Numeric Permission Monitor

Are you on top of security on your SQL server?

Legal requirements for documentation of access rights on sensitive personal data is not a new thing. However, the requirements have grown significantly with the EU's new General Data Protection Regulation (GDPR).

Allocation of access rights on an SQL server from Microsoft can occur in numerous ways and in various systems and levels, and the server software does not provide a sufficient overview about who can do what with data.

This issue is solved by Numeric Permission Monitor (NPM). NPM easily creates a detailed overview of users and rights on an SQL server. NPM is the cheap and ideal tool for the IT Department, who needs to be in control of who can view, share and handle sensitive data in the organisation.

What does NPM include

The tool consists of an Excel rapport with a collection of Pivot charts, which collect data from a database, which is installed on the relevant SQL server. The database collects information from the server concerning:

- Which logins are set up on the server, including which type of login
- Which users are set up on the individual databases
- Which rights the users possess in database roles, and which database objects the roles in question grant access to – including which permission type applies (select, write, execute etc. on grant or deny level, respectively)
- Which rights the users possess directly in regard to database objects (not role based)
- Which Server roles the various logins possess access to
- Which Windows users should have access to what through AD groups

As a standard, information is collected every 30 minutes and saved in the system for a duration of 10 days with this rate. Longer back in time the information is saved once per 24 hours. The rate for collection as well as the duration of saving is configured for the individual client at the installation stage and can be changed subsequently. Therefore, it is also possible to change that data longer back in time is saved more than once per 24 hours, if so desired.

Apart from providing an immediate overview, the information can be applied for historical analysis of access rights.

In the installation of NPM it can be configured so that the information of users pertaining to selected AD groups is not collected. Thus it is, as an example, possible to include large AD groups in the monitoring, without the users of the group displaying.

Application of NPM

NPM supports a wide analysis and reporting on access rights. As examples:

Overview

- Obtain a general overview over all databases, users and logins on the server
- On the basis of the overview it is possible to further examine the security structure and display which users have access to which databases and subjacent objects
- In one of the displays you can obtain a quick overview of all Windows groups, which are set up as login, and which users are a part of the group.

Analysis of a specific user
- Select a specific AD user, as an example "numeric\dpo". In the rows of the display you can view which databases the user has access to, and further examine on role and database object level.
- In the columns of the display you can view which login(s) carry these access rights. As an example, it could be the user "numeric\dpo" that is set up as login, and through this has access to two specific databases, but that the user's membership of "numeric\consultants" grants further access to other databases (and subjacent objects).
- If you are interested in focusing on a particular database, the display can be filtered with a slicer.

Analysis of a specific database
- Select a specific database to receive an overview of which users hold access to which objects, independently of which type of access they possess on the server.

Historical overview
- As a default, the various overviews and analyses display how rights in the server are allocated this very moment. However, the timeframe of the rapport can easily be changed to an alternative historical time, where NPM has been installed.

Technology

NPM includes the following components:

- Excel report
- SQL Server Permission Monitor-database
- SQL Server Agent Job for collection of data
- Linked Server for Active Directory (AD)

The installation requires the following components on the client's platform:

- SQL Server 2008R2 or more recent version
- Excel 2010 or more recent version
- Active Directory

The installation requires sysadmin access to the database.

The installation includes:

- Installing the audit database
- Configuration of settings for local environment
- Configuration of SQL Server Agent Job
- Copying of Excel rapport for relevant destination and adjustment of data connections

Limitations

- The tool does not display access on other SQL servers, than the one installed upon.
- The tool does not account for applications who, by means of a service user, provides unknown users (for the server) access to the databases of the server, as examples, SRSS, SSAS, CRM, Navision etc.

- To utilize the Excel rapport, reading access on the audit database of the SQL server is required.
- Certain system relating Windows groups (Default Security Groups) are not supported.

Prices and information

NPM costs 15,000 DKK for the first SQL server server, and 5000 DKK per subsequent server. Yearly remuneration constitutes 25 % of the purchase price. For clients with many SQL servers we offer an individual site licence.

Send an e-mail to info@numeric.dk or call Kaare Thyregod at +45 4142 1568 for ordering or further information.

