

Distribution EOLE - Proposition Scénario #31404

Synchronisation pwdLastSet pour gérer la demande de changement à la 1ere connexion

11/12/2020 16:00 - Gilles Grandgérard

Statut:	Fermé	% réalisé:	0%
Priorité:	Normal	Temps estimé:	0.00 heure
Assigné à:	Daniel Dehennin	Temps passé:	0.00 heure
Catégorie:			
Version cible:			

Description

Dans le cas ou un administrateur force le changement de mot de passe dans RSAT, un attribut **pwdLastSet** est modifié:

```
--- prof1.init      2020-12-11 16:09:43.493864053 +0100
+++ prof1.reset    2020-12-11 16:09:48.646040330 +0100
@@ -16,6 +16,7 @@
instanceType: 4
lastLogoff: 0
lastLogon: 0
+lockoutTime: 0
logonCount: 0
mail: prof1@etb1.ac-test.fr
memberOf: CN=professeurs,CN=Users,DC=dompedago,DC=etb1,DC=lan
@@ -30,12 +31,12 @@
personalTitle: M.
primaryGroupID: 513
profilePath: \\scribe\prof1\profil
-pwdLastSet: 132521233510864030
+pwdLastSet: 0
sAMAccountName: prof1
sAMAccountType: 805306368
sn: Prof1
userAccountControl: 544
-uSNChanged: 4354
+uSNChanged: 4389
uSNCreated: 4341
-whenChanged: 20201211012231.0Z
+whenChanged: 20201211150014.0Z
whenCreated: 20201211012226.0Z
```

A la connexion, l'utilisateur DOIT modifier son mot de passe. Suite à la cette modification l'attribut est modifié pour signaler que le mot de passe est modifié :

```
--- prof1.reset    2020-12-11 16:09:48.646040330 +0100
+++ prof1.after-first-login 2020-12-11 16:10:37.831723787 +0100
@@ -15,9 +15,10 @@
info: EOLE
instanceType: 4
lastLogoff: 0
-lastLogon: 0
+lastLogon: 132521728582620010
+lastLogonTimestamp: 132521728567002350
lockoutTime: 0
-logonCount: 0
+logonCount: 4
mail: prof1@etb1.ac-test.fr
memberOf: CN=professeurs,CN=Users,DC=dompedago,DC=etb1,DC=lan
name: prof1
@@ -31,12 +32,12 @@
personalTitle: M.
```

```
primaryGroupID: 513
profilePath: \\scribe\profl\profil
-pwdLastSet: 0
+pwdLastSet: 132521728567262260
sAMAccountName: prof1
sAMAccountType: 805306368
sn: Prof1
userAccountControl: 544
-uSNChanged: 4389
+uSNChanged: 4391
uSNCreated: 4341
-whenChanged: 20201211150014.0Z
+whenChanged: 20201211150736.0Z
whenCreated: 20201211012226.0Z
```

Dans OpenLdap du Scribe, il n'existe pas de transfert de AD -> OpenLdap.

Il faut ajouter :

- une tâche de synchronisation dans **IsC.xml** pour les attributs implémentant les [politiques de mot de passe LDAP](#)
- définir les attributs qui vont bien dans **changepasswordeole.pl** afin d'annuler le délai de synchronisation.

Demandes liées:

Lié à SSO - Scénario #31512: Gérer le changement de mot de passe des utilisat...	Terminé (Sprint)	2/01/2021	19/02/2021
Lié à EoleSSO - Scénario #31615: Gérer le changement de mot de passe des util...	Terminé (Sprint)	2/02/2021	12/03/2021

Historique

#1 - 11/12/2020 16:14 - Daniel Dehennin

- Description mis à jour

#2 - 11/12/2020 16:22 - Daniel Dehennin

- Description mis à jour

#3 - 11/12/2020 16:26 - Daniel Dehennin

Je vais tester sur un scribeAD:

1. installer **lemonldap-ng-scribe**
2. activer le module de changement de mot de passe expiré
3. tenter une connexion sur la mire d'authentification LemonLDAP::NG avec différentes valeurs pour différents attributs afin de déterminer quels sont les attributs à modifier côté **OpenLDAP**.

#4 - 11/12/2020 16:27 - Gilles Grandgérard

dans OpenLdap:

```
sambaPwdLastSet: 1607595133
sambaPwdMustChange: 1607595133
```

#5 - 14/12/2020 16:17 - Daniel Dehennin

Il y a [plus simple, semble-t-il](#) :

- utiliser OpenLDAP comme référentiel utilisateur
- utiliser l'Active Directory comme référentiel de mot de passe

#6 - 15/12/2020 09:20 - Daniel Dehennin

- Assigné à mis à Daniel Dehennin

#7 - 16/12/2020 15:26 - Daniel Dehennin

Et bien non, ce [n'est pas plus simple](#).

La combinaison des modules entraine :

1. Le module **LDAP** est responsable d'obtenir le **DN** de l'utilisateur
2. Le module **AD** utilise le **DN** obtenu par le module **LDAP** pour jouer l'authentification

Cela ne fonctionne pas car les deux annuaires n'ont pas la même structure.

La seule solution actuellement disponible serait de faire un [module personnalisé](#) qui combinerait les deux modules en ajoutant une recherche du **DN** par le module **AD** afin de l'utiliser pour l'authentification (et le changement de mot de passe ?)

#8 - 05/01/2021 11:52 - Joël Cuissinat

- Echéance 18/12/2020 supprimé

- Version cible sprint 2020 49-51 Equipe MENSUR supprimé

- Début 11/12/2020 supprimé

#9 - 08/01/2021 11:53 - Daniel Dehennin

- Lié à Scénario #31512: Gérer le changement de mot de passe des utilisateurs depuis les SSO web ajouté

#10 - 02/02/2021 15:05 - Daniel Dehennin

- Release changé de EOLE 2.8.0 à EOLE 2.8.0.1

#11 - 02/02/2021 15:06 - Daniel Dehennin

- Lié à Scénario #31615: Gérer le changement de mot de passe des utilisateurs depuis EOLE SSO ajouté

#12 - 02/02/2021 15:11 - Daniel Dehennin

- Statut changé de Nouveau à Terminé (Sprint)

Les scénarios [#31512](#) et [#31615](#) prennent en charge la gestion du changement de mot de passe.

#13 - 02/07/2021 14:55 - Joël Cuissinat

- Tracker changé de Scénario à Proposition Scénario

- Statut changé de Terminé (Sprint) à Fermé