**Samba**

Služba pro sdílení souborů a tiskáren, sériových portů a další komunikaci mezi uzly sítě, využívá k tomuto účelu protokol: SMB/CIFS (server message block / common internet file system). Protokol SMB používá též pro tyto služby operační systém Microsoft Windows, lze díky němu propojit sdílené prostředky pod Windows a Linux. Linux vedle smb může využívat systém NFS, který je UNIXově nativní.

**Komunikace přes TCP/IP:**

* přímá komunikace přes TCP/UDP port 445
* přes API NetBIOS – UDP porty 137, 138, TCP porty 137,139 (NetBIOS over TCP/IP)

**NetBIOS služby jsou rozděleny na:**

* Jmennou službu TCP (137)
* Jmennou službu UDP (137)
* Beze stavové spojení, distribuce datagramů přes port UDP 138
* Stavové spojení přes port TCP 139

Pro zpracování názvů používá NetBIOS broadcasty, kterými se aplikace ptá všech uzlů v síti, jestli nenesou daný název. Pakliže žádný uzel v časovém limitu neodpoví, má se za to, že jméno neexistuje. Toto vede k nízkému výkonu celého systému, a proto je možné nakonfigurovat centrální jmennou službu NBNS (pod Windows WINS), která pracuje podobně jako DNS.

Přímá komunikace SMB přes port TCP/UDP 445 používá jako jmennou službu DNS, záznamy v systémech NBNS a DNS jsou podobné.

**Samba server může plnit jednu z následujících rolí:**

Standalone Server – samostatný server, není doménovým kontrolérem, není členem žádné domény

Domain Member Server – samba je členem win domény, server může být členem:

* Active Directory Domain Server
* Win NT4 Domain Server

Domain Controller

* Primary Domain Controller (PDC) – primární doménový kontrolér v doméně NT4
* Backup Domain Controller (BDC) – záložní doménový kontrolér v doméně NT4
* ADS Domain Controller – samba je primární doménový kontrolér, který slouží jako Active Directory server

**Hlavní daemoni Samba serveru:**

nmbd – démon pro registraci, správu a rozpoznávání jmenných názvů, všechny služby na protokolu UDP, měl by být spuštěn jako první

smbd – všechny služby pro sdílení souborů a tiskáren, pracuje s protokolem TCP, spouštěn jako druhý v pořadí za nmbd

winbindd – démon pro spolupráci s Win NT4 a ADS doménami.

**Konfigurační soubor a nástroje:**

Konfigurační soubor s hlavní konfigurací se nachází v /etc/samba/smb.conf.

Je rozdělen do sekcí:

[global] – základní konfigurace celého serveru  
[homes] – automatické vytváření domovských složek uživatelů  
[printers] – připojování ke sdíleným tiskárnám

a sekcí pro definované sdílené složky:

[sdílená složka] – nastavení sdílené složky

Údaje o uživatelích a skupinách ukládá Samba do souborů v adresáři /var/lib/samba/:

* private/passdb.tdb (uživatelé)
* private/secrets.tdb (hesla)

Konfigurace Samby může být uložena ve formě souboru registru jako ve Windows.

**Nástroje Samby:**

* *testparm* – otestuje správnou syntaxi konfiguračního souboru
* *smbpasswd* – (a, x, e, d) správa uživatelů samby (přidání a odebrání, povolení a zakázání uživatele, nastavení hesla atd.)
* *smbclient* – práce se sdílenými složkami (připojení a odpojení sdílené složky pod Linuxem, seznam sdílených složek – *smbclient -L název\_serveru*)
* *smbstatus* – stav Samba serveru, aktivní spojení
* *pdbedit -L* – vypíše seznam uživatelů

**Příklad konfigurace**

Konfigurační soubor /etc/samba/smb.conf

Nejprve provedeme zálohu konfiguračního souboru.

[Global]  
workgroup = pracovní skupina  
server string = Samba server %v ;(%v – verze samba serveru)  
netbios name = jméno netbios ;(název serveru v síti)  
security = user ;(může být i samba, shared, domain, ADS)[[1]](#footnote-1)  
map to guest = bad user ;(akce při zadání špatných přihlašovacích informací)[[2]](#footnote-2)  
dns proxy = no ;(názvy pomocí DNS, pokud neexistují ve WINS)  
encrypt passwords = yes ;(šifrovat hesla přenášená po síti)

[allusers]

comment = Všichni uživatelé

path = /home/shares/allusers ;(cesta k fyzické složce)

valid users = @users ;(povolení uživatelé, @ znamená skupinu uživatelů)

force group = users ;(přiřazení výchozí skupiny k přistupujícím uživatelům)

create mask = 0660 ;(výchozí práva souborů logický AND DOS a unix práv)

directory mask = 0771 ; (výchozí práva souborů logický AND DOS a unix práv)

writable = yes ;(opak read-only, umožňuje zápis do sdílené složky)

**Domovské adresáře**

[homes]

comment = Home Directories

path = /home/shares/%S ;(fyzická cesta k domovským adresářům)

root preexec = bash -c '[ -d /home/shares/%S ] || mkdir -m 0700 /home/shares/%S && chown %S:"skupina" /home/shares/%S' ;(automatické vytvoření domovské složky)

browseable = no ;(zobrazení ve výpisu sdílených složek net view)

valid users = %S ;(povolení uživatelé)

writable = yes

create mask = 0700

directory mask = 0700

%S – toto je makro, místo tohoto symbolu se dosadí jméno uživatele, který vznesl požadavek na sdílenou složku

**Vytvoření adresářů fyzických adresářů**

mkdir -p /home/shares/allusers  
chown -R root:users /home/shares/allusers/  
chmod -R ug+rwx,o+rx-w /home/shares/allusers/

**Restart serveru**

systemctl restart nmbd && systemctl restart smbd && systemctl restart winbindd

nebo samostatnými příkazy pro každou službu

1. Udává, jakým způsobem jsou řízeny přístupy ke sdíleným složkám. *User* odešle přihlašovací jméno a heslo na server při přístupu ke složce. Přístup k dalším složkám je pak automatický bez zadávání údajů. *Shared* pracuje stejně jako user, ale požaduje přihlašovací údaje pro přístup i k dalším složkám. *Domain* – Samba je členem domény, stále je vyžadován linuxový účet, ověření uživatele ale probíhá přes doménový kontrolér. *ADS* – samba pracuje jako člen Active directory domény. Je vyžadován protokol Kerberos. [↑](#footnote-ref-1)
2. *Bad user (špatné jméno uživatele, správné heslo).* Může být ještě *never* (nikdy), *bad password* (dobré uživ. jméno, špatné heslo), *bad UID* (pro doménu a ads, uživatel existuje v doméně, ale ne jako účet v linuxu) [↑](#footnote-ref-2)