EoleSSO - Scénario #35906

Forcer le changement de mot de passe à la première connexion au portail web

16/04/2024 11:17 - Laurent Brillard

Statut:	Nouveau	**Début:**	21/05/2024
Priorité:	Normal	**Echéance:**	01/01/2026
Assigné à:	Joël Cuissinat	**% réalisé:**	50%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Carnet MENSR	**Temps passé:**	0.00 heure

Description

Bonjour,

Le forçage du changement de mot de passe à la première connexion a toujours fonctionné au niveau de la session Windows, mais sur Scribe 2.7 ou 2.8 sans SASLAuth, ce mécanisme n'est plus possible.

Serait-il possible de forcer le changement à la première connexion au portail ?

Merci d'avance !
Laurent

Bien à vous,
Laurent

Sous-tâches:

Tâche # 35947: changepasswordeole.pl : modifier le shadowLastChange d'OpenLDAP au lieu...	**Résolu**
Tâche # 35948: Réactiver les options "Changement de mot de passe à la première connexio...	**En cours**

Demandes liées:

Lié à Distribution EOLE - Scénario #35657: Scribe : Les options "Changement d...	**Terminé (Sprint)**	**01/10/2022**	**01/01/2024**

Révisions associées

Révision aee5b0c9 - 03/05/2024 11:53 - Joël Cuissinat

changepasswordeole.pl : update OpenLDAP shadowLastChange

Ref: #35906

Historique

#1 - 03/05/2024 11:36 - Joël Cuissinat

Proposition de Christophe : identifier un attribut OpenLDAP pouvant être utilisé en tant que sémaphore sans toutefois empêcher l'authentification EoleSSO.
Une fois authentifié, le portail (dispacher) pourrait vérifier cet attribut et rediriger l'utilisateur vers EOE si nécessaire.

#2 - 03/05/2024 11:42 - Joël Cuissinat

L'attribut pourrait être **shadowLastChange** avec une règle à définir (exemple : le mot de passe a plus de 40 jours).
Encore faut-il qu'il soit mis à jour !

=> proposition de patch sur le script perl /usr/sbin/changepasswordeole.pl à intégrer :

```
    use Time::Piece;
    &modify_password( $openldap, $openldap_entry->dn, 'shadowLastChange',int(localtime->epoch / 86400));
```

Dans ce cas, le **travail côté PCLL** serait de rétablir les options de changement de mot de passe (cf. #35657 !) et de faire en sorte que lors de leur application, cet attribut soit mis à jour avec une valeur convenue (zéro ?).

the value of shadowLastChange is replaced with the number of days between January 1, 1970 and the day when the user password is updated.

#3 - 03/05/2024 11:43 - Joël Cuissinat

- Lié à Scénario #35657: Scribe : Les options "Changement de mot de passe à la première connexion" devraient être masquées si la délégation d'authentification SASL est désactivée ajouté

#4 - 03/05/2024 11:47 - Laurent Brillard

En complément de cette demande, afin de récupérer le paramètre shadowLastChange dans l'OpenLDAP de Scribe 2.7 et 2.8, Christophe a ajouté au fichier /usr/sbin/changepasswordeole.pl ligne 185 :

```
use Time::Piece;
&modify_password( $openldap, $openldap_entry->dn, 'shadowLastChange',int(localtime->epoch / 86400));
```

Nous l'avons déjà déployé mais ce serait bien si cela pouvait être remis en standard dans le cas où OpenLDAP contient toujours l'authentification (mode SASLAuth coupé).

Merci !
Laurent

#5 - 03/05/2024 11:52 - Laurent Brillard

Pour utiliser shadowLastChange, une règle de la DNE nous demande de forcer le changement de mot de passe au bout de 3 ans.
Christophe a traité sur edispatcher.

Donc le forçage du changement de mot de passe pourrait être fait en positionnant shadowLastChange à plus de 3 ans ?

#6 - 03/05/2024 14:45 - Joël Cuissinat

Dans les interfaces, c'est toujours sur une initialisation ou un changement de mot de passe qu'il est possible demander un changement forcé, on passe forcément par donc forcément par **changepasswordeole.pl** pour les comptes AD.
FIXME : en 2.7.2 c'est désactivé par défaut pour tous les modes !

Sur EOLE ≥ 2.8.0, le script est appelé avec "1" en 3ème paramètre. On pourrait donc jouer sur la valeur du shadowLastChange à cet endroit.

Il suffirait :

1. de forcer la variable creole **forced_password_modification_allowed** à **oui** (cela évite d'aller re-modifier tout ce qui a été touché dans #35657)

```
root@scribe:~# rgrep forced_password_modification_allowed /usr/share/eole/creole/distrib/
/usr/share/eole/creole/distrib/ldapconf.conf:forced_password_modification_allowed=%%getVar('ldap_sasl_auth_del
egation', 'non')
```

2. gérer le + de 3 ans dans le script **changepasswordeole.pl**

```
my $last_change = int(localtime->epoch / 86400) );
if( defined $changePwd && $changePwd == 1 ) {
    $last_change = $last_change - 1095
}
&modify_password( $openldap, $openldap_entry->dn, 'shadowLastChange',
    $last_change );
```

#7 - 21/05/2024 12:15 - Laurent Brillard

Parfait !

Si cela peut être mis sur 2.8, on est prêt pour tester.

Merci !

#8 - 21/05/2024 14:19 - Joël Cuissinat

- Tracker changé de Demande à Scénario

- Echéance mis à 01/01/2026

- Assigné à mis à Joël Cuissinat

- Version cible mis à Carnet MENSR

- Release mis à EOLE 2.8.0

- Points de scénarios mis à 1.0