openssh-ldap-pubkey Documentation

Release 0.3.0

Kouhei Maeda

May 18, 2020

Contents

Contents:

CHAPTER 1

openssh-ldap-pubkey

1.1 Status

1.2 Requirements

1.2.1 LDAP server

- Add openssh-lpk schema.
- Add an objectClass ldapPublicKey to user entry.
- Add one or more sshPublicKey attribute to user entry.

1.2.2 OpenSSH server

- OpenSSH over 6.2.
- Installing this utility.
- Setup `AuthorozedKeysCommand` and `AuthorizedKeysCommandUser` in `sshd_config`.

1.3 See also

- OpenSSH 6.2 release

- openssh-lpk

CHAPTER 2

How to setup LDAP server for openssh-lpk

2.1 Precondition

This article restricts OpenLDAP with `slapd_config` on Debian systems only.

2.2 Requirements

- Debian Wheezy later or Ubuntu Precise later.
- OpenLDAP(slapd) 2.4.28 over.
- debconf-utils
- ldap-utils
- ldapvi
- openssh-lpk schema

2.3 Install

1. Prepare debconf configuration for slad. Replace each parameters for your envirionment.

```
$ cat << EOF > debconf.txt
slapd     slapd/password1 password
slapd     slapd/internal/adminpw  password
slapd     slapd/internal/generated_adminpw        password
slapd     slapd/password2 password
slapd     slapd/unsafe_selfwrite_acl      note
slapd     slapd/allow_ldap_v2     boolean false
slapd     shared/organization     string  example.org
```

(continues on next page)

(continued from previous page)

```
slapd     slapd/move_old_database boolean true
slapd     slapd/password_mismatch note
slapd     slapd/dump_database     select  when needed
slapd     slapd/dump_database_destdir     string  /var/backups/slapd-VERSION
slapd     slapd/invalid_config    boolean true
slapd     slapd/domain    string  example.org
slapd     slapd/backend   select  HDB
slapd     slapd/purge_database    boolean true
slapd     slapd/no_configuration  boolean false
EOF
```

Note: debconf separator is `tab`.

See `sample debconf configuration`.

2. Install packages except of slapd.

```
$ sudo apt-get install debconf-utils ldap-utils ldapvi
```

3. Download openssh-lpk schema and convert to LDIF.

```
$ curl https://openssh-lpk.googlecode.com/svn/trunk/schemas/openssh-lpk_openldap.
↪schema | sed "
1i\dn: cn=openssh-lpk,cn=schema,cn=config\nobjectClass: olcSchemaConfig\ncn:␣
↪openssh-lpk
/^#/d
/^$/d
:a
/ $/N
/ $/b a
s/\n//g
s/\t//g
/octetStringMatch$/N
s/\n/ /
/AUXILIARY$/N
s/\n/ /
/objectclass'$/N
s/\n//
s/^attributetype (/olcAttributeTypes: {0}(/
s/^objectclass (/olcObjectClasses: {0}(/
:b
/ $/N
/ $/b b
s/\n//g
s/\t//g
" > openssh-lpk.ldif
```

See `the convert script, openssh-lpk schema ldif`.

4. Prepare the LDIF for changing for rootdn password.

```
$ cat << EOF > rootdnpw.ldif
dn: olcDatabase={1}hdb,cn=config
changetype: modify
replace: olcRootPW
```

(continues on next page)

(continued from previous page)

```
olcRootPW: {SSHA}BADfSMMJo53/L/gaFiG0xqKnOsmds4fW
EOF
```

Replace the `olcRootPW` value by generated with `slappasswd` command.[1]

See `the change rootdn password LDIF`.

5. Prepare the LDIF of `organizationalUnit` entry.

```
$ cat <<EOF > ou.ldif
dn: ou=People,dc=example,dc=org
objectClass: organizationalUnit
ou: People
EOF
```

Replace the `dn` and `ou` value.

See `the adding ou LDIF`.

6. Prepare the LDIF of user entry.

```
$ cat << EOF > users.ldfi
dn: uid=user0,ou=People,dc=example,dc=org
cn: user0
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: ldapPublicKey
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
sn: user0
homeDirectory: /home/user0
mail: user0@example.org
uid: user0
sshPublicKey: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8OldtAiW9lQ0/
↪2VJcc9UpRW9nfcusGXEu2sS+p5kh05zTYWGd8xHgZD0vfoQfpTfSKuHsL6qlMyKQMfsULWQoMJmMhJZc2hU1LH4u9HXYwJ
↪qfE4lc5A0xd2En9Qc172naHD+cRHZxhfNNYEGhW7E6eYm02Gn4fBN8hSpuZzv3WlpRgFiAWGv9CqObdQUEFFnpYLnC2kma
↪DmGyEg8nIBu4U74Sigfcl6dsJmA2qlOqSxia21mnQEFiSARB74pakgiywFV user0@workstation
sshPublicKey: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCrMQOAP3o58yl96HjEsheDAO/qgQ/
↪mLVJK7DW+VFbJ9dGJpJfB4CBXPoT9bfSn4y6dotqjBA1eDbpDyzrhLkIe1MWZrRjkFbzAtB54ydKSU48URsb+XtGnN6kKK
↪iaORVO/tZRPA0vdQwP0qkUf//neUmXXbSxOSm+ekQvZI9KfJ2tWxe+mVSFt+PcC2P4A/
↪bW9dCNplqZdFTMQxLYFpl5ZOz3fwWcy34Shcb5nSZbjpKZdNrpuUCLwq2FMxorupko8kf4RmvMYO3G6p6OqpoIt6raB8DD
↪f6jdgPA31HK0sejX user0@vm01
userPassword:{SSHA}eKfVPm3raZmYPx5Os+KGKVUPVb6P+766

dn: uid=user1,ou=People,dc=example,dc=org
(snip)
EOF
```

Replace the values of `dn`, `cn`, `loginShell`, `uidNumber`, `gidNumber`, `sn`, `homeDirectory`, `mail`, `uid`, `sshPublicKey`.

See `the adding users LDIF`.

7. Change slapd configuration.

[1] `slappasswd` command is contained in `slapd` package. Use `slappasswd` command in other system.

```
$ sudo ldapadd -H ldapi:/// -Y EXTERNAL -f openssh-lpk.ldif
$ sudo ldapmodify -H ldapi:/// -Y EXTERNAL -f rootdnpw.ldif
$ sudo ldapadd -x -h localhost -D cn=admin,dc=example,dc=org -W -f ou.ldif
$ sudo ldapadd -x -h localhost -D cn=admin,dc=example,dc=org -W -f users.ldif
```

footnote

CHAPTER 3

How to setup OpenSSH server

3.1 Precondition

This article restricts OpenSSH 6.2 over on Debian systems only.

Note: You can use openssh-ldap package instead of this utility in the distribution based RHEL.

3.2 Requirements

- Debian Jessie later or Ubuntu Trusty later.
- OpenSSH 6.2 over
- openssh-ldap-pubkey
- Go 1.2 over

3.2.1 Optional

- nslcd

3.3 Install with nslcd (recommend)

When the following precondition is sufficient, `openssh-ldap-pubkey` can loads parameters from `/etc/nslcd.conf`.

- `nslcd` package is installed.
- There is `/etc/nslcd.conf`.

- Set `root` to `AuthorizedKeysCommandUser` of `/etc/ssh/sshd_config`.

The parameters are follows.

Table 1: nslcd.conf keys compare openssh-ldap-pubkey options.

nslcd.conf	openssh-ldap-pubkey
`uri` ldap://example.org ldaps://example.org	`host`, `port`, `tls` example.org, 389, false example.org, 636, true
`base` dc=example,dc=org	`base` dc=example,dc=org
`pam_authz_search` (&(objectClass=posixAccount)(uid=$username))	`filter` (&(objectClass=posixAccount)(uid=%s))
`tls_reqcert` never, allow try, demand, hard	`skip` true false
`binddn` (option for bind) cn=admin,dc=example,dc=org	n/a
`bindpw` (option for bind) examplepassword	n/a

1. Download binary.

```
$ export GOPATH=/path/to/gocode
$ go get github.com/mkouhei/openssh-ldap-pubkey
$ chmod 0755 /path/to/gocode/bin/openssh-ldap-pubkey
$ sudo chown root: /path/to/gocode/bin/openssh-ldap-pubkey
```

2. Setup sshd_config.

   Appends `AuthorizedKeysCommand` and `AuthorizedKeysCommandUser`.

```
AuthorizedKeysCommand /path/to/openssh-ldap-pubkey
AuthorizedKeysCommandUser root
```

3. Restart sshd.

```
$ sudo service ssh restart
```

3.4 Install without nslcd

If `nslcd` is not installed and there is not `/etc/nslcd.conf`, you should prepare wrapper script of `openssh-ldap-pubkey`.

1. Download binary.

```
$ export GOPATH=/path/to/gocode
$ go get github.com/mkouhei/openssh-ldap-pubkey
$ chmod 0755 /path/to/gocode/bin/openssh-ldap-pubkey
$ sudo chown root: /path/to/gocode/bin/openssh-ldap-pubkey
```

2. Prepare wrapper script.

   without TLS,

```
$ sudo bash -c "cat << EOF > /etc/ssh/openssh-ldap-pubkey.sh
#!/bin/sh -e
/path/to/openssh-ldap-pubkey -host=ldap.example.org -base=dc=example,dc=org $1
EOF
$ sudo chmod +x /etc/ssh/openssh-ldap-pubkey.sh
```

   with TLS.

```
$ sudo bash -c "cat << EOF > /etc/ssh/openssh-ldap-pubkey.sh
#!/bin/sh -e
/path/to/openssh-ldap-pubkey -host=ldap.example.org -port 636 -base=dc=example,
↪dc=org -tls=true $1
EOF
$ sudo chmod +x /etc/ssh/openssh-ldap-pubkey.sh
```

3. Setup sshd_config.

   Appends `AuthorizedKeysCommand` and `AuthorizedKeysCommandUser`.

```
AuthorizedKeysCommand /etc/ssh/openssh-ldap-pubkey.sh
AuthorizedKeysCommandUser root
```

4. Restart sshd.

```
$ sudo service ssh restart
```

CHAPTER 4

History

4.1 0.3.0 (2020-05-18)

- Supports Golang 1.11 - 1.14.
- Use system CA certs.
- Updates snakeoil certs for testing.
- Fixes golint path.

4.2 0.2.0 (2018-09-30)

- Supports Golang 1.10.
- Refactorng.
- Supports IPv6 link-local address.

4.3 0.1.3 (2018-08-18)

- Supports binddn/bindpw for nslcd.
  - Thanks Nicolas Ledez (@nledez)
- Fixes LDAPS default port.

4.4 0.1.2 (2017-11-25)

- Supports Go 1.9, and more over.

- Adds debug mode.

4.5 0.1.1 (2015-10-16)

- Fixes #2 Cannot resolve LDAP server FQDN by IPv6.

4.6 0.1.0 (2015-10-16)

- First release.

CHAPTER 5

Contributors

- Nicolas Ledez (@nledez)
- Sebastien BLAISOT (@sblaisot)

CHAPTER 6

Indices and tables

- genindex
- modindex
- search