eole-asgard - Tâche #31750

Scénario # 31098 (Terminé (Sprint)): kerberisation de postgresql

Étude de l'utilisation de kerberos

24/02/2021 16:32 - Benjamin Bohard

Statut:	Fermé	**Début:**	26/10/2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	100%
Version cible:	MTES - prestation cadoles 43-46	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 24/02/2021 16:47 - Benjamin Bohard

Rappel : le service qui doit être redémarré (sur 2.7.2, adapter le numéro de version sur les autres) est postgresql@10-main.service
h2. sur le DC (testé avec Samba) :

- création d'un utilisateur postgres (samba-tool user create postgres)
- création d'un SPN postgres/fqdn_serveur_pg attaché à l'utilisateur postgres (samba-tool spn add postgres/<fqdn> postgres)
- vérification que le serveur postgresql dispose bien d'une entrée DNS dans la zone et dans la zone inverse
- export de la keytab pour le spn à copier dans /var/lib/postgresql/ sur le serveur postgresql

sur le filer (servant de serveur postgres dans la cible) :

L'emplacement de la keytab est indiqué dans /etc/postgres/<ver>/main/postgresql.conf, variable krb_server_file.
Le fichier doit être la propriété de l'utilisateur postgres (lecture, écriture pour le propriétaire uniquement)

configurer pg_hba.conf en fonction du mode de connexion

pour une connexion avec

```
psql -U admin@DOMSETH.AC-TEST.FR -h file.domseth.ac-test.fr
```

```
host    all          all  0.0.0.0/0     gss include_realm=1 krb_realm=DOMSETH.AC-TEST.FR
```

gss pour l'utilisation de gssapi, include_realm pour conserver le realm dans le nom d'utilisateur

pour une connexion avec

```
psql -U admin -h file.domseth.ac-test.fr
```

```
host    all          all  0.0.0.0/0     gss include_realm=0 krb_realm=DOMSETH.AC-TEST.FR
```

L'utilisation de pg_ident reste un mystère pour l'instant

#2 - 03/08/2021 14:17 - Vincent Chavanon

- Statut changé de Nouveau à Fermé

- % réalisé changé de 0 à 100

- Temps estimé mis à 0.00 h

- Restant à faire (heures) mis à 0.0