SSH PublicKeys in LDAP

Bron: http://pig.made-it.com/ldap-openssh.html

Deze Wiki pagina beschrijft de configuratie van OpenSSH voor het gebruik van sshPublicKeys in LDAP.

Voorbeeld machine: **wordpress** op Pilot platform.

Op **wordpress** moet de volgende ldapsearch query lukken:

```
$ ldapsearch -H ldaps://ldap.pilot.scz.lab.surf.nl -b 'dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl' -D 'cn=Admin,
dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl' -w *** sshPublicKey
```

```
# vi /opt/fetchSSHKeysFromLDAP
```

```
#!/bin/sh
ldapsearch \
 -H ldaps://ldap.pilot.scz.lab.surf.nl \
 -b 'dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl' \
 -D 'cn=Admin,dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl' \
 -w *** \
 '(&(objectClass=ldapPublicKey)(uid='"$1"'))' \
 'sshPublicKey' \
 | sed -n '/^ /{H;d};/sshPublicKey:/x;$g;s/\n *//g;s/sshPublicKey: //gp'
```

```
# chmod 500 /opt/fetchSSHKeysFromLDAP
```

```
# vi /etc/ssh/sshd_config
```

```
+ AuthorizedKeysCommand /opt/fetchSSHKeysFromLDAP
+ AuthorizedKeysCommandUser root
```

```
# systemctl restart sshd
```

Maak een pub/priv keypair

```
$ ssh-keygen
```

copy-paste .ssh/id_rsa.pub in COmanage id SSH Key (without "ssh-rsa" prefix!)

CO manage id add identifiers:

- uid
- uidNumber
- gidNumber
- homeDirectory

COManage: Reprovision All

Controleer LDAP sshPublicKey:

```
# /opt/fetchSSHKeysFromLDAP martinus
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA.... martinus@wordpress ...
```

```
# apt install libnss-ldap
```

```
# vi /etc/nsswitch.conf
```

```
- passwd: compat
- group: compat
+ passwd: compat ldap
+ group: compat ldap
```

In case apt install libnss-ldap did not ask for configuration questions:

```
# vi /etc/libnss-ldap.conf
```

```
+ base dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl
+ uri ldaps://ldap.pilot.scz.lab.surf.nl/
+ ldap_version 3
+ rootbinddn cn=Admin,dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl
```

```
# vi /etc/libnss-ldap.secret
```

```
+ *****
```

```
# vi /etc/pam_ldap.conf
```

```
+ base dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl
+ uri ldaps://ldap.pilot.scz.lab.surf.nl/
+ ldap_version 3
+ binddn cn=Admin,dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl
+ bindpw ******
+ rootbinddn cn=Admin,dc=pilot,dc=scz,dc=lab,dc=surf,dc=nl
```

```
# vi /etc/pam_ldap.secret
```

```
+ *****
```

```
# vi /usr/share/pam-configs/mkhomedir
```

```
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
 required pam_mkhomedir.so umask=0022 skel=/etc/skel
```

```
# vi /etc/pam.d/sshd
```

```
+ session required pam_mkhomedir.so umask=0022 skel=/etc/skel
# Standard Un*x session setup and teardown.
```

Test configuration.

```
# getent passwd
```

```
...

martinus:*:1035:1035:Bassie Baas:/home/baas:/bin/bash
```

```
# id <testuser in ldap>
```

```
uid=1035(martinus) gid=1035 groups=1035
```

Test ssh login:

```
$ ssh -i ~martin/.ssh/id_rsa martinus@localhost
```

```
Linux wordpress 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 25 11:53:04 2018 from 127.0.0.1
martinus@wordpress:~$ pwd
/home/baas

martinus@wordpress:~$
```