EOLE AD DC - Tâche #17211

Scénario # 17798 (Terminé (Sprint)): Export Keytab: export de la keytab pour un compte système

Ne pas exporter la keytab lors de l'instanciation d'un AD additionnel

22/09/2016 19:47 - christophe guerinot

Statut:	Fermé	**Début:**	22/09/2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Gilles Grandgérard	**% réalisé:**	100%
Version cible:	sprint 2016 45-47 - Équipe MENSR	**Temps estimé:**	2.00 heures
		Temps passé:	1.17 heure

Description

Tranquil IT propose de ne pas exporter la keytab vers un AD additionnel

cette table pourrait éventuellement être utilisée si un service (comme 'squid' par exemple) aurait besoin d'un mot de passe pour s'exécuter.

Dans notre cas il ne semble pas qu'il y ait de besoin, et la présence de cette table peut présenter un gros trou de sécurité

Dans la fonction samba_init_additional(), il faudrait supprimer le paragraphe

```
    # export keytab ${AD_ADMIN}
    [[ -f "${AD_ADMIN_KEYTAB_FILE}" ]] && rm "${AD_ADMIN_KEYTAB_FILE}"
    samba-tool domain exportkeytab "${AD_ADMIN_KEYTAB_FILE}"
    if [[ "$?" -ne 0 ]]
    then
        echo "Impossible de générer le keytab ${AD_ADMIN}"
        exit 1
    fi
```

Révisions associées

Révision 185899be - 06/10/2016 15:41 - christophe guerinot

Ne pas exporter la keytab Administrator lors de l'instanciation d'un AD additionnel (fixes #17211 @1)

Révision e836b888 - 06/10/2016 15:55 - Gilles Grandgérard

revue : suppression référence CreoleGet dans les scripts (ajout dans
samba4-vars.conf)

REF #17211 @10m

Historique

#1 - 06/10/2016 13:36 - christophe guerinot

Je propose l'évolution suivante

ajout de la variable 'ad_additional_dc_export_keytab' dans le dico '25_smb_ad.xml'

```
(...)
        <family name='Active Directory' icon='group'>

(...)
            <variable name="ad_additional_dc_export_keytab" type="oui/non" mode="expert"
                      description="Export de la keytab administrator pour un  contrôleur de domaine additionne
l">
                <value>oui</value>
            </variable>
(...)
```

adaptation dans le script '/usr/lib/eole/samba4.sh'

```
#
function samba_init_additional()
{
(...)
    # export keytab ${AD_ADMIN}
    if [[ "$(CreoleGet ad_additional_dc_export_keytab)" == "oui" ]] || [[ -f "${AD_ADMIN_KEYTAB_FILE}" ]]; the
n
        [[ -f "${AD_ADMIN_KEYTAB_FILE}" ]] && rm "${AD_ADMIN_KEYTAB_FILE}"
        samba-tool domain exportkeytab "${AD_ADMIN_KEYTAB_FILE}"
        if [[ "$?" -ne 0 ]]
        then
            echo "Impossible de générer le keytab ${AD_ADMIN}"
            exit 1
        fi
    fi
(...)
```

l'idée est que si l'instance est relancée, dans le doute, s'il existe déjà un fichier 'AD_ADMIN_KEYTAB_FILE', l'export de la keytab Administrator est forcée quelque soit le contenu de la variable 'ad_additional_dc_export_keytab'

#2 - 06/10/2016 15:46 - christophe guerinot

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

Appliqué par commit 185899bea3b60c3b9ce7704d4969d451baa62565.

#3 - 14/11/2016 11:40 - Benjamin Bohard

- Tâche parente changé de #17183 à #17798

Récupération de la demande auparavant attachée à la proposition de scénario https://dev-eole.ac-dijon.fr/issues/17183

#4 - 15/11/2016 12:10 - Joël Cuissinat

- Assigné à mis à Gilles Grandgérard

- Temps estimé mis à 2.00 h

- Restant à faire (heures) mis à 0.15

#5 - 16/11/2016 10:03 - Scrum Master

- Statut changé de Résolu à Fermé

- Restant à faire (heures) changé de 0.15 à 0.0