Configure Samba to use FreeIPA authentication

This tutorial aims at guiding through the process of configuring a CentOS 7-based SAMBA server using the centralized authentication and user management provided by FreeIPA.

This tutorial acknowledges the information available here. However, it adds important steps to make the setup work.

Configure FreeIPA server

Install FreeIPA server on machine auth.example.com **(This machine has to have 2 GiB of RAM, otherwise, the installation fails)**.

```
firewall-cmd --permanent --add-service=freeipa-ldap --add-service=freeipa-ldaps --add-service=ntp --add-service=dns --add-service=dhcp --add-service=kerberos
firewall-cmd --reload
yum install -y ipa-server ipa-client
ipa-server-install -r EXAMPLE.COM -n example.com --mkhomedir --hostname="$(hostname --fqdn )" --admin-password='password' --ds-password='password'
```

Configure samba server

Install FreeIPA client on samba host (storage.example.com).

```
yum install -y ipa-client
ipa-client-install --mkhomedir --force-ntpd --enable-dns-updates
```

Install samba server on samba host (storage.example.com).

```
yum -y install samba samba-client sssd-libwbclient
systemctl enable nmb.service
systemctl enable smb.service
```

Create the CIFS principal for samba on FreeIPA host (auth.example.com).

```
ipa service-add cifs/storage.example.com
```

Fetch the keytab to the samba host (storage.example.com).

```
kinit -kt /etc/krb5.keytab
ipa-getkeytab -s auth.example.com -p cifs/storage.example.com -k /etc/samba/samba.keytab
```

Configure SELinux on the samba server (storage.example.com).

```
setsebool -P samba_enable_home_dirs on
setsebool -P use_samba_home_dirs on
setsebool -P samba_portmapper 1
```

Install adtrust components on the FreeIPA host (auth.example.com), answering “yes” to everything.

```
yum -y install ipa-server-trust-ad
ipa-adtrust-install --add-sids
```

Install the ipa-server-trust-ad package on the samba server (storage.example.com). This package is needed to get the ipasam config option in smb.conf.

```
yum -y install ipa-server-trust-ad
```

Run the following script on samba server (storage.example.com):

setup_firewall.sh

```
tf=/lib/firewalld/services/freeipa-samba.xml
touch "${tf}"; chmod 0644 "${tf}"; chown root:root "${tf}"; restorecon
"${tf}"
cat <<EOFXML > "${tf}"
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>IPA and Samba</short>
  <description>This service provides the ports required by the ipa-
adtrust-install command.</description>
  <port protocol="tcp" port="135"/>
  <port protocol="tcp" port="138"/>
  <port protocol="tcp" port="139"/>
  <port protocol="tcp" port="445"/>
  <port protocol="tcp" port="1024-1300"/>
  <port protocol="udp" port="138"/>
  <port protocol="udp" port="139"/>
  <port protocol="udp" port="389"/>
  <port protocol="udp" port="445"/>
</service>
EOFXML
systemctl restart firewalld
firewall-cmd --permanent --add-service=freeipa-samba
firewall-cmd --reload
echo done
```

Run this on auth.example.com to give special permissions to the samba service to read user passwords.

```
ipa permission-add "CIFS server can read user passwords" \
   --attrs={ipaNTHash,ipaNTSecurityIdentifier} \
   --type=user --right={read,search,compare} --bindtype=permission
ipa privilege-add "CIFS server privilege"
ipa privilege-add-permission "CIFS server privilege" \
   --permission="CIFS server can read user passwords"
ipa role-add "CIFS server"
ipa role-add-privilege "CIFS server" --privilege="CIFS server privilege"
ipa role-add-member "CIFS server" --services=cifs/storage.example.com
```

Run this script to finish the setup on samba server (storage.example.com):

setup_smb_conf.sh

```
tf=/etc/samba/smb.conf
touch "${tf}"; chmod 0644 "${tf}"; chown root:root "${tf}"; restorecon
"${tf}"
cat <<EOFCONF > "${tf}"
[global]
    # freeipa configurations
    debug pid = yes
    realm = EXAMPLE.COM
    workgroup = EXAMPLE
    domain master = Yes
    ldap group suffix = cn=groups,cn=accounts
    ldap machine suffix = cn=computers,cn=accounts
    ldap ssl = off
    ldap suffix = dc=example,dc=com
    ldap user suffix = cn=users,cn=accounts
    log file = /var/log/samba/log
    max log size = 100000
    domain logons = Yes
    registry shares = Yes
    disable spoolss = Yes
    dedicated keytab file = FILE:/etc/samba/samba.keytab
    kerberos method = dedicated keytab
    passdb backend = ipasam:ldap://auth.example.com
ldap://auth.example.com
    security = USER
    create krb5 conf = No
    rpc_daemon:lsasd = fork
    rpc_daemon:epmd = fork
    rpc_server:tcpip = yes
    rpc_server:netlogon = external
    rpc_server:samr = external
    rpc_server:lsasd = external
    rpc_server:lsass = external
    rpc_server:lsarpc = external
    rpc_server:epmapper = external
    ldapsam:trusted = yes
    idmap config * : backend = tdb
```

```
        idmap config * : range = 10000-999999
    ldap admin dn = cn=Directory Manager

    # public share configurations
    map to guest = bad user

[homes]
    comment = Home Directories
    valid users = %S, %D%w%S
    browseable = No
    read only = No
    inherit acls = Yes

[shared]
    comment = Public Share
    path = /home/shared
    writable = yes
    browsable = yes
    guest ok = yes
    read only = no
EOFCONF
mkdir /home/shared
chown -R nobody:nobody /home/shared
chcon -R -t samba_share_t /home/shared
systemctl restart nmb.service
systemctl restart smb.service
```