Log into Linux Using LDAP Credentials

These instructions apply to RedHat/CentOS, Debian/Ubuntu and SuSE. Different steps are required for Solaris and FreeBSD which are not covered in this guide.

Configure the LDAP Server

Start by adding the following to /opt/symas/etc/openldap/ldap.conf located on the LDAP server

```
sudo vi /opt/symas/etc/openldap/ldap.conf
BASE   dc=example,dc=com
URI    ldapi:///
TLS_CACERT    /opt/symas/ssl/CACert.pem
```

Note: The TLS_CACERT is unnecessary if not using SSL Certificate/Key pairs for encrypted connectivity.

The settings in the ldap.conf file are global for all connections to the LDAP server.

Configure nsswitch.conf

Next, update the /etc/nsswitch.conf file with the following:

```
sudo vi /etc/nsswitch.conf
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
gshadow:        files

hosts:          files dns hostname
# mdns4_minimal [NOTFOUND=return] dns myhostname
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

If the user is not in the LDAP database, /etc/passwd will be used instead.

Install nslcd and nscd

Install Commands

Run the follow commands as sudo.


```
yum  nss-pam-ldapd nscd -y
```

```
apt-get install nslcd nscd –y
```

```
zypper nss-pam-ldapd nscd
```

Configure nscd and nslcd

NSCD

The defaults in /etc/nscd.conf are acceptable. No changes are required

NSLCD

Configure /etc/nslcd.conf as follows:

```
sudo vi /etc/nslcd.conf
# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable. If this
is the local box
# this can be the ldapi:///
uri ldap://ldapserver.example.com

# The search base that will be used for all queries.
base dc=example,dc=com

# The LDAP protocol version to use.
ldap_version 3

# The DN to bind with for normal lookups. Do not
binddn uid=system-authority,ou=applications,dc=example,dc=com
bindpw <This password must be plain text. Protect this file.>

# The DN used for password modifications by root. (Optional)
#rootpwmoddn dc=example,dc=com
#rootpwmodpw <This password must be plain text. Protect this file.>

# SSL options (optional)
#ssl off
#tls_reqcert try
tls_cacertfile /etc/ssl/certs/<ldap server CA>.crt

# The search scope.
scope sub

nss_initgroups_ignoreusers ALLLOCAL
```

CA Certificate

Copy the CA.crt file from the LDAP server to /etc/ssl/certs/ on the local client.

Enable NSLCD Service

```
update-rc.d nslcd enable
```

Restart NSCD & NSLCD Services

```
/etc/init.d/nscd restart

/etc/init.d/nslcd restart
```

Test Connectivity

Use the getent command to test local connectivity using ldap credentials:

```
getent passwd | grep <ldap uid>
```

You should get the result twice. If so the nsswitch works fine. See my responses below as an example:

```
jtrupp:x:1000:1000:Jason Trupp,,,:/home/jtrupp:/bin/bash
jtrupp:x:2029:2029:Jason Trupp:/home/jtrupp:/bin/bash
```