Samba 4 AD telepítése RHEL/Almalinux 9 (x86_64) rendszeren.

A telepítéshez és az üzemeltetéshez szükséges dokumentáció a https://samba.tranquil.it/doc/en/ címen érhető el.

Előkészítés

Kiindulásként AlmaLinux 9 (x86_64) operációs rendszer telepítését kell elvégezni. A telepítés minimal telepítés.

Telepítést követő lépések

Módosítani kell a /etc/dnf/dnf.conf állományt a felesleges gyenge függőségek telepítésének tiltásához:

```
# if [ ! -f /etc/dnf/dnf.conf.orig ] ; then cp -a /etc/dnf/dnf.conf
/etc/dnf/dnf.conf.orig && echo 'install_weak_deps=False' >>
/etc/dnf/dnf.conf ; fi
```

Érdemes kikapcsolni a kernel üzenetek megjelenítését

```
# grubby --update-kernel=ALL --args=quiet
```

A SElinux-ot átmenetileg megengedő módba kell kapcsolni

```
# sed -i 's/^SELINUX=.*/SELINUX=permissive/' /etc/selinux/config
```

Be kell állítani a rendszer locale-t en_US.UTF-8-ra

```
# localectl
```

Be kell állítani a rendszer hostnevét a kívánt gépnév + realm formában

```
# hostnamectl set-hostname dc1.adomain.lan
```

Samba 4 AD telepítése

Előkészítő műveletek

A telepítés előtt be kell állítani a gép hálózatát statikus IP-re. A példában a dc1.adomain.lan gép IP címe 192.168.110.11/24.

Fel kell venni a gép FQDN-t a /etc/hosts állományba

```
# cat > /etc/hosts <<EOF
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6

192.168.110.11 dc1.adomain.lan
EOF
```

Telepíteni kell az EPEL release csomagot

```
# dnf install epel-release
```

Telepíteni kell néhány kiegészítő csomagot

```
# dnf install bind-utils chrony krb5-workstation
```

Le kell tölteni és telepíteni kell a csomagok aláíró kulcsát

```
# curl -o /etc/pki/rpm-gpg/RPM-GPG-KEY-TISSAMBA-9
https://samba.tranquil.it/RPM-GPG-KEY-TISSAMBA-9
  % Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
                                 Dload  Upload   Total   Spent    Left
Speed
100  3147  100  3147    0     0  16650      0 --:--:-- --:--:-- --:--:--
16650

# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-TISSAMBA-9
```

Létre kell hozni a samba csomagokat tartalmazó repo fájlt

```
# echo -e "[tis-samba]\nname=tis-
samba\nbaseurl=https://samba.tranquil.it/redhat9/samba-4.20/\nenabled=1\ngpg
check=1\ngpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-TISSAMBA-9\npriority=98"
> /etc/yum.repos.d/tissamba.repo
```

Telepíteni kell a samba-dc csomagot

```
# dnf install samba-dc
```

Biztonsági másolatot kell készíteni a /etc/krb5.conf állományról

```
# [ ! -f /etc/krb5.conf.orig ] && cp -a /etc/krb5.conf /etc/krb5.conf.orig
```

Biztonsági másolatot kell készíteni a /etc/samba/smb.conf állományról (az állományt magát törölni kell).

```
# [ ! -f /etc/samba/smb.conf.orig ] && mv /etc/samba/smb.conf
/etc/samba/smb.conf.orig
```

Érdemes biztonsági másolatot készíteni a /var/lib/samba könyvtárról. Ez a könytár visszaállítható, ha a provisioning sikertelen.

```
# [ ! -d /var/lib/samba.orig ] && cp -a /var/lib/samba /var/lib/samba.orig
```

Tűzfal konfiguráció módosítása

```
# firewall-cmd --permanent --remove-service=cockpit --remove-service=dhcpv6-
client
success

# firewall-cmd --permanent --add-service=samba-dc
success

# firewall-cmd --reload
success

# firewall-cmd --list-services
samba-dc ssh
```

Samba 4 provision

A domain előkészítéséhez az alábbi utasítást kell futtatni

```
# samba-tool domain provision --use-rfc2307 --domain=ADOMAIN --
realm=ADOMAIN.LAN --server-role=dc --host-name=dc1.adomain.lan

INFO 2025-09-06 13:36:56,500 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #2414: gkdi/gmsa root key added with
guid 2a4c9b44-1396-beda-f6f7-b30e2970cf03
INFO 2025-09-06 13:36:56,500 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #2425: A Kerberos configuration
suitable for Samba AD has been generated at /var/lib/samba/private/krb5.conf
INFO 2025-09-06 13:36:56,501 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #2427: Merge the contents of this file
with your system krb5.conf or replace it with this one. Do not create a
symlink!
INFO 2025-09-06 13:36:56,556 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #2086: Setting up fake yp server
settings
INFO 2025-09-06 13:36:56,628 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #492: Once the above files are
installed, your Samba AD server will be ready to use
INFO 2025-09-06 13:36:56,628 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #497: Server Role:           active
directory domain controller
```

```
INFO 2025-09-06 13:36:56,628 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #498: Hostname:
dc1.adomain.lan
INFO 2025-09-06 13:36:56,628 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #499: NetBIOS Domain:        ADOMAIN
INFO 2025-09-06 13:36:56,629 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #500: DNS Domain:
adomain.lan
INFO 2025-09-06 13:36:56,629 pid:17 /usr/lib64/python3.9/site-
packages/samba/provision/__init__.py #501: DOMAIN SID:
S-1-5-21-3755515453-789900971-4137546087
```

Be kell állítani az admin felhasználó jelszavát

```
# samba-tool user setpassword administrator
New Password:
Retype Password:
Changed password OK
```

Át kell állítani a /etc/krb5.conf állományát

```
# rm -f /etc/krb5.conf
# ln -s ../var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Engedélyezni kell és el kell indítani a samba szolgáltatást

```
# systemctl --now enable samba
```

Ellenőrzések

Konfiguráció érvényessége

```
# samba-tool testparm
INFO 2025-09-07 21:38:45,357 pid:257 /usr/lib64/python3.9/site-
packages/samba/netcmd/testparm.py #96: Loaded smb config files from
/etc/samba/smb.conf
INFO 2025-09-07 21:38:45,357 pid:257 /usr/lib64/python3.9/site-
packages/samba/netcmd/testparm.py #97: Loaded services file OK.
Press enter to see a dump of your service definitions

# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1.ADOMAIN.LAN
    realm = ADOMAIN.LAN
    server role = active directory domain controller
    workgroup = ADOMAIN
    idmap_ldb:use rfc2307 = yes
```

```
[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/adomain.lan/scripts
    read only = No
```

Névfeloldás működése

```
# host -t A hup.hu 127.0.0.1
hup.hu has address 92.119.122.43

# host -t A adomain.lan 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

# host -t SRV _ldap._tcp.adomain.lan 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

_ldap._tcp.adomain.lan has SRV record 0 100 389 dc1.adomain.lan.adomain.lan.
```

A tesztek végén módosítható a gép nameserver beállítása

```
# cat /etc/resolv.conf
# Generated by NetworkManager
search adomain.lan
nameserver 127.0.0.1
```

Kerberos működése

```
# kinit administrator@ADOMAIN.LAN
Password for administrator@ADOMAIN.LAN:
Warning: Your password will expire in 41 days on Sat 18 Oct 2025 01:46:03 PM
CEST

# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@ADOMAIN.LAN

Valid starting       Expires              Service principal
09/06/2025 14:17:40  09/07/2025 00:17:40  krbtgt/ADOMAIN.LAN@ADOMAIN.LAN
    renew until 09/07/2025 14:17:28
```

Ha nem működik, akkor törölni kell a /etc/krb5.conf szimbolikus linket és létre kell hozni a fájlt az

alábbi tartalommal

```
# cat > /etc/krb5.conf <<EOF
[libdefaults]
    default_realm = ADOMAIN.LAN
    dns_lookup_realm = true
    dns_lookup_kdc = true

[realms]
ADOMAIN.LAN = {
    kdc = dc1.adomain.lan
    admin_server = dc1.adomain.lan
}
EOF
```

Domain szintű ellenőrzések

```
# samba-tool domain level show
Domain and forest function level for domain 'DC=adomain,DC=lan'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2

# samba-tool user list
Guest
krbtgt
Administrator
```

Időszinkron beállítása

A tartományba léptetett Windows kliensek a tartományvezérlőt használják időszinkronként. Ennek beállításához szükséges a chrony konfigurációjának módosítása.

Eredeti konfiguráció (felesleges üres sorok és a kommentezett tartalom nélkül)

```
# cat /etc/chrony.conf
pool 2.almalinux.pool.ntp.org iburst
sourcedir /run/chrony-dhcp
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
keyfile /etc/chrony.keys
ntsdumpdir /var/lib/chrony
leapsectz right/UTC
logdir /var/log/chrony
```

Módosított konfiguráció (engedélyezett kliens tartomány és samba aláíró socket könyvtár megadással)

```
pool 2.almalinux.pool.ntp.org iburst
```

```
sourcedir /run/chrony-dhcp
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
keyfile /etc/chrony.keys
ntsdumpdir /var/lib/chrony
leapsectz right/UTC
logdir /var/log/chrony

allow 192.168.110.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
```

Zárt hálózaton a *pool* és a *server* sorokat törölni kell és be kell állítani a helyi forrást

```
sourcedir /run/chrony-dhcp
driftfile /var/lib/chrony/drift
makestep 1.0 3
rtcsync
keyfile /etc/chrony.keys
ntsdumpdir /var/lib/chrony
leapsectz right/UTC
logdir /var/log/chrony

allow 192.168.110.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
local stratum 10
```

Újra kell indítani a szolgáltatást

```
# systemctl restart chronyd
```

Ellenőrizni kell, hogy a status oldalon megjelenik az 'MS-SNTP authentication enabled' bejegyzés.

Engedélyezni kell a tűzfalon az NTP szolgáltatást

```
# firewall-cmd --permanent --add-service=ntp
success

# firewall-cmd --add-service=ntp
success
```

Általános műveletek

Listázzuk a jelenlegi jelszó beállításokat

```
# samba-tool domain passwordsettings show
Password information for domain 'DC=adomain,DC=lan'

Password complexity: on
```

```
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Módosítsunk néhány beállítást

```
# samba-tool domain passwordsettings set --complexity=off --min-pwd-age=0 --
max-pwd-age=180 --min-pwd-length=5 --history-length=0
Password complexity deactivated!
Password history length changed!
Minimum password length changed!
Minimum password age changed!
Maximum password age changed!
All changes applied successfully!
```

Ellenőrizzük a módosítást

```
# samba-tool domain passwordsettings show
Password information for domain 'DC=adomain,DC=lan'

Password complexity: off
Store plaintext passwords: off
Password history length: 0
Minimum password length: 5
Minimum password age (days): 0
Maximum password age (days): 180
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Felhasználó létrehozása

```
# samba-tool user add teszt.elek 12345678 --surname=Teszt --given-name=Elek
User 'teszt.elek' added successfully

# samba-tool user list
Administrator
teszt.elek
krbtgt
Guest

# samba-tool user show teszt.elek
dn: CN=Elek Teszt,CN=Users,DC=adomain,DC=lan
objectClass: top
```

```
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Elek Teszt
sn: Teszt
givenName: Elek
instanceType: 4
whenCreated: 20250907181629.0Z
whenChanged: 20250907181629.0Z
displayName: Elek Teszt
uSNCreated: 4286
name: Elek Teszt
objectGUID: eaaebe56-2ea8-43c4-a3e3-cac45d4eb7dc
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-4057828206-964441470-1345394844-1104
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: teszt.elek
sAMAccountType: 805306368
userPrincipalName: teszt.elek@adomain.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=adomain,DC=lan
pwdLastSet: 134017425895426721
userAccountControl: 512
uSNChanged: 4288
distinguishedName: CN=Elek Teszt,CN=Users,DC=adomain,DC=lan
```

Felhasználó átnevezése

```
# samba-tool user rename teszt.elek --force-new-cn='Teszt Elek'
Renamed CN of user "teszt.elek" from "Elek Teszt" to "Teszt Elek"
successfully

# samba-tool user show teszt.elek
dn: CN=Teszt Elek,CN=Users,DC=adomain,DC=lan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
sn: Teszt
givenName: Elek
instanceType: 4
whenCreated: 20250907182955.0Z
displayName: Elek Teszt
uSNCreated: 4290
```

```
objectGUID: 9a3b3706-9934-4d04-8239-4d809059fad8
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-4057828206-964441470-1345394844-1105
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: teszt.elek
sAMAccountType: 805306368
userPrincipalName: teszt.elek@adomain.lan
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=adomain,DC=lan
pwdLastSet: 134017433955222440
userAccountControl: 512
cn: Teszt Elek
name: Teszt Elek
whenChanged: 20250907183000.0Z
uSNChanged: 4293
distinguishedName: CN=Teszt Elek,CN=Users,DC=adomain,DC=lan
```

Felhasználó jelszavának alaphelyzetbe állítása

```
# samba-tool user setpassword teszt.elek
New Password:
Retype Password:
Changed password OK
```

Felhasználó törlése

```
# samba-tool user delete teszt.elek
Deleted user teszt.elek
```

Különleges műveletek

LDAP szerkesztő használata

Telepítés

```
# dnf install ldapvi
```

Használat (jelszó megadása nélkül)

```
EDITOR=mcedit ldapvi -h ldaps://adomain.lan -D 'administrator@adomain.lan' -
```

```
b dc=adomain,dc=lan --tls allow
```

Használat (jelszó megadásával)

```
EDITOR=mcedit ldapvi -h ldaps://adomain.lan -D 'administrator@adomain.lan' -
w 'JELSZÓ' -b dc=adomain,dc=lan --tls allow
```

Tanúsítványok ellenőrzése

Alap beállításban a tanúsítványok 2 évig érvényesek. Lehetőségünk van a beépített CA vagy külső CA által létrehozott tanúsítványok használatára.

CA tanúsítvány

```
# openssl x509 -in /var/lib/samba/private/tls/ca.pem -noout -subject -issuer
-dates
subject=O=Samba Administration, OU=Samba - temporary autogenerated CA
certificate, CN=DC1.ADOMAIN.LAN.adomain.lan
issuer=O=Samba Administration, OU=Samba - temporary autogenerated CA
certificate, CN=DC1.ADOMAIN.LAN.adomain.lan
notBefore=Sep  6 18:34:00 2025 GMT
notAfter=Aug  7 18:34:00 2027 GMT
```

Szerver tanúsítvány

```
# openssl x509 -in /var/lib/samba/private/tls/cert.pem -noout -subject -
issuer -dates
subject=O=Samba Administration, OU=Samba - temporary autogenerated HOST
certificate, CN=DC1.ADOMAIN.LAN.adomain.lan
issuer=O=Samba Administration, OU=Samba - temporary autogenerated CA
certificate, CN=DC1.ADOMAIN.LAN.adomain.lan
notBefore=Sep  6 18:34:00 2025 GMT
notAfter=Aug  7 18:34:00 2027 GMT
```

Jelszó kiolvasása

Alapértelmezetten a Samba/AD környezetben nem olvashatók a felhasználók jelszavai. Az alábbi módszer elérhetővé teszi a felhasználók jelszavait különböző formátumokban.

Az eredeti leírás itt érhető el
https://dev.tranquil.it/wiki/SAMBA_-_Synchronisation_des_mots_de_passe_entre_un_Samba4_et_une_OpenLDAP

Telepítsük a rng-tools csomagot

```
# dnf install rng-tools
```

Indítsuk el az rngd programot

```
# rngd -r /dev/urandom
```

Hozzunk létre a root home könyvtárában egy samba-key állományt

Jelszó nélküli változat

```
# cat > ~/samba-key <<EOF
%no-protection
Key-Type: 1
Key-Length: 2048
Subkey-Type: 1
Subkey-Length: 2048
Name-Real: samba
Name-Email: root@localhost
Expire-Date: 0
%commit
EOF
```

Jelszavas változat (nem javasolt)

```
# cat > ~/samba-key <<EOF
Key-Type: 1
Key-Length: 2048
Subkey-Type: 1
Subkey-Length: 2048
Name-Real: samba
Name-Email: root@localhost
Expire-Date: 0
Passphrase: titkosjelszo123
%commit
EOF
```

Kulcs generálása

```
# gpg --batch --gen-key samba-key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 8BD35A7382342574 marked as ultimately trusted
gpg: directory '/root/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/.gnupg/openpgp-
revocs.d/4FF18900270A797E203556178BD35A7382342574.rev'
```

Kulcsazonosító kinyerése

```
# gpg --list-keys --with-colon samba 2> /dev/null | awk -F: '/^pub:/ { print
$5 }'
8BD35A7382342574
```

A /etc/samba/smb.conf [global] szakaszának módosítása a 'password hash gpg key ids' paraméterrel.

```
# cat /etc/samba/smb.conf
```

```
# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = DC1.ADOMAIN.LAN
    realm = ADOMAIN.LAN
    server role = active directory domain controller
    workgroup = ADOMAIN
    idmap_ldb:use rfc2307 = yes
    password hash gpg key ids = 8BD35A7382342574

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/adomain.lan/scripts
    read only = No
```

Újraindítás

```
# systemctl restart samba
```

Felhasználói jelszó kiolvasása (még nem történt jelszó csere)

```
# samba-tool user getpassword --filter=samaccountname=administrator --
attributes=msDS-
KeyVersionNumber,unicodePwd,virtualClearTextUTF16,virtualClearTextUTF8 --
decrypt-samba-gpg
dn: CN=Administrator,CN=Users,DC=adomain,DC=lan
msDS-KeyVersionNumber: 2
unicodePwd:: BAs5tGohOTjuEgFnlyYGIQ==

Any available password returned OK
```

Felhasználói jelszó kiolvasása (az új felhasználó létrehozása után vagy jelszó csere esetén látható az eredmény)

```
# samba-tool user getpassword --filter=samaccountname=teszt.elek --
attributes=msDS-
KeyVersionNumber,unicodePwd,virtualClearTextUTF16,virtualClearTextUTF8 --
decrypt-samba-gpg
dn: CN=Teszt Elek,CN=Users,DC=adomain,DC=lan
msDS-KeyVersionNumber: 2
unicodePwd:: JZdFyxI6UqouaTqqzKLbUg==
virtualClearTextUTF16:: MQAyADMANAA1ADYANwA4AA==
virtualClearTextUTF8:: MTIzNDU2Nzg=

Any available password returned OK

# echo -n MTIzNDU2Nzg= | base64 -d
```

12345678

From:
https://wiki.r-l.hu/ - **Reverse-Logic wiki**

Permanent link:
https://wiki.r-l.hu/doku.php?id=linux:samba4&rev=1757351442

Last update: **2025/09/08 17:10**