openLDAP

Chris Sivanich - csivanich@gmail.com

February 23, 2015

1 Server Setup

1.1 Configs

- /etc/openldap/
  - openldap.config - main config

1.2 Base LDIF file

- ```
  [root@alpha openldap]# cat /tmp/base.ldif
  # sivanich.org
  dn: dc=sivanich,dc=com
  dc: sivanich
  o: Example Organization
  objectClass: dcObject
  objectClass: organization

  # Manager, sivanich.org
  dn: cn=Manager,dc=sivanich,dc=com
  cn: Manager
  description: LDAP administrator
  objectClass: organizationalRole
  objectClass: top
  roleOccupant: dc=sivanich,dc=com

  # People, sivanich.org
  dn: ou=People,dc=sivanich,dc=com
  ou: People
  objectClass: top
  objectClass: organizationalUnit

  # Groups, sivanich.org
  dn: ou=Groups,dc=sivanich,dc=com
  ou: Groups
  objectClass: top
  objectClass: organizationalUnit
  ```
  ```

1.3 User LDIF File

- Be careful that the *cn* created with the wiki steps always match. They use *root* initially, but later switch over to *Manager*

```
[root@alpha openldap]# cat /tmp/user_chris.ldif
dn: uid:chris,ou=People,dc=sivanich,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: chris
cn: Chris Sivanich
sn: Sivanich
givenName: Christopher
title: Owner
mobile: +1 XXX XXX XXXX
userPassword: {CRYPT}XXXXXX
labeledURI: https://google.com
loginShell: /bin/zsh
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/chris
description: User Chris Sivanich
```

- The *objectClass* attributes are necessary, and outline the available attributes

2 Client Setup

2.1 /etc/openldap/ldap.conf

```
BASE    dc=sivanich,dc=com          # Set domain controller
URI     ldaps://alpha.sivanich.com  # Set DC location
TLS_REQCERT allow                   # Allow self signed certs
```

2.2 NSS and PAM

- Install `nss nss-pam-ldapd`

2.3 /etc/nsswitch.conf

- Edit to have this:

```
BASE    dc=sivanich,dc=com
URI     ldaps://alpha.sivanich.com
TLS_REQCERT allow
```

2.4 /etc/nslcd.conf