

Automount von Sambalaufwerken beim Login - inkl. Kerberos und Nomachine Terminalserver



Die Folgende Anleitung bezieht sich auf folgende Konzelation:

- Serverumgebung [Univention Corporate Server](#) auf Debian Basis (Active Directory/LDAP/Kerberos)

Als Clients kommen folgende Systeme getestet zum Einsatz:

- KDE Neon 18.04 mit [Nomachine](#) Freeedition
- Ubuntu 18.04/20.04 Server (über SSH)
- Lubuntu 20.04 (LXQT) als Nomachine Workstation Enterprise

Auch in Linuxumgebungen ist die Automation von Desktops voll und ganz ein Standart. Da dies aber meist nur größeren Enterpriseumgebungen vorbehalten ist, findet man im Internet hierüber sehr wenig ausführlich gute Dokumentation. Aus diesem Grund hab ich mir mal gedacht ich schreib darüber doch auch mal einen Artikel um Enterprisefeatures auch zu dir zu bringen.

Voraussetzung

Voraussetzung ist eine laufende funktionierende [UCS4.4.x Umgebung](#) inkl. Kerberos. Sollest du eine andere Umgebung mit als AD/LDAP benutzen ist das selbstverständlich auch ok. Hast das nicht [installiere dir diese mal schnell](#).

Überprüfung am Client

Bist du am Linuxclient eingeloggt, öffne eine Konsole und tippe `klist`. Dies zeigt dir dein aktuelles Kerberosticket und die Gültigkeit. Würde als Output so etwas kommen,

```
klist: No ticket file: /tmp/krb5cc_0
```

bist wohl nicht richtig an deinem ActiveDirectory registiert.

Funktioniert alles gut, ist an dieser Stelle ein kleineres Helferlein zu erwähnen. Installiere dir gleich `krb5-auth-dialog` nach. Das erneuert bequem deine Tickets. Immer dann wenn du wo dein Passwort eingeben sollest, z.B. wenn du deinen Bildschirm entsperrst.

Installation und Konfiguration am Client

Als erstes sind ein paar Pakete zu installieren.

```
apt install libpam-mount davfs2 keyutils -y
```

Dies bearbeitet die Pamconfiguration. Dies lässt du zu, oder editierst sie später manuell, falls du mal selbst Änderungen vorgenommen haben solltest. `nano /etc/pam.d/common-auth`. Die folgende Zeile kommt vor der Zeile `auth optional pam_cap.so`.

```
...  
auth      optional      pam_mount.so
```

In der Datei `/etc/pam.d/common-password` fügst du vor der Zeile `password optional pam_gnome_keyring.so` folgendes ein:

```
...  
password      optional      pam_mount.so disable_interactive  
...
```

Verwendest du Nomachine auf deinem Rechner inkl. SDDM als Loginmanager, musst du noch einen weiteren speziellen Eintrag in der Pamkonfiguration vor der Zeile `session optional pam_systemd.so` setzen. Die normale Pammountzeile kommentierst du aus. Den Artikel von Nomachine darüber [findest du hier](#).

```
nano /etc/pam.d/common-session
```

```
...  
session optional      pam_mount.so disable_interactive  
#session      optional      pam_mount.so  
session optional      pam_systemd.so  
...
```

Setzen der pam_mount.conf.xml

Die Standardoptionen haben bei meinen Konfigurationen immer gepasst. In diesem File trägt alle Laufwerke ein die in deiner Umgebung erreichbar sind. Loggst du dich mit deinem Benutzer ein, werden automatisch alle Laufwerke in dein Home eingebunden. Beim Logout, wieder sauber getrennt. Die Funktion kann mit **Cifs**, **NFS4.x** und **Webdav** wesentlich umgehen.

Hier nun ein Beispiel:

[pam_mount.conf.xml](#)

```
...  
<!-- pam_mount parameters: Volume-related -->  
<volume fstype="cifs" server="server.tux.lan"  
options="vers=3.0,sec=krb5,cuid=%(USERID)" path="Downloads"
```

```

mountpoint="~/Downloads"> <not><user>root</user></not>
<not><user>sddm</user></not> <not><user>nx</user></not> </volume>
<volume fstype="cifs" server="server.tux.lan"
options="vers=3.0,sec=krb5,cuid=%(USERUID)" path="Dokumente"
mountpoint="~/Dokumente"> <not><user>root</user></not>
<not><user>sddm</user></not> <not><user>nx</user></not> </volume>
<volume fstype="cifs" server="server.tux.lan"
options="vers=3.0,sec=krb5,cuid=%(USERUID)" path="Bilder"
mountpoint="~/Bilder"> <not><user>root</user></not>
<not><user>sddm</user></not> <not><user>nx</user></not> </volume>
<volume fstype="cifs" server="server.tux.lan"
options="vers=3.0,sec=krb5,cuid=%(USERUID)" path="%(USER)"
mountpoint="~/MYHOME"> <not><user>root</user></not>
<not><user>sddm</user></not> <not><user>nx</user></not> </volume>
<mkmountpoint enable="1" remove="true" />
. . .

```

Die User Root, Sddm und NX werden ignoriert. Sprich diese machen keine Mountabfrage. Macht ja auch keinen Sinn. Der große Vorteil: Angabe von Passwort und Benutzer sind natürlich nicht notwendig. Um das kümmert sich LDAP/Kerberos von UCS erledigt beim Loginvorgang den Rest.

Macht man das ganze mit PAM ohne Kerberos, könnte man jetzt wieder paranoid reagieren und sagen, „ja die Passwortheingabe wird ja beim Login PAM übergeben, das ist doch unsicher!“. Ja das stimmt schon wenn man es aus technischer Sicht ganz genau betrachten würde, ist das so. Aber das

lass ich jetzt mal im Raum so stehen



Hier noch ein Beispiel für Webdav, CIFS und NFS. In dieser Konfig gehen diese beiden nicht über Kerberos.

[pam_mount.conf.xml](#)

```

. . .
<volume fstype="davfs" path="https://daten.tux.com/webdav-daten"
mountpoint="~/webdav-daten"
options="username=%(USER),rw,nosuid,nodev,uid=%(USER)">
<not><user>root</user></not> <not><user>sddm</user></not> </volume>
<volume fstype="nfs" server="servername.bla.at" path="/home/Dokumente"
mountpoint="~/Dokumente" />
<volume fstype="cifs" server="servername.bla.at" options="vers=3.0"
path="Organisation" mountpoint="~/Organisation" />

```

Du kannst schon erkennen, das der Mechanismus sehr mächtig ist. Die Manpage ist hier sehr ausführlich. Mit ein wenig Zeit und tun, kannst du dir hier etwas schönes bauen.

`man pam_mount.conf`

Ab diesem Zeitpunkt bekommst du deine Laufwerke beim Login über dem Displaymanager SDDM oder Lightdm (getestet) bereits eingebunden.

Automount über SSH und Kerberos

Auch da tun wir uns dank [UCS](#) sehr leicht. Wir editieren unsere SSHD am Server und unsere Clientconfig.

Server: /etc/ssh/sshd_config

```
...
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
KerberosAuthentication yes
KerberosOrLocalPasswd yes
KerberosTicketCleanup yes
...
```

Client: /etc/ssh/ssh_config

```
...
GSSAPIAuthentication yes
GSSAPIDelegatedCredentials yes
...
```

Nach einem Restart des SSH-Servers, bekommst man seine Laufwerke auch darüber bequem eingebunden.

From:
<https://deepdoc.at/dokuwiki/> - DEEPDOC.AT - enjoy your brain

Permanent link:
https://deepdoc.at/dokuwiki/doku.php?id=server_und_serverdienste:automount_von_sambalaufwerken_beim_login_-_inkl_kerberos_und_nomachine_terminalserver&rev=1593191865

Last update: 2020/06/26 19:17

