FreeIPA

FreeIPA is an Identity Policy and Authentication solution. We are currently using this for our internal management networks.

Server

Basically follow this. Also DNS is *suuuuuuuppppeeeerrrrr* important.

As a note, you should install `libsss_sudo`. Otherwise you might get this error:

```
sudo: unable to load /usr/lib64/libsss_sudo.so: /usr/lib64/libsss_sudo.so:
cannot open shared object file: No such file or directory
sudo: unable to initialize SSS source. Is SSSD installed on your machine?
```

When running sudo on the server.

Client

On RHEL based ones (and Ubuntu 16.04), install `freeipa-client`. Super easy. Then run:

```
ipa-client-install --mkhomedir --enable-dns-updates --ssh-trust-dns
```

However, if you're on debian-master-race, you don't need hand holding and an “automated client”. Let's dig into some config files.

Debian Installation

1. Install `sssd`
2. Copy the configuration file to `/etc/sssd/sssd.conf`
    1. Don't forget to `s/name.ubnetdef.net/your-hostname.ubnetdef.net/g`
3. `chown root:root /etc/sssd/sssd.conf` and `chmod 0600 /etc/sssd/sssd.conf`
4. Grab your krb5.keytab, and dump it to `/etc/krb5.keytab`
    1. `ipa-getkeytab -p host/name.ubnetdef.net -k /tmp/keytab`
5. Grab the CA cert (`/etc/ipa/ca.crt` on the FreeIPA server) and save it to `/etc/sssd/ipa.crt`
6. Append the following line to `/etc/pam.d/common-session`
    1. `session required pam_mkhomedir.so skel=/etc/skel/`
7. Append the following lines to `/etc/ssh/sshd_config` to allow public key logins
    1. `AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys`
    2. `AuthorizedKeysCommandUser nobody`
8. Append the following line to `/etc/systemd/timesyncd.conf`

    1. Servers=tick.cse.buffalo.edu tock.cse.buffalo.edu ticktock.cse.buffalo.edu
9. Enable NTP: `timedatectl set-ntp yes`
10. GG, you're done.

/etc/sssd/sssd.conf

```
[domain/ubnetdef.net]
cache_credentials = True
krb5_store_password_if_offline = True
id_provider = ipa
auth_provider = ipa
access_provider = ipa
chpass_provider = ipa
sudo_provider = ldap

# Configure IPA
ipa_domain = ubnetdef.net
ipa_hostname = name.ubnetdef.net

# Configure sudo
ldap_uri = ldaps://master.ubnetdef.net
ldap_tls_cacert = /etc/sssd/ipa.crt
ldap_sudo_search_base = ou=sudoers,dc=ubnetdef,dc=net
ldap_sasl_mech = GSSAPI
ldap_sasl_authid = host/name.ubnetdef.net
ldap_sasl_realm = UBNETDEF.NET
krb5_server = master.ubnetdef.net
krb5_realm = UBNETDEF.NET

[sssd]
services = nss, pam, ssh, sudo
config_file_version = 2
domains = ubnetdef.net
```

LDAP Integrations

Include the specific settings (search stuff, bind user, etc). Link to each service's page on how to finalize the configuration.

General

- Bind User: uid=bind,cn=users,cn=accounts,dc=ubnetdef,dc=net
- Search Base DN: cn=users,cn=accounts,dc=ubnetdef,dc=net
- User Search Pattern: (&(objectClass=inetorgperson)(uid=#USERNAME#))
- Group Search Base DN: cn=groups,cn=accounts,dc=ubnetdef,dc=net
- Group Search Pattern: (&(objectClass=groupofnames)(cn=#GROUPNAME#))