EOLE AD DC - Tâche #19756

Scénario # 19975 (Terminé (Sprint)): Évolution sur la sécurité des mots de passe et procédure de jonction au domaine

Le mot de passe admin du domaine ne doit pas être stocké sur les RWDC ou RODC

03/16/2017 12:04 PM - Emmanuel IHRY

Status:	Fermé	**Start date:**	03/16/2017
Priority:	Haut	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	100%
Target version:	sprint 2017 13-15 Equipe PNE-SR	**Estimated time:**	12.00 hours
		Spent time:	15.00 hours

Description

root@dc1:~# cat /var/lib/samba/.eole-ad-dc --> contient le mot de passe en clair

Vérifié sur le RWDC je suppose que c'est la mẽme chose sur le RODC

Associated revisions

Revision f25dd529 - 04/04/2017 04:57 PM - Benjamin Bohard

Ne pas stocker le mot de passe dans un fichier.

La fonction python ne fait que valider le mot de passe.

Ref #19756

Revision 20aba0a2 - 04/04/2017 04:57 PM - Benjamin Bohard

Restreindre les caractères autorisés pour les mots de passe.

Ref #19756

Revision ba9892ec - 04/06/2017 03:09 PM - Benjamin Bohard

Défaire les changements entrepris pour la conversion de la bibliothèque en python

Ref #19756

History

#1 - 03/16/2017 02:54 PM - Michel BALLY

confirmation, même fichier présent sur RODC et serveur membre

#2 - 03/28/2017 08:37 AM - Emmanuel IHRY

- Parent task set to #19975

#3 - 03/29/2017 09:16 AM - Emmanuel IHRY

- Description updated

- Assigned To set to Benjamin Bohard

#4 - 03/31/2017 09:51 AM - Benjamin Bohard

- Status changed from Nouveau to En cours

#5 - 03/31/2017 10:05 AM - Benjamin Bohard

- Estimated time set to 12.00 h

- Remaining (hours) set to 8.0

Le traitement du mot de passe utilise une commande extérieure qui ne permet pas, proprement, de transmettre le mot de passe sans l'écrire dans un fichier intermédiaire.

L'ensemble du script est réécrit en python pour disposer des facilités de traitement des chaînes de caractères (validation du mot de passe) et ne pas avoir à faire passer les variables d'un langage à l'autre.

Changement nécessaire dans le script posttemplate également.

Gérer le fichier cron pour la réplication avec les mécanismes creole plutôt qu'avec l'écriture dans le script.

#6 - 03/31/2017 05:47 PM - Benjamin Bohard

- % Done changed from 0 to 70

- Remaining (hours) changed from 8.0 to 2.0

#7 - 04/03/2017 04:31 PM - Benjamin Bohard

- % Done changed from 70 to 90

- Remaining (hours) changed from 2.0 to 1.0

Tester sur le contrôleur primaire de domaine, "bug" samba découvert au passage, avec une méthode de résolution locale. À voir pour le report upstream (mail envoyé sur la liste samba-technical dans un premier temps).

#8 - 04/06/2017 12:33 PM - Benjamin Bohard

- Status changed from En cours to Résolu

- % Done changed from 90 to 100

- Remaining (hours) changed from 1.0 to 0.25

#9 - 04/10/2017 01:38 PM - Emmanuel IHRY

- Status changed from Résolu to Fermé

- Remaining (hours) changed from 0.25 to 0.0

testé sur infra de Dijon, le fichier /var/lib/samba/.eole-ad-dc n'est plus présent

#10 - 04/10/2017 02:37 PM - Emmanuel IHRY

- Status changed from Fermé to Résolu

PB lors de l'instance d'un DC2

```
/var/lib/samba/.eole-ad-dc n'est pas trouvé sur le DC1
```

#11 - 04/10/2017 02:37 PM - Emmanuel IHRY

- Remaining (hours) changed from 0.0 to 0.25

#12 - 04/10/2017 02:56 PM - Emmanuel IHRY

Pour la jonction au domaine, on demande le compte Administrator, ou tout autre compte

Initialisation DC Secondaire
Generation de la clef SSH pour les echanges entre DC
Envoi de la clef SSH dc2 vers le DC 192.168.0.5
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.0.5's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.0.5'"
and check to make sure that only the key(s) you wanted were added.

id_rsa.pub 100% 390 0.4KB/s 00:00
Jonction au domaine
Compte pour joindre le serveur au domaine [Administrator] :

Create password for delegation:

Redémarrage service

#13 - 04/10/2017 04:13 PM - Emmanuel IHRY

- Status changed from Résolu to Fermé

- Remaining (hours) changed from 0.25 to 0.0

La procédure d'instance du SETH DC secondaire demande désormais la saisie du compte root pour les besoins d'échange de clé (réplication) et du compte AD (par défaut Administrator), mais il est possible d'en désigner un autre

voir cependant cette demande de correction mineure #20142