

Numeric Permission Monitor

Har du styr på, hvem der har adgang og rettigheder på dine SQL-servere?

Dansk lovgivning har længe stillet krav til dokumentation af adgange og rettigheder i forhold til bl.a. personfølsomme data. Med EU's nye persondataforordning (GDPR) øges og specificeres kravene.

Tildelingen af adgange og rettigheder på en SQL-server fra Microsoft kan finde sted på mange niveauer og i flere systemer, og serversoftwarens giver ikke et godt overblik over, hvem der må og kan hvad med data.

Det problem løser Numeric Permission Monitor (NPM). NPM skaber let og detaljeret overblik over brugere og brugerrettigheder på en SQL Server. NPM er det billige og ideelle værktøj for den nye Data Protection Officer, der som en af sine første handlinger vil have styr på, hvem der allerede kan se, dele og behandle følsomme data i organisationen.

Hvad indeholder NPM

Værktøjet består af en Excel-rapport med en samling Pivot-visninger, der trækker data fra en database, som installeres på den relevante SQL Server instans. Databasen samler oplysninger fra instansen omkring:

- Hvilke logins der er oprettet på instansen, herunder hvilken logintype
- Hvilke brugere der er oprettet på de enkelte databaser
- Hvilke rettigheder brugerne har på databaseroller, og hvilke databaseobjekter disse roller giver adgang til – herunder hvilken permission type der gælder (select, write, execute mv. på hhv. grant- eller deny-niveau)
- Hvilke rettigheder brugerne har direkte på databaseobjekter uden om roller
- Hvilke Server-roller de forskellige logins har adgang til
- Hvilke Windows-brugere der måtte have adgang til hvad gennem AD-grupper

Oplysninger indsamles som standard hver 30. minut og lagres i systemet i en periode på 10 dage med denne frekvens. Længere tilbage i tid er oplysningerne gemt én gang i døgnet. Frekvensen for indsamling og lagring af oplysninger og periodelængden opsættes specifikt for den enkelte kunde ved installation og kan også ændres efterfølgende. Det er også muligt at ændre således, at data længere tilbage i tid gemmes mere end en gang pr. døgn, hvis dette ønskes.

Oplysningerne kan, ud over at give et overblik her og nu, anvendes til historiske analyser af adgange og rettigheder.

I opsætningen af NPM kan det sættes op, at der for valgte AD-grupper ikke hentes oplysninger om underliggende brugere. Dermed er det muligt lade eksempelvis meget store AD-grupper indgå i overvågningen uden at gruppens brugere vises.

Anvendelse af NPM

NPM understøtter en bred analyse og rapportering på adgange og rettigheder. For eksempel:

Overblik

- Få et overordnet overblik over samtlige databaser, brugere og logins på instansen
- Med udgangspunkt i overblikket kan man drille ned i sikkerhedsstrukturen og se hvilke brugere, der har adgang til hvilke databaser og underliggende objekter.
- I en af visningerne kan man få et hurtigt overblik over alle windows-grupper, der er oprettet som login, og se hvilke brugere, der tilhører.

- # Analyse på en konkret bruger
 - Vælg en specifik AD-bruger, f.eks. "numeric\dpo". På visningens rækker kan man se hvilke databaser brugeren har adgang til, og drille ned på rolle og databaseobjekt niveau.
 - På visningens kolonner kan man se, hvilke login(s) der medfører disse rettigheder. Det kunne eks. være, at brugeren "numeric\dpo" er oprettet som login og gennem dette har adgang til 2 specifikke databaser, men at brugerens medlemskab af "numeric\konsulenter" giver adgang til andre databaser (og underliggende objekter).
 - Hvis man er interesseret i at fokusere på en enkelt database kan visningen filtreres med en slicer.
- # Analyse på en specifik database
 - Vælg en specifik database for at få et overblik over hvilke brugere, der har adgang til hvilke objekter, uafhængigt af hvilken type adgang, de har på instansen.
- # Historisk overblik
 - De forskellige oversigter og analyser viser som udgangspunkt, hvordan rettighedsbilledet ser ud netop nu. Tidsperspektivet i rapporten kan dog nemt skiftes til et alternativt historisk tidspunkt, hvor NPM har været installeret.

Teknologi

NPM indeholder følgende komponenter:

- Excel-rapport
- SQL Server Permission Monitor-database
- SQL Server Agent Job til indsamling af data
- Linked Server til Active Directory (AD)

Installation forudsætter følgende komponenter på kundens platform:

- SQL Server 2008R2 eller nyere
- Excel 2010 eller nyere
- Active Directory

Installation kræver sysadmin-adgang til databasen.

Installationen omfatter:

- Idriftsættelse af audit-database
- Konfigurering af indstillinger til lokalt miljø
- Opsætning af SQL Server Agent Job
- Kopiering af Excel-rapport til relevant destination og tilpasning af dataforbindelser

Afgrænsninger

- Værktøjet viser ikke adgange på andre instanser af SQL Server, end hvor det er installeret.
- Værktøjet tager ikke højde for, at mange typer af applikationer, gennem en servicebruger, giver ukendte brugere (for instansen) adgang til instansens databaser, eks. SRSS, SSAS, CRM, Navision etc.
- For at benytte Excel-rapporten kræver det læseadgang på SQL serverens audit-database
- Visse systemmæssige Windows-grupper (Default Security Group's) understøttes ikke.

Priser og information

NPM koster kr. 15.000 for den første SQL server instans og kr. 5.000 pr. instans derefter. Årsvederlag udgør 25 % af købsprisen. For kunder med mange SQL-servere tilbyder vi en individuel sitelicens uden begrænsning på antal instanser.

Send en e-mail til info@numeric.dk eller ring til Kaare Thyregod på 4142 1568 for bestilling eller yderligere information.