Monday, March 30. 2015

freeipa server and SSSD on Ubuntu

Hi

I have spend a quality time for freeipa-server and that fantastic tool SSSD as I wanted to install JUST SSSD on the ubuntu without the whole freeipa-client which I did not need for administrative purposes..

My biggest challenge was the OLD of the distribution as it was a 12.04 and some libraries were a long way old so they could not comply with my requirements...

so ENSURE you get the following into your system (below 64 bits) (just download from the official repos and install, that should go straight as the DO NOT have dependencies but will just replace what you got)

sudo_1.8.9p5-1ubuntu2_amd64.deb
libsss-sudo_1.11.7-3_amd64.deb

in relation to the configuration:

sudo -E apt-add-repository http://ppa.launchpad.net/freeipa/ppa/ubuntu
sudo -E apt-add-repository http://ppa.launchpad.net/sssd/updates/ubuntu
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
reboot
sudo apt-get install sssd sssd-tools ldap-auth-client ldap-utils nscd
sudo mkdir /etc/ldap/cacerts/
Do not forget to install the client ldap cert on /etc/ldap/cacerts/ (i.e.: /etc/ldap/cacerts/cert.crt to comply with the config for sssd below)

The version of SSSD I currently got after that is:

Package: sssd
***Status: install* ok installed**
Multi-Arch: foreign
Priority: extra
Section: metapackages
Installed-Size: 43
Maintainer: Ubuntu Core Developers <ubuntu-devel@lists.ubuntu.com>
Architecture: amd64
Version: 1.11.5-1ubuntu3~precise1
Depends: sssd-common (= 1.11.5-1ubuntu3~precise1), sssd-ad (= 1.11.5-1ubuntu3~precise1), sssd-ipa (= 1.11.5-1ubuntu3~precise1), sssd-krb5 (= 1.11.5-1ubuntu3~precise1), sssd-ldap (= 1.11.5-1ubuntu3~precise1), sssd-proxy (= 1.11.5-1ubuntu3~precise1), python-sss (= 1.11.5-1ubuntu3~precise1)

Description: System Security Services Daemon -- metapackage
Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
.
This package is a metapackage which installs the daemon and existing authentication back ends.
Homepage: https://fedorahosted.org/sssd/
Original-Maintainer: Debian SSSD Team <pkg-sssd-devel@lists.alioth.debian.org>
[geshi]
Below it is a SIMPLE configuration which it worked as tested, from there you can explore all the security possibilities you might need.
Note I have done the following:
****
id_provider = ldap
#id_provider = ipa
******
So I am showing you can use the standard ldap or the IPA implementation which provides extra security. (the 2nd one will come with some extra work as you need the security tab installed in the client machines, that might be an issue in the long term as can be hard to maintain if you got thousands of systems unless you got a good plan behind)
/etc/sssd/sssd.conf
[geshi lang=bash ln=n]
[domain/company.com]
cache_credentials = True
id_provider = ldap
#id_provider = ipa
auth_provider = ldap
chpass_provider = ldap
access_provider = simple
simple_allow_groups = <allowed_groups>

ldap_tls_cacert = /etc/ldap/cacerts/cert.crt
enumerate = False
ldap_tls_reqcert = demand
ldap_uri = ldaps://freeipa-server.com
ldap_search_base = cn=accounts,dc=company,dc=com
ldap_schema = rfc2307bis
ldap_user_search_base = cn=users,cn=accounts,dc=company,dc=com
ldap_group_search_base = cn=groups,cn=accounts,dc=company,dc=com
ldap_default_bind_dn = uid=<BINDING_USER>,cn=users,cn=accounts,dc=company,dc=com
ldap_default_authtok_type = obfuscated_password
ldap_default_authtok = <PASSWORD>
ldap_sudo_search_base = ou=sudoers,dc=company,dc=com
[sssd]
services = nss, pam, ssh, sudo
config_file_version = 2
domains = company.com
[nss]
[pam]
[sudo]

[autofs]
[ssh]
[pac]

This bit ldap_default_authtok is created as follows: sss_obfuscate -d company.com

Create the pam profile (/usr/share/pam-configs/mkhomedir)

```
ldap_client_ubuntu_pam
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
   required    pam_mkhomedir.so umask=0022 skel=/etc/skel
```

Then execute: pam-auth-update

Create an auth config profile for sssd

```
cat >/etc/auth-client-config/profile.d/sss <<__EOF__
[sss]
nss_passwd=   passwd:   compat sss
nss_group=    group:    compat sss
nss_shadow=   shadow:   compat
nss_netgroup= netgroup: nis

__EOF__
```

And now execute: auth-client-config -t nss -p sss

```
service nscd restart
service sssd start
service sudo restart
```

And if I haven't forgotten anything you should be ready to go!

Posted by Gonzalo at 03:43