Distribution EOLE - Tâche #24000

Scénario # 26377 (Terminé (Sprint)): Évolution de la configuration de Samba

Ajout de variables permettant de générer les hash HA256 et SHA512

29/05/2018 10:45 - Emmanuel IHRY

Statut:	Fermé	**Début:**	29/05/2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	80%
Version cible:	sprint 2019 2-4 Equipe MENSR	**Temps estimé:**	6.00 heures
		Temps passé:	3.00 heures

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
```

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

Ajouter une variable qui permette de saisir une ou deux valeurs de ce type : CryptSHA256 CryptSHA512:rounds=4500

Modifier le template smb.conf en ajoutant cette ligne si génération de hash demandée dans gen_config :

password hash userPassword schemes = CryptSHA256 CryptSHA512:rounds=4500

Pour chaque Hash, il faudra définir ces deux infos :
~~Type de Hash : SHA256 ou SHA512~~
Nb de rounds : vide par défaut, autres valeurs possibles à vérifier avec la doc samba

Demandes liées:

Lié à Documentations - Tâche #26606: Documenter les variables permettant de g...	**Fermé**	**28/01/2019**

Révisions associées

Révision 7502c32e - 21/01/2019 11:50 - Benjamin Bohard

Let configure password hash userPassword schemes in smb.conf.

Ref #24000

Révision 6c1ce7e2 - 21/01/2019 11:50 - Emmanuel GARETTE

Implement constraints for crypt round number.

Ref #24000

Historique

#1 - 21/06/2018 10:34 - Emmanuel IHRY

- Description mis à jour

- Assigné à mis à Benjamin Bohard

#2 - 08/01/2019 08:31 - Emmanuel IHRY

Le besoin précis en terme d'éolisation du paramétrage de la génération des Hash sera spécifié par le MTES pour le 11/01 au + tard

#3 - 08/01/2019 09:36 - Benjamin Bohard

- Tâche parente changé de #23999 à #26377

#4 - 08/01/2019 09:39 - Benjamin Bohard

- Description mis à jour

#5 - 08/01/2019 16:58 - Gilles Grandgérard

1°) Changelog samba 4.8: Etudier "--plaintext-secrets" et ses conséquences sur les mots de passe.
L'idée pourrait être d'ajouter une variable dans le dico qui activerait ou non ce mécanisme
Par défaut, nous ne l'utiliserions pas

2°) Se poser la question de la sauvegarde de 'encrypted_secrets.key'

```
Encrypted secrets
-----------------

Attributes deemed to be sensitive are now encrypted on disk. The sensitive
values are currently:
    pekList
    msDS-ExecuteScriptPassword
    currentValue
    dBCSPwd
    initialAuthIncoming
    initialAuthOutgoing
    lmPwdHistory
    ntPwdHistory
    priorValue
    supplementalCredentials
    trustAuthIncoming
    trustAuthOutgoing
    unicodePwd
    clearTextPassword

This encryption is enabled by default on a new provision or join, it can be disabled at provision or join time
 with the new option '--plaintext-secrets'.

However, an in-place upgrade will not encrypt the database.

Once encrypted, it is not possible to do an in-place downgrade (eg to 4.7) of the database. To obtain an unenc
rypted copy of the database a new DC join should be performed,
specifying the '--plaintext-secrets' option.

The key file "encrypted_secrets.key" is created in the same directory as the database and should NEVER be disc
losed.  It is included by the samba_backup script.
```

#6 - 10/01/2019 13:41 - Emmanuel IHRY

Pour ce qui est de la génération des SHA256 et SHA512, je propose cette évolution :

Coté DICO, en mode expert :
Après le bloc "Gestion des services samba", et donc a avant le bloc "Environnnement réseau"

Ajout d'un bloc intitulé "Gestion des empreintes de mots de passe" avec ce contenu :

```
*Gestion des empruntes de mots de passe*

Générer une empreinte de type SHA256 :  oui/non  nombre de tour de hachage à utiliser : valeur de 1000 à 99999
9999, val par défaut = 5000

Générer une empreinte de type SHA512 :  oui/non   nombre de tour de hachage à utiliser : valeur de 1000 à 9999
99999, val par défaut = 5000
```

NB : en bulle d'aide indiquer que les empreintes seront générées après le prochain changement de mot de passe et récupérables via cette commande :
amba-tool user getpassword <USER>° --attributes=virtualCryptSHA512,virtualCryptSHA256

PS : Je suis preneur d'avis sur l'utilité de l'option : nombre de tour de hachage à utiliser

Cote SMB.CONF

En fonction des options choisies, générer une de lignes pouvant avoir ce type de valeurs :

```
password hash userPassword schemes = CryptSHA256

password hash userPassword schemes = CryptSHA256 CryptSHA512

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

#7 - 18/01/2019 09:55 - Benjamin Bohard

- Projet changé de EOLE AD DC à Distribution EOLE

- Statut changé de Nouveau à En cours

#8 - 18/01/2019 14:36 - Benjamin Bohard

Le nombre d'itération pour le calcul du hash ne devrait peut-être pas avoir une valeur par défaut fixe (commune à tous les serveurs si la variable en mode expert n'est pas éditée).
D'un autre côté, il faut, a priori, avoir le même nombre d'itération sur les différentes serveurs DC d'un domaine.
Le nombre d'itération pourrait-il être aléatoire sur le DC primaire et non rempli pour celui des DC additionnels ?

#9 - 18/01/2019 17:15 - Emmanuel GARETTE

- % réalisé changé de 0 à 80

- Temps estimé mis à 6.00 h

- Restant à faire (heures) mis à 3.0

Reste a voir les valeurs par défaut.

#10 - 21/01/2019 12:08 - Benjamin Bohard

- Statut changé de En cours à Résolu

#11 - 21/01/2019 12:08 - Benjamin Bohard

- Statut changé de Résolu à Fermé

- Restant à faire (heures) changé de 3.0 à 0.0

#12 - 28/01/2019 11:30 - Joël Cuissinat

- Lié à Tâche #26606: Documenter les variables permettant de générer les hash SHA256 et SHA512 ajouté