EOLE AD DC - Tâche #20003

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

SETC DC : Expliquer le fonctionnement de la synchro du sysvol et jonction au domaine

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

Status:	Ne sera pas résolu	**Start date:**	03/16/2017
Priority:	Normal	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	100%
Target version:	sprint 2017 13-15 Equipe PNE-SR	**Estimated time:**	5.00 hours
		Spent time:	5.00 hours

Description

Lors de la jonction d'un DC additionnel, il est nécessaire de connaître le PWD du primaire :

- est-ce du au process Rsync à mettre en place pour sysvol ?
- rsync est il mono (depuis le primaire vers le secondaire) ou bi directionnel ?
- y aurait il une solution pour joindre le DC uniquement en désignant un compte du domaine AD (à saisir lors de l'instance comme le membre ?). Comme c'est demandé dans le demande #19757

- sinon on laisse tel quel à condition que le mot de passe admin du domaine ne soit plus stocké sur les SETH (voir #19756)

History

#1 - 03/29/2017 11:29 AM - Benjamin Bohard

- Estimated time set to 5.00 h

- Remaining (hours) set to 5.0

Le mot de passe est utilisé pour mettre en place les mécanismes de réplication.

Ce qu'il est prévu de faire : se dispenser de la création du fichier intermédiaire stockant le mot de passe, utiliser un compte autre qu'Administrator, supprimer les scripts obsolètes nécessitant un mot de passe.

#2 - 04/04/2017 04:40 PM - Benjamin Bohard

- % Done changed from 0 to 80

- Remaining (hours) changed from 5.0 to 1.0

La synchronisation fait appel à ssh utilisable uniquement avec un compte système dans l'état actuel de la configuration.

Il y a deux aspects pour la sécurisation des accès et l'accès lui-même.

Configuration sshd

Modifier les groupes autorisés à se connecter au serveur sshd (variable ssh_allow_groups déjà existante dans la configuration, dans l'onglet sshd en mode expert)

Compte accessible

Créer un compte système dédié avec des privilèges restreints

Nécessite la création du compte sur le DC avec le renseignement d'un mot de passe (étape supplémentaire lors de l'instance ou traitement à part avant la jonction au domaine des autres serveurs.

DC

Ajouter un compte dédié (paramétrable ?) et restreindre ses droits (sudo ou shell restreint, droits d'accès)

DC additionnel

Renseigner le compte dans la configuration si besoin (paramétrable ?).
Utiliser ce compte pour les scripts JobSynchroSysvol et samba4.sh

Permettre de se connecter avec un compte du domaine

activer winbind en backend d'authentification

Installation nécessaire de libpam_winbind pour permettre de se connecter avec un compte du domaine.

configuration samba

winbind doit remonter un shell valide pour les utilisateurs pour que la connexion soit possible.
Il est possible de déclarer le shell dans la fiche de l'utilisateur dans le cadre de la rfc2307 ou de remonter un shell particulier pour tous les utilisateurs (/bin/false par défaut).

rfc2307

L'annuaire est déjà provisionné avec les bonnes options.

Il est nécessaire d'ajouter le champ loginShell au compte.
Il faut ajouter des options à la configuration samba pour tenir compte des informations de l'annuaire

```
idmap_ldb:use rfc2307 = yes
```

Tests non concluant pour l'instant : le shell renseigné dans la fiche n'est pas remonté correctement, l'utilisateur conserve le shell /bin/false et se retrouve déconnecter aussitôt.

template shell

Modification globale du shell remonté par winbind.

```
template shell = /bin/sh
```

Test concluant : ssh et scp fonctionnel.

#3 - 04/05/2017 03:31 PM - Emmanuel IHRY

- Status changed from Nouveau to En cours

#4 - 04/06/2017 11:12 AM - Benjamin Bohard

- Status changed from En cours to Ne sera pas résolu

- % Done changed from 80 to 100

- Remaining (hours) changed from 1.0 to 0.0

#5 - 04/06/2017 11:51 AM - Emmanuel IHRY

proposition de scénario à envisager pour la 2.6.2 : #20095