# Active Directory Group Management – Chapter 28 (Chris Bellee)

## Steps for configuring example application

1. Modify Create\_SQL\_DB.sql
2. Modify Create\_SQL\_Job.sql
3. Modify Main.ps1
4. Modify SQLJob.ps1
5. Execute Create\_SQL\_DB.sql in SQL Server Management Studio Query Pane (Creates Database)
6. Execute Create\_SQL\_Job.sql in SQL Server Management Studio Query Pane (Creates SQL Job)
7. Modify the following lines in Create\_SQL\_DB.sql

* Replace with your SQL installation DATA directory path
* N.B. Installed SQL version must minimum of SQL 2012 WEB edition (SQL 2012 Express does not include SQLAgent Service)

Line 7

( NAME = N'ADGroupManagementDB', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\ADGroupManagementDB.mdf' , SIZE = 4672KB , MAXSIZE = UNLIMITED, FILEGROWTH = 1024KB )

Line 9

( NAME = N'ADGroupManagementDB\_log', FILENAME = N'C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA\ADGroupManagementDB\_Log.ldf' , SIZE = 4672KB , MAXSIZE = 2048GB , FILEGROWTH = 10%)

## Modify the following lines in Create\_SQL\_Job.sql

* Create a domain user account in Active Directory Users and Computers (ADUC) to perform the group additions/removals for the SQL Job running the PowerShell ‘SQL\_Job.ps1’ script.
  + Right-Click domain ‘head’ in ADUC, select ‘Delegate Control’
  + Assign the user account the following rights
    - Create, delete, and manage user accounts
    - Modify the membership of a group

Line 1 – Change to AD Service Account Name

CREATE CREDENTIAL [ADGroupManagementCred] WITH IDENTITY = N'CORP\SVC-ADGroupManage',

Line 2 – Change to AD Service Account Password

SECRET = N'P@ssword'

Line 6 – Change to AD Service Account Name

CREATE LOGIN [CORP\SVC-ADGroupManage] FROM WINDOWS WITH DEFAULT\_DATABASE=[ADGroupManagementDB]

Line 8 – Change to AD Service Account Name

ALTER LOGIN [CORP\SVC-ADGroupManage] ADD CREDENTIAL [ADGroupManagementCred]

Line 25 – Change to AD Service Account Name

@login\_name=N'CORP\SVC-ADGroupManage'

Line 30 – Change to AD Service Account Name

CREATE USER [CORP\SVC-ADGroupManage] FOR LOGIN [CORP\SVC-ADGroupManage

Line 31 – Change to AD Service Account Name

ALTER ROLE [db\_datareader] ADD MEMBER [CORP\SVC-ADGroupManage]

Line 61 – Change to Database owner Owner Login Name

@owner\_login\_name=N'CORP\Administrator', @job\_id = @jobId OUTPUT

Line 75 – Change to SQLJob.ps1 path

@command=N'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -file "C:\ADGroupManagement\SQLJob.ps1"',

## Modify Main.ps1

* Change the SQL Server FQDN to your Server Name

Line 307 – Change to your SQL Server Fully-Qualified Domain Name (or ‘localhost’ if running on same machine)

$script:SQLServer = "WIN8-01.corp.fabrikam.com"

## Modify SQLJob.ps1

* Change the SQL Server FQDN to your Server Name
* Change log file path to local path on SQL server

Line 40

$script:SQLServer = "WIN8-01.corp.fabrikam.com"

Line 42

$logfilepath = "C:\ADGroupManagement\logfile.txt"