Bascule de l'authentification sur sssd

dixit Guillaume Seith "ça permet d'avoir un cache local des utilisateurs. Comme ça, même si les serveurs d'authentifications ne sont pas joignables ça ne pose pas de problème."

La "home directory" est toujours sous labo4

Voici les manipulations de Guillaume :

1. Création du fichier /etc/sssd/sssd.conf (le fichier d'une machine existante)
2. apt-get remove libnss-ldap
3. apt-get install sssd oddjob-mkhomedir
4. ajouter sss comme source pour login et mot de passe dans /etc/nsswitch.conf
5. vérifier que dans le fichier /etc/pam.d/common-session la ligne suivante a été supprimé ou est en commentaire : `session required pam_mkhomedir.so umask=0022 skel=/etc/skel`

========== /etc/nsswitch.conf

```
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Valid entries include:
#
#   nisplus             Use NIS+ (NIS version 3)
#   nis              Use NIS (NIS version 2), also called YP
#   dns              Use DNS (Domain Name Service)
#   files              Use the local files
#   db              Use the local database (.db) files
#   compat             Use NIS on compat mode
#   hesiod             Use Hesiod for user lookups
#   [NOTFOUND=return]    Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis
```

```
passwd:     files ldap sss
shadow:     files ldap sss
group:      files ldap sss

#hosts:     db files nisplus nis dns
hosts:      files dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files sss

netgroup:   nisplus sss

publickey:  nisplus

automount:  files ldap
#automount:  files
aliases:    files nisplus

sudoers:        files sss
```

========== /etc/sssd/sssd.conf

```
[nss]
filter_groups = root
filter_users = root
reconnection_retries = 3

[pam]
reconnection_retries = 3

[sssd]
config_file_version = 2
reconnection_retries = 3
sbus_timeout = 30
services = nss, pam
domains = IGBMC.U-STRASBG.FR
```

```
[domain/igbmc.u-strasbg.fr]
#With this as false, a simple "getent passwd" for testing won't work. You
must do getent passwd user@domain.com
enumerate = true
cache_credentials = true

id_provider = ldap
#access_provider = ldap
auth_provider = krb5
chpass_provider = krb5

#ldap_uri = ldaps://igbmc.u-strasbg.fr
ldap_uri = ldaps://igbmc.u-strasbg.fr
ldap_search_base = dc=igbmc,dc=u-strasbg,dc=fr
#ldap_tls_cacert = /etc/ssl/certs/ca-certificates.crt
#ldap_access_filter = memberOf=CN=info-igbmc_eq,OU=Equipes,OU=EMC
Celerra,DC=igbmc,DC=u-strasbg,DC=fr

#This parameter requires that the DC present a completely validated
certificate chain. If you're testing or don't care, use 'allow' or 'never'.
#ldap_tls_reqcert = demand
ldap_tls_reqcert = allow

krb5_realm = IGBMC.U-STRASBG.FR
dns_discovery_domain = IGBMC.U-STRASBG.FR

ldap_schema = rfc2307bis
ldap_access_order = expire
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true

ldap_user_search_base = dc=igbmc,dc=u-strasbg,dc=fr
ldap_group_search_base = dc=igbmc,dc=u-strasbg,dc=fr
ldap_user_object_class = user
ldap_user_name = sAMAccountName
ldap_user_fullname = displayName
ldap_user_home_directory = unixHomeDirectory
#ldap_user_principal = userPrincipalName
ldap_group_object_class = group
ldap_group_name = sAMAccountName

#Bind credentials
#ldap_sasl_mech = GSSAPI
#krb5_keytab = /etc/emcldap.keytab
#ldap_krb5_keytab = /etc/emcldap.keytab
#ldap_sasl_authid = emcldap@IGBMC.U-STRASBG.FR
ldap_default_bind_dn = CN=Authentification Cavarelli-Wurtz,OU=Comptes de
service,DC=igbmc,DC=u-strasbg,DC=fr
ldap_default_authtok = 52S5rF(JrNP5xU

#override_homedir = /home/%u
```

```
#override_shell = /bin/bash

dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600

debug_level = 7
```

========== /etc/pam.d/common-session

```
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]            pam_permit.so
# here's the fallback if no module succeeds
session requisite             pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required            pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions
etc.
# See "man pam_umask".
session optional            pam_umask.so
# and here are more per-package modules (the "Additional" block)
session optional            pam_krb5.so
session required    pam_unix.so
#session    optional            pam_ldap.so
session optional    pam_systemd.so
# end of pam-auth-update config
```