

[Aide](#) / [WLangage](#) / [Gestion des bases de données](#) / [HFSQL](#) / [Gestion de HFSQL Client/Serveur](#)

Authentification par Active Directory

[Voir Aussi](#)

Disponible uniquement avec ce type de connexion

Présentation

Kerberos est un mode d'authentification basé sur l'utilisation de tickets et de clés secrètes. Ce mode est en particulier utilisé par Windows et l'Active Directory.

A partir de la version 23, il est possible de paramétrer le serveur HFSQL afin qu'il authentifie les utilisateurs selon la norme Kerberos. C'est le compte Kerberos (Active Directory, ...) qui est utilisé.

Prérequis

Avant de mettre en place une authentification par Active Directory, il est nécessaire de créer un compte utilisateur du domaine.

Ce compte doit avoir au minimum les droits suivants :

- droits d'accès (Lecture et Ecriture) au répertoire des bases de données et au fichier HFConf.INI.
- droits d'accès (au moins Lecture et Ecriture pour la mise à jour automatique des données) sur les binaires du serveur (manta64.exe, *.exe...)

Remarque : Pour faire des sauvegardes à chaud performantes, il faut avoir le droit local correspondant sur le volume ("Effectuer les tâches de maintenance de volume").

Mise en place pour un serveur HFSQL Windows

Installation automatique

Lors de l'installation ou de la mise à jour d'un serveur HFSQL en version 23 (et supérieures), l'assistant d'installation effectue automatiquement les différentes étapes nécessaires.

Après l'installation du serveur HFSQL, il est nécessaire de finaliser le paramétrage du serveur. Pour cela, il suffit de lancer la ligne de commande suivante en utilisant un compte ayant les droits sur le domaine :

```
setspn -U -S HFSQL/<srv1.mondomaine.com> <nom du compte>
```



où :

- <srv1.mondomaine.com> est le nom complet (FQDN) de la machine hébergeant le serveur HFSQL.
- <nom du compte> est le nom du compte utilisateur du domaine créé dans les prérequis.

Installation manuelle

Pour information, les différentes étapes nécessaires à la prise en compte de l'authentification par Active Directory pour un serveur HFSQL pour Windows (version 23 et supérieures) sont les suivantes :

1. Installer un serveur HFSQL (version 23 et supérieures) sur une machine.

2. Modifier le compte exécutant le service du serveur HFSQL pour utiliser le compte utilisateur du domaine créé dans les prérequis.

Attention : Ce compte doit avoir les droits d'accès au répertoire des bases de données et au fichier HFSQL.INI.

3. Créer le ServicePrincipalName en exécutant la ligne de commande suivante avec un compte ayant les droits sur le domaine :

```
setspn -U -S HFSQL/<srv1.mondomaine.com> <nom du compte>
```



où :

- <srv1.mondomaine.com> est le nom complet (FQDN) de la machine hébergeant le serveur HFSQL.
- <nom du compte> est le nom du compte utilisateur du domaine créé dans les prérequis.

4. Activer le support de Active Directory dans le serveur :

- soit via la fonction [HGèreServeur](#).
- soit via le Centre de Contrôle HFSQL.

Mise en place pour un serveur HFSQL Linux

Les différentes étapes nécessaires à la prise en compte de l'authentification par Active Directory pour un serveur HFSQL pour Linux (version 23 et supérieures) sont les suivantes :

1. Joindre le serveur au domaine si cela n'est pas déjà fait. Sur un Linux récent, la commande suivante peut être utilisée :

```
>sudo realm join mondomaine.com -U 'admin@MONDOMAIN.COM' -v
```



où :

- mondomaine.com est le nom du domaine.
- admin@MONDOMAIN.COM est un compte qui possède les droits nécessaires pour ajouter une machine dans le domaine.

2. Vérifier que le serveur récupère les informations du contrôleur d'Active Directory en saisissant la commande :

```
>id <nom du compte>@mondomain.com
```



où <nom du compte> est le nom du compte utilisateur du domaine créé dans les prérequis.

Les informations suivantes sont affichées :

```
uid= 10003(<nom du compte>@mondomain.com)
gid= 10000(utilisa.dudomaine@mondomain.com)
groups= 10000(utilisa.dudomaine@mondomain.com), 10000(compta@mondomain.com)
```



3. Créer le ServicePrincipalName en exécutant la ligne de commande suivante sur une machine Windows avec un compte ayant les droits sur le domaine :

```
setspn -U -S HFSQL/<srv1.mondomaine.com> <nom du compte>
```



où :

- <srv1.mondomaine.com> est le nom complet (FQDN) de la machine hébergeant le serveur HFSQL.
- <nom du compte> est le nom du compte de domaine créé dans les prérequis.

4. Configurer la "keytab" :

```
>kinit <nom du compte>@MONDOMAIN.COM
>kvno HFSQL/srv1.mondomain.com
HFSQL/srv1.mondomain.com@MONDOMAIN.COM:kvno = 2
>ktutil
ktutil: addent -password -p HFSQL/srv1.mondomain.com@MONDOMAIN.COM -k
<kvno> -e aes256-cts-hmac-sha1-96
ktutil: addent -password -p HFSQL/srv1.mondomain.com@MONDOMAIN.COM -k
<kvno> -e rc4-hmac
ktutil: wkt /opt/<nom du compte>/<nom du compte>.keytab
quit
```



où :

- <kvno> est le numéro retourné par la commande kvno,
- srv1.mondomain.com est le nom complet de la machine serveur,
- MONDOMAIN.COM est le nom de domaine (toujours en majuscules).
- <nom du compte> est le nom du compte de domaine créé dans les prérequis.

Dans ce code, adapter le chemin de la commande 'wkt' pour stocker la "keytab" à un endroit approprié. Vérifier que le serveur HFSQL possède les droits nécessaires pour accéder à ce fichier.

5. La librairie "libgssapi_krb5.so" est nécessaire. Selon la distribution, il peut être nécessaire de faire un lien symbolique depuis "libgssapi_krb5.so.x" vers "libgssapi_krb5.so".

6. Configurer le serveur HFSQL en ajoutant dans le fichier HFConf.ini du serveur les lignes suivantes :

```
[ActiveDirectory]
Enable=1
kerberosKeyFile=/opt/<nom du compte>/<nom du compte>.keytab
```



où <nom du compte> est le nom du compte de domaine créé dans les prérequis.

Utilisation

Connexion

La syntaxe pour utiliser une connexion avec une authentification par Active Directory est la suivante :

```
cnx_sso est une Connexion
cnx_sso.Provider = hAccèsHFClientServeur
cnx_sso.Serveur = "srv1.mondomaine.com"
cnx_sso.ActiveDirectory = Vrai
```



Cette connexion permet de se connecter au serveur en utilisant l'identité de l'utilisateur courant. Il n'est pas nécessaire pour l'utilisateur de re-saisir ses informations de login (Single Sign-On).

Note : Sous Windows et sous un Linux équipé d'une couche Kerberos compatible, il est possible de forcer l'utilisation d'un autre compte de domaine via la syntaxe suivante :

```
cnx est une Connexion
cnx.Provider = hAccèsHFClientServeur
cnx.Serveur = "srv1.mondomaine.com"
cnx.ActiveDirectory = Vrai
cnx.Utilisateur = "<Nom du compte>@mondomaine.com"
cnx.MotDePasse = "xxxxxx"
```



Gestion des droits sur le serveur

Sur le serveur HFSQL, il est possible de créer des utilisateurs et des groupes correspondant respectivement à des comptes du domaine et des groupes du domaine.

Lorsqu'un utilisateur se connecte avec un compte du domaine :

- La liste des groupes auxquels l'utilisateur appartient est automatiquement mise à jour à partir des informations sur les groupes du domaine.
- Si l'utilisateur n'existe pas mais appartient à un groupe de domaine ayant un groupe HFSQL correspondant, alors le compte utilisateur est automatiquement créé (sans aucun droit, il hérite des droits du groupe).

Voir Aussi

- [HGèreServeur \(Fonction\)](#)
- [Fichier HFConf.Ini](#)
- [Gestion des groupes et des utilisateurs \(HFSQL Client/Serveur\)](#)

Version minimum requise

- Version 23

Documentation également disponible pour...

- [WINDEV Mobile](#)
- [WINDEV](#)
- [WEBDEV](#)

Commentaires



Centre de contrôle

Fonctionne avec le centre de contrôle installé localement sur le serveur.

Avec le même compte utilisateur Active Directory depuis un centre de contrôle installé sur une autre machine du domaine, il est impossible de se connecter.



EMMANUEL MEDINA
23 août. 2023

