Einheitliche Linux-Benutzerverwaltung mit Active Directory

Tuebix 2018

Mark Pröhl

abstract:

- Benutzerverwaltung in heterogenen Linux-/Windows-Umgebungen
- Ziel: Anbindung von Linux-Systeme an Active Directory (AD)
- Technologische Grundlagen:
  - Kerberos
  - Lightweight Directory Access Protocol (LDAP)
  - Name Service Switch (NSS)
  - Pluggable Authentication Modules (PAM)
  - System Security Services Daemon (SSSD)
- Workshop: Konfigurationen für verschiedene Anwendungsszenarien ausarbeiten und testen
- Ausgearbeitete Konfigurationen werden anschließend unter https://www.kerberos-buch.de/tuebix-2018/ veröffentlicht

about me

- In Tübingen Physik studiert
- Beruflich IT-ler
- Nebenberuflich Author
- Linux seit Anfang 90er
- Themengebiete:
  - Identity Management
  - Security
  - Verzeichnisdienste, Authentisierung und Single Sign-on

Technologische Grundlagen

Kerberos

- Sicherheitsinfrastruktur
- Authentisierungsdienst für:
  - Klassische Client-Server-Applikationen
  - Web-Applikationen
  - System-Anmeldung
- Trusted 3rd-Party
- Single Sign-on (SSO) auf Basis von Kerberos-Tickets
- Primärauthentisierung über
  - einfaches Passwort
  - X.509-Clientzertifikat / Smartcard
  - One Time Passwort (OTP)

Kerberos (cont.)

- Kerberos-Service: Key Distribution Service (KDC)
- bis ca. 2000 hauptsächslich in Unix-Umgebungen eingesetzt
- Heute Primäres Authentisierungsverfahren in Windows-Domänen
- zentraler Service von Active Directory: jeder Domain Controller ist ein Kerberos-KDC

Kerberos (cont.)

- Live-Vorführung: Kerberos unter Linux
  - Die Kommandos `kinit`, `klist` und `kdestroy`
  - `ssh`-Login mit Kerberos-Authentisierung
  - Was sind “Principals”?
  - Unterschied Ticket-Cache und Keytab
  - Beispiel für “kerberisierten” Netzwerkzugriff: `ldapsearch`
- Analyse mit Wireshark

LDAP

- Kerberos ist primär ein Authentisierungsdienst – Systeme benötigen i.d.R. zusätzliche Informationen. Beispiele:
  - Anmeldenamen
  - Numerische Benutzer-ID
  - Berechtigungsinformationen (z.B. Gruppenmitgliedschaften)
  - Numerische Gruppen-IDs
  - Email-Adresse
  - ...
- LDAP-Verzeichnisdienste ergänzen Kerberos-Infrastrukturen u.a. um derartige Informationen.
- LDAP ist auch ein zentraler Service von Active Directory: jeder Domain Controller ist ein LDAP-Server

LDAP (cont.)

- Live-Vorführung: LDAP-Operationen mit Linux-Kommandozeile gegen Active Directory durchführen
- Das LDIF-Format
- Netzwerkanalyse mit Wireshark
- LDAP und Sicherheit: TLS vs. Kerberos

NSS

- Name Service Switch
- Modulares Konzept für Linux für verschiedenste Namensinformationen:
  - `passwd`
  - `shadow`
  - `group`
  - `hosts`
  - `netgroup`
  - ...

NSS (cont.)

- In `/usr/lib` und `/usr/lib64` gibt es Module für die verschiedene Quellen. Beispiele:
  - `libnss_files.so`: liefert Namensinformationen aus Dateien wie `/etc/passwd`, `/etc/group` oder `/etc/hosts`
  - `libnss_db.so`: liefert Informationen aus lokalen Binärdateien
  - `libnss_nis.so`: befragt den (altertümlichen) Network Information Service (NIS)
  - `libnss_dns.so`: befragt DNS-Server
  - `libnss_ldap.so`: befragt LDAP-Server
  - `libnss_sss.so`: befragt den `sssd` (s.u.)

NSS (cont.)

- Konfiguration über Module in `/etc/nsswitch.conf`
- Beispiel:

```
passwd: files ldap
shadow: files
group: files ldap
hosts: files dns
netgroup: ldap
...
```

NSS (cont.)

- Demonstration am Linux-System...

PAM

- Pluggable Authentication Modules
- Konfiguration über Module unterhalb `/etc/pam.d/`
- Modulares Konzept für Linux für verschiedenste Authentisierungsquellen:
  - Traditionelle Unix-Authentisierung über Hashes in `/etc/shadow`
  - LDAP – kann man ja auch als Authentisierer (miss)brauchen
  - Kerberos

SSSD

- System Security Services Daemon
- https://pagure.io/SSSD/sssd
- Beschafft Namensinformationen und regelt Authentisierung
- Verschiedene SSSD Provider für die unterschiedlichen Netzwerkdienste, u.a.:
  - Kerberos Provider: `libsss_krb5.so`
  - LDAP Provider: `libsss_ldap.so`
  - FreeIPA Provider: `libsss_ipa.so`
  - Active Directory Provider: `libsss_ad.so`
- NSS-Modul: `libnss_sss.so.2`
- PAM-Modul: `pam_sss.so`

Workshop

- Vagrantfile: https://www.kerberos-buch.de/tuebix-2018
- Startden der VM mit `vagrant up`
- DNS-Resolver: `/etc/resolv.conf`:

```
search tuebix.example.com
nameserver 81.169.235.122
```

- Kerberos-Konfiguration `/etc/krb5.conf`:

```
[libdefaults]
default_realm = TUEBIX.EXAMPLE.COM
```

Workshop (cont.)

- Tests:

```
[root@centos7 ~]# ping dc1.tuebix.example.com
[root@centos7 ~]# dig +short dc1.tuebix.example.com \
                                @dc1.tuebix.example.com
81.169.235.122
[root@centos7 ~]# kinit Administrator
Password for Administrator@TUEBIX.EXAMPLE.COM:
[root@centos7 ~]# ldapsearch -Q -Y GSSAPI -LLL \
                  -H ldap://dc1.tuebix.example.com \
                  -b "DC=tuebix,DC=example,DC=com" \
                  sAMAccountNAme=Administrator cn
dn: CN=Administrator,CN=Users,DC=tuebix,DC=example,DC=com
cn: Administrator

...
```

Workshop (cont.)

- Host-Keytab erstellen

```
[root@centos7 ~]# yum install msktutil
[root@centos7 ~]# kinit Administrator
[root@centos7 ~]# msktutil --create
[root@centos7 ~]# kdestroy
```

- Tests:
  - `ldapsearch` mit `KRB5_CLIENT_KTNAME`

Workshop (cont.)

- Übersicht über die AD-Struktur

```
[root@centos7 ~]# ldapsearch -Q -Y GSSAPI -LLL \
                  - H ldap://dc1.tuebix.example.com \
                  -b "DC=tuebix,DC=example,DC=com" \
                   '(objectclass=container)'  -s one
dn: CN=Computers,DC=tuebix,DC=example,DC=com
dn: CN=Managed Service Accounts,DC=tuebix,DC=example,DC=com
dn: CN=Program Data,DC=tuebix,DC=example,DC=com
dn: CN=Users,DC=tuebix,DC=example,DC=com
dn: CN=ForeignSecurityPrincipals,DC=tuebix,DC=example,DC=com
dn: CN=System,DC=tuebix,DC=example,DC=com
```

Workshop (cont.)

- Container-Objekt erzeugen:

```
[root@centos7 ~]# cat cn\=tuebix-tests.ldif
dn: CN=TuebixTests,DC=tuebix,DC=example,DC=com
objectClass: top
objectClass: container
cn: TuebixTests

[root@centos7 ~]# ldapadd -Q -Y GSSAPI \
                  -H ldap://dc1.tuebix.example.com \
                  < cn\=tuebix-tests.ldif
adding new entry "CN=TuebixTests,DC=tuebix,DC=example,DC=com"
```

Workshop (cont.)

- OU-Objekt erzeugen:

```
[root@centos7 ~]# cat ou\=tuebix-users.ldif
dn: ou=TuebixUsers,DC=tuebix,DC=example,DC=com
objectClass: top
objectClass: organizationalUnit
ou: TuebixUsers

[root@centos7 ~]# ldapadd -Q -Y GSSAPI \
                  -H ldap://dc1.tuebix.example.com \
                  < ou\=tuebix-users.ldif
adding new entry "ou=TuebixUsers,DC=tuebix,DC=example,DC=com"
```

Workshop (cont.)

- User-Objekt erzeugen:

```
[root@centos7 ~]# echo -n '"P@ssw0rd"' | iconv -t UCS2  | \
                  openssl base64 -e
IgBQAEAAcwBzAHcAMAByAGQAIgA=


[root@centos7 ~]# cat cn\=jdoe.ldif
dn: cn=John Doe,ou=TuebixUsers,DC=tuebix,DC=example,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: John Doe
sn: Doe
givenName: John
instanceType: 4
displayName: John Doe
name: John Doe
userAccountControl: 512
sAMAccountName: jdoe
userPrincipalName: jdoe@TUEBIX.EXAMPLE.COM
unicodePwd:: IgBQAEAAcwBzAHcAMAByAGQAIgA=
pwdLastSet: 0
[root@centos7 ~]#

[root@centos7 ~]# ldapadd -Y GSSAPI -Q -H ldap://dc1.tuebix.example.com < cn\=jdoe.ldif
adding new entry "cn=John Doe,ou=TuebixUsers,DC=tuebix,DC=example,DC=com"
```

Workshop (cont.)

- mehrere User Anlegen:

```
[root@centos7 ~]# for i in `seq -w 1 100`; do \
                  cat cn\=jdoe.ldif | \
                  sed -e 's/jdoe/tuebix'$i'/'  \
                      -e 's/John/Tue_'$i'/'  \
                      -e 's/Doe/Bix/' ; echo ;  done \
                  | ldapadd -Q -Y GSSAPI \
                    -H ldap://dc1.tuebix.example.com
```

Workshop (cont.)

- SSSD-Konfiguration:

```
[root@centos7 ~]# yum install sssd sssd-ad
[root@centos7 ~]# cat /etc/sssd/sssd.conf
[sssd]
domains = TUEBIX.EXAMPLE.COM
services = nss, pam
config_file_version = 2

[domain/TUEBIX.EXAMPLE.COM]
id_provider = ad
auth_provider = ad
access_provider = ad
chpass_provider = ad
enumerate = true
fallback_homedir = /home/%u
default_shell = /bin/bash

[root@centos7 ~]# authconfig --kickstart \
                    --enablesssd --enablesssdauth
```

- Test der AD-Anbindung:

```
[root@centos7 ~]# id tuebix0100
uid=982801207(tuebix0100) gid=982800513(domain users) groups=982800513(doma
[root@centos7 ~]#
[root@centos7 ~]# ssh -l tuebix0100 localhost
tuebix0100@localhost's password:
Password expired. Change your password now.
Last failed login: Fri Jun  8 21:56:50 CEST 2018 from ::1 on ssh:notty
There was 1 failed login attempt since the last successful login.
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tuebix0100.
Current Password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Connection to localhost closed.
[root@centos7 ~]#
```

Weitere Themen

- RFC-2307 (bis) / SSSD-Usermapping
- Login-Rechte verwalten / SSSD-Access-Provider
- Kerberisierter SSH-Login
- Fragen und Antworten