Nastavení ověřování Freeradiusu přes Windows AD

Návod je testovaný na Debianu 8 s instalací Freeradiusu z distribučního balíčku. Eduroam má nastavené ověřování na EAP PEAP. Všechny systémy musí být korektně zaregistrované v dns.

OS se musí nejdříve zaregistrovat ve Windowsové doméně, pomocí samby a winbindu. A potom lze používat ověření *ntlm_auth* ze Samby ve Freeradiusu. Hesla v AD jsou uložena jako NT hash a tuto hash lze použít v MS-CHAPv2 autorizaci (bez potřeby znát plain textové heslo). AD DC musí povolovat NTLMv1 ověření, což je trochu v rozporu s best practice od M$.

Nejdříve doinstalujte balíky:

- freeradius
- samba
- winbind
- krb5-config a krb5-user

přidání systému do Windows domény

Nejdříve naplníme konfigurační soubory.

/etc/krb5.conf

```
[libdefaults]
        default_realm = UNIVERZITA.CZ
        dns_lookup_realm = false
        dns_lookup_kdc = false
[realms]
        UNIVERZITA.CZ = {
                kdc = 192.168.0.2
                kdc = 192.168.0.3
                admin_server = ldapdc.univerzita.cz
                default_domain = univerzita.cz
                }
[domain_realm]
        .univerzita.cz = UNIVERZITA.CZ
        univerzita.cz = UNIVERZITA.CZ
[appdefaults]
        pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Pozor na malé a velké znaky, ty je nutno dodržet. Dva kdc jsou zde kvůli zvýšené dostupnosti, systém je schopen při výpadku přecházet plynule mezi dvěma DC. IP jsou zde použity, aby se systém zaregistroval na oba DC zároveň, lze také použít unikátní FQDN.

smb.conf

```
[global]
workgroup = UNIVERZITA
security = ads
password server = 192.168.0.2, 192.168.0.3
realm = UNIVERZITA.CZ
```

Pozor, workgroup není doména, jméno musí být uvedeno bez koncovky domény 1. řádu. DC jsou

opět dva.

```
nsswitch.conf
passwd:         compat files windbind
group:          compat files windbind
shadow:         compat files windbind
```

Samba a winbind musí být spuštěné. Při změně konfigurace je třeba winbind nejdříve zastavit, restartovat sambu a winbind opět spustit.

```
~# kinit bezny_uzivatel
~# klist
~# kdestroy -A
```

Nejdříve si těmito příkazy otestujeme, zda DC vidíme a jsme schopni se přihlásit, vytvoříme si kerberosový tiket. Identifikátor domény vyplňovat nemusíme, použije se defaultní. Uživatel nemusí být doménovým administrátorem. Na konci pokusu se musí přihlášení zrušit, krb5 tiket totiž platí 8 hodin. Prostupy jsou trochu oříšek, já vypozoroval používání TCP 88, 389, 445 a UDP 88.

```
~# kinit admin_uzivatel
~# net ads join -U admin_uzivatel
Using short domain name -- UNIVERZITA
Joined 'HONZA-LAB' to dns domain 'univerzita.cz'
~# kdestroy -A
~# systemctl restart winbind.service
```

Teď můžeme systém zaregistrovat do AD pomocí doménového administrátora. Po zaregistrování lze krb5 tiket zrušit (hlavně když správce radiusu a doménový admin nejsou jedna osoba a doménový admin se obává, abyste jeho jménem nepáchali nějaké nepravosti :-)). Připojení do domény si samba ukládá do adresáře */var/run/samba/*.

```
~# wbinfo -u
~# wbinfo -g
~# wbinfo -P

~# ntlm_auth --request-nt-key --domain=UNIVERZITA --username=bezny_uzivatel
--require-membership-of="UNIVERZITA\g_eduroam"
Password:
NT_STATUS_OK: Success (0x0)

~# ntlm_auth --request-nt-key --domain=UNIVERZITA --username=bezny_uzivatel
--require-membership-of="UNIVERZITA\g_zakazano"
Password:
NT_STATUS_LOGON_FAILURE: Logon failure (0xc000006d)
```

Nyní ověříme zda vidíme informace z AD, uživatele a skupiny. Ping na DC doporučuji použít i jako test v dohledovém systému. Pak můžeme otestovat přihlášení přímo pomocí ntlm, které používá freeradius. Druhý test je kvůli ověření fungování skupin.

konfigurace freeradiusu

Nejdříve je třeba povolit procesu freeradius přístup k winbindové pipe.

```
chown root:freerad /var/lib/samba/winbindd_privileged
```

```
eap.conf
eap {
 default_eap_type = peap
 tls {
  private_key_file = /etc/ssl/private/honza-lab-key.pem
  certificate_file = /etc/ssl/certs/honza-lab-crt.pem
  CA_file = /etc/ssl/certs/chain_TERENA_SSL_CA_3.pem
```

```
  }
 ttls {
  default_eap_type = mschapv2
  copy_request_to_tunnel = no
  use_tunneled_reply = no
  virtual_server = "inner-tunnel"
  }
 peap {
  default_eap_type = mschapv2
  copy_request_to_tunnel = no
  use_tunneled_reply = no
  virtual_server = "inner-tunnel"
  }
```

Konfigurace EAPu je podobná jako u standardní konfigurace pro eduroam. PEAPové požadavky jsou předávany na virtuální server inner-tunnel.

proxy.conf

```
realm univerzita.cz { }
realm DEFAULT {
 authhost        = localhost:11812
 secret          = vase_heslo
 nostrip
 }
realm NULL { }
```

modules/mschap

```
mschap {
 use_mppe = yes
 require_encryption = yes
 require_strong = yes
 with_ntdomain_hack = yes
 ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-
Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-
response=%{%{mschap:NT-Response}:-00} --require-membership-
of='UNIVERZITA\\g_eduroam'"
 }
```

Zde se nastaví ověření pomocí sambového ntlm_auth. Pozor na nutnost escapování znaku backslash.

sites-enabled/inner-tunnel

```
server inner-tunnel {
 listen {
  ipaddr = 127.0.0.1
  port = 18120
  type = auth
  }
 authorize {
  chap
  mschap
  suffix
 update control {
  Proxy-To-Realm := LOCAL
  }
 eap {
  ok = return
  }
 expiration
 logintime
 }
 authenticate {
```

```
  Auth-Type MS-CHAP {
   mschap
   }
  eap
  }
}
```

Nezapomeňte udělat symbol link tak, aby virtuální server inner-tunnel skutečně naběhl.

odkazy a zdroje

- https://wiki.debian.org/AuthenticatingLinuxWithActiveDirectory
- http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO
- https://www.eduroam.us/node/89
- https://wiki.samba.org/index.php/Samba,_Active_Directory_&_LDAP
- teorie vysvětlená Jiřím Benešem v konferenci *eduroam-admin* ve vlákně *freeradius a AD*
- https://technet.microsoft.com/en-us/library/jj852207%28v=ws.11%29.aspx