Montar LDAP perquè radius agafi els usuaris d'ell

LDAP

Engegar LDAP

```
docker run --name ldap_msf -d -p 389:389 -e SLAPD_PASSWORD=asdasd -e
SLAPD_DOMAIN=matarosensefils.net dinkel/openldap
```

Búsqueda:

```
ldapsearch -x -h localhost -b dc=matarosensefils,dc=net -D
"cn=admin,dc=matarosensefils,dc=net" -w asdasd
```

Insertar usuari. Creem fitxer amb el següent contingut::

```
usuaris.txt
```

```
dn: ou=persones, dc=matarosensefils,dc=net
ou: persones
description: All people in organisation
objectclass: organizationalunit

dn: cn=Jose Legido,ou=persones,dc=matarosensefils,dc=net
objectclass: inetOrgPerson
cn: Jose Legido
sn: Legido
uid: jose.legido
userpassword: 12345678

dn: cn=Usuari Lectura,ou=persones,dc=matarosensefils,dc=net
objectclass: inetOrgPerson
cn: Usuari Lectura
sn: Lectura
uid: usuari.lectura
userpassword: 87654321
```

Consultem:

```
ldapadd -x -h localhost -D "cn=admin,dc=matarosensefils,dc=net" -w asdasd -f
usuaris.ldif
```

Creem els grups:

```
grups.ldif
```

```
dn: ou=grups,dc=matarosensefils,dc=net
objectClass: organizationalUnit
```

```
ou: grups

dn: cn=admin,ou=grups,dc=matarosensefils,dc=net
cn: admin
objectclass: groupofNames
member: cn=Jose Legido,dc=matarosensefils,dc=net

dn: cn=read,ou=grups,dc=matarosensefils,dc=net
cn: read
objectclass: groupofNames
member: cn=Usuari Lectura,dc=matarosensefils,dc=net
```

```
ldapadd -x -h localhost -D "cn=admin,dc=matarosensefils,dc=net" -w asdasd -f
grups.ldif
```

Per buscar un usuari en concret:

```
ldapsearch -x -h localhost -b dc=matarosensefils,dc=net -D
"cn=admin,dc=matarosensefils,dc=net" -w asdasd "uid=jose.legido"
```

Freeradius

https://www.golinuxcloud.com/freeradius-ldap-authentication-authorization/

```
docker run --name radius_msf -p 5000:5000 -p 1812:1812/udp -ti
freeradius/freeradius-server
```

```
/etc/freeradius/3.0/sites-enabled# cat /etc/freeradius/3.0/mods-enabled/ldap
```

Modifiquem aquests paràmetres:

```
ldap {
   server = '172.17.0.1'
   base_dn = 'CN=persones,DC=matarosensefils,DC=net'
   identity = 'cn=admin,dc=matarosensefils,dc=net'
   password = 'asdasd'

   user {
      filter = "(sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}})"
   }

}
```

Ens quedaria quelcom així

```
ldap {
        server = '172.17.0.1'
        identity = 'cn=admin,dc=matarosensefils,dc=net'
```

```
        password = asdasd
        base_dn = 'dc=matarosensefils,dc=net'
        update {
                control:Password-With-Header    += 'userPassword'

                control:                        += 'radiusControlAttribute'
                request:                        += 'radiusRequestAttribute'
                reply:                          += 'radiusReplyAttribute'
        }
        user_dn = "LDAP-UserDn"

        user {
                base_dn = "${..base_dn}"
                filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        }

        group {
                base_dn = "${..base_dn}"
                filter = '(objectClass=posixGroup)'
                membership_attribute = 'memberOf'
        }

        client {
                base_dn = "${..base_dn}"
                filter = '(objectClass=radiusClient)'
                attribute {
                        ipaddr                          =
'radiusClientIdentifier'
                        secret                          =
'radiusClientSecret'
                }
        }
        accounting {
                reference = "%{tolower:type.%{Acct-Status-Type}}"
                type {
                        start {
                                update {
                                        description := "Online at %S"
                                }
                        }
                        interim-update {
                                update {
                                        description := "Last seen at %S"
                                }
                        }
                        stop {
                                update {
                                        description := "Offline at %S"
                                }
                        }
                }
```

```
        }

        post-auth {
                update {
                        description := "Authenticated at %S"
                }
        }

        options {
                chase_referrals = yes
                rebind = yes
                res_timeout = 10
                srv_timelimit = 3
                net_timeout = 1
                idle = 60
                probes = 3
                interval = 3
                ldap_debug = 0x0028
        }

        pool {
                start = ${thread[pool].start_servers}
                min = ${thread[pool].min_spare_servers}
                max = ${thread[pool].max_servers}
                spare = ${thread[pool].max_spare_servers}
                uses = 0
                retry_delay = 30
                lifetime = 0
                idle_timeout = 60
        }
}
```

```
/etc/freeradius/3.0/clients.conf
```

```
client xarxa {
   ipaddr = 10.0.0.0/8
   secret = mataro
}
```

Esborrem aquesta línea

```
rm /etc/freeradius/3.0/mods-enabled/eap
```

```
radtest jose.legido 12345678 127.0.0.1 1812 mataro
```

Mikrotik

```
docker-compose.yml
```

```
services:
    routeros:
      image: evilfreelancer/docker-routeros
      restart: unless-stopped
      cap_add:
        - NET_ADMIN
      devices:
        - /dev/net/tun
      ports:
        - "12222:22"
        - "8291:8291"
        - "12223:23"
        - "18728:8728"
        - "18729:8729"
        - "8090:80"
      networks:
        lan_internal:
          priority: 1000
          ipv4_address: 182.18.18.2
        lan_net:
          priority: 900
          ipv4_address: 172.16.16.2

networks:
    lan_net:
      driver: bridge
      ipam:
        driver: default
        config:
          - subnet: "172.16.16.0/24"
            gateway: 172.16.16.1
    lan_internal:
      ipam:
        driver: default
        config:
          - subnet: "182.18.18.0/24"
            gateway: 182.18.18.1
```