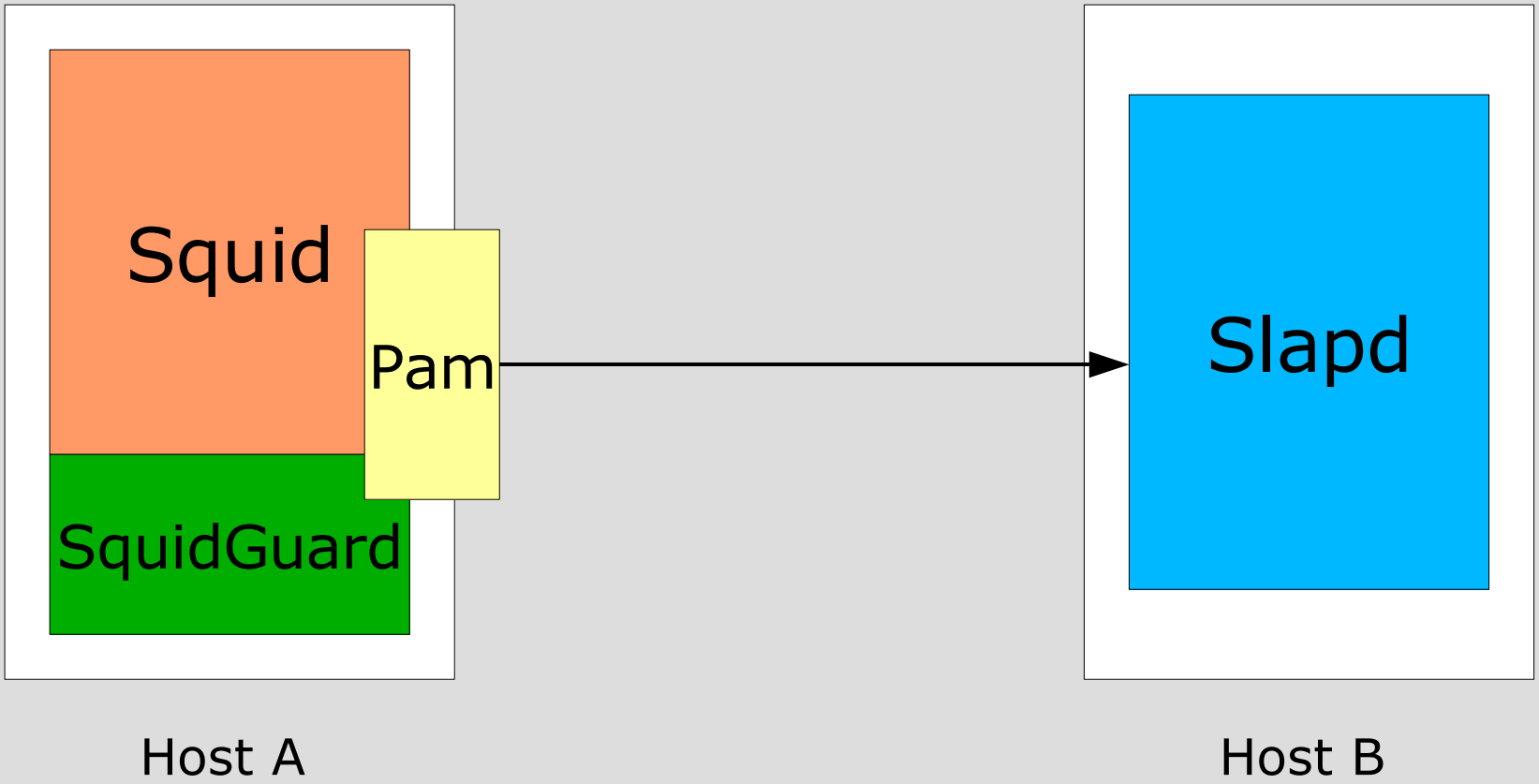
Squid+SquidGuard+PAM+OpenLDAP



Squid

Squid is...

* a full-featured Web proxy cache
* designed to run on Unix systems
* free, open-source software
* the result of many contributions by unpaid (and paid) volunteers

Squid

Squid supports...

* proxying and caching of HTTP, FTP, and other URLs
* proxying for SSL
* cache hierarchies
* ICP, HTCP, CARP, Cache Digests
* transparent caching
* WCCP (Squid v2.3 and above)
* extensive access controls
* HTTP server acceleration
* SNMP
* caching of DNS lookups

Squid: installazione e configurazione

-apt-get install squid

-configurazione:

```
http_port 8080
visible_hostname localhost
cache_mem 20 MB
cache_mgr root
```

-configurazione ACL:

```
acl myacl1 proxy_auth REQUIRED
acl myacl2 time 08:00-19:00
acl myacl3 src 127.0.0.1/255.255.255.255
http_access allow myacl1 myacl2 myacl3
http_access deny all
```

Squid: configurazione

-configurazione dello schema di autenticazione:

auth_param basic program /usr/lib/squid/pam_auth -n squid

-configurazione del redirector:

redirect_program /usr/bin/squidGuard

SquidGuard

SquidGuard is a combined filter, redirector and access controller plugin for Squid. It is

* free
* very flexible
* extremely fast *)
* easily installed
* portable

SquidGuard

squidGuard can be used to

* limit the web access for some users to a list of accepted/well known web servers and/or URLs only.
* block access to some listed or blacklisted web servers and/or URLs for some users. **)
* block access to URLs matching a list of regular expressions or words for some users. **)
* redirect unregistered user to a registration form.
* have different access rules based on time of day, day of the week, date etc.
* have different rules for different user groups.
* and much more..

SquidGuard: installazione e configurazione

-installazione: apt-get install squidguard

-modifica di /etc/squid/squidGuard.conf: definizione dei **source groups**

```
src stud-clients {
    ip      127.0.0.1/24
    user        stud1 stud2
    within      workhours
}
```

```
src prof-clients {
    ip      127.0.0.1/24
    user        prof1 prof2
    within      workhours
}
```

```
src admin {
    ip      127.0.0.1/24
    user        admin
}
```

SquidGuard: configurazione

definizione dei **destination groups**

```
dest all{
}
dest adult{
    domainlistadult/domains
    urllist        adult/urls
    expressionlist     adult/expressions
    log anonymous   porn.log
}
dest unife{
    domainlistunife/domains
}
```

SquidGuard: configurazione

definizione delle ACL:

```
admin {
    pass    any
}

stud-clients within workhours{
    pass unife none
    redirect http://localhost...
}

prof-clients within workhours {
    pass !adult all
    redirect http://localhost...
}

default {
        pass   none
        redirect http://localhost...
}
```

PAM

PAM = Pluggable Authentication Modules

PAM provides a way to develop programs that are independent of authentication scheme. These programs need "authentication modules" to be attached to them at run-time in order to work. Which authentication module is to be attached is dependent upon the local system setup and is at the discretion of the local system administrator.

PAM: installazione e configurazione

-installazione del modulo per l'autenticazione via ldap:

```
apt-get install libpam-ldap
```

-configurazione del sistema di autenticazione per il servizio “squid”:

```
auth      sufficient /lib/security/pam_ldap.so
account  sufficient /lib/security/pam_ldap.so
```

-configurazione specifica di pam-ldap:

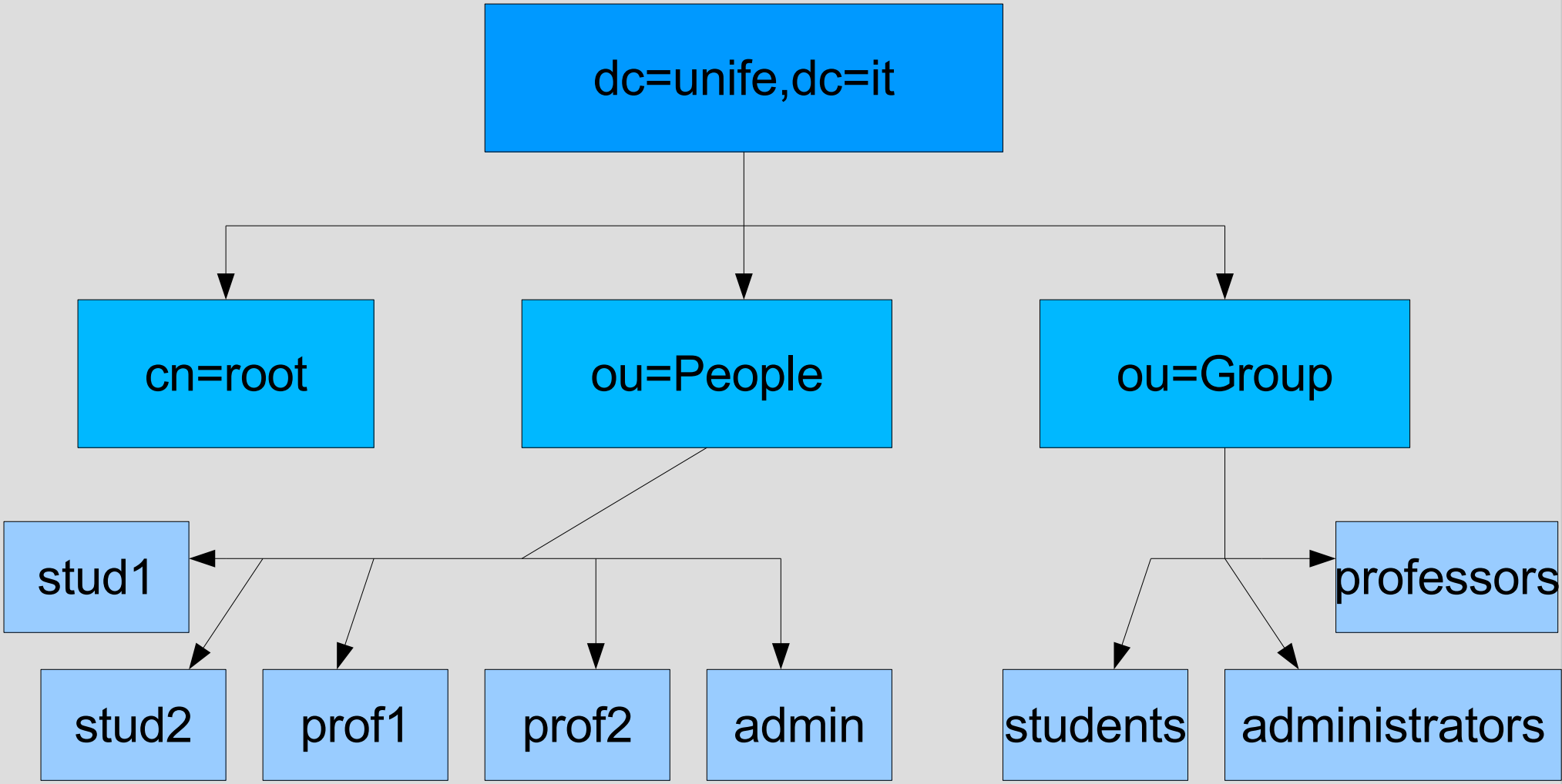
```
host 127.0.0.1
base dc=unife,dc=it
rootbinddn cn=root,dc=unife,dc=it
pam_password crypt
```

OpenLDAP

OpenLDAP Software is an Open Source suite of directory software developed by the Internet community.

Slapd is the stand-alone LDAP daemon.
It listens for LDAP connections on any number of ports (default 389), responding to the LDAP operations it receives over these connections.

OpenLDAP: l'albero



OpenLDAP: installazione e configurazione

-installazione
apt-get install libldap
apt-get install slapd
apt-get install ldap-utils

-configurazione di base: modifica di /etc/ldap/slapd.conf

```
suffix      "dc=unife,dc=it"
rootdn      "cn=root,dc=unife,dc=it"
rootpw{SSHA}Gl+IafCczR5K38INF/hFEMQMjGlrsHF2
```

OpenLDAP: ACL

configurazione delle ACL:

```
access to attrs=userPassword
        by dn="cn=root,dc=unife,dc=it" write
        by anonymous auth
        by self write
        by * none

access to *
      by dn="cn=root,dc=unife,dc=it" write
     by anonymous auth
     by * read
```

OpenLDAP: l'albero come file LDIF

-scrittura del file LDIF che rappresenta l'albero

```
dn: dc=unife,dc=it
objectclass: dcObject
objectclass: organization
o: University of Ferrara
dc: unife

dn: cn=root,dc=unife,dc=it
objectclass: organizationalRole
cn: root

[...]
```

OpenLDAP: inserimento dell'albero

-inserimento dell'albero tramite ldapadd:

```
ldapadd -x -D 'cn=root,dc=unife,dc=it' -W -f top.ldif
ldapadd -x -D 'cn=root,dc=unife,dc=it' -W -f people.ldif
ldapadd -x -D 'cn=root,dc=unife,dc=it' -W -f groups.ldif
```

-conferma:

```
root@kubuntu:~# ldapsearch -x -D 'uid=stud1,ou=people,dc=unife,dc=it' -W -u -t
"(uid=stud2)" dn cn
Enter LDAP Password:

# stud2, people, unife.it
dn: uid=stud2,ou=people,dc=unife,dc=it
ufn: stud2, people, unife.it
cn: Secondo Studente

[...]
```