Kerberos Ausfallsicherheit und richtige Config von SSSD am KDE NEON, Ubuntuclient mit UCS

Du möchtest dich gerne für unsere Hilfe erkenntlich zeigen 🥹. Gerne. Wir bedanken uns bei dir für deine Spende! 🤣

Hauseigenes Apt-Repo: https://apt.iteas.at

GITLAB Enterprise: 

Getestet mit KDE NEON 20.04.1

Ausgegangen wird hier von einem erfolgreichem Join zur UCS Domäne. Am Linuxclient wird immer nur der Masterserver eingetragen. In Foren wird behauptet dass wenn der Master ausfällt sich über DNS alle weiteren Kerberos und LDAPserver melden. Ich hab das getestet, dem muss ich wiedersprechen, zumindest war es mir auf keinen bekanntem Weg klar wie das denn gehen soll, und jeder Test verlief negativ. Beim einem erzeugtem Ausfall von einem Master und einem Backup, sollte der zweite Backup übernehmen, doch das passierte nicht.

Mit der nachstehenden Konfiguration ist eine Ausfallsicherheit gegeben.

```
[sssd]
config_file_version = 2
reconnection_retries = 3
sbus_timeout = 30
services = nss, pam, sudo
domains = TUX.LAN

[nss]
reconnection_retries = 3

[pam]
reconnection_retries = 3

[domain/TUX.LAN]
auth_provider = krb5
krb5_realm = TUX.LAN
krb5_server = dc1.tux.lan,dc2.tux.lan
krb5_backup_server = dc3.tux.lan
krb5_kpasswd = dc1.tux.lan
id_provider = ldap
```

```
ldap_uri = ldap://dc1.tux.lan:7389,ldap://dc2.tux.lan:7389
ldap_backup_uri = ldap://dc3.tux.lan:7389
ldap_search_base = dc=tux,dc=lan
ldap_tls_reqcert = demand
ldap_tls_cacert = /etc/univention/ssl/ucsCA/CAcert.pem
cache_credentials = true
enumerate = true
ldap_default_bind_dn = cn=linuxpc01,cn=home,cn=computers,dc=tux,dc=lan
ldap_default_authtok_type = password
ldap_default_authtok = geheim
```

Es gibt dann noch direkt unten angehängt den Sudoteil. Dieser ist aber nur bis 18.04 erforderlich und auch nur wenn man sudo vollinheitlich am UCS zentral pflegt. Default gibt es so ein Modul nicht, das darf man selbst programmieren. Aus Erfahrung darf ich berichten, es funktioniert wunderbar.

```
...
sudo_provider=ldap
ldap_sudo_search_base=cn=SUDOers,cn=apps,dc=tux,dc=lan
ldap_sudo_full_refresh_interval=86400
ldap_sudo_smart_refresh_interval=300
[sudo]
```

Die Kerberosconfig sieht wie folgt aus: `/etc/krb5.conf`

```
[libdefaults]
    default_realm = TUX.LAN
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    default_tkt_enctypes = arcfour-hmac-md5 des-cbc-md5 des3-hmac-sha1 des-
cbc-crc des-cbc-md4 des3-cbc-sha1 aes128-cts-hmac-sha1-96 aes256-cts-hmac-
sha1-96
    permitted_enctypes = des3-hmac-sha1 des-cbc-crc des-cbc-md4 des-cbc-md5
des3-cbc-sha1 arcfour-hmac-md5 aes128-cts-hmac-sha1-96 aes256-cts-hmac-
sha1-96
    allow_weak_crypto=true
    rdns = false

[realms]
TUX.LAN = {
   kdc = dc1.tux.lan dc2.tux.lan dc3.tux.lan
   admin_server = dc1.tux.lan
   kpasswd_server = dc1.tux.lan
}
```

Und noch LDAP: `/etc/ldap/ldap.conf`

```
TLS_CACERT /etc/univention/ssl/ucsCA/CAcert.pem
URI ldap://dc1.tux.lan:7389 ldap://dc2.tux.lan:7389 ldap://dc3.tux.lan:7389
```

```
BASE dc=tux,dc=lan
```

Und von nun ist eure Kerberosverbindung/LDAP redundant.

krb5-auth-dialog

Das ist ein kleines Programm für die Symbolleiste was sich in den Autostart wirft. Sollte meiner Meinung nach in der Kerberos Standard Installation der Clientanbindung immer dabei sein. Warum?

Hat man das nicht, läuft nach 600 Minuten das Ticket aus, und wird nicht mehr erneuert. Das darf man dann auf der CMD mit `kinit` selbst tun. Dieses super geniale kleine Tool sorgt dafür das bei jeder Passworteingabe im System die vom User getätigt wird, da zählt auch die Bildschirmsperre dazu, das Ticket wieder auf 600 Minuten gesetzt wird. Luxus pur, richtig?

Fährt man nun Kerberos im Notbetrieb, sprich fällt der Master aus, funktioniert dieses Tool nicht mehr und man darf in dieser Zeit, sofern das Ticket ausläuft sich ein neues auf der CMD holen. Für den Notbetrieb, völlig ok. Beim Login am Desktop bekommt man selbstvertändlich ganz normal sein Ticket ausgestellt.