EOLE AD DC - Proposition Scénario #23999

Génération de Hash supplémentaires dans l'attribut SupplementalCredentials

29/05/2018 10:39 - Emmanuel IHRY

Statut:	Fermé	**% réalisé:**	0%
Priorité:	Normal	**Temps estimé:**	0.00 heure
Assigné à:	force bleue	**Temps passé:**	0.00 heure
Catégorie:			
Version cible:			

Description

A partir de la version samba 4.7, il est possible de générer des Hash supplémentaires qui sont stockés dans l'attribut SupplementalCredentials

La configuration est simple, il suffit d'ajouter un ligne dans smb.conf avec les formats attendus :

- password hash userPassword schemes = CryptSHA256 CryptSHA512*

Dans cette exemple, au prochain changement de mot de passe du user via CTRL ALT SUPP ou bien via samba-tool, cela génèrera dans l'attribut supplementalCredentials deux hash :

```
root@pdc-ad1:~# samba-tool user getpassword toto --attributes=virtualCryptSHA512,virtualCryptSHA25
6
dn: CN=toto,CN=Users,DC=ac-test,DC=eole

Got password OK
root@pdc-ad1:~# samba-tool user getpassword toto --attributes=virtualCryptSHA512,virtualCryptSHA25
6
dn: CN=toto,CN=Users,DC=ac-test,DC=eole
virtualCryptSHA256: {CRYPT}$5$Bg0Vq1Nm22S4ITbE$YUIa8/bDvD58iBT6KzAmVT4sRIb3brY
ri5B2do4ap77
virtualCryptSHA512: {CRYPT}$6$V8BOezBunSOZ7fcK$uzngXi8P4GhC06JM9PQ/125KHKuiIr5
Yxz7WYkdjwdxmj0VPbbZ3PvKR35qbEUhFKAcG66mrm750KapIIU3pu.

Got password OK
```

Les formats proposés sont décrits dans MAN smb.conf :

```
password hash userPassword schemes (G)

This parameter determines whether or not samba(8) acting as an Active Directory Domain Controller
will attempt to store additional passwords hash types for the user

The values are stored as 'Primary:userPassword' in the supplementalCredentials attribute. The valu
e of this option is a hash type.

The currently supported hash types are:

· CryptSHA256

· CryptSHA512

Multiple instances of a hash type may be computed and stored. The password hashes are calculated u
sing the crypt(3) call. The number of rounds used to compute the hash can be specified by
adding ':rounds=xxxx' to the hash type, i.e. CryptSHA512:rounds=4500 would calculate an SHA512 has
h using 4500 rounds. If not specified the Operating System defaults for crypt(3) are used.

As password changes can occur on any domain controller, you should configure this on each of them.
 Note that this feature is currently available only on Samba domain controllers.
```

```
Currently the NT Hash of the password is recorded when these hashes are calculated and stored. Whe
n retrieving the hashes the current value of the NT Hash is checked against the stored NT
Hash. This detects password changes that have not updated the password hashes. In this case samba-
tool user will ignore the stored hash values.

Being able to obtain the hashed password helps, when they need to be imported into other authentic
ation systems later (see samba-tool user getpassword) or you want to keep the passwords in
sync with another system, e.g. an OpenLDAP server (see samba-tool user syncpasswords).

Related command: unix password sync

Default: password hash userPassword schemes =

Example: password hash userPassword schemes = CryptSHA256

Example: password hash userPassword schemes = CryptSHA256 CryptSHA512

Example: password hash userPassword schemes = CryptSHA256:rounds=5000 CryptSHA512:rounds=7000
```

H2. Evolution à faire coté EOLE : ajouter un attribut permettant de désigner les hash à générer

Demandes liées:

Duplique Distribution EOLE - Scénario #26377: Évolution de la configuration d...	**Terminé (Sprint)**	**29/01/2018**	**25/01/2019**

Historique

#1 - 29/05/2018 10:39 - Emmanuel IHRY

- Points de scénarios mis à 2.0

#2 - 21/06/2018 10:31 - Emmanuel IHRY

- Echéance mis à 13/07/2018

- Version cible mis à Sprint 2018 26-28 Equipe PNE-SR

- Début mis à 25/06/2018

#3 - 21/06/2018 10:31 - Emmanuel IHRY

- Assigné à mis à force bleue

#4 - 25/06/2018 13:57 - Emmanuel GARETTE

- Points de scénarios changé de 2.0 à 1.0

#5 - 17/07/2018 09:55 - Emmanuel IHRY

- Version cible changé de Sprint 2018 26-28 Equipe PNE-SR à Sprint 2018 29-34 Equipe PNE-SR

#6 - 17/07/2018 10:16 - Emmanuel IHRY

- Version cible changé de Sprint 2018 29-34 Equipe PNE-SR à Sprint 2018 35-37 Equipe PNE-SR

#7 - 27/08/2018 15:51 - Emmanuel IHRY

- Version cible changé de Sprint 2018 35-37 Equipe PNE-SR à Sprint 2018 38-40 Equipe PNE-SR

#8 - 08/10/2018 08:47 - Emmanuel IHRY

- Version cible changé de Sprint 2018 38-40 Equipe PNE-SR à Sprint 2018 44-46 Equipe PNE-SR

#9 - 26/10/2018 10:07 - Emmanuel IHRY

- Version cible changé de Sprint 2018 44-46 Equipe PNE-SR à Sprint 2018 47-49 Equipe PNE-SR

#10 - 12/11/2018 17:03 - Emmanuel IHRY

- Version cible changé de Sprint 2018 47-49 Equipe PNE-SR à Sprint 2018 44-46 Equipe PNE-SR

#11 - 26/11/2018 13:34 - Emmanuel IHRY

- Version cible changé de Sprint 2018 44-46 Equipe PNE-SR à Sprint 2018 50-52 Equipe PNE-SR

#12 - 05/12/2018 08:52 - Emmanuel IHRY

- Echéance 13/07/2018 supprimé

- Version cible Sprint 2018 50-52 Equipe PNE-SR supprimé

- Début 29/05/2018 supprimé

#13 - 08/01/2019 08:31 - Emmanuel IHRY

- Echéance mis à 25/01/2019

- Version cible mis à sprint 2019 2-4 Equipe MENSR

- Début mis à 07/01/2019

#14 - 08/01/2019 09:40 - Benjamin Bohard

- Dupliqué par Scénario #26377: Évolution de la configuration de Samba ajouté

#15 - 08/01/2019 09:59 - Joël Cuissinat

- Tracker changé de Scénario à Proposition Scénario

- Statut changé de Nouveau à Fermé

- Version cible sprint 2019 2-4 Equipe MENSR supprimé

#16 - 08/01/2019 10:04 - Joël Cuissinat

- Dupliqué par Scénario #26377: Évolution de la configuration de Samba supprimé

#17 - 08/01/2019 10:06 - Joël Cuissinat

- Duplique Scénario #26377: Évolution de la configuration de Samba ajouté