eCDL - Tâche #10210

Scénario # 10170 (Terminé (Sprint)): eCDL : finalisation 2.4

eole-client-annuaire: vérification/adaptation du template ldap.conf pour l'eCdl

09/01/2015 14:46 - christophe guerinot

Statut:	Fermé	**Début:**	05/01/2015
Priorité:	Normal	**Echéance:**	
Assigné à:	christophe guerinot	**% réalisé:**	100%
Version cible:	sprint 2015 2-4 - Equipe PNE-SR	**Temps estimé:**	4.00 heures
		Temps passé:	6.13 heures

Description

Révisions associées

Révision 82a18e3a - 16/01/2015 12:03 - Benjamin Bohard

Configuration annuaire et client annuaire.

- triage des templates et fonctions : annuaire dans eole-ecdlannuaire et client annuaire (destiné à être mutualisé dans eole-client-annuaire) dans conf-ecdl ;
- activation de l'annuaire local de secours par une variable dédiée.
- fichier de configuration ldap.conf compatible modules EOLE ;
- ajout des variables pour le support du fichier de configuration ldap.conf.

Ref #10210

Révision 8a46b77f - 16/01/2015 14:18 - Benjamin Bohard

Répercussion des changements de la configuration du client ldap dans les scripts.

Ref #10210

Révision 1ec71775 - 16/01/2015 15:01 - Benjamin Bohard

Ajout de l'attribut redefine pour la balise file.

Cet attribut ne semble pas être pris en charge mais permet de contourner les problèmes de doublon de fichier dans les templates (utile pour gérer les modules meddtl en attendant l'occasion d'harmoniser les configurations).

Ref #10210

Révision 540d6571 - 16/01/2015 16:23 - Benjamin Bohard

Utilisation d'un template générique pour ldap.conf.

Ref #10210

Révision e5306ac4 - 16/01/2015 18:05 - Benjamin Bohard

Il est nécessaire d'utiliser le protocole ldaps pour le meddtl.

Ref #10210

Révision 29e2bf7e - 16/01/2015 18:45 - christophe guerinot

Retour sur protocole ldaps/port 636 (ref #10210 @0.30).

Révision 0a143b10 - 19/01/2015 12:42 - christophe guerinot

smb.conf: MEDDE introduction du mode mixte comme défini en 2.3 (fixes #10209 @2.0).

- pour les adaptations sur le template ldap.conf (voir ref #10210)

Révision f31e78b4 - 20/01/2015 17:18 - Benjamin Bohard

cn=admin,%%ldap_base_dn est équivalent à %%smb_ldap_admin_dn.

L'identifiant de l'admin n'est cn=admin quand sur les modules EOLE. L'utilisation
d'une variable est nécessaire pour le fonctionnement des autres modules.

Ref #10210

Révision 5d843f7d - 20/01/2015 22:38 - christophe guerinot

Adaptation des fichiers de configuration ldap.conf (fixes #10210) - smbldap.conf et smbldap_bind.conf (ref #10207)

- Ajout du fichier de mise à jour des mots de passe (fichier.ini)
- 'smbldap.conf.ecdl' est une mise à niveau du fichier de la version 2.3
- 'smbldap_bind.conf' devrait encore évoluer afin de pouvoir supprimer le template 'smbldap_bind.conf.ecdl'

Historique

#1 - 15/01/2015 16:56 - christophe guerinot

Si on part sur l'idée d'éviter d'avoir un template du genre ldap.conf.ecdl :(
Il y aurait un compromis pour éviter de faire une usine à gaz serait d'introduire une variable 'ldap_medde' dans le projet conf-ecdl avec une série de is_defined ... dans le template

```
%if %%active_ldap == 'oui'
host %%adresse_ip_ldap
%if %%is_defined('ldap_medde') and  %%is_defined('smb_ldap_suffix') and %%ldap_medde == 'oui'
base %%smb_ldap_suffix
port 636
TLSCACertificateFile            %%ecdl_ca_cert
DEREF always
timelimit 120
TIMEOUT 20
nss_base_passwd %%smb_ldap_suffix?sub
nss_base_group %%smb_ldap_suffix?sub
 %else
base %%ldap_base_dn
port 389
timelimit 10
```

```
nss_base_passwd %%ldap_base_dn?sub
nss_base_group %%ldap_base_dn?sub
%end if
(...)
%end if
```

avec peut être des directives à paramétrer timelimit, timeout ?

#2 - 15/01/2015 17:20 - Benjamin Bohard

```
%set %%active_ldap = 'non'

# cas Amon sans AmonEcole
%if (%%getVar('activer_nufw', 'non') == 'oui' and  %%activer_client_ldap == 'non') or %%activer_client_ldap !=
 'non'
%set %%active_ldap = 'oui'
%set %%ldap_servers = [%%adresse_ip_ldap]
 %if %%getVar('activer_ldap_secours', 'non') == 'oui'
%set %%ldap_servers = %%ldap_servers + ['localhost']
 %end if
%set %%nss_map_base_passwd = [%%ldap_base_dn, 'sub', %%getVar(%%nss_map_base_passwd_filter, '')]
%set %%nss_map_base_passwd = [el for el in %%nss_map_base_passwd if el != '']
%set %%nss_map_base_group = [%%ldap_base_dn, 'sub', %%getVar(%%nss_map_base_group_filter, '')]
%set %%nss_map_base_group = [el for el in %%nss_map_base_group if el != '']
%end if

%if %%active_ldap == 'oui'

# paramètres de connexion
URI %%custom_join(['ldap://{0}:389'.format(ldap) for ldap in %%ldap_servers], ' ')
ldap_version 3
 %if %%ldap_tls == 'oui'
ssl start_tls
tls_checkpeer no
%if not %%is_empty(%%ldap_ca_cert)
TLS_CACERT %%ldap_ca_cert
%end if
TLSVerifyClient never
TLS_REQCERT     never
 %else
ssl off
 %end if

# options de recherche
base %%ldap_base_dn
scope sub
pam_login_attribute uid
pam_password md5
nss_map_attribute gecos displayName
nss_base_passwd %%custom_join(%%nss_base_passwd, '?')
nss_base_group %%custom_join(%%nss_base_passwd, '?')
#fixe #1809
nss_initgroups_ignoreusers root

# optimisations
timelimit %%ldap_timelimit
bind_time_limit %%ldap_bind_time_limit
bind_policy %%ldap_bind_policy
%end if
```

Cette approche nécessite une nouvelle variable "activer_ldap_secours" pour ajouter localhost (ou autre ?) dans le fichier de configuration et *activer* les balises fichiers dans le dictionnaire.

Les variables *nss_map_base_passwd* et *nss_map_base_group* sont les équivalents des variables *meddtl_suffixe_ldap_nss_base_passwd* et *meddtl_suffixe_ldap_nss_base_group*

Les options d'optimisation pourrait être des variables (elles n'ont pas la même valeur actuellement).

#3 - 15/01/2015 17:21 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#4 - 15/01/2015 18:20 - christophe guerinot

Impeccable :)
l'accès au ldap samba centralisé est fonctionnel

Apparemment juste une bricole dans le template à modifier

```
nss_base_passwd %%custom_join(%%nss_map_base_passwd, '?')
nss_base_group %%custom_join(%%nss_map_base_group, '?')
```

au lieu de %%nss_base_passwd

#5 - 16/01/2015 16:33 - Benjamin Bohard

- % réalisé changé de 0 à 90

- Restant à faire (heures) changé de 4.0 à 0.2

#6 - 20/01/2015 22:50 - christophe guerinot

- Statut changé de En cours à Résolu

- % réalisé changé de 90 à 100

Appliqué par commit conf-ecdl:5d843f7d9e30a429d2c2ba6680cc7d5e58ec63b5.

#7 - 20/01/2015 23:08 - christophe guerinot

A l'attention de Benjamin

j'ai du adapter la partie activer_annuaire_secours
- duplication des 3 lignes concernant le certificat (il est necessaire même si tls n'est pas activé (ldaps)
- réinitialiser la variable ldap_base_dn avec smb_ldap_suffix
- rajouter les deux lignes
deref always
referrals on
en fait elles sont nécessaires même sans proxy ldap

#8 - 22/01/2015 13:44 - Thierry Bertrand

- Statut changé de Résolu à Fermé

- Restant à faire (heures) changé de 0.2 à 0.0