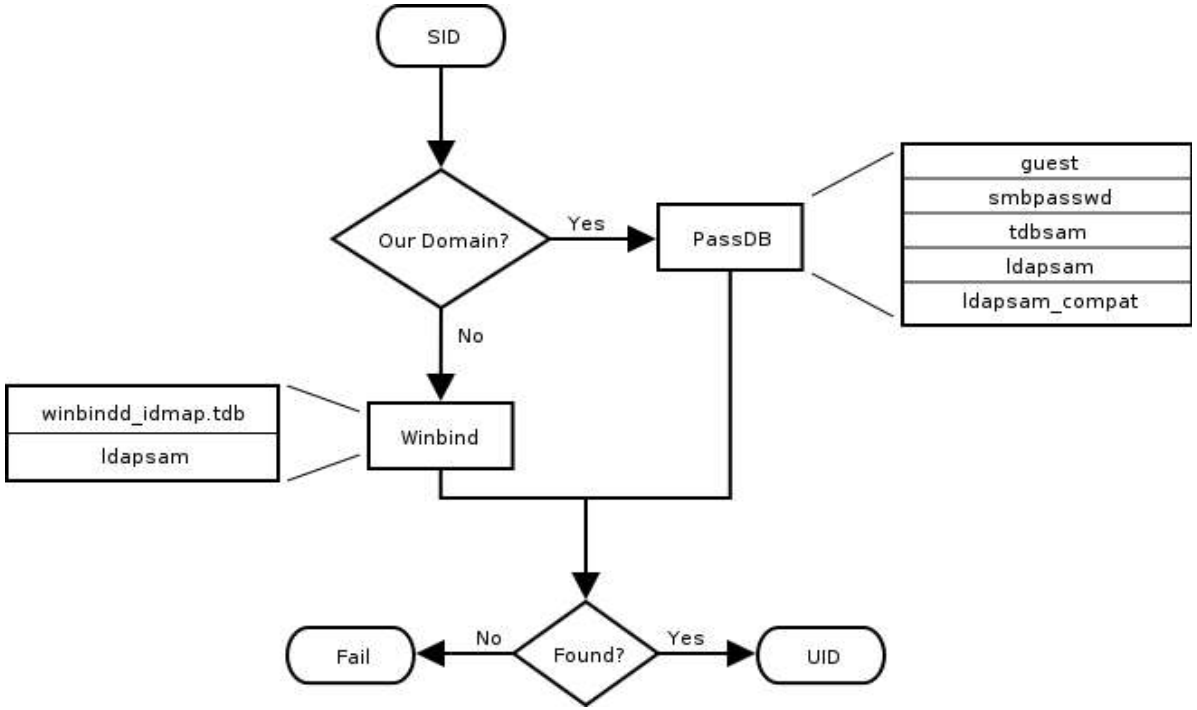


Baze podataka o korisnicima

- Plain text
  - Prije - /etc/samba/smbpasswd ili /etc/smbpasswd
  - Danas – PAM
- smbpasswd
- ldapsam_compat – Samba 2.2
- tdbsam
- ldapsam
- mysqlsam ili pgsqlsam
- XML

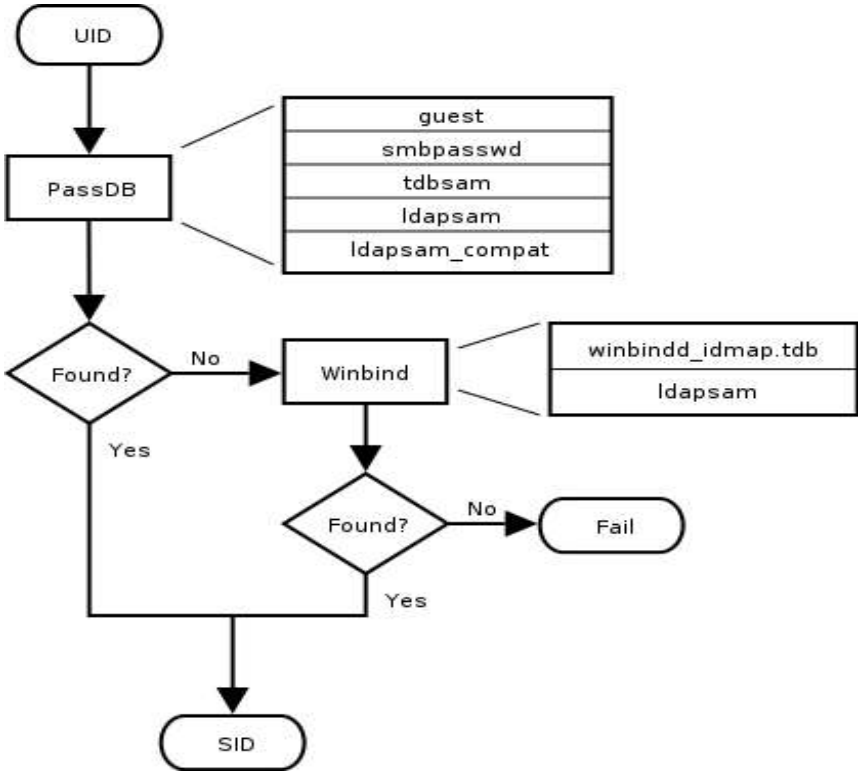
Baze podataka o korisnicima

- IDMAP – pretvaranje SID u UID



Baze podataka o korisnicima

- IDMAP – pretvaranje iz UID u SID



Baze podataka o korisnicima

- ldapsam - OpenLDAP i Sun iPlanet Directory Server
  - http://www.unav.es/cti/ldap-smb/ldap-smb-3-howto.html
  - *cp samba.schema /etc/openldap/schema/*
    - *## /etc/openldap/slapd.conf*
      ## schema files (core.schema is required by default)
      include /etc/openldap/schema/core.schema
      ## needed for sambaSamAccount
      include /etc/openldap/schema/cosine.schema
      include /etc/openldap/schema/inetorgperson.schema
      include /etc/openldap/schema/nis.schema
      include /etc/openldap/schema/samba.schema

Baze podataka o korisnicima

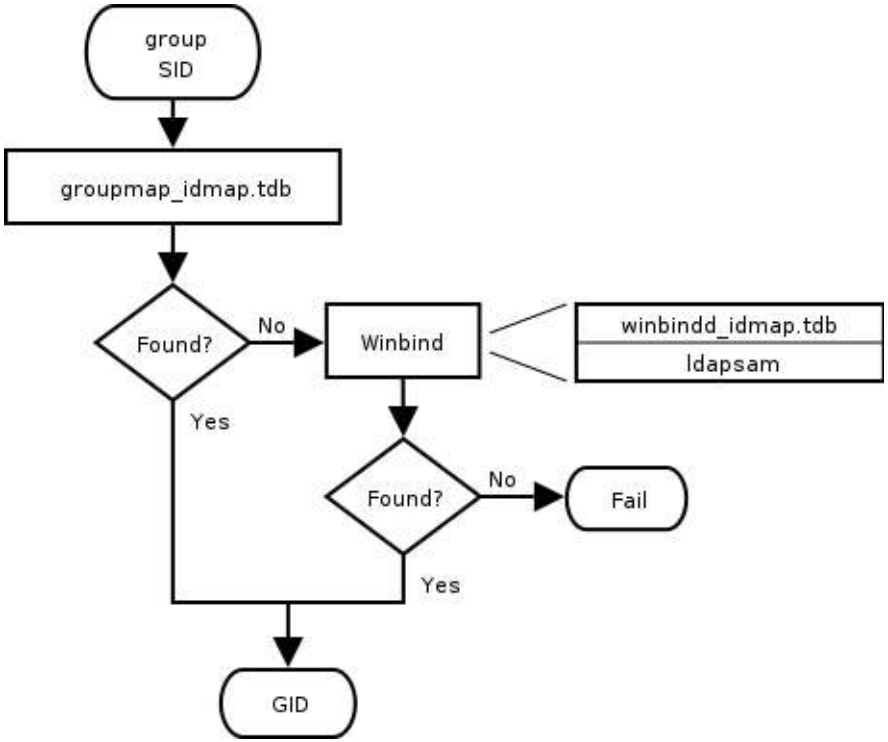
- ldapsam
  - *./sbin/slapindex -f slapd.conf*
  - */etc/init.d/slapd restart*
  - *Kreiranje accoun kontainera putem LDIF datoteke*
  - *slapadd -v -l initldap.dif*

Baze podataka o korisnicima

- ldapsam
  - *[global]*
    security = user
    encrypt passwords = yes
    netbios name = MORIA
    workgroup = NOLDOR
    ldap admin dn = "cn=Manager,dc=quenya,dc=org"
    ldap ssl = start tls
    passdb backend = ldapsam:ldap://frodo.quenya.org
    ldap delete dn = no
    ldap user suffix = ou=People
    ldap group suffix = ou=Groups
    ldap machine suffix = ou=Computers
    ldap suffix = dc=quenya,dc=org
    ldap filter = (uid=%u)

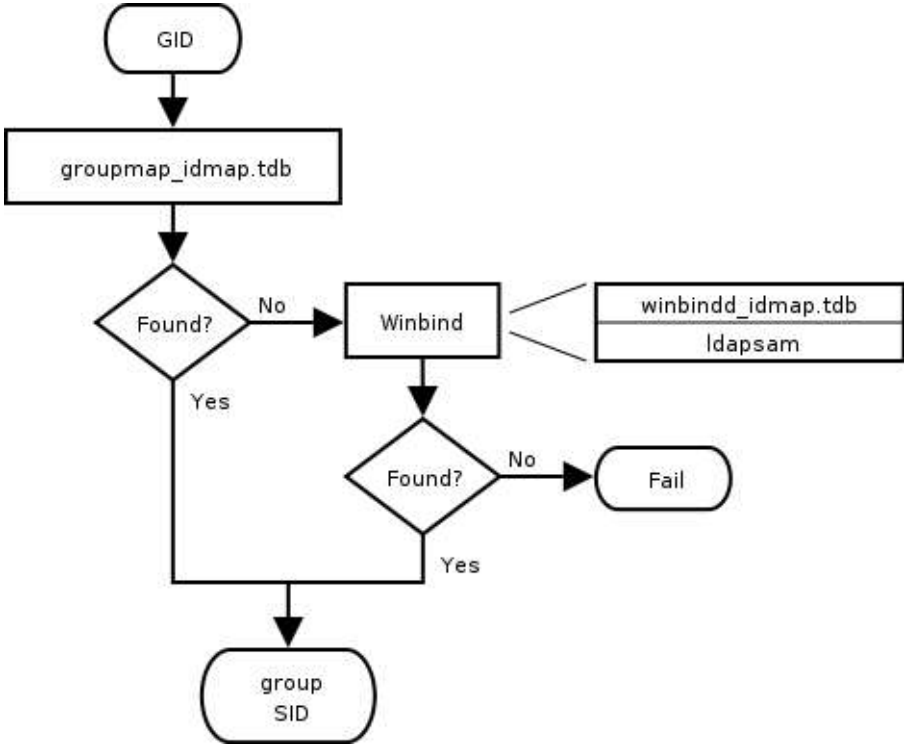
Rad s Windows i Unix grupama

- IDMAP – iz SID u GID



Rad s Windows i Unix grupama

- IDMAP – iz GID u SID



Unix grupa

- Kreiranje Unix grupe *domadm u /etc/group*
  - *domadm:x:502:joe,john,mary*
  - *net groupmap add ntgroup="Domain Admins" unixgroup=domadm*
  - *net groupmap add rid=1000 ntgroup="Accounting" unixgroup=acct*
  - *net groupmap list*

Identity mapping - IDMAP

- Podsustav mapiranja između MS Windows SID (Security Identifiers) i Unix UID (User Identifier) i GID (Group Identifier)
- Način uporabe ovisi o serverskom modelu koji se koristi:
  - Stand-Alone
  - Domain Member Server/Client
  - Primary Domain Controller
  - Backup Domain Controller

Identitiy mapping - IDMAP

- Stand-Alone
  - Korisnici i grupe lokalno na serveru
  - Identitet mrežnog korisnika mora odgovarati lokalnom Unix/Linux korisniku
  - Nisu potrebni ni IDMAP ni winbind

Identity mapping - IDMAP

- Domain Member Server/Client
  - Winbind se ne koristi, korisnici i grupe lokalni
  - Winbind se ne koristi, pristup korisnicima i grupama putem NSS
  - Winbind/NSS sa lokalnom IDMAP tablicom
  - Winbind/NSS pomoću RID (Relative Identifier) IDMAP
  - Winbind s NSS/LDAP baziranim IDMAP
  - Winbind s NSS za razdiobu Unix/Linux UID/GID

Identity mapping - IDMAP

- Primary Domain Controller
  - Samba izračunava jedinstveni SID za UID/GID kombinacije - *“algorithmic mapping”*
  - *algorithmic rid base = 1000*
  - *RID = (2 x UID ili GID) + algoritamski RID*
  - *Generira se SID računala i domene i dodaje mu se izračunati RID*
    - *aRID = 1000, UID = 4321, dSID = S-1-5-21-89238497-92787123-12341112*
      RID = 2 x 4321 + 1000 = 9642
      konačni SID = S-1-5-21-89238497-92787123-12341112-9642

Identity mapping - IDMAP

- Backup Domain Server
  - Read-only pristup u LDAP repozitorij
  - Promjene se šalju PDC-u, jedino on ima pravo mjenjati korisničke podatke
  - Podatci se mogu upisati u LDAP server, ako svi DC imaju pristup master LDAP serveru.
  - Samba 3 nije u stanju obraditi zahtjeve za LDAP preusmjeravanje u IDMAP podsustavu, ne preporuča se korištenje LDAP slave (replicate) servera.

Identity mapping - IDMAP

- Primjer korištenja winbinda
  - NT4 Domene
    - smb.conf

[global]
workgroup = MEGANET2
security = DOMAIN
idmap uid = 10000-20000
idmap gid = 10000-20000
template primary group = "Domain Users"
template shell = /bin/bash

    - /etc/nsswitch

passwd: files winbind
shadow: files winbind
group: files winbind
hosts: files wins
...

Identity mapping - IDMAP

- Primjer korištenja winbinda
  - NT4 domene
    - *root# net rpc join -UAdministrator%password*
      Joined domain MEGANET2.
      root# net rpc testjoin
      Join to 'MIDEARTH' is OK

    - *Situacija s greškom*
      root# net rpc testjoin
      [2004/11/05 16:34:12, 0] utils/net_rpc_join.c:net_rpc_join_ok(66)
      Join to domain 'MEGANET2' is not valid
    - *Nakon uspješnog postavljanja, pokrenuti **nmbd**, **winbind** i **smbd** u navedenom redosljedu.*

Identity mapping - IDMAP

- Primjer korištenja winbinda
  - ADS
    - smb.conf

[global]
workgroup = BUTTERNET
netbios name = GARGOYLE
realm = BUTTERNET.BIZ
security = ADS
template shell = /bin/bash
idmap uid = 500-10000000
idmap gid = 500-10000000
winbind use default domain = Yes
winbind nested groups = Yes
printer admin = "BUTTERNET\Domain Admins"

Identity mapping - IDMAP

- Primjer korištenja winbinda
  - ADS
    - /etc/nsswitch

      passwd: files winbind
      shadow: files winbind
      group: files winbind
      hosts: files wins
      ...
    - *root# net ads join -UAdministrator%password*
      Joined domain BUTTERNET.
      root# net ads testjoin
      Using short domain name -- BUTTERNET
      Joined 'GARGOYLE' to realm 'BUTTERNET.BIZ'

Identity mapping - IDMAP

- Primjer korištenja winbinda
  - ADS
    - Greška pri spajanju u domenu
      root# net ads testjoin
      GARGOYLE$@'s password:
      [2004/11/05 16:53:03, 0] utils/net_ads.c:ads_startup(186)
      ads_connect: No results returned
      Join to domain is not valid
    - Nakon uspješnog postavljanja, pokrenuti ***nmbd***, ***winbind*** i ***smbd*** u navedenom redosljedu.

Identity mapping - IDMAP

- IDMAP skladište u LDAP-u putem winbind
  - Primjer za ADS
    - smb.conf

```
[global]
workgroup = SNOWSHOW
netbios name = GOODELF
realm = SNOWSHOW.COM
server string = Samba Server
security = ADS
log level = 1 ads:10 auth:10 sam:10 rpc:10
ldap admin dn = cn=Manager,dc=SNOWSHOW,dc=COM
ldap idmap suffix = ou=Idmap
ldap suffix = dc=SNOWSHOW,dc=COM
idmap backend = ldap:ldap://ldap.snowshow.com
idmap uid = 150000-550000
idmap gid = 150000-550000
template shell = /bin/bash
winbind use default domain = Yes
```

Identity mapping - IDMAP

- IDMAP skladište u LDAP-u putem winbind
  - Primjer za ADS
    - MIT Kerberos - /etc/krb5.conf

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
default_realm = SNOWSHOW.COM
dns_lookup_realm = false
dns_lookup_kdc = true
[appdefaults]
pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false }
```

Identity mapping - IDMAP

- IDMAP skladište putem LDAP-a u winbindu
  - Primjer za ADS
    - Heimdal Kerberos - /etc/krb5.conf

```
[libdefaults]
        default_realm = SNOWSHOW.COM
         clockskew = 300
[realms]
         SNOWSHOW.COM = {
                kdc = ADSDC.SHOWSHOW.COM
         }
[domain_realm]
         .snowshow.com = SNOWSHOW.COM
```

Identity mapping - IDMAP

- IDMAP skladište putem LDAP-a u winbindu
  - Primjer za ADS
    - /etc/nsswitch
      passwd: files ldap
      shadow: files ldap
      group: files ldap
      hosts: files wins

Identity mapping - IDMAP

- IDMAP skladište putem LDAP-a u winbindu
  - Primjer za ADS
    - Potrebno je skinuti **nss_ldap alat sa http://www.padl.com/**
    - **/etc/ldap/ldap.conf**

host 192.168.2.1
base dc=snowshow,dc=com
binddn cn=Manager,dc=snowshow,dc=com
bindpw not24get
pam_password exop
nss_base_passwd ou=People,dc=snowshow,dc=com?one
nss_base_shadow ou=People,dc=snowshow,dc=com?one
nss_base_group ou=Groups,dc=snowshow,dc=com?one
ssl no

Identity mapping - IDMAP

- IDMAP skladište putem LDAP-a u winbindu
  - Primjer za ADS
    - **U postojeći LDAP ubaciti slijedeći LDIF**

dn: dc=snowshow,dc=com
objectClass: dcObject
objectClass: organization
dc: snowshow
o: The Greatest Snow Show in Singapore.
description: Posix and Samba LDAP Identity Database
dn: cn=Manager,dc=snowshow,dc=com
objectClass: organizationalRole
cn: Manager
description: Directory Manager
dn: ou=Idmap,dc=snowshow,dc=com
objectClass: organizationalUnit
ou: idmap

Identity mapping - IDMAP

- IDMAP skladište putem LDAP-a u winbindu
  - Primjer za ADS
    - ***root# net ads testjoin***
      Using short domain name -- SNOWSHOW
      Joined 'GOODELF' to realm 'SNOWSHOW.COM'
    - ***Nakon uspješnog spajanja, treba pokrenuti nmbd, winbind, i smbd u navedenom redosljedu.***

Korisnička prava

- Ime računala, za razliku od imena korisnika, završava sa znakom “$”
- Do Samba 3.0.10 ADS administratorski račun mapiran na Unix root račun. Od 3.0.11 podržan Windows privilege model.
- Podržana prava:
  - SeMachineAccountPrivilege – dodavanje računala u domenu
  - SePrintOperatorPrivilege – upravljanje pisačima
  - SeAddUsersPrivilege – dodavanje korisnika i grupa u domenu
  - SeRemoteShutdownPrivilege – gašenje s udaljenog računala
  - SeDiskOperatorPrivilege – upravljanje disk share

Korisnička prava

- net rpc rights – samba 3.0.11
  - list [name|accounts]
  - grant <user> <right [right...]>
    - *root# net -S server -U domadmin rpc rights grant 'DOMAIN\Domain Admins' SeMachineAccountPrivilege*
  - *revoke <user> <right [right...]>*
- *Za korištenje ovih mogućnosti potrebno je biti član grupe Domain Admins. Ta mogućnost "ugrađena" je u Domain Admins group i ne može se promjeniti.*

Pristup datotekama, mapama, shareovima

- Metode upravljanja:
  - Dozvole pristupa Unix datoteka i direktorija
  - Samba Share definicije
  - Samba Share ACL (Access Control List)
  - MS Windows ACL putem Unix POSIX ACL

Pristup datotekama, mapama, shareovima

- Razlike Unix i MS Win datotečnih sustava
  - Name space
    - MS – 254 znaka, ekstenzija označava tip datoteke, folder
    - Unix – 1024 znaka, proizvoljne ekstenzije, direktorij
  - Case Sensitivity
    - MS – velika slova, 8.3, duža imena čuvaju case no svejedno je
    - Unix – čuvaju case i nije svejedno koja su slova
      - Imena datoteka jedinstvena za Unix ali ista za MS
        - MYFILE.TXT, MyFile.txt, myfile.txt
      - Samba zanemaruje sve osim abecedno prve datoteke

Pristup datotekama, mapama, shareovima

- Razlike Unix i MS Win datotečnih sustava
  - Znak razdvajanja direktorija
    - MS - \
    - Unix - /
  - Oznaka particija
    - MS – C: D: E: ...
    - Unix logički koristi jedinstveno stablo datotečnog sustava
  - Konvencije naziva datoteka
    - MS – . na početku imena datoteke nebitna
    - Unix - . na početku imena datoteke označava skrivenu datoteku (najčešće u korisničkom poddirektoriju)

Pristup datotekama, mapama, shareovima

- Razlike Unix i MS Win datotečnih sustava
  - Link i shortcut
    - MS – posebne datoteke koje preusmjeravaju pristup na pravu datoteku, ne poznaje koncept hard linka
    - Unix – simbolički linkovi sadrže odgovarajuću lokaciju podataka (datoteka ili direktorij). Pisanje i/ili čitanje će se obaviti na konkretnim podatcima. Hard link – jedna fizička datoteka s više imena, obriše li se jedno, obrisani su svi.

Pristup datotekama, mapama, shareovima

- Dozvole pristupa Unix datoteka i direktorija
  - (r)read
  - (w)write
  - (x)execute
  - (d)directory
  - (l)link
  - (s)set UID/GID
  - (t)sticky
  - (c)character device, (b)block device, (p)pipe device, (s) Unix Domain socket

Pristup datotekama, mapama, shareovima

- Samba Share definicije
  - Za korisnike i grupe
    - admin users
    - force group
    - force user
    - guest ok
    - invalid users
    - only user
    - read list
    - username
    - valid user
    - write list

Pristup datotekama, mapama, shareovima

- Samba Share definicije
  - Za datoteke i direktorije
    - create mask
    - directory mask
    - dos filemode
    - force create mode
    - force directory mode
    - force directory security mode
    - force security mode
    - hide unreadable
    - hide unwriteable files
    - nt acl support
    - security mask

Pristup datotekama, mapama, shareovima

- Samba Share definicije
  - Ostale naredbe
    - case sensitive, default case, short preserve case
    - csc policy
    - dont descend
    - dos filetime resolution
    - dos filetimes
    - fake oplocks
    - hide dot files, hide files, veto files
    - read only
    - veto files

Pristup datotekama, mapama, shareovima

- Samba Share ACL
  - Trenutno ne postoji samba alat koji bi dodjeljivao prava pristupa shareovima, moguće jedino pomoću NT4 Server Manager ili Windows 200x MMC
  - Postavke se spremaju u *share_info.tdb*, standardna postavka u Debianu je */var/lib/samba/var/share_info.tdb*
  - Pomoću tdbdump moguće je pogledati sadržaj *share_info.tdb*

Pristup datotekama, mapama, shareovima

- MS Windows ACL putem Unix POSIX ACL
  - MS Windows klijenti mogu pristupiti i mjenjati Unix dozvole.
  - MS Windows ACL je detaljniji od POSIX ACL-a, no Samba se pridržava samo POSIX mogućnosti.
  - Auditing putem MS Windows klijenata zasad nije podržan
  - Take Ownership putem GUI nije trenutno moguće, jer pod Unixom samo root može mjenjati vlasništvo nad datotekama.
  - NT chown naredba, no može ju izvršiti samo korisnik s Administrator pravima spojen na Samba server kao root. Taj alat je u sklopu Seclib NT paketa, dostupnog sa Samba FTP-a.

Pristup datotekama, mapama, shareovima

- MS Windows ACL putem Unix POSIX ACL
  - Moguće je mjenjati dozvole nad datotekama i poddirektorijima s MS Windows klijenata, pod uvjetom da je u smb.conf
    nt acl support = yes
  - *Samba create mask parametri*
    - *security mask*
    - *force security mode*
    - *directory security mask*
    - *force directory security mode*

Zaključavanje datoteka i zapisa

- Record locking – dijelovi datoteke
  - MS Windows podržava 2^32 do 2^64 byte locking ovisno o klijentu, Unix samo do 2^32.
  - Samba zaključava zapise samo ako to klijent zatraži, ali ako je *strict locking = yes provjerava se stanje za svako pisanje i čitanje*
- Deny modes – cijela datoteka
  - DENY_NONE, DENY_READ, DENY_WRITE, DENY_ALL
  - Posebni modovi DENY_FCB, DENY_DOS

Zaključavanje datoteka i zapisa

- Oportunistic locking (oplock) – keširanje datoteka na klijentu omogućuje
  - Read-ahead
    - Klijent čita lokalnu kopiju datoteke
  - Write caching
    - Klijent piše u lokalnu kopiju datoteke
  - Lock caching
    - Klijent drži podatke o zaključavanju lokalno
- Samba standardno ima uključen oplock
  - *oplocks = yes*

Zaključavanje datoteka i zapisa

- 4 vrste Windows oplocka
  - Level1 Oplock
    - Čitanje i pisanje na lokalnom klijentu
  - Level2 Oplock
    - Čitanje na lokalnom klijentu
  - Filter Oplock
    - Onemogućeno pisanje i brisanje datoteka
  - Batch Oplock
    - Upravljanje otvaranjem i zatvaranjem datoteka, te keširanje atributa datoteka

Zaključavanje datoteka i zapisa

- Oplock – koristiti ili ne?
  - Ekskluzivan pristup shareovima
    - Keširanje se vrši na lokalnom klijentu, svaki klijent ekskluzivno pristupa podatcima, nema višestrukih zahtjeva za datotekama
    - Direktoriji/datoteke korisnika u home direktorijima
  - Datoteke i shareovi nad kojima postoji više zahtjeva
    - Slanje zahtjeva za uspostavom i prekidom oplocka
    - Usporenje pristupa zbog brisanja oplock keša
    - Svaki novi zahtjev dodatno usporava rad

Zaključavanje datoteka i zapisa

- Oplock – koristiti ili ne?
  - Datoteke kojima se pristupa putem Unix i/ili NFS klijenata
    - Nisu u stanju poslati i primati oplock zahtjeve, i moguć je sukob s MS Win klijentima, a samim time i oštećenje podataka
  - Spore i/ili nepouzdane mreže
    - Prednost, jer korisnik nesmetano može raditi s podatcima lokalno
    - Mana, pouzdanost oplock mehanizma pada, jer obrada zaključavanja ovisi o ispravnom radu mreže

Zaključavanje datoteka i zapisa

- Oplock – koristiti ili ne?
  - Višekorisničke baze podataka
    - Velika opterećenost, česti pristupi različitih korisnika, problemi s oplock mehanizmom
  - PDM (Process Data Management) aplikacije – npr. IMAN, Enovia, Clearcase
    - Već imaju vlasiti mehanizam upravljanja pristupom podatcima

Zaključavanje datoteka i zapisa

- Oplock – koristiti ili ne?
  - Samba opcija *force user*
    - *Šalje se oplock break svaki put kad neki korisnik pristupa datoteci, u slučaju sporih ili nepouzdanih mreža opadaju performanse*
    - *Izbjegavati kombinacije force user, spora ili nepouzdana mreža i oplock*
  - *Napredni Samba oplock parametri*
    - *oplock break wait time i oplock contention limit – preporuka je ne mjenjati ako nije poznato kako točno samba oplock implementacija radi*

Zaključavanje datoteka i zapisa

- Oplock – koristiti ili ne?
  - Mission-Critical High-Availability
    - MS Windows klijenti ovise o uspostavljenoj TCP vezi. U slučaju prekida, različiti programi često nisu u stanju nsataviti rad, već zahtjevaju ponovno spajanje, što prolazi kroz oplock mehanizam, lokalni cache se prazni, a samim time i svi do tad postojeći podatci.
  - Za svaku situaciju poželjno je testiranje oplock funkcionalnosti prije konačne implementacije

Zaključavanje datoteka i zapisa

- Samba podržava i kernel oplock, podsustav koji omogućuje SMB i Unix/Linux klijentima pristup datotekama kroz locking mehanizam

- Trenutno kernel oplock podržavaju samo Linux i SGI IRIX. Standardno isključeno, uključuje se sa

  kernel oplocks = yes

Zaključavanje datoteka i zapisa

- Onemogućavanje oplocka - samba
  - Za pojedini share
    [acctdata]
    oplocks = False
    level2 oplocks = False
  - *Za pojedinu datoteku*
    veto oplock files = /.mdb/*.MDB/*.dbf/*.DBF/*

Zaključavanje datoteka i zapisa

- Onemogućavanje oplocka – MS Win, slijedeće registry vrijednosti treba promjeniti
  - Dodjela oplocka (ako je računalo data server)
    HKEY_LOCAL_MACHINE\System\
    CurrentControlSet\Services\MRXSmb\Parameters
    OplocksDisabled REG_DWORD 0 or 1
    Default: 0 (omogućeno)
  - *Traženje oplocka (ako je računalo klijent)*
    HKEY_LOCAL_MACHINE\System
    CurrentControlSet\Services\LanmanServer\Parameters
    EnableOplocks REG_DWORD 0 or 1
    Default: 1 (omogućeno)

    EnableOpLockForceClose REG_DWORD 0 or 1
    Default: 0 (onemogućeno)

Sigurnost

- Nekoliko stupnjeva zaštite
  - Host-Based
    - smb.conf
      hosts allow = 127.0.0.1 192.168.2.0/24 192.168.3.0/24
      hosts deny = 0.0.0.0/0
  - User-Based
    - smb.conf
      [global]
      valid users = @smbusers, jacko

Sigurnost

- Interface
  - smb.conf
    interfaces = eth lo*
    bind interfaces only = yes
- Firewall
  - UDP/137 - nmbd
  - UDP/138 - nmbd
  - TCP/139 - smbd
  - TCP/445 - smbd

Sigurnost

- IPC$ Share-Based
  - smb.conf
    [IPC$]
    hosts allow = 192.168.115.0/24 127.0.0.1
    hosts deny = 0.0.0.0/0
- NTLMv2
  - Slanje isključivo NTLMv2 odgovora
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
    "lmcompatibilitylevel"=dword:00000003
  - *Primanje isključivo NTLMv2 zahtjeva*
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0]
    "NtlmMinClientSec"=dword:00080000

Sigurnost

- **Redovna instalacija najnovijih patcheva**

Odnosi povjerenja među domenama

- Samba 3 može sudjelovati u Samba-Samba i Samba-NT4 odnosima povjerenja
- Za NT4 PDC/BDC domene
  - Lokalna domena SAMBA, udaljena domena RUMBA
    - *root# smbpasswd -a -i rumba*
      New SMB password: XXXXXXXX
      Retype SMB password: XXXXXXXX
      Added user rumba$
    - *Na NT4 Serveru, User Manager for Domains, Policies, Trust Relationship, Add tipka*

Odnosi povjerenja među domenama

- Za NT4 PDC/BDC domene (nastavak)
  - Lokalna domena SAMBA, udaljena domena RUMBA
    - Unijeti ime domene SAMBA i trust relationship lozinku
    - *Na samba serveru*
      root# net rpc trustdom establish rumba
    - *Unijeti trust relationship lozinku (ista kao i kod NT4), pričekati "Success" poruku (kod većih mreža može potrajati), nakon čega je povjerenje uspostavljeno.*
    - *Kod AD, ADC može uspostaviti trust, ali samba zasad ne može.*

MS DFS (Distributed File System)

symlinkovi moraju biti *lower case* – trenutno samba ograničenje.

root# cd /export/dfsroot
root# chown root /export/dfsroot
root# chmod 755 /export/dfsroot
root# ln -s msdfs:storageA\\shareA linka
root# ln -s msdfs:serverB\\share,serverC\\share linkb

smb.conf

[global]
netbios name = GANDALF
host msdfs = yes
[dfs]
path = /export/dfsroot
msdfs root = yes

VFS (Virtual File System) moduli

- VFS moduli omogućuju dodatnu funkcionalnost pri radu s Unix/Linux FS, koju možda Unix/Linux FS nema.
  - smb.conf

    [audit]
    comment = Audited /data directory
    path = /data
    vfs objects = audit recycle
    writeable = yes
    browseable = yes

VFS (Virtual File System) moduli

- smb.conf s više VFS modula

```
[test]
comment = VFS TEST
path = /data
writeable = yes
browseable = yes
vfs objects = example:example1 example
example:test
example1: parameter = 1
example: parameter = 5
test: parameter = 7
```

VFS (Virtual File System) moduli

- Moduli uključeni u Sambu
  - audit – praćenje pristupa datotekama upisom u syslog
    - share, connect/disconnect, directory open/create/remove, file open/close/rename/unlink/chmod
  - extd_audit – praćenje pristupa datotekama upisom u syslog i smbd log
  - fake_perms – postavlja Roaming Profile datoteke i direktorije u read-only mod, a klijentima javlja da su writeable.

VFS (Virtual File System) moduli

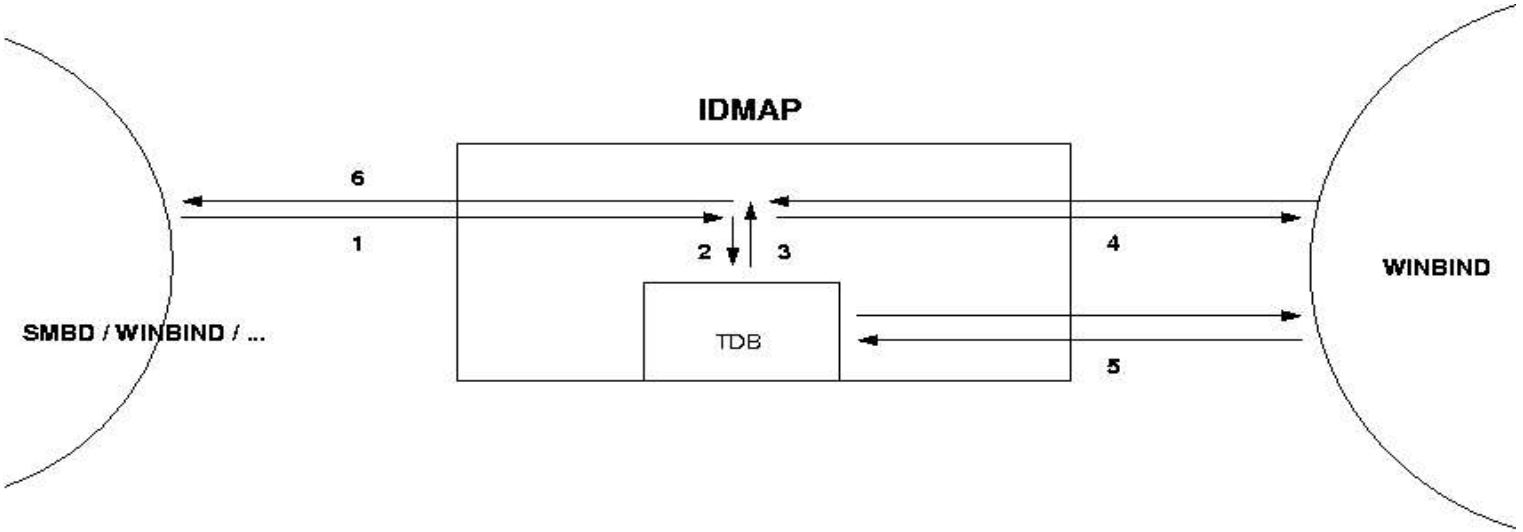
- Moduli uključeni u Sambu
  - recycle – simulira ponašanje Recycle Bin, datoteke se ne brišu nego prebacuju u postavljeni direktorij
  - netatalk – suživot Samba i netatalk usluga djeljenja datoteka (Apple Macintosh)
  - shadow_copy – simulira MS Shadow Copy funkcionalnost – nije još dovoljno testiran

Winbind

- Rješava unificirani logon problem – putem MS RPC, PAM i NSS omogućuje NT domain korisnicima da izlgedaju i ponašaju se kao Unix korisnici na Unix serverima.
- Tri funkcije koje pruža
  - Autentifikacija korisnika kroz PAM
  - Identity resolution kroz NSS
  - Baza mapiranja UID/GID i SID parova u winbind_idmab.tdb

Winbind

- Prikaz rada winbinda



LOCAL MAP HAVE MAPPING
1 someone asks for mapping
2 tdb find and
3 reply
6 someone get the mapping back

LOCAL MAP DOES NOT HAVE MAPPING
1 someone asks for mapping
2 tdb search and does not find it
4 remote mapping is asked (winbind in this case)
5 winbind resolves the map and stores it into tdb
6 someone get the mapping back

Winbind

- NSS – Name Service Switch
  - Sustav koji omogućuje dobavku podataka o korisnicima, mail aliasima i imenima računala (hostname) iz različitih izvora - /etc/shadow, NIS, LDAP, DNS...
  - Omogućuje winbindu da se Unix/Linux serveru predstavi kao izvor podataka o korisničkim imenima i grupama
  - Potrebna je */lib/libnss_winbind.so datoteka i u /etc/nsswitch.conf staviti*
    passwd: files winbind

Winbind

- Pluggable Authentication Modules – PAM
  - Sustav apstrakcije autentifikacije i autorizacije
  - Omogućuje postavljanje različitih autentifikacijskih metoda za različite aplikacije bez rekompajliranja tih aplikacija
  - Svaka aplikacija ima svoju datoteku s opisom autentifikacije u /etc/pam.d/
  - Za winbind, potrebno je datoteku *pam_winbind.so* prebaciti u */lib/security*

Winbind

NAPOMENA! Potrebno je spremiti sigurnosnu kopiju */etc/pam.d/* poddirektorija prije bilo kakve promjene u PAM konfiguraciji, jer pogreška može onemogućiti bilo kakav login pristup serveru, bilo putem mreže, bilo putem konzole!

Winbind

- Primjer postavljanja winbind
  - /etc/nsswitch.conf

    passwd: files winbind
    shadow: files
    group: files winbind
  - *smb.conf*

    [global]
    *winbind separator = *
    idmap uid = 10000-20000
    idmap gid = 10000-20000
    winbind enum users = yes
    winbind enum groups = yes
    template homedir = /home/winnt/%D/%U
    template shell = /bin/bash

Winbind

- Primjer postavljanja winbind (nastavak)
  - Pridjeljivanje Samba servera PDC-u
    - *root# /usr/local/samba/bin/net rpc join -S PDC -U Administrator*
  - Pokretanje winbind
    (obično putem /etc/init.d/winbind)
  - *Test*
    root# /usr/local/samba/bin/wbinfo -u
  - *Trebao bi se prikazati popis svih PDC korisnika*

Winbind

- Primjer postavljanja winbind (nastavak)
  - */etc/pam.d/samba*

```
auth       required    /lib/security/pam_stack.so service=system-auth
account  required    /lib/security/pam_stack.so service=system-auth
```

  - */etc/pam.d/login*

```
auth       required     /lib/security/pam_securetty.so
auth       sufficient   /lib/security/pam_winbind.so
auth       sufficient   /lib/security/pam_unix.so use_first_pass
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_nologin.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
session    optional     /lib/security/pam_console.so
```

Winbind

- Primjer postavljanja winbind (nastavak)
  - */etc/pam.d/ftp*

```
auth       required     /lib/security/pam_listfile.so item=user sense=deny \
file=/etc/ftpusers onerr=succeed
auth       sufficient   /lib/security/pam_winbind.so
auth       required     /lib/security/pam_stack.so service=system-auth
auth       required     /lib/security/pam_shells.so
account    sufficient   /lib/security/pam_winbind.so
account    required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

- *Napomena:* ***nscd servis ne smije biti aktivan istovremeno kad i winbind, winbind neće ispravno raditi!***

System i account policy

- System i account policy je skup prava i mogućnosti pojedinih korisnika i sustava nad resursima mreže.
- Samba koristi slijedeće alate za upravljanje system i account policy postavkama
  - smbpasswd
  - pdbedit
  - net
  - rpcclient

Desktop profile management

- Drugačija je podrška profila za Windows 9x/ME i Windows NT4/200x klijente
- Windows 9x/ME šalju NetUserGetInfo zahtjev za lokaciju profila, no u povratnom odgovoru ima prostora samo za korisnički home share, tako da se ti profili spremaju samo u home
- Windows NT4/200x šalju NetSAMLogon RPC zahtjev, koji ima nekoliko polja, uključujući i zasebno za lokacije korisničkih profila.

Desktop profile management

- smb.conf

  [global]
  logon path = \\profileserver\profileshare\profilepath\%U\moreprofilepath
  ili
  logon path = \\%L\Profiles\%u

  %L – ime servera, %u – korisničko ime

- *Windows 9x/ME*

  logon home = \\%L\%U\.profiles

- *Mješani Windows 9x/ME i NT4/200x profili*

  logon home = \\%L\%u\.profiles
  logon path = \\%L\profiles\%u

Desktop profile management

- Onemogućavanje profila, tri načina
  - smb.conf
    logon home =
    logon path =
  - *MS Windows Registry (putem MMC)*
    Local Computer Policy
    Computer Configuration
    Administrative Templates
    System
    User Profiles
    Disable: Only Allow Local User Profiles
    Disable: Prevent Roaming Profile Change from Propagating to the Server
  - *Promjena vrste profila na User Profiles tabu u local*

Desktop profile management

- Migracija profila sa Win NT4/200x na Sambu
  - Korištenjem Windows alata
  - Označimo profil koji želimo migrirati
  - Kopiramo ga u novu putanju
  - Postavimo prava pristupa

Backup

- Neke od mogućnosti
  - BackupPC – http://backuppc.sourceforge.net
  - rsync
  - Amanda – http://www.amanda.org
  - BOBS – za mješane linux/windows/apple okoline – http://bobs.sourceforge.net
- U biti, bilo koji backup sustav koji može pravilno backupirati Unix/Linux FS

Ispis pomoću sambe

- “Klasičan” ispis
  - Jednostavne postavke
  - Proširene postavke

Jednostavne postavke

- smb.conf

[global]
printing = bsd
load printers = yes
[printers]
path = /var/spool/samba
printable = yes
public = yes
writable = no

Proširene postavke

- [global]
  printing = bsd
  load printers = yes
  show add printer wizard = yes
  printcap name = /etc/printcap
  printer admin = @ntadmin, root
  max print jobs = 100
  lpq cache time = 20
  use client driver = no
  [printers]
  comment = All Printers
  printable = yes
  path = /var/spool/samba
  browseable = no
  guest ok = yes
  public = yes

- read only = yes
  writable = no
  [my_printer_name]
  comment = Printer with Restricted Access
  path = /var/spool/samba_my_printer
  printer admin = kurt
  browseable = yes
  printable = yes
  writable = no
  hosts allow = 0.0.0.0
  hosts deny = turbo_xp, 10.160.50.23, 10.160.51.60
  guest ok = no

Ispis pomoću sambe

- CUPS ispis
  - Osnovne postavke
  - Napredne postavke
  - Mrežni ispis

Osnovne postavke

- Većina distribucija (tako i Debian) već ima ukompajliranu podršku za CUPS. Možemo to provjeriti sa

  root# ldd `which smbd`

  Ako postoji linija nalik

  libcups.so.2 => /usr/lib/libcups.so.2 (0x40123000)

  CUPS je ukompajliran u sambi.

Osnovne postavke

- smb.conf

[global]
load printers = yes
printing = cups
printcap name = cups
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
public = yes
guest ok = yes
writable = no
printable = yes
printer admin = root, @ntadmins

Napredne postavke

- Centralni spool naspram “Peer-to-Peer” ispisa
  - U imalo većoj radnoj okolini dolazi do sukoba zahtjeva za ispisom, zato je bolje imati centralni server.
- Raw ispis korištenjem drivera s Windows klijenata
  - Samba prima samo “sirove” zahtjeve, a svu obradu vrše Windows klijenti
  - U */etc/cups/mime.types i /etc/cups/mime.convs otkomentirati red*
    #application/octet-...

Napredne postavke

- Raw ispis korištenjem drivera s Windows klijenata (nastavak)
  - Dodati “raw” printer putem web sučelja na CUPS serveru – http://localhost:631
  - Odabrati *raw queue*
  - *smb.conf*

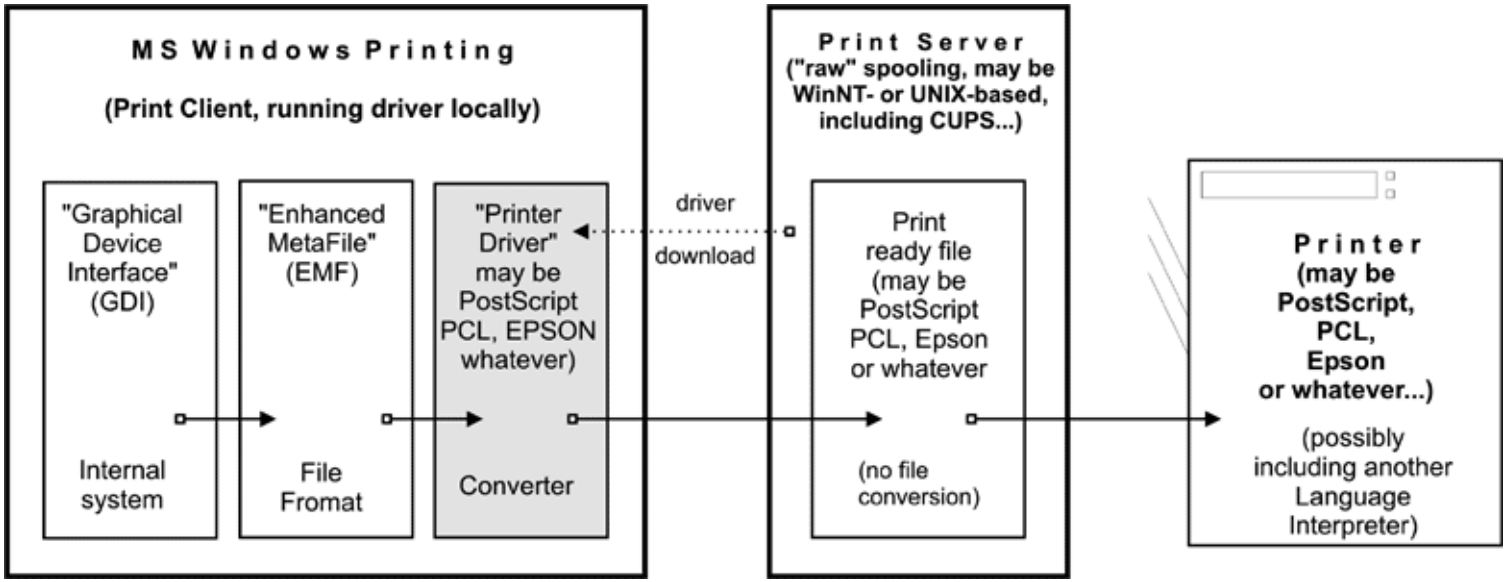
```
[global]
printing = CUPS
printcap = CUPS
[printers]
use client driver = Yes
```

Napredne postavke

- Raw ispis korištenjem drivera s Windows klijenata (nastavak)
  - Na klijentu instalirati pisač kao da je lokalni, odnosno odabrati “Printing to LPI1:”
  - Na “Detail” tabu konfiguracije printera kreirati “local port” koji pokazuje na *raw queue prethodno kreiran, npr. \\server\raw_q gdje je raw_q ime print queue-a kako je kreiran pod CUPS-om*

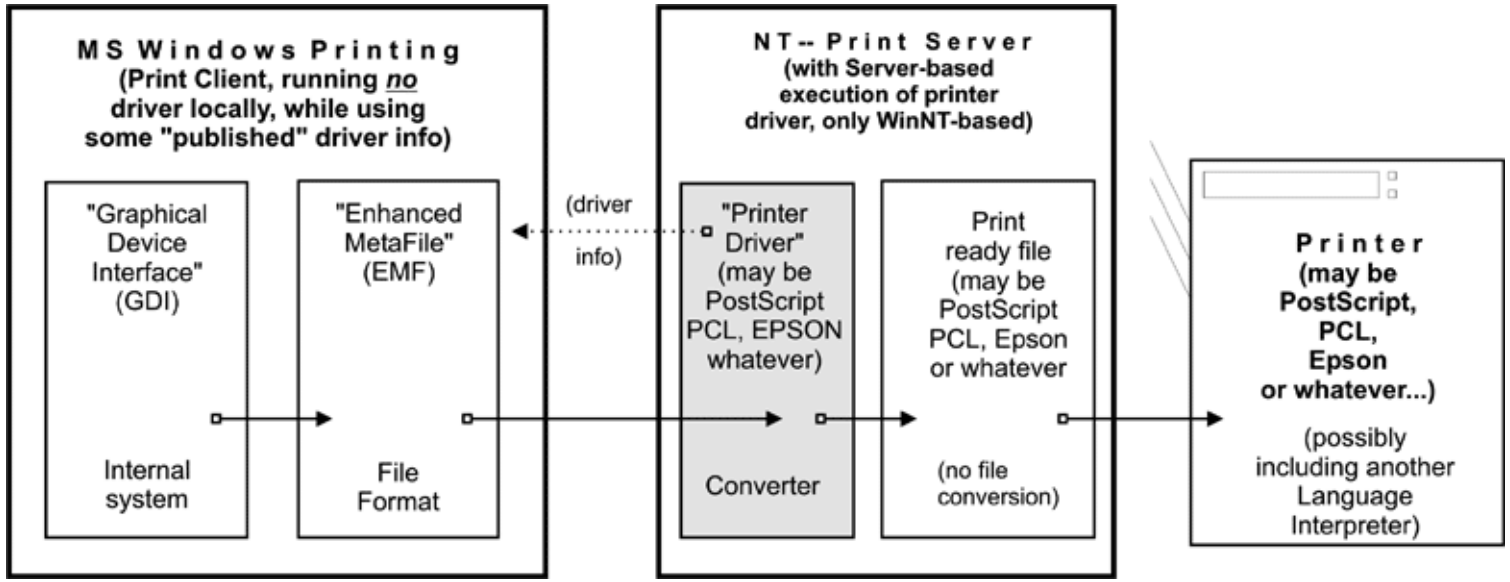
Mrežni ispis

- Kako to MS Windows radi
  - Kreiranje ispisa lokalno (na klijentu)



Mrežni ispis

- Kako to MS Windows radi
  - Kreiranje ispisa udaljeno (na serveru)

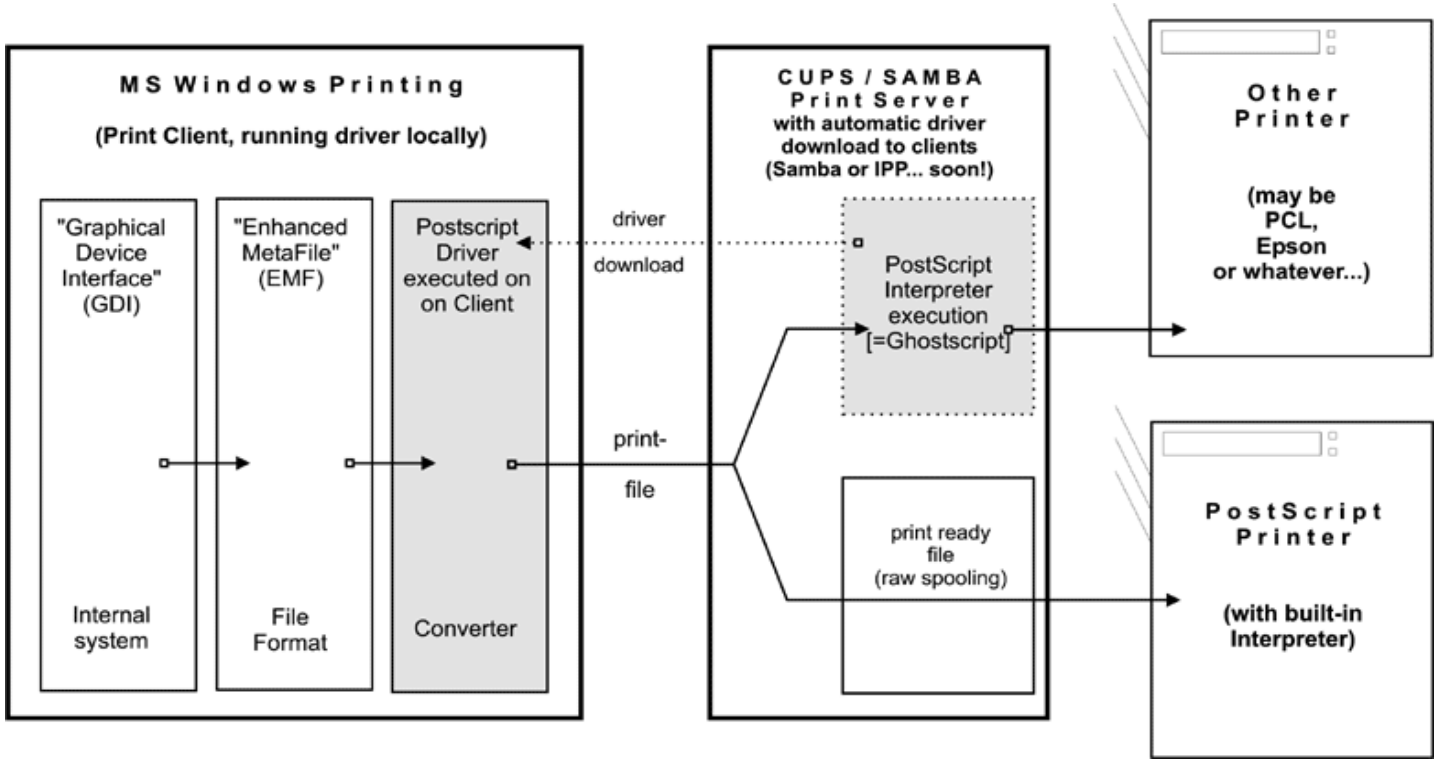


Mrežni ispis

- Windows klijenti, Unix Samba ispisni server
  - Nije moguće izvršavati Win32 programe
  - Windows klijenti mogu slati PostScript CUPS serveru
    - Klijenti moraju koristiti PostScript driver
    - smb.conf
      [global]
      printing = cups
      printcap = cups
    - *Samba mora koristiti vlastiti (različit od CUPS-a) spool direktorij, u koji prihvaća zahtjeve za ispis, i zatim ih prebacuje CUPS-u.*

Mrežni ispis

- Windows klijenti, Unix Samba ispisni server



Migracije i nadogradnje

- Sa sambe 2.x na sambu 3
- Sa NT4 PDC na sambu 3

Migracije i nadogradnje

- Sa sambe 2.x na sambu 3
  - Standardna postavka pod Sambom 3 je da se lozinke šalju kriptirano
  - Domain i machine SID ostaju isti
  - Ako je korišten LDAP, privremeno koristiti *ldapsam_compat backend, a kasnije migrirati podatke s pdbedit*
  - *S obzirom na količinu promjena, potrebno je analizirati stari smb.conf i izgenerirati novi ispočetka.*

Migracije i nadogradnje

- Sa NT4 PDC na Samba PDC
  - Postaviti sambu kao netlogon share, profile share, postaviti da je BDC
  - Dok je samba neaktivna, kreirati BDC account u NT4 domeni
  - net rpc join -S NT4PDC -w DOMNAME -U Administrator%passwd
  - net rpc vampire -S NT4PDC -U administrator%passwd
  - pdbedit -L
  - Zatim dodjeliti svaku od Unix grupa NT grupama

Migracije i nadogradnje

- Sa NT4 PDC na Samba PDC
  - *# Prvo dodjela dobro poznatih grupa*
    net groupmap modify ntgroup="Domain Admins" unixgroup=root
    net groupmap modify ntgroup="Domain Users" unixgroup=users
    net groupmap modify ntgroup="Domain Guests" unixgroup=nobody
    # Zatim dodane grupe
    net groupmap add ntgroup="Designers" unixgroup=designers type=d rid=3200
    net groupmap add ntgroup="Engineers" unixgroup=engineers type=d rid=3210
    net groupmap add ntgroup="QA Team"   unixgroup=qateam   type=d rid=3220
  - *net groupmap list*
  - Zatim migriranje profila i policy, te odabir database backenda

Što ako...?

- Samba checklist
- Pretpostavke za ovaj checklist su da se samba server zove BIGSERVER, PC klijent ACLIENT, oba u radnoj grupi TESTGROUP, a dostupni share *tmp*
- *Treba obratiti pažnju na poruke o greškama. Ako dobijemo poruke da je server unfriendly, treba provjeriti radi li IP resolution – ispravno podešen /etc/resolv.conf*

Što ako..?

- Najbolje je provjeriti ispravnost postavki pomoću *testparm*
  - *U direktoriju gdje je smb.conf, pokrenuti testparm smb.conf. Ako javi ijednu grešku, loše su postavke.*
  - *ping BIGSERVER i ping ACLIENT – ako se ne javljaju, TCP/IP podsustav nije dobro postavljen, a možda je i problem u vatrozidu*
  - *smbclient -L BIGSERVER*
    - *Ako javi "bad password", neispravni su hosts allow, hosts deny ili valid users postavke*

Što ako..?

- *smbclient -L BIGSERVER*
  - Ako je poruka “connection refused”, vjerojatno smbd nije aktivan
  - Treba provjeriti da li je u konfiguraciji dozvoljeno spajanje samo sa pojedinih subneta
- nmblookup -B BIGSERVER_SAMBA_
  - Ako ne vrati nazad IP adresu servera, nmbd nije ispravno instaliran
- nmblookup -B ACLIENT `*'
  - Ako ne vrati nazad IP adresu klijenta, programi na klijentu nisu ispravno instalirani, klijent nije aktivan ili je unešeno krivo ime klijenta

Što ako..?

- nmblookup -B ACLIENT `*'
  - Ako se klijent ne može rezolvati preko DNS-a, treba ga prozvati sa IP adresom umjesto imena
- nmblookup -d 2 '*'
  - Ako se ne javi ni jedan server, broadcast ne radi kako treba. Treba pogledati postavke IP adrese, netmask i broadcast. Treba dodati -B parametar ako su u različitim subnetima
- smbclient //BIGSERVER/TMP -Ujohndoe
  - Nakon unosa lozinke (ako je potrebno) trebao bi se javiti prompt “smb>”

Što ako..?

- smbclient //BIGSERVER/TMP -Ujohndoe
  - Ako vrati nazad “bad password”
    - nije uključena podrška za password backend
    - neispravne postavke za korisnika
    - mixed case lozinka a nije uključena podrška
    - neispravna putanja do password backenda
    - omogućena enkripcija lozinki ali mapiranje samba – unix nije postavljeno kako treba
- Na klijentu *net view \\BIGSERVER*
  - *“network name not found” - ne radi rezolvanje imena, vjerojatno problem u nmbd*

Što ako..?

- Na klijentu *net view \\BIGSERVER*
  - *“network name not found” - ne radi rezolvanje imena, vjerojatno problem u nmbd*
    - *popravak nmbd instalacije*
    - *unijeti IP adresu BIGSERVER u wins server u “advanced TCP/IP setup”*
    - *Windows name rezolution pomoću DNS-a*
    - *Ubacivanje BIGSERVER u lmhosts na klijentu*
- *net use x: \\BIGSERVER\TMP*
  - *Ako ne pita za lozinku i ne javi “command completed successfuly” PC je neispravno instaliran ili je greška u smb.conf*

Što ako..?

- net use x: \\BIGSERVER\TMP
  - Moguće je i da server ne zna na koje korisničko ime povezati ovaj zahtjev. Treba dodati
    [tmp]
    user = korisničko_ime
  - korisničko_ime treba odgovarati lozinki koja je unešena
  - Ako klijent šalje kriptirane lozinke, i samba ih treba prihvatiti, u smb.conf treba biti *encrypt passwords = yes*
- nmblookup -M testgroup
  - Ako ne vrati master browsera, izbor master browsera nije uspio.

Budućnost

- Samba 4.x
  - Najbitnije – potpuna sukladnost s *Active Directory Servisom*

Literatura

- Službeni “Howto”

  http://us2.samba.org/samba/docs/man/Samba-

- Popis knjiga o sambi:
  http://us2.samba.org/samba/docs/

Pitanja u potrazi za odgovorima