:: Centralised Authentication ::

An overview of LDAP & Radius deployments using open source components.

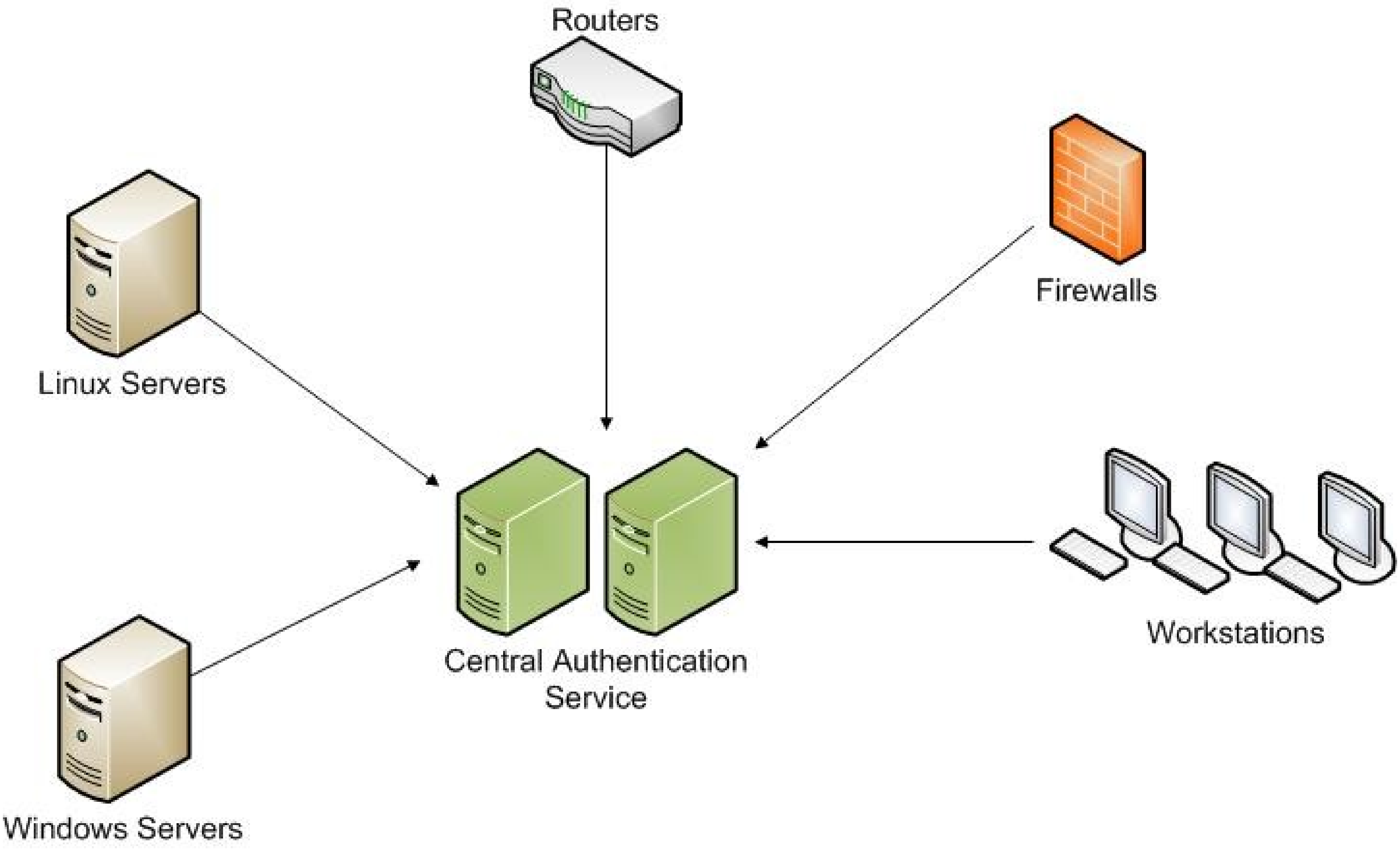
www.jethrocarr.com

jethro.carr@jethrocarr.com

:: what is centralised authentication? ::

- Centralised location for management of user and group information.
- Typically supports multiple operating systems & applications – usually based around a standard.
- One place to add, change or revoke user credentials.
- Ability to define what permissions particular users have.
- Examples: LDAP, Kerberos and Active Directory.

:: everyone loves diagrams ::

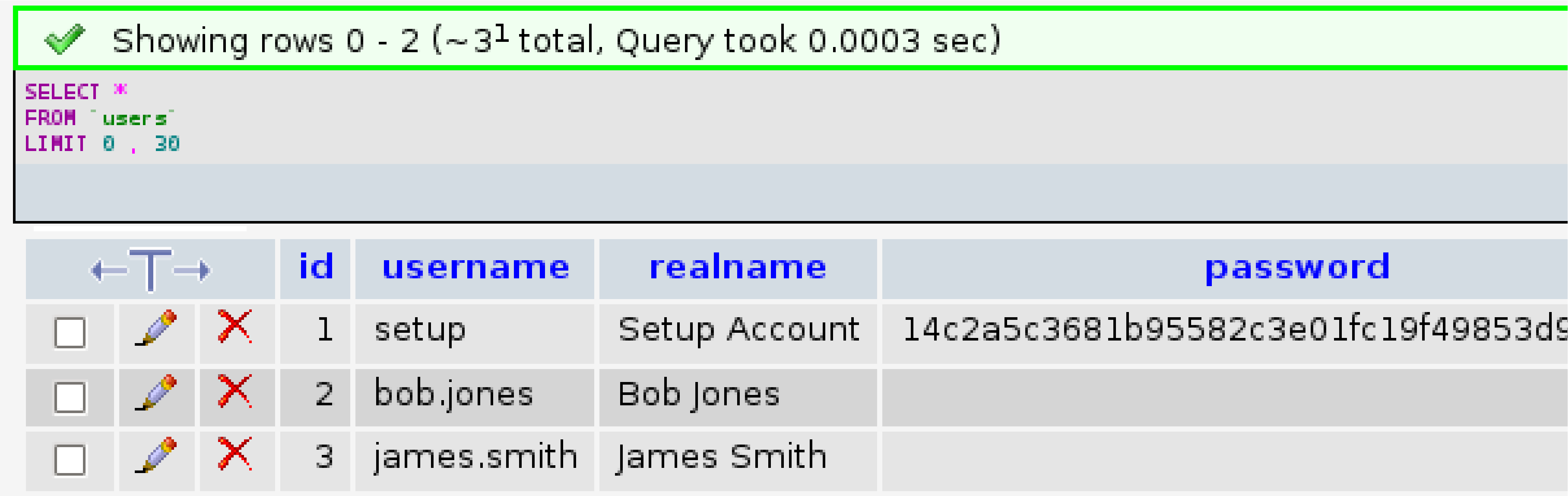


:: Lightweight Directory Access Protocol ::

“is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network” ~ Wikipedia

LDAP is commonly considered to be a user storage database – LDAP is no more a “user storage database” than is MySQL, both are tools which provide this functionality, along with many other possibilities.

:: NOT a relational database ::

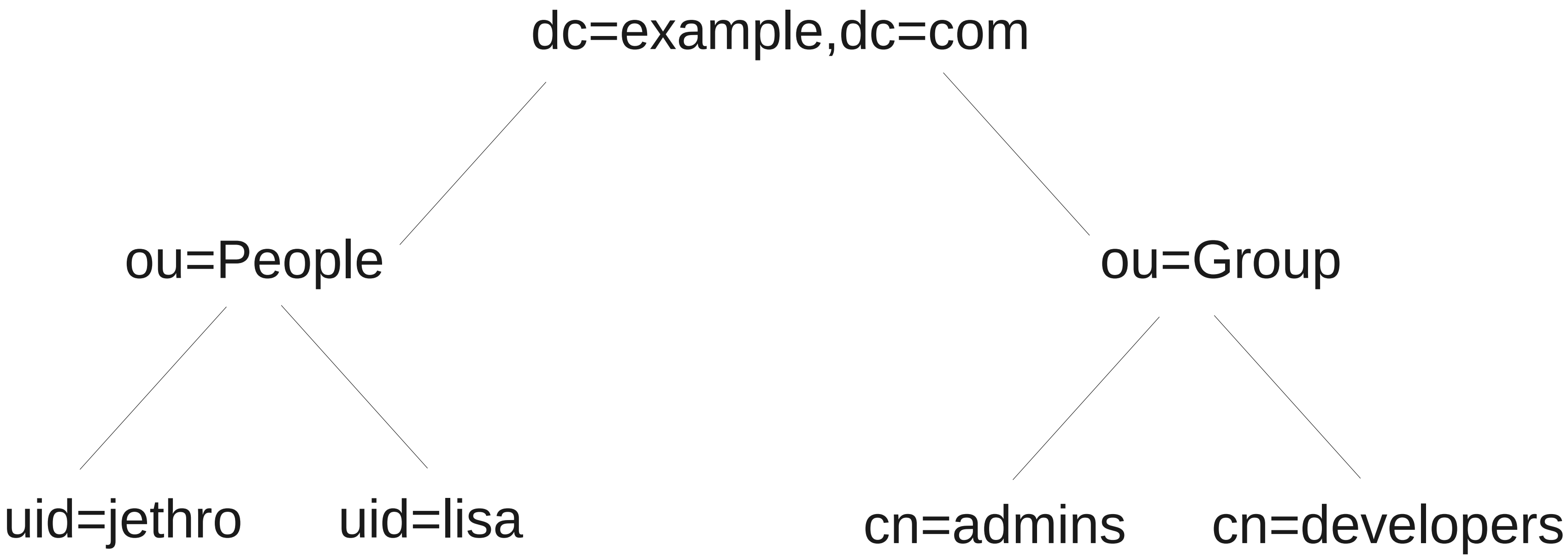


✓ Showing rows 0 - 2 (~3[1] total, Query took 0.0003 sec)

```
SELECT *
FROM `users`
LIMIT 0 , 30
```

←T→			id	username	realname	password
☐	✎	✗	1	setup	Setup Account	14c2a5c3681b95582c3e01fc19f49853d9
☐	✎	✗	2	bob.jones	Bob Jones	
☐	✎	✗	3	james.smith	James Smith	

:: Tree Based Structure ::



dc=example,dc=com

ou=People

ou=Group

uid=jethro

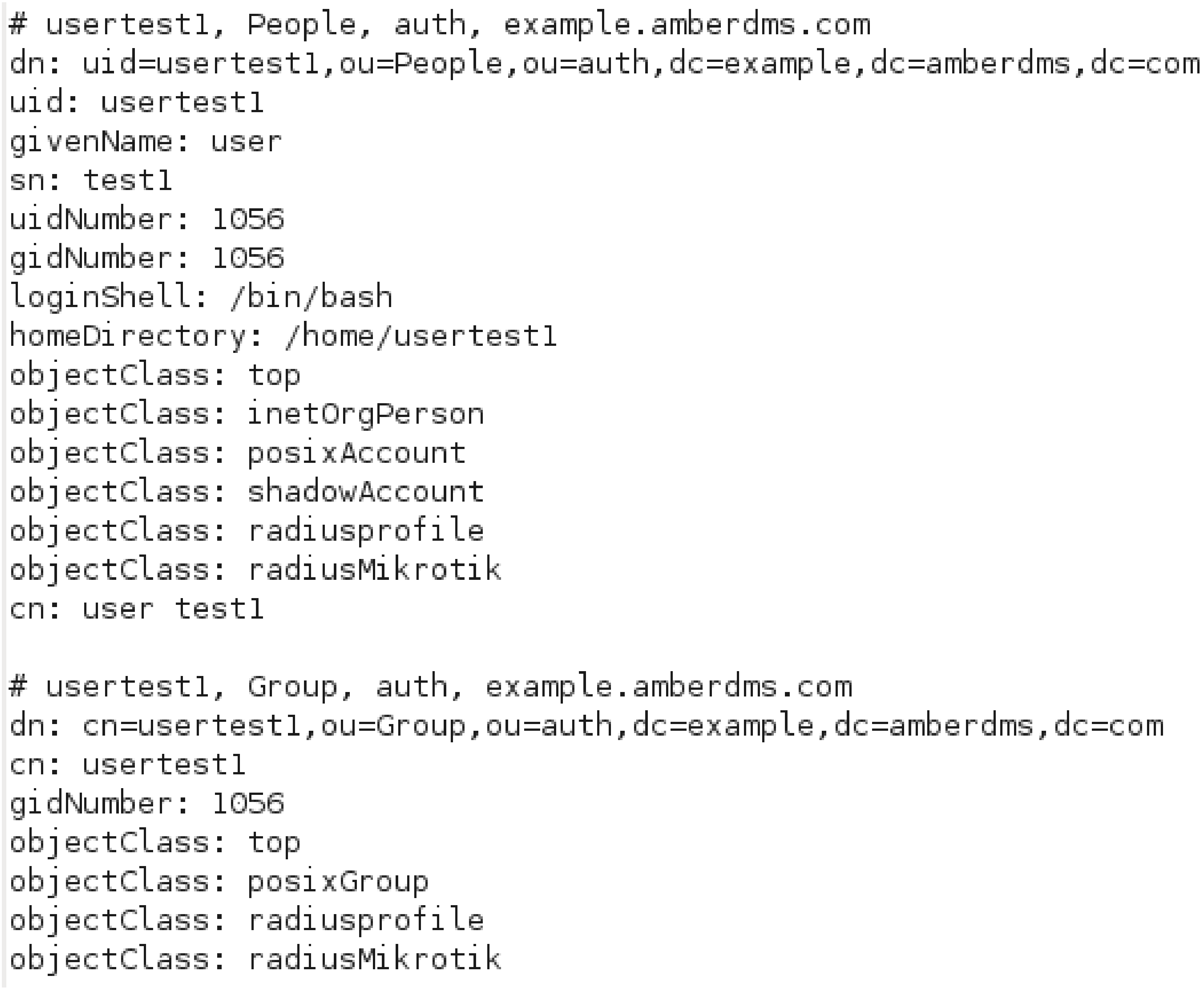
uid=lisa

cn=admins

cn=developers

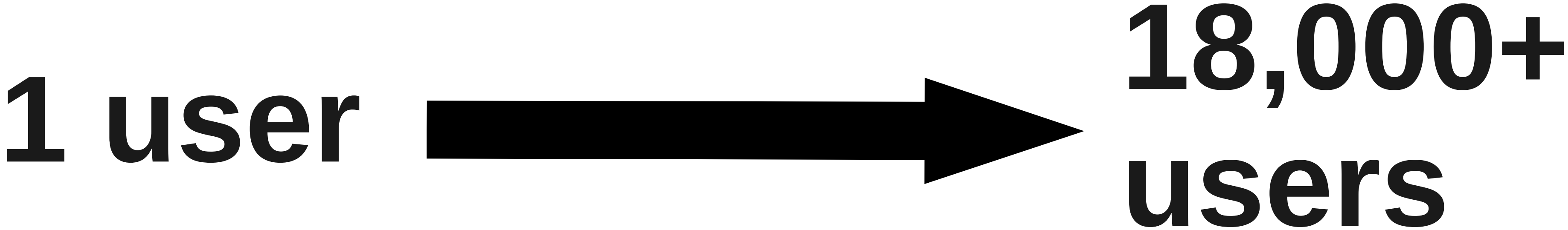
http://en.wikipedia.org/wiki/X.500

:: LDAP Records ::



```
# usertest1, People, auth, example.amberdms.com
dn: uid=usertest1,ou=People,ou=auth,dc=example,dc=amberdms,dc=com
uid: usertest1
givenName: user
sn: test1
uidNumber: 1056
gidNumber: 1056
loginShell: /bin/bash
homeDirectory: /home/usertest1
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: radiusprofile
objectClass: radiusMikrotik
cn: user test1

# usertest1, Group, auth, example.amberdms.com
dn: cn=usertest1,ou=Group,ou=auth,dc=example,dc=amberdms,dc=com
cn: usertest1
gidNumber: 1056
objectClass: top
objectClass: posixGroup
objectClass: radiusprofile
objectClass: radiusMikrotik
```

:: Scalibility ::



1 user

18,000+ users

:: Popular ::

Linux, Windows, Solaris, Applications, VoIP Phones, Routers, PHP, Perl, Python, C#/.NET, and more

:: Open Source ::

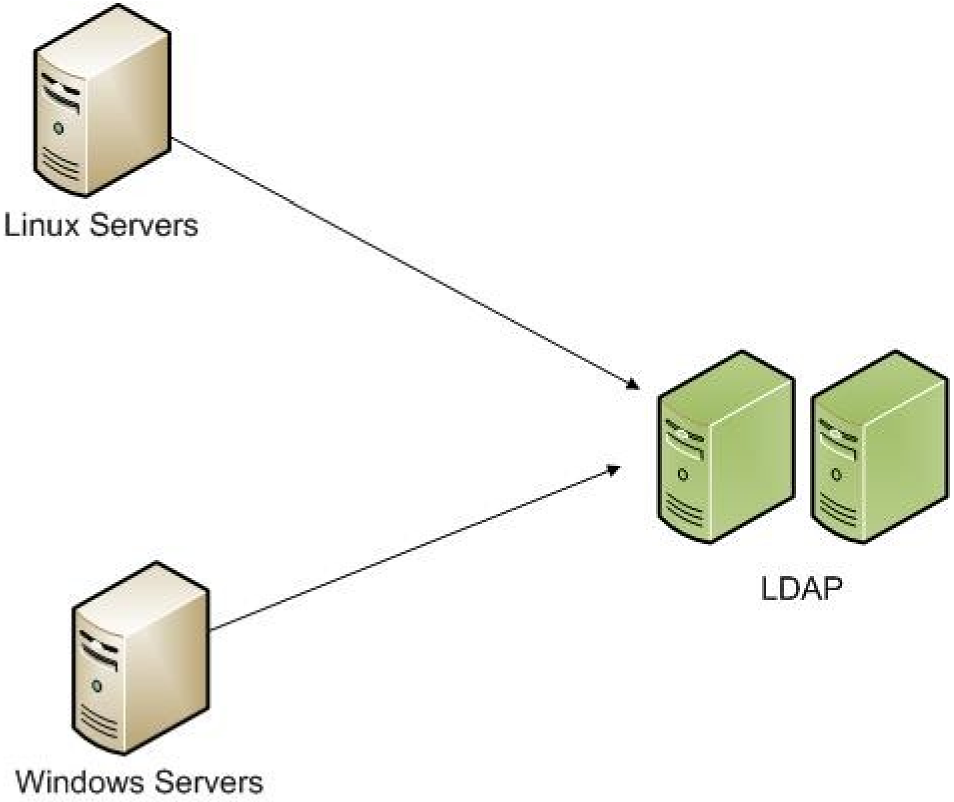
- OpenLDAP – popular, reliable, ships with almost every Linux distribution.
  http://www.openldap.org/

- 389 Directory Server – Red Hat / Fedora's LDAP server
  http://directory.fedoraproject.org/wiki/Main_Page

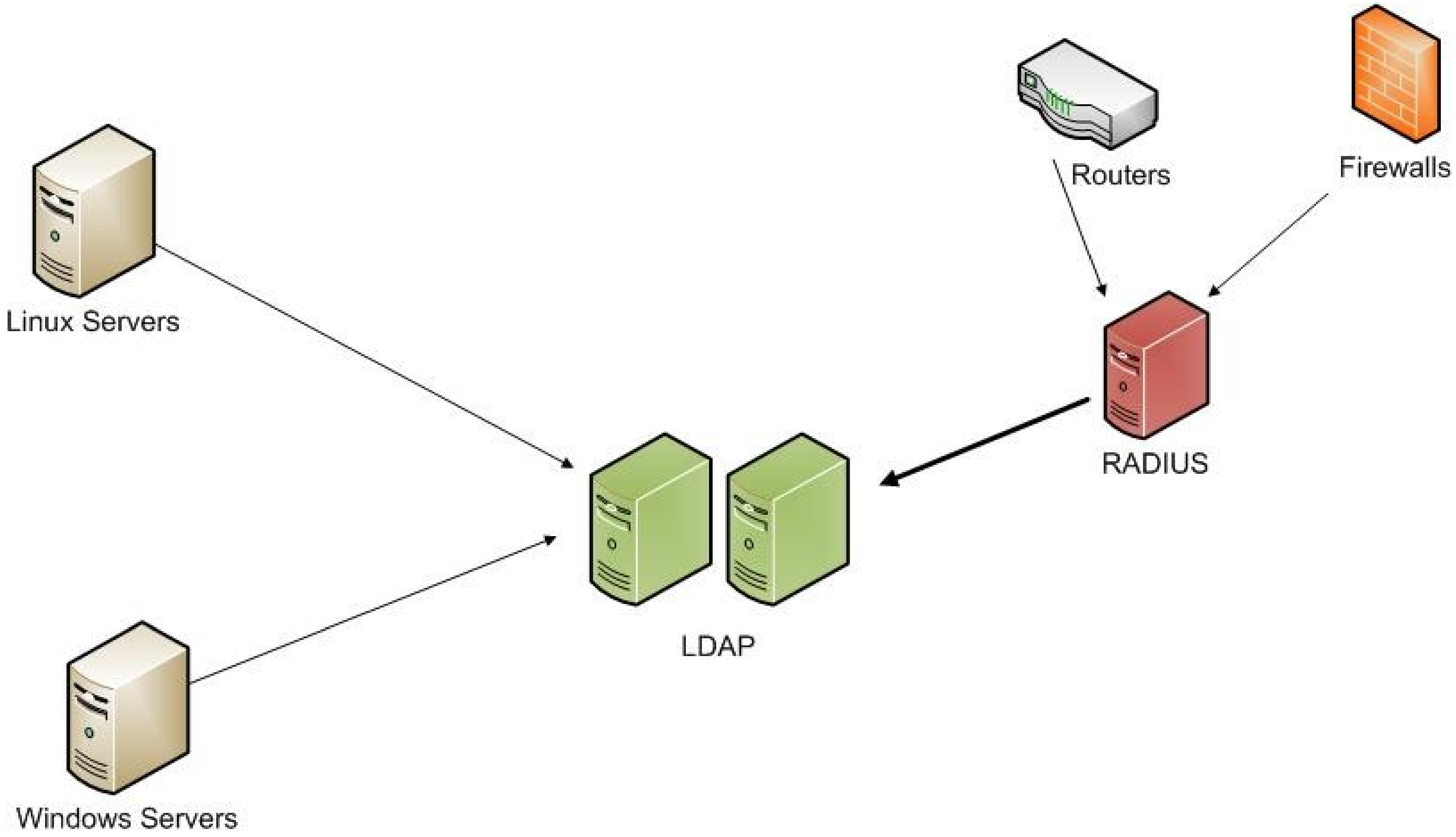
  (Also known as “Red Hat Directory Server”, “Fedora Directory Server” and once upon a time, “Netscape Directory Server”).

- FreeRadius – most widly deployed RADIUS server in the world.
  http://freeradius.org/

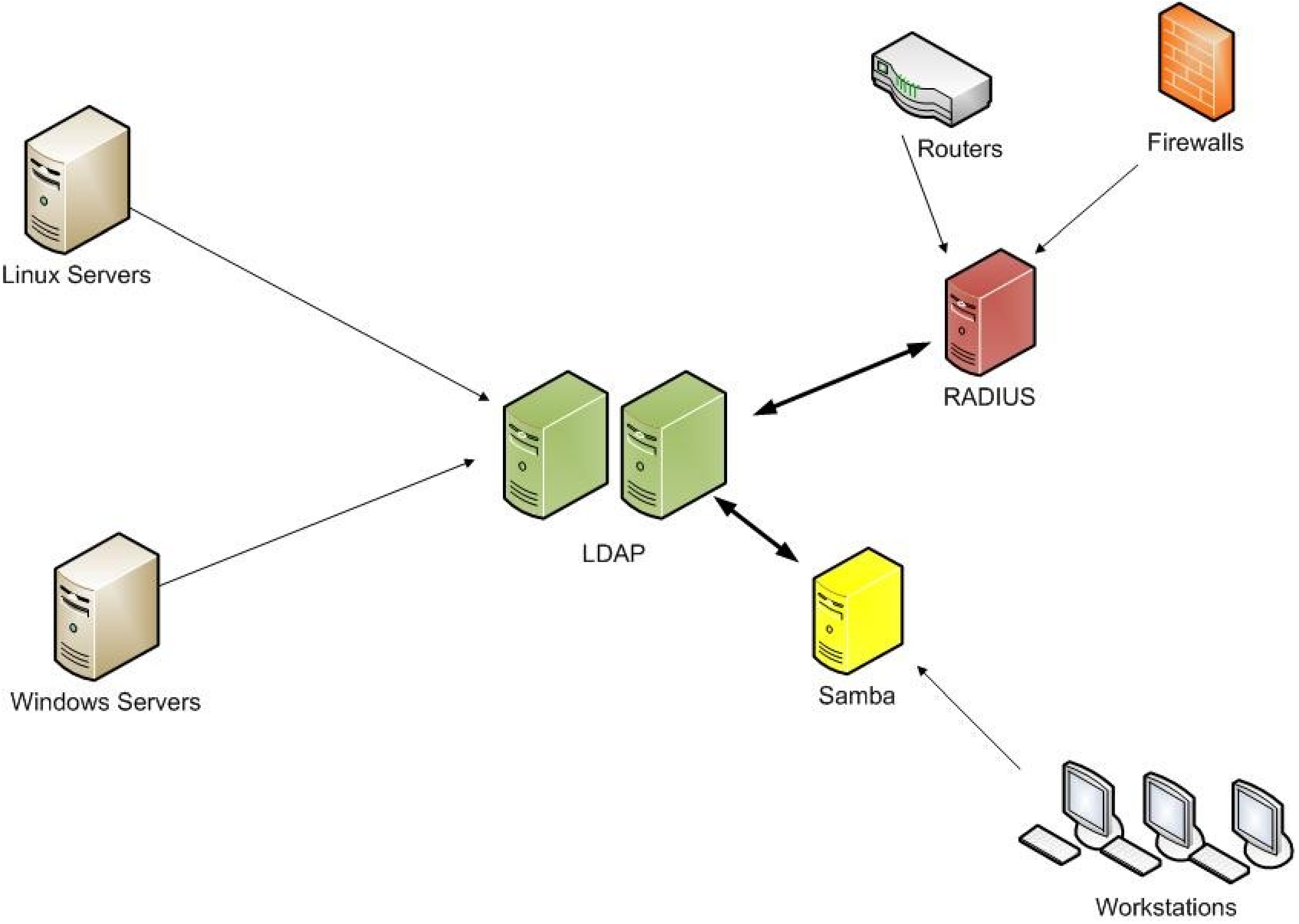
:: If LDAP is so awesome, why RADIUS? ::



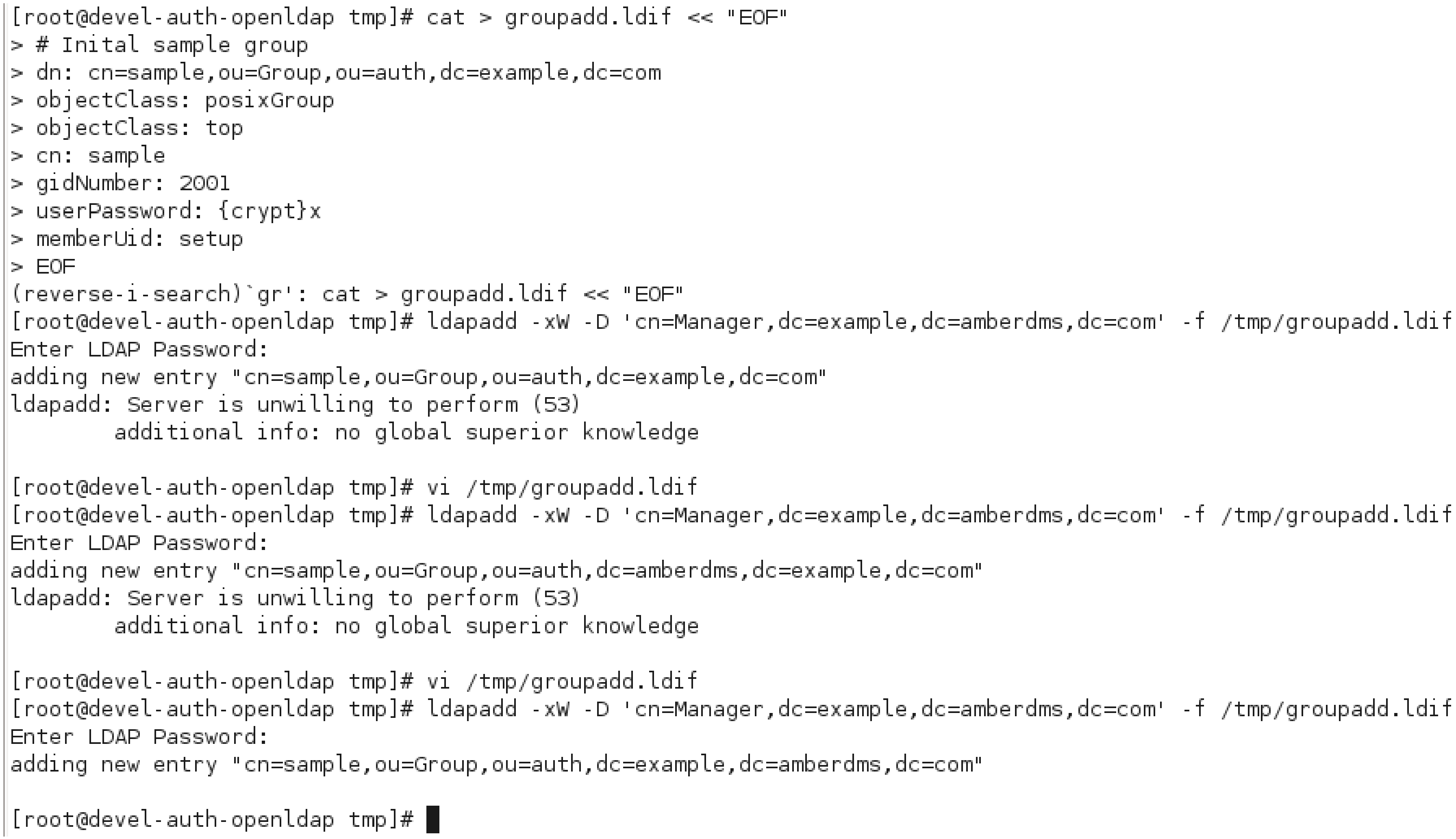
:: If LDAP is so awesome, why RADIUS? ::



:: And more... ::


Routers
Firewalls
Linux Servers
RADIUS
LDAP
Windows Servers
Samba
Workstations

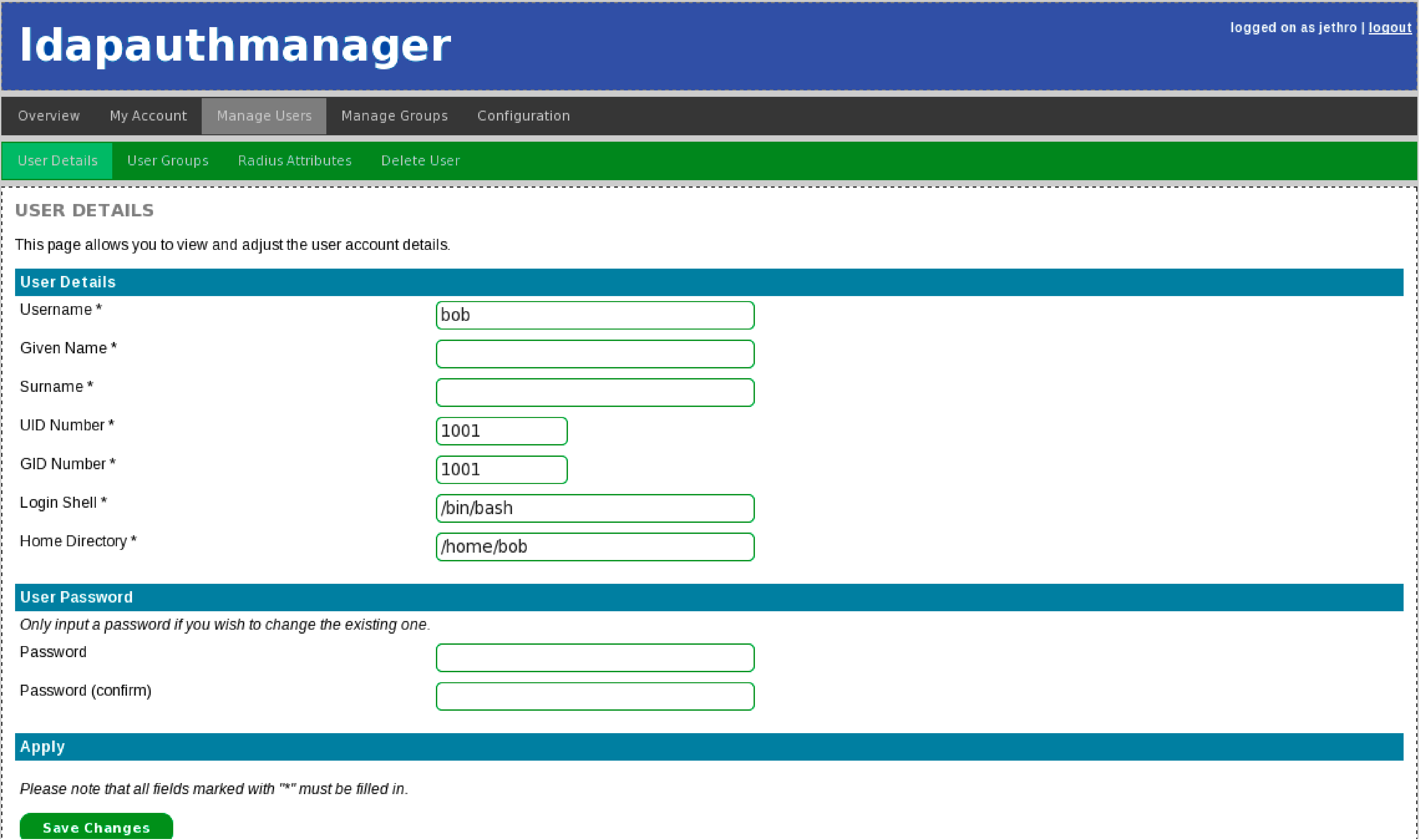
:: But isn't user management.... a bit ugly? ::



```
[root@devel-auth-openldap tmp]# cat > groupadd.ldif << "EOF"
> # Inital sample group
> dn: cn=sample,ou=Group,ou=auth,dc=example,dc=com
> objectClass: posixGroup
> objectClass: top
> cn: sample
> gidNumber: 2001
> userPassword: {crypt}x
> memberUid: setup
> EOF
(reverse-i-search)`gr': cat > groupadd.ldif << "EOF"
[root@devel-auth-openldap tmp]# ldapadd -xW -D 'cn=Manager,dc=example,dc=amberdms,dc=com' -f /tmp/groupadd.ldif
Enter LDAP Password:
adding new entry "cn=sample,ou=Group,ou=auth,dc=example,dc=com"
ldapadd: Server is unwilling to perform (53)
        additional info: no global superior knowledge

[root@devel-auth-openldap tmp]# vi /tmp/groupadd.ldif
[root@devel-auth-openldap tmp]# ldapadd -xW -D 'cn=Manager,dc=example,dc=amberdms,dc=com' -f /tmp/groupadd.ldif
Enter LDAP Password:
adding new entry "cn=sample,ou=Group,ou=auth,dc=amberdms,dc=example,dc=com"
ldapadd: Server is unwilling to perform (53)
        additional info: no global superior knowledge

[root@devel-auth-openldap tmp]# vi /tmp/groupadd.ldif
[root@devel-auth-openldap tmp]# ldapadd -xW -D 'cn=Manager,dc=example,dc=amberdms,dc=com' -f /tmp/groupadd.ldif
Enter LDAP Password:
adding new entry "cn=sample,ou=Group,ou=auth,dc=example,dc=amberdms,dc=com"

[root@devel-auth-openldap tmp]#
```

:: LDAPAuthManager ::

http://www.amberdms.com/ldapauthmanager



USER DETAILS

This page allows you to view and adjust the user account details.

User Details

Username *	bob
Given Name *	
Surname *	
UID Number *	1001
GID Number *	1001
Login Shell *	/bin/bash
Home Directory *	/home/bob

User Password

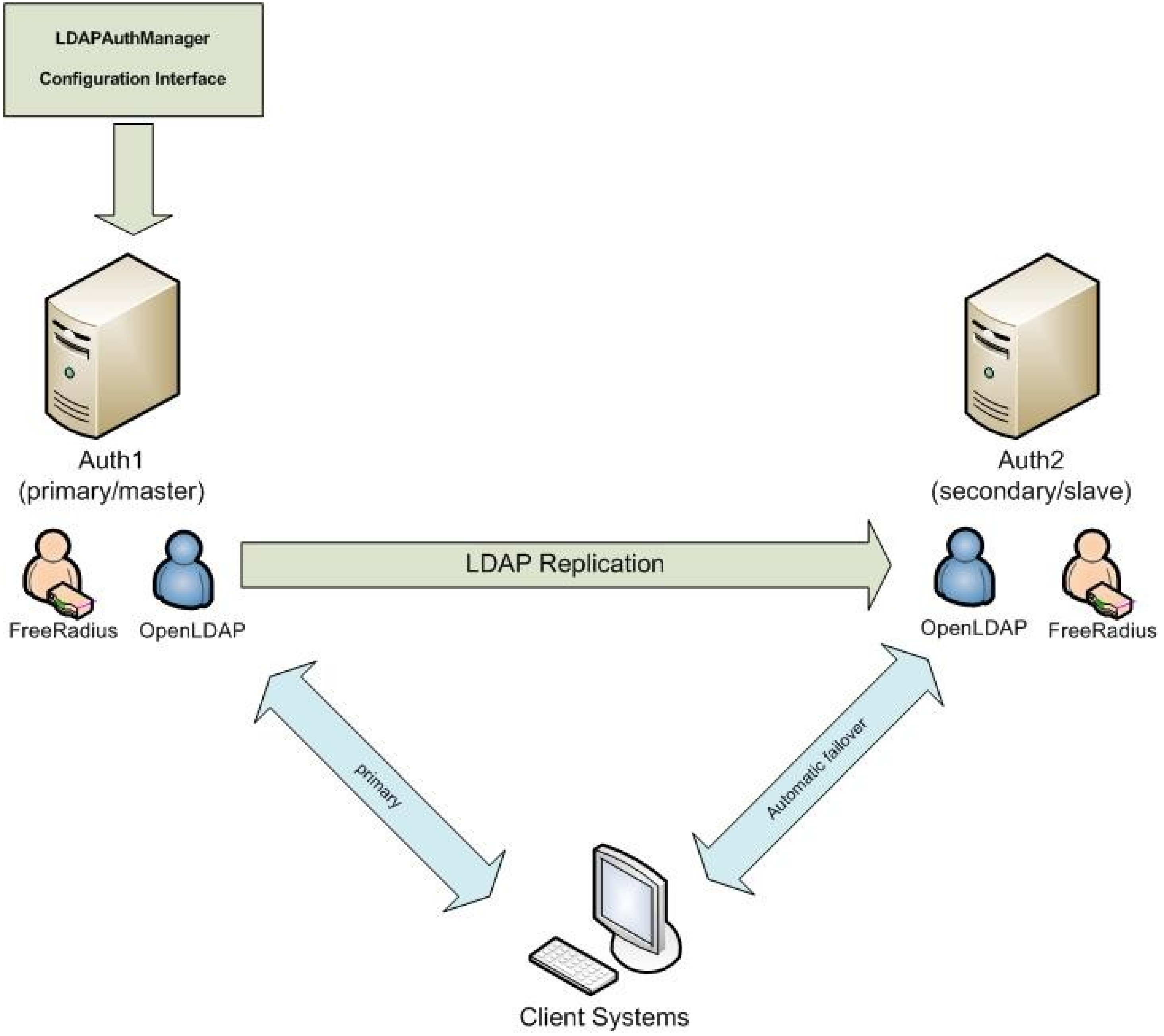
Only input a password if you wish to change the existing one.

Password	
Password (confirm)	

Apply

Please note that all fields marked with "" must be filled in.*

:: Example Auth Build ::



:: DEMO TIME ::