Samba server jako člen Active Directory domény

Máme AD doménu např. **nasead.local** a jméno našeho linux stroje se jmenuje **sambasrv**

Nejprve nainstalujte samba-common libpam-krb5 krb5-config krb5-user

V /etc/resolv.conf' ověříme nastavení DNS. Jako nameserver použijeme stroj, na kterém běží DNS naší AD sítě <code> domain nasead.local search nasead.local nameserver 172.16.7.10 nameserver 172.16.7.9 </code> Do /etc/hosts přidáme IP adresu interface, na které bude probíhat spojení na DC server a pojmenujeme ji plným DNS jménem. tj <code> 127.0.0.1 localhost 172.16.7.73 sambasrv.nasead.local sambasrv </code> Nyní nastavíme Kerberos <file /etc/krb5.conf> [libdefaults] default_realm = NASEAD.LOCAL dns_lookup_realm = false dns_lookup_kdc = true ticket_lifetime = 24h # renew_lifetime = 7d [realms] NASEAD.LOCAL = { kdc = dc01.nasead.local kdc = dc02.nasead.local admin_server = dc01.nasead.local } </file> **POZOR: zde musí být jako default_realm uvedena doména VELKÝMA PÍSMENAMA** Jako kdc se uvednou fqdn jména doménových řadičů v naší síti, jako admin_server uvádím primární řadič Nyní přichází na řadu konfigurace smb.conf <file /etc/samba/smb.conf> #======================= Global Settings ======================= [global] server role = MEMBER SERVER security = ads realm = nasead.local workgroup = nasead netbios name = SAMBASRV client signing = yes client use spnego = yes kerberos method = secrets and keytab server string = Komentar #### Debugging/Accounting #### # This tells Samba to use a separate log file for each machine # that connects log file = /var/log/samba/log.%m log level = 5 # Cap the size of the individual log files (in KiB). max log size = 1000 encrypt passwords = yes winbind nss info = rfc2307 winbind trusted domains only = no winbind use default domain = yes winbind enum users = yes winbind enum groups = yes winbind refresh tickets = yes # Default ID mapping configuration for local BUILTIN accounts # and groups on a domain member. The default (*) domain: # - must not overlap with any domain ID mapping configuration! # - must use a read-write-enabled back end, such as tdb. idmap config * : backend = tdb idmap config * : range = 3000-7999 # - You must set a DOMAIN backend configuration idmap config nasead : backend = rid idmap config nasead : range = 10000-999999 vfs objects = acl_xattr map acl inherit = yes store dos attributes = yes winbind refresh tickets = yes domain master = no local master = no [share] comment = sdileny disk path = /home/SHARE valid users = @nejakaskupina, @administrators browseable = yes read only = no inherit acls = yes inherit permissions = yes </file> Následujícím krokem ověříme, že se dokážeme autentizovat k DC serveru <code> # kinit Administrator Password for Administrator@NASEAD.LOCAL: # klist </code> Pokud je vše OK, po zadání příkazu **klist** uvidíte vystavený kerberos ticket <code> Ticket cache: FILE:/tmp/krb5cc_0 Default principal: Administrator@NASEAD.LOCAL Valid starting Expires Service principal 06/05/2019 18:25:13 06/06/2019 04:25:13 krbtgt/NASEAD.LOCAL@NASEAD.LOCAL renew until 06/12/2019 18:24:56 </code> Pokud jste se dostal až sem, můžeme přistoupit k připojení samba serveru do domény. <code> # net ads join -U

Administrator Enter administrator's password: Using short domain name – NASEAD Joined 'SAMBASRV' to dns domain 'nasead.local' </code> Pokud se nepovede, přidejte parametr -d 1 pro zobrazení debug hlášek. Stav připojení do domény mužete ověřit příkazem net ads status -U Administrator <code> Enter Administrator's password: objectClass: top objectClass: person objectClass: organizationalPerson objectClass: user objectClass: computer cn: sambasrv distinguishedName: CN=sambasrv,OU=Servers,DC=nasead,DC=local instanceType: 4 whenCreated: 20190607131211.0Z whenChanged: 20190617143204.0Z uSNCreated: 11206462 uSNChanged: 11255367 name: lih-zpsx001 objectGUID: 8fe38593-36b4-41e3-993a-77c506e589d userAccountControl: 69632 badPwdCount: 0 codePage: 0 countryCode: 0 badPasswordTime: 132052716929628168 lastLogoff: 0 lastLogon: 132052783714159406 localPolicyFlags: 0 pwdLastSet: 132043867314721394 primaryGroupID: 515 objectSid: S-1-5-21-2395078511-4245873061-2388994840-17615 accountExpires: 9223372036854775807 logonCount: 66 sAMAccountName: sambasrv$ sAMAccountType: 805306369 dNSHostName: sambasrv.nasead.local servicePrincipalName: HOST/sambasrv.nasead.local servicePrincipalName: HOST/SAMBASRV objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=nasead,DC=local isCriticalSystemObject: FALSE dSCorePropagationData: 20190607150627.0Z dSCorePropagationData: 16010101000001.0Z mS-DS-CreatorSID: S-1-5-21-2395078511-4245873061-2388994840-17613 lastLogonTimestamp: 132052555244011908 msDS-SupportedEncryptionTypes: 31 </code> **Nyní nainstalujte samba attr winbind libpam-winbind libnss-winbind** a nastartuje sambu. Pokud je naše samba členem domény, nastal čas pro nastartování démona **winbind** Potom do souboru /etc/nsswitch.conf přidáme možnost načtění uživatelů a skupin z ad. Přidejte **winbind** na konec řádku passwd a group <file /etc/nsswitch.conf> passwd: compat winbind group: compat winbind shadow: compat gshadow: files </file> Nyní můžeme otestovat wbinfo --ping-dc - musí zobrazit checking the NETLOGON for domain[NASEAD] dc connection to "dc01.nasead.local" succeeded
wbinfo -g - vypíše skupiny v AD
wbinfo -u - vypíše uživatele v AD
getent passwd - načte všechny uživatele - pokud uvidíte uživatele z AD ve tvaru linuxového passwd tak máte vyhráno.
getent group'' - načte všechny skupiny (stejné jméno pak použijeme ve **valid user** pro ověření práv ke sdílené složce)

```
# getent group | grep nejaka
nejakaskupina:x:31166:
```

Nyní lze používat klasicky nastavení práv přes chown atd. Ještě ověření funkční samby -

```
# smbclient -L sambasrv.nasead.local -U NASEAD\\Administrator
WARNING: The "syslog" option is deprecated
Enter NASEAD\Administrators's password:
Domain=[NASEAD] OS=[Windows 6.1] Server=[Samba 4.5.16-Debian]

    Sharename       Type      Comment
    ---------       ----      -------
    share           Disk      sdileny disk
```

```
    IPC$            IPC       IPC Service (Komentar)
Domain=[NASEAD] OS=[Windows 6.1] Server=[Samba 4.5.16-Debian]

    Server               Comment
    ---------            -------
    SAMBASRV          Komentar

    Workgroup            Master
    ---------            -------
    NASEAD
```