SQL Server et Active Directory

Comment requêter AD depuis SQL Server

Comment exécuter des requêtes de sélection sur un Active Directory depuis SQL Server ? L'utilisation du principe des serveurs liés adapté à cette question nous permet d'y répondre.

Introduction

Un grand classique lors de la mise en place d'un annuaire est la récupération des informations issues de l'Active Directory interne.

En effet, on y retrouve des informations de base comme le login ou l'adresse Mail (si on a aussi un Exchange), mais aussi des informations qui ont déjà été entrées telles que le Numéro de téléphone ou le Fax.

Bref, on voudrait donc bien mettre en place une solution de récupération de ces informations directement depuis le serveur SQL, ce qui permet de se faire des vues et des jointures utilisable facilement par la suite.

Présentation

Pour faire cela, il faut donc passer par la solution des Serveurs Liés. SQL Server permet en effet de lier un serveur SQL Server (2000 ou 2005) avec d'autres serveurs ou sources de données.

Dans notre cas, nous utiliserons le connecteur "Active Directory Services 2.5" sur un moteur SQL Server 2000. Nous verrons donc comment effectuer cette mise en place et créer une vue récupérant des informations sur les utilisateurs.

Attention, il est impossible de lier MSDE avec Active Directory, car cette version de SQL Server 2000 ne possède pas les pilotes de connexion ADSI.

Mise en place du serveur lié

La meilleure solution pour effectuer cette liaison est de coupler deux parties :

- Un script SQL de création
- La modification du paramètre de login

Il est aussi conseillé de mettre en place de serveur lié avec le compte de service qui sera utilisé pour SQL Server. En effet, afin de permettre à tous les utilisateurs SQL Server d'effectuer une requête sur ce serveur lié, il faut que le contexte de sécurité soit suffisant.

Nous prendrons donc un exemple avec le compte de service utilisé pour le moteur SQL Server et SQL Agent :

- ServiceSQLServerAccount

Script SQL

```
-- Ajoute AD dans les serveurs liés ---

EXEC sp_addlinkedserver 'MONSERVEURLIEAD', 'Active Directory Services 2.5',
'ADSDSOObject', 'adsdatasource'
GO

-- Ajoute le Login de connexion pour les requettes AD
EXEC sp_addlinkedsrvlogin 'MONSERVEURLIEAD', false, 'Domain\ServiceSQLServerAccount',
'CN=ServiceSQLServerAccount,DC=ServerControler,DC=Domain,DC=net', 'PasswordSQLServerAccount'
```

Ce script nous permet de dire que les requêtes exécutées par le compte "ServiceSQLSerAccount" vont renvoyer des résultats. En revanche, toutes les requêtes des autres comptes ne passeront pas et renverront le message :

```
Serveur : Msg 7399, Niveau 16, État 1, Ligne 1
OLE DB provider 'ADSDSOObject' reported an error.
The provider indicates that the user did not have the permission to perform the operation.
OLE DB error trace [OLE/DB Provider 'ADSDSOObject' ICommandPrepare::Prepare returned 0x80040e09:
The provider indicates that the user did not have the permission to perform the operation.].
```

Ce message indique donc que le login courant n'a pas le droit d'exécuter cette requête sur l'AD et que le moteur SQL ne peut donc pas retourner les résultats.

Dans le cas présent, une requête de sélection fonctionnera si vous êtes connecté sur SQL Server avec le login "ServiceSQLServerAccount". En revanche si vous êtes connecté avec un autre compte, cela provoquera la même erreur signalée juste au dessus.

Il faut donc pour corriger cela, modifier le paramètre d'authentification sur le serveur lié.

La modification du paramètre de login

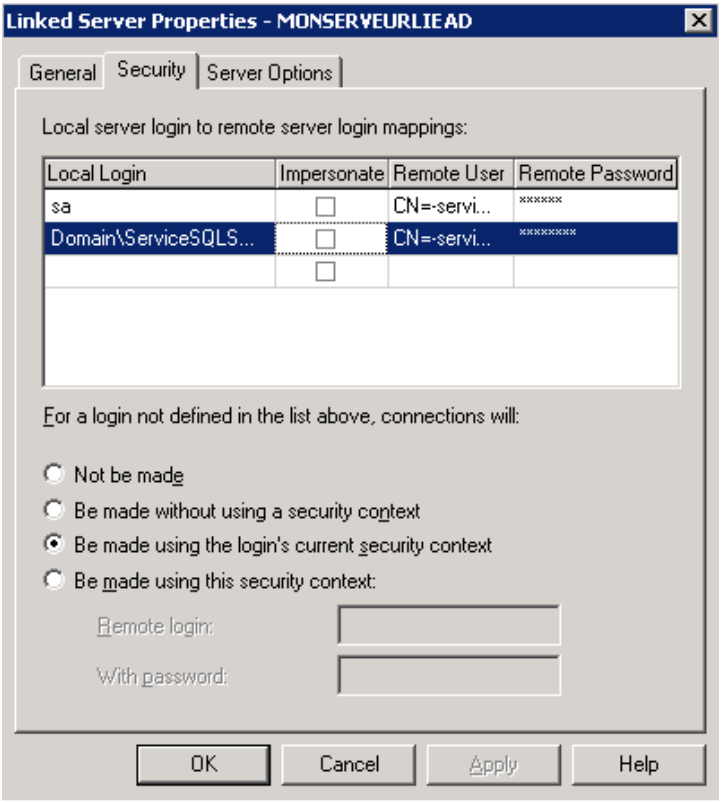
Nous devons maintenant utiliser SQL Server Enterprise Manager pour effectuer cette modification.

Une fois connecté sur le serveur SQL depuis Enterprise Manager, nous devons ouvrir :

- [Serveur] > Sécurité > Serveurs Liés

On trouvera alors le nom qui a été donné [MONSERVEURLIEAD]. On doit alors cliquer avec le bouton droit sur lui et choisir "Propriétés".

On ouvre alors les paramètres de connexion pour ce serveur lié. On doit prendre alors l'onglet "Sécurité".



Dans le cas ou des données sont renseignées dans la première ligne de mappage, il faut tout supprimer.
Cette ligne permet simplement de faire une liaison entre un compte local SQL Server et le compte adapté sur le serveur lié. La capture montre justement un exemple avec deux mappages différents pour cette connexion.

Cela fonctionne donc bien pour un compte donné mais si on souhaite permettre de faire une vue exécutable par tous les comptes, il est plus simple de forcer l'identification avec un compte donné.
Pour cela, il faut supprimer ces lignes de mappage et sélectionner la ligne :

- Etre effectué avec ce contexte de sécurité

Dans la case dessous, il faut donc ajouter les paramètres du compte :

- **Connexion distante :** Domain\ServiceSQLServerAccount
- **Avec mot de passe :** PasswordSQLServerAccount

On clique alors sur OK.

Dès ce moment, quelle que soit le compte connecté sur le serveur SQL, il pourra exécuter des requêtes sur le serveur Active Directory.

Utilisation du serveur lié

Nous pouvons dès lors exécuter des requêtes telles que :

Liste des groupes NT du domaine

```
SELECT
    *
FROM
 OPENQUERY(MONSERVEURLIEAD,
   'SELECT cn
    FROM ''LDAP://DC=ServerControler,DC=Domain,DC=net''
    WHERE objectCategory=''Group''')
```

Liste des utilisateurs du domaine

```
SELECT
    *
FROM
 OPENQUERY(MONSERVEURLIEAD,
  'SELECT title, displayName, sAMAccountName,
  givenName, telephoneNumber, facsimileTelephoneNumber, sn
  FROM ''LDAP://DC=ServerControler,DC=Domain,DC=net''
  where objectClass = ''User''')
```

Liste des compte commençant par R

```
SELECT
    *
FROMOPENQUERY(MONSERVEURLIEGEAD,
    'SELECT ADsPath, cn
FROM ''LDAP://OU=GE,DC=gmgead,DC=vdge,DC=net''
WHERE objectCategory=''person'' AND objectClass=''user''
AND sn = ''R*'' ORDER BY sn')
```

On peut donc imaginer de nombreuses solutions basées sur cette idée, en faisant des vues ou des procédures stockées basées ou inspirées de ces exemples.

Conclusion

Nous pouvons donc imaginer des solutions en corrélation avec l'Active Directory, cela permet de ne pas passer par un outil intermédiaire stockant les données de l'AD dans une base de données.

Il faut tout de même faire attention à la charge des contrôleurs de domaine. En effet, les performances de l'AD sont moins rapides que celles du moteur relationnel.

Voici quelques liens utiles si cet article vous a intéressé :

- **Create a SQL Server View of your AD Users (US)**
- **How to link different data sources together (US)**
- **Distributed Query (US)**
- **SQL Dialect (US)**
- **Search Filter Syntax (US)**

En vous souhaitant de bons projets de développement.

Romelard Fabrice (alias F___)
Consultant Technique **ilem SA**