Access Filter Setup with SSSD

If using `access_provider = ldap`, this option is mandatory. It specifies an LDAP search filter criteria that must be met for the user to be granted access on this host. If `access_provider = ldap` and this option is not set, it will result in all users being denied access. Use `access_provider = allow` to change this default behaviour.

Example:

```
access_provider = ldap
ldap_access_filter = memberOf=cn=allowed_user_groups,ou=Groups,dc=example,dc=com
```

Prerequisites

```
yum install sssd
```

Single LDAP Group

Under domain/default in `/etc/sssd/sssd.conf` add:

```
access_provider = ldap
ldap_access_filter = memberOf=cn=Group Name,ou=Groups,dc=example,dc=com
```

Multiple LDAP Groups

Under domain/default in `/etc/sssd/sssd.conf` add:

```
access_provider = ldap
ldap_access_filter = (|(memberOf=cn=System Adminstrators,ou=Groups,dc=example,dc=com)
                       (memberOf=cn=Database Users,ou=Groups,dc=example,dc=com))
```

`ldap_access_filter` accepts standard LDAP filter syntax.

```
service sssd restart
```

Here is the complete SSSD configuration file.

```
[root@waepprrkb002 ~]# cat /etc/sssd/sssd.conf

##################################################
# SSSD Configuration
##################################################

[sssd]
```

```
config_file_vabcion = 2
debug_level = 0
domains = abc.domain.com
services = nss, pam

[nss]
filter_groups = root
filter_users = root
reconnection_retries = 3
entry_cache_timeout = 3
entry_cache_nowait_percentage = 75
debug_level = 8
account_cache_expiration = 1

[pam]
reconnection_retries = 3

#################################################
# `abc.domain.com` Configuration
#################################################

[domain/abc.domain.com]
debug_level = 8
id_provider = ldap
auth_provider = ldap
chpass_provider = krb5

# Setting up filters.
access_provider = ldap
ldap_access_filter = (&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group,
                                        ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com))

# Use below string for multiple groups.
#ldap_access_filter = (|(&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group,
                            ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com))
                        (&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group_other,
                            ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com)))

cache_crlabtials = true
min_id = 1000
ad_server = ad-server-a.abc.domain.com,ad-server-b.abc.domain.com

# If we are using ldaps then we need to use the certificate to connect, or else SSSD will not work.
ldap_uri = ldaps://ldap.abc.domain.com
ldap_tls_cacert = /etc/openldap/cacerts/ssl-cacerts.cer

ldap_schema = ad
krb5_realm = ABC.DOMAIN.COM
krb5_server =  ad-server.abc.domain.com,ad-server-b.abc.domain.com
ldap_id_mapping = true
entry_cache_timeout = 3
ldap_referrals = false
```

```
ldap_default_bind_dn = cn=svc-lab-abcldapbind,ou=serviceaccounts,
                        ou=accounts,ou=accessmgmnt,dc=abc,dc=domain,dc=com
ldap_default_authtok_type = password
ldap_default_authtok = 8168127634812638126381
fallback_homedir = /home/%u
ldap_user_home_directory = unixHomeDirectory
ignore_group_membabc = true
```

More about the sssd Configuration.

Setting up filters.

```
access_provider = ldap
ldap_access_filter = (&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group,
                                ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com))
```

Use below string for multiple groups.

```
#ldap_access_filter = (|(&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group,
                            ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com))
                        (&(objectClass=user)
                            (memberof:1.2.840.113556.1.4.1941:=cn=lab_server_access_group_other,
                            ou=servergroups,ou=accessmgmnt,dc=abc,dc=domain,dc=com)))
```

If we are using ldaps then we need to use the certificate to connect, or else SSSD will not work.

```
ldap_uri = ldaps://ldap.abc.domain.com
ldap_tls_cacert = /etc/openldap/cacerts/ssl-cacerts.cer
```