Query Active Directory Data from SQL Server using T-SQL

December 2, 2009

www.databasejournal.com/features/mssql/article.php/3849891

Active Directory Service Interfaces, also known as
ADSI, is a set of COM interfaces used to access
the directory services to retrieve data. Though it
is predominantly used by network administrators
and system administrators, there are situations
where SQL Server Database administrators or the application that uses SQL Server as the backend
needs to get data from ADSI.

This article illustrates how to use SQL Server Transact SQL with OPENROWSET and OPENQUERY
commands to access and retrieve data from Active Directory.

In order to query data from Active Directory, you need to know the Organizational Units, containers
and domain controllers. All the three are not mandatory to retrieve information. You could query
ADSI just by using the domain name and domain container.

- **CN** is containers that are usually defined as users, contacts, groups
- **OU** is organizational units that usually contain objects such users, contacts, groups and other
  OUs
- **DC is** domain containers that are created by separating the full internal domain name

In this article, I am going to use the following OU and DC.

DomainName=Domainname.company.com

OU=northamerica

DC=domainname,dc=company,dc=com

CN=

Note: Please replace the OU, DC and CN information mentioned here with your company's OU, CN
and DC.

The first method to query Active Directory from SQL Server is by using OpenRowSet. If you want to
know more about openrowset please read this article.

You can access information from Active directory by executing the following query.

```
USE [master]
GO
sp_configure 'show advanced options',1
GO
reconfigure with override
GO
sp_configure 'Ad Hoc Distributed Queries',1
GO
reconfigure with override
GO

SELECT Name, displayName,givenname,distinguishedName,
```

```
        SAMAccountName
FROM
OPENROWSET('ADSDSOObject','adsdatasource' ,
'SELECT  Name, displayName,givenname,distinguishedName,
        SAMAccountName
    FROM ''LDAP://Domainname.company.com/ou=northamerica,
         dc=domainname,dc=company,dc=com''
    WHERE Name = ''BlackieHong''')
GO
```

You may see an error message, similar to the message shown below, if you do not have access to Active Directory.

```
Msg 7321, Level 16, State 2, Line 1
An error occurred while preparing the query "SELECT  Name,
    displayName,givenname,distinguishedName, SAMAccountName
    FROM 'LDAP://Domainname.company.com/ou=northamerica,
        dc=domainname,dc=company,dc=com'
    WHERE Name = 'BlackieHong'" for execution against OLE DB provider
        "ADSDSOObject" for linked server "(null)".
```

In such cases, you can pass the login and password as part of your openrowset command as shown below.

```
SELECT Name, displayName,givenname,distinguishedName, SAMAccountName
FROM
OPENROWSET('ADSDSOObject','adsdatasource'; 'Domainname\MAK';'*******',
'SELECT  Name, displayName,givenname,distinguishedName, SAMAccountName
    FROM
''LDAP://Domainname.company.com/ou=northamerica,dc=domainname,dc=company,dc=com''
WHERE Name = ''BlackieHong''')
```

Note: Please replace Domainname\MAK with your domain and login name and ******* with your password or replace it with the login and password that have access to Active Directory.

In the above query we are getting information about a particular user, "BlackieHong," from Active Directory. The first method can be used when you don't need to query Active Directory that often.

The second method of getting data from Active Directory is by using Linked Server. This method can be used when you query Active Directory many times.

Let us create a linked server as shown below.

```
USE [master]
GO
sp_configure 'show advanced options',1
GO
reconfigure with override
GO
sp_configure 'Ad Hoc Distributed Queries',1
GO
reconfigure with override

GO
USE [master]
GO
/****** Object:  LinkedServer [ADSI]    Script Date: 10/23/2009 05:41:54 ******/
IF  EXISTS (SELECT srv.name FROM sys.servers srv WHERE srv.server_id != 0
```

```
        AND srv.name = N'ADSI')EXEC master.dbo.sp_dropserver @server=N'ADSI',
@droplogins='droplogins'
GO
/****** Object:  LinkedServer [ADSI]    Script Date: 10/23/2009 05:42:16 ******/
EXEC master.dbo.sp_addlinkedserver @server = N'ADSI', @srvproduct=N'Active Directory
Service Interfaces',
        @provider=N'ADSDSOObject', @datasrc=N'adsdatasource'
 /* For security reasons the linked server remote logins password is changed with
######## */
EXEC master.dbo.sp_addlinkedsrvlogin
@rmtsrvname=N'ADSI',@useself=N'True',@locallogin=NULL,@rmtuser=NULL,@rmtpassword=NULL

GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'collation compatible',
@optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'data access',
@optvalue=N'true'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'dist', @optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'pub', @optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'rpc', @optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'rpc out',
@optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'sub', @optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'connect timeout',
@optvalue=N'0'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'collation name',
@optvalue=null
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'lazy schema validation',
@optvalue=N'false'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'query timeout',
@optvalue=N'0'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'use remote collation',
@optvalue=N'true'
GO

EXEC master.dbo.sp_serveroption @server=N'ADSI', @optname=N'remote proc transaction
promotion', @optvalue=N'true'
GO
```

Now let's query the Active Directory using OPENQUERY, as shown below.

```
SELECT * FROM OPENQUERY( ADSI, 'SELECT Name, displayName,givenname,distinguishedName,
SAMAccountName
        FROM
''LDAP://Domainname.company.com/ou=northamerica,dc=domainname,dc=company,dc=com''
WHERE Name = ''BlackieHong''')
GO
```

You may see an error message, similar to the message shown below, if you do not have access to Active Directory.

```
Msg 7321, Level 16, State 2, Line 2
An error occurred while preparing the query "SELECT Name,
displayName,givenname,distinguishedName, SAMAccountName
        FROM
'LDAP://Domainname.company.com/ou=northamerica,dc=domainname,dc=company,dc=com'
        WHERE Name = 'BlackieHong'" for execution against OLE DB provider
"ADSDSOObject" for linked server "ADSI".
```

In such cases, you should set up the remote login for the linked server that you have created. Execute the TSQL command as shown below.

```
EXEC sp_addlinkedsrvlogin @rmtsrvname = N'ADSI', @locallogin = NULL , @useself =
N'False',
        @rmtuser = N'Domainname\MAK', @rmtpassword = N'**********'
GO

SELECT * FROM OPENQUERY( ADSI, 'SELECT Name, displayName,givenname,distinguishedName,
SAMAccountName
        FROM
''LDAP://Domainname.company.com/ou=northamerica,dc=domainname,dc=company,dc=com''
            WHERE Name = ''BlackieHong''')
GO
```

Note: Please replace Domainname\MAK with your domain and login name and ******* with your password or replace it with the login and password that have access to Active Directory.

Conclusion

This article illustrated how to use SQL Server Transact SQL with OPENROWSET and OPENQUERY commands to access and retrieve data from Active Directory.