



Identity and Access Management

av

Pål Karlsen

Ola Grytting

Kristoffer Svendsen

Jorund Sandnes

IKT 207

Cybersikkerhet

Veiledet av

Sigurd Kristian Brinch

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, Oktober 2020

1 Google Authenticator

1. Installerte Google Authenticator på server og telefon.
2. Brukte kommandoene:
`yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm`
og `"yum install google-authenticator"`
3. Etter installasjon brukte vi kommandoen: `google-authenticator`.
Fikk ja/nei spørsmål å svare på. Etter fler ja svar dukket en QR-kode opp. 4. Scannet QR-koden som ble vist. Lagde en ny autentikator.
5. Logget inn på serveren på nytt ved hjelp av autentikatoren.

2 LDAP

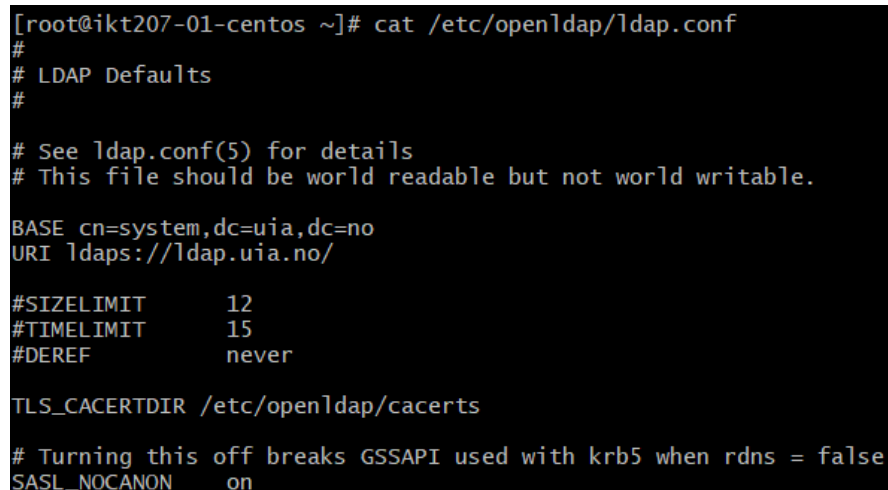
2.1 Konfigurerings

Når vi skulle konfigurere LDAP, brukte vi config filen fra en virtuell maskin fra ikt-208 som inspirasjon. Vi kopierte ikke filen, men så hvordan den var satt opp, og brukte de innstillingene som var relevante for vår oppgave. For å skjønne hvordan LDAP fungerer, søkte vi opp diverse parametrene og fant ut av hva de gjorde og hvordan man brukte dem.

1. Installere LDAP
2. Kommando:
`"yum install authconfig authconfig-gtk openLDAP openLDAP-clients sssd oddjob-mkhomedir.x86_64 -y"`
3. Installasjon funket så vi brukte denne kommandoen:
`"authconfig --enableldap --enableldapauth /`
`--ldapserver=ldap.example.com --ldapbasedn="dc=example,dc=com" --enablemkhomedir --update"`

Vi måtte også endre URI-en i `ldap.conf` fordi URI-en vi fikk etter kommandoen over var URI `ldap://ldap.uia.no`, men vi skal ha `ldaps` og ikke `ldap`.

Endte da med figur 1:



```
[root@ikt207-01-centos ~]# cat /etc/openldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE cn=system,dc=uia,dc=no
URI ldaps://ldap.uia.no/

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

TLS_CACERTDIR /etc/openldap/cacerts

# Turning this off breaks GSSAPI used with krb5 when rdns = false
SASL_NOCANON    on
```

Figure 1: LDAP.conf

4. Gikk inn på `sssd.conf` som ligger inne på `/etc/sss/sss.conf` og endret det til figur 2.

```
[root@ikt207-01-centos ~]# cat /etc/sss/sss.conf
[domain/default]

autofs_provider = ldap
cache_credentials = True
ldap_search_base = cn=system,dc=uia,dc=no
ldap_user_search_base = cn=users,cn=system,dc=uia,dc=no
ldap_group_search_base = cn=filegroups,cn=system,dc=uia,dc=no
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldaps://ldap.uia.no/
ldap_id_use_start_tls = True
ldap_tls_reqcert = allow
ldap_tls_cacertdir = /etc/openldap/cacerts
access_provider = simple
simple_allow_users = paaltk16,kristoffes
min_id = 500
enumerate = False
debug_level = 9
[sss]
config_file_version = 2
reconnection_retries = 3
sbus_timeout = 30
services = nss, pam, autofs

domains = default
[nss]
filter_groups = root
filter_users = root
reconnection_retries = 3
override_homedir = /home/%u

[pam]
reconnection_retries = 3

[sudo]

[autofs]

[ssh]

[pac]

[ifp]

[secrets]

[session_recording]
```

Figure 2

5. for å kunne bruke UiA brukernavn og passord måtte vi inn på `/etc/pam.d/sshd` og deaktivere google-autentikator. Vi måtte også legge til

```
auth required pam_listfile.so item=user sense=allow file=/etc/ssh/sshd.allow.
```

Denne linja sjekker navnene i filen: `/etc/ssh/sshd.allow`. Det er strengt tatt bare hvis brukernavnene er der at de får ssh tilgang.

```
#auth required pam_google_authenticator.so
auth required pam_listfile.so item=user sense=allow file=/etc/ssh/sshd.allow
```

Figure 3: Endring i `/etc/pam.d/sshd`

3 Refleksjon

Selv om vi støtte på noen små problemer underveis, var ikke denne oppgaven like krevende som den forrige. Google authenticator var veldig rett frem og sette opp og gikk relativt fort. LDAP slet vi litt mer med, men dette var mest vår egen feil: Vi begynte med å endre en fil som egentlig ikke skulle endres på. Vi fikk resatt disse og begynte på nytt. Det var fortsatt ikke helt rett frem, og var litt kronglete og finne rett informasjon

LDAP var ganske vanskelig å sette opp. Vi klarte å få kontakt med UiA sin LDAP server, men vi kunne

ikke logge inn med våre brukere. For å få fikset dette måtte vi inn på `sssd.conf` filen og legge til `override_homedir = /home/$u`. Når dette var gjort kunne vi bruke kommandoen `su bruker` og logge oss inn med UiA passordet og brukeren vår. Men vi klarte fortsatt ikke å ssh-e oss inn med bruk av passord inn på brukeren. Etter mye søk på nettet fant vi endelig en løsning som tillatte oss å ssh-e inn med UiA brukernavn og passord

Vi fant et program som heter `AuthConfig` og `Authconfig-gtk` som satt opp LDAP for oss. Selv om alt var satt opp automatisk måtte vi endre et par parametere siden vi skulle ha en litt annen URI enn den vi fikk av programmet. Vi måtte også manuelt endre mye i `sssd.conf` filen som gjorde at vi faktisk fikk lov til å aksessere `ldap.uia.no`.

Av personlig erfaring var denne oppgaven tung på starten, men rettet seg mer ut mot slutten. Det var utrolig mange config filer å lese gjennom for å finne ut hva som faktisk skjedde og hvordan det fungerte. Når vi hadde fått lest gjennom dette gikk det litt på løpende bånd. Vi fikk satt opp alt vi skulle, endret på det vi skulle. Litt innimellom stoppet det opp fordi serveren ikke ville tillate oss å gjøre det vi ville, men det løsnet når vi fikk søkt litt opp på nett om det.

4 Pakkelister

4.1 Google-authenticator pakke

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: centos.mirror.far.fi
* epel: epel.mirror.omnilance.com
* extras: centos.mirror.far.fi
* updates: centos.mirror.far.fi
package: google-authenticator.x86_64 1.04-1.el7
dependency: libc.so.6(GLIBC_2.14)(64bit)
  provider: glibc.x86_64 2.17-307.el7.1
dependency: libdl.so.2()(64bit)
  provider: glibc.x86_64 2.17-307.el7.1
dependency: libdl.so.2(GLIBC_2.2.5)(64bit)
  provider: glibc.x86_64 2.17-307.el7.1
dependency: libpam.so.0()(64bit)
  provider: pam.x86_64 1.1.8-23.el7
dependency: libpam.so.0(LIBPAM_1.0)(64bit)
  provider: pam.x86_64 1.1.8-23.el7
dependency: rtld(GNU_HASH)
  provider: glibc.x86_64 2.17-307.el7.1
  provider: glibc.i686 2.17-307.el7.1
```

4.2 LDAP Pakke

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: centos.mirror.far.fi
* epel: epel.mirror.omnilance.com
* extras: centos.mirror.far.fi
* updates: centos.mirror.far.fi
package: openldap.i686 2.4.44-21.el7_6
dependency: /bin/bash
  provider: bash.x86_64 4.2.46-34.el7
dependency: /bin/sh
  provider: bash.x86_64 4.2.46-34.el7
dependency: coreutils
  provider: coreutils.x86_64 8.22-24.el7
dependency: findutils
  provider: findutils.x86_64 1:4.5.11-6.el7
```

```
dependency: libc.so.6(GLIBC_2.12)
  provider: glibc.i686 2.17-307.el7.1
dependency: libcrypto.so.10
  provider: openssl-libs.i686 1:1.0.2k-19.el7
dependency: libcrypto.so.10(OPENSSL_1.0.1_EC)
  provider: openssl-libs.i686 1:1.0.2k-19.el7
dependency: libcrypto.so.10(libcrypto.so.10)
  provider: openssl-libs.i686 1:1.0.2k-19.el7
dependency: libdl.so.2
  provider: glibc.i686 2.17-307.el7.1
dependency: libnspr4.so
  provider: nspr.i686 4.21.0-1.el7
dependency: libnss3.so
  provider: nss.i686 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.12)
  provider: nss.i686 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.12.5)
  provider: nss.i686 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.2)
  provider: nss.i686 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.9)
  provider: nss.i686 3.44.0-7.el7_7
dependency: libnssutil3.so
  provider: nss-util.i686 3.44.0-4.el7_7
dependency: libplc4.so
  provider: nspr.i686 4.21.0-1.el7
dependency: libplds4.so
  provider: nspr.i686 4.21.0-1.el7
dependency: libpthread.so.0
  provider: glibc.i686 2.17-307.el7.1
dependency: libpthread.so.0(GLIBC_2.0)
  provider: glibc.i686 2.17-307.el7.1
dependency: libpthread.so.0(GLIBC_2.1)
  provider: glibc.i686 2.17-307.el7.1
dependency: libpthread.so.0(GLIBC_2.3.2)
  provider: glibc.i686 2.17-307.el7.1
dependency: libresolv.so.2
  provider: glibc.i686 2.17-307.el7.1
dependency: libresolv.so.2(GLIBC_2.2)
  provider: glibc.i686 2.17-307.el7.1
dependency: libsasl2.so.3
  provider: cyrus-sasl-lib.i686 2.1.26-23.el7
dependency: libsmime3.so
  provider: nss.i686 3.44.0-7.el7_7
dependency: libssl.so.10
  provider: openssl-libs.i686 1:1.0.2k-19.el7
dependency: libssl.so.10(libssl.so.10)
  provider: openssl-libs.i686 1:1.0.2k-19.el7
dependency: libssl3.so
  provider: nss.i686 3.44.0-7.el7_7
dependency: nss-tools
  provider: nss-tools.x86_64 3.44.0-7.el7_7
dependency: rpm
  provider: rpm.x86_64 4.11.3-43.el7
dependency: rtld(GNU_HASH)
  provider: glibc.x86_64 2.17-307.el7.1
  provider: glibc.i686 2.17-307.el7.1
package: openldap.x86_64 2.4.44-21.el7_6
dependency: /bin/bash
```

```
provider: bash.x86_64 4.2.46-34.el7
dependency: /bin/sh
provider: bash.x86_64 4.2.46-34.el7
dependency: coreutils
provider: coreutils.x86_64 8.22-24.el7
dependency: findutils
provider: findutils.x86_64 1:4.5.11-6.el7
dependency: libc.so.6(GLIBC_2.14)(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libcrypto.so.10()(64bit)
provider: openssl-libs.x86_64 1:1.0.2k-19.el7
dependency: libcrypto.so.10(OPENSSL_1.0.1_EC)(64bit)
provider: openssl-libs.x86_64 1:1.0.2k-19.el7
dependency: libcrypto.so.10(libcrypto.so.10)(64bit)
provider: openssl-libs.x86_64 1:1.0.2k-19.el7
dependency: libdl.so.2()(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libnspr4.so()(64bit)
provider: nspr.x86_64 4.21.0-1.el7
dependency: libnss3.so()(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.12)(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.12.5)(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.2)(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libnss3.so(NSS_3.9)(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libnssutil3.so()(64bit)
provider: nss-util.x86_64 3.44.0-4.el7_7
dependency: libplc4.so()(64bit)
provider: nspr.x86_64 4.21.0-1.el7
dependency: libplds4.so()(64bit)
provider: nspr.x86_64 4.21.0-1.el7
dependency: libpthread.so.0()(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libpthread.so.0(GLIBC_2.2.5)(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libpthread.so.0(GLIBC_2.3.2)(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libresolv.so.2()(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libresolv.so.2(GLIBC_2.2.5)(64bit)
provider: glibc.x86_64 2.17-307.el7.1
dependency: libsasl2.so.3()(64bit)
provider: cyrus-sasl-lib.x86_64 2.1.26-23.el7
dependency: libmime3.so()(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: libssl.so.10()(64bit)
provider: openssl-libs.x86_64 1:1.0.2k-19.el7
dependency: libssl.so.10(libssl.so.10)(64bit)
provider: openssl-libs.x86_64 1:1.0.2k-19.el7
dependency: libssl3.so()(64bit)
provider: nss.x86_64 3.44.0-7.el7_7
dependency: nss-tools
provider: nss-tools.x86_64 3.44.0-7.el7_7
dependency: rpm
provider: rpm.x86_64 4.11.3-43.el7
```

```
dependency: rtld(GNU_HASH)
provider: glibc.x86_64 2.17-307.el7.1
provider: glibc.i686 2.17-307.el7.1
```

5 Konfigurasjonsfiler for LDAP

```
/etc/openldap/check_password.conf
/etc/openldap/schema/collective.ldif
/etc/openldap/schema/collective.schema
/etc/openldap/schema/corba.ldif
/etc/openldap/schema/corba.schema
/etc/openldap/schema/core.ldif
/etc/openldap/schema/core.schema
/etc/openldap/schema/cosine.ldif
/etc/openldap/schema/cosine.schema
/etc/openldap/schema/duaconf.ldif
/etc/openldap/schema/duaconf.schema
/etc/openldap/schema/dyngroup.ldif
/etc/openldap/schema/dyngroup.schema
/etc/openldap/schema/inetorgperson.ldif
/etc/openldap/schema/inetorgperson.schema
/etc/openldap/schema/java.ldif
/etc/openldap/schema/java.schema
/etc/openldap/schema/misc.ldif
/etc/openldap/schema/misc.schema
/etc/openldap/schema/nis.ldif
/etc/openldap/schema/nis.schema
/etc/openldap/schema/openldap.ldif
/etc/openldap/schema/openldap.schema
/etc/openldap/schema/pmi.ldif
/etc/openldap/schema/pmi.schema
/etc/openldap/schema/ppolicy.ldif
/etc/openldap/schema/ppolicy.schema
/etc/openldap/slapd.conf
/etc/openldap/slapd.conf.bak
/etc/sysconfig/slapd
/usr/lib/tmpfiles.d/slapd.conf
/etc/openldap/ldap.conf
/usr/lib/tmpfiles.d/openldap.conf
```