# Problem MS SQL Server og Kerberos authentificering

Det er vedtaget i SDS at Sikkerheden skal højnes.

Al adgang til personhenførbare data skal logges.

For at sikre at det kun er godkendte konti/brugere, og ikke konti med hengemte passwords fra NTLM, skal forbindelserne til serverne Kerberous authentificeres.

Al data / serveradgang tildeles via AD grupper.

Brugeres almindelige, udviklende og administrative brugere skal adskilles.

Alle brugere skal være defineret i AD, og styres af Servicedesk brugeradministration.

Passwords skal sikres i Thycotic Secret Server, de skal være lange og komplekse.

Men vi skal stadig kunne arbejde og få adgang til data på database servere.

For mange MS SQL servere er ikke sat korrekt op.

### Løsninger

Microsoft har lanceret gMSA (group Managed Service Accounts) en udvidelse af MSA, hvor man kan definere en konto (bruger), der er beregnet til kun at bruges af tjenester forbundet til AD.

AD styrer password & passwordskift, man skal blot definere hvilke servere/hosts der skal have adgang til at forespørge / hente dette password.

Der kan tilknyttes Kerberos authentificering via SPN (serviceProviderName).

MS SQL Server kan startes via gMSA, og på Enterprise versionen, kan der sættes Auditering , så man kan få vist hvad der er sket. Denne audit logning fylder dog så store mængder, at vi har valgt at udlicitere, så audit log data leveres til Logpoint som opbevarer dem for os i 5 år.

Hos Logpoint kan man søge og finde dokumentation for hvad der er foregået.

### Forudsætninger

For at oprette en gMSA i ad, skal man have de korrekte privilegier.

Man skal have adgang til serveren, og de rigtige AD-PowerShell moduler.

Man skal undersøge de nuværende opsætninger og SPN, og planlægge de nye.

Man skal kende servicevindue, så man ved hvornår man kan genstarte SQL services.

Der er lavet et par PowerShell scripts, til at støtte processen

# Oversigt

## Forberedelse:

1. Find egnet server med fungerende PowerShell
2. Find-SpnHost.ps1 <FQSnavn>
3. Kør SetSPN –l <servicekonto> (for alias)
4. Check SQL instanser i SQL Server 20xx Configuration Manager
5. Vælg en max 7 char. forkortelse for server & instans <servershort>
6. Planlæg via chk-gMSA.ps1 <FQSnavn> <servershort> <instansnavn>
7. Gem gamle og nye servicekonti i regneark, p:\AnjeT2\ps1\spn\servere.xlms
8. Check AD-rettigheder: Gem ADComputer info i $comAD variabel, og opret gMSA: svd-sqla.....
9. Check og ret Audit log placeringerne

## Udførsel:

1. Drop gamle SPN
2. opret gMSA, enkeltvis.
3. Skift Service Konti via SQL Server 20xx Configuration Manager
4. Start alle SQL Services, også SQL Browser.
5. Genstart server, vent 5 min til AD-logon servere er syynkroniserede.

## Kontroller:

1. Connect fra anden server sql & ssas til alle instanser.
2. Check: SELECT auth\_scheme FROM sys.dm\_exec\_connections WHERE session\_id = @@
3. giver resuktat: KERBEROS
4. Opret svd-sqla.... som syslog & giv gpedit.msc: log on as a batch job
5. Opret Konverteringsjob fra audit format til csv format.
6. Tilret Logpoint opsætningen og genstart.

## Oprydning:

1. Vent 10 dage, fjern gl serviceaccount & SecretServer password

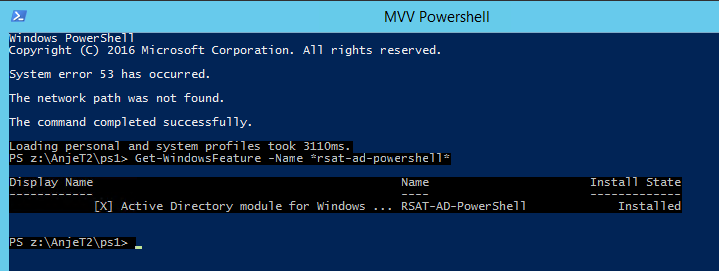
# Detailleret procedure.

## Forberedelse: Analyser server og evt. nuværende SPN.

1. Find en server i destinations domænet hvor PowerShell AD modulerne er installeret. Brug:

Get-WindowsFeature -Name \*rsat-ad-powershell\*

For at kontrollere om de er loaded. (kan ikke loades på windows ws.)



1. Check nuværende SPN via PowerShell: Fra p:\AnjeT2\ps1\spn: Find-SpnHost.ps1 <FQSnavn>

Her listes hvilke SPN der er tilknyttet serveren og hvilke der er tilknyttet evt. eksisterende servicekonti

Noter i regneark, p:\AnjeT2\ps1\spn\servere.xlms (Gl SQL Servicekonto = Kolonne G) hvilke servicekonti, der er tilknyttet hvilke instanser, samt de nye i kolonne c,d,e.

1. Kør SetSPN –l <servicekonto> på de i 3) fundne servicekonti, for at finde evt. andre Alias, der skal med på gMSA oprettelses kommandoerne, eller tilføjes efter denne via setSPN –S kommandoen
2. På serveren; check hvilke SQL instanser der er installeret, via Services & SQL Server 20xx Configuration Manager.

Al ændring SKAL foretages fra Config-Manageren! Hvis der er flere versioner af SQL på samme server, kan det være nødvendigt at checke flere versioner af Config-Managere. Her kan man også se hvilke instanser der har SSIS, SSAS eller SSRS, default og named instanser.

1. Find / vælg en max 7 char. forkortelse for server & instans <servershort>, da gMSA max må være 15 char., og de

første 8 bruges af navnestandarden.

### Forbered SPN til Server

Planlæg gMSA & SPN via PowerShell:

Fra p:\AnjeT2\ps1\spn: chk-gMSA.ps1 <FQSnavn> <servershort> <instansnavn>

Her skal angives:

<FQSnavn> : servernavn inkl. .domain

<servershort> : server & instans forkortelsen max 7 char

<instansnavn> : instansnavn (eller ingen hvis default instans)

Hvis der er angivet instansnavn bliver man promptet for et portnummer (50000-65000) som man skal finde i sql server Config-Manageren. Se bilag

Resultat bliver vist i et planlægningsark, der skal bruges i udførslen. Husk Gem som hvis der skal samles i fælles dok.

Hvis der er alias til server / instans, køres flere gennemløb, et for hver alias, med samme shortname & instansnavn, som den oprindelige. Her skal SPN MANUELT samles på den oprindelige new-ADServiceAccount, med komma (,) mellem hver SPN

Hvis der er flere instanser på serveren, køres flere gennemløb, et for hver instans- shortname & instansnavn hvor slutresultatet MANUELT skal samles i et samlet planlægningsark, hvor der er new-ADServiceAccount og Service konti klargjort for hver instans.

Check AD-rettigheder: Gem ADComputer info i $comAD variabel, og opret gMSA: svd-sqla.....

Hvis dette går som forventet, kan agenten klargøres med rettigheder

### Check Audit log placeringerne.

På MSSQL serverens logdisk (T:/S:) skal der være en Auditlog folder under Instansnavn, hvor auditlogs fra MSSQL lægges.

Hvis der ikke er det, så 1) Opret folder med de gældende rettigheder, 2) Disable Audit, 3) flyt data fra forkert placering til ny folder, 4) i SQL\<instans>\Security\Audits\ dobbeltklik på auditlog og tilret File Path 5) Enable audit igen

På MSSQL serverens Backupdisk (U:) skal der være en Audit folder under Instansnavn, her skal PowerShell konverterings scriptet være.

På MSSQL serverens Backupdisk (U:) skal der være en Logpoint folder under Instansnavn\Audit, hvor de til csv konverterede auditlogs placeres, og hentes af Logpoint programmet: nxlog (se senere)

# Udførsel

Når der er servicevindue for serveren, stop services (engine, agent & SSAS for hver instans) på MS SQL Server fra SQL Server Configuration manager.

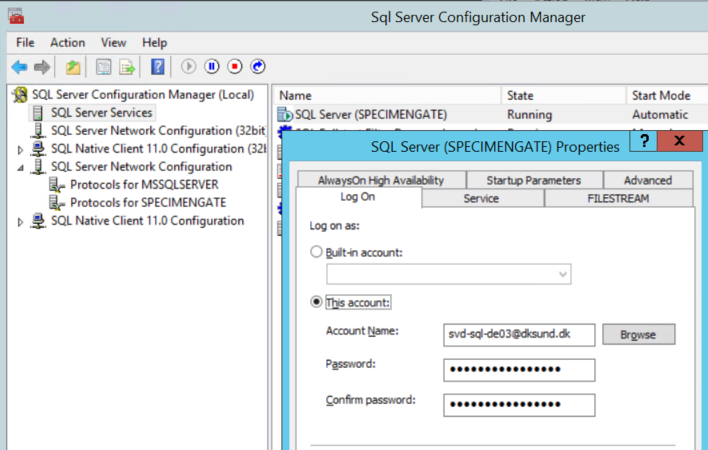
Fra planlægningsarket, kopieres kommandoer til PowerShell på server, og køres således:

Kør sektion 1: drop gamle spn: enkeltvis

Kør sektion 2: Gem ADComputer info i $comAD variabel, og opret gMSA: enkeltvis.

På serveren i SQL Server Configuration manager\SQL Server Services\

Vælges fra sektion 3 for hver instans & service type, indsæt gMSA som SQL <type>(instans) Properties: log on.

Vælg This account

Tryk Browse

Vælg Locations

Vælg Entire Directory (ok)

Vælg Object Types

Enable (hak) Groups & Service Accounts (ok)

Angiv gMSA-navn

(Check Names)

Når godkendt (ok)

Tryk Apply og password bliver fundet og tildelt.

Tryk Start, for at starte service med ny gMSA service account

Tryk Ok

Gentag med de andre konti

Efter sidste gMSA er sat ind, og alle services er oppe, genstart server for at checke at alt er ok efter genstart.

## Kontroller

Efter genstart vent 5 min for at sikre AD replikering er ok.

Fra p:\AnjeT2\ps1\spn: Find-SpnHost.ps1 <FQSnavn> for at kontrollere at resultat er som forventet.

Kør Kerberos Configuration Manager mod server, for at kontrollere at alle SPN er sat. (KCM kan fejle)

Log på anden MSSQL server i samme domæne, start SQL Management services, og connect til den tilrettede server

Prøv at connect forskellige formater: <FQSnavn>, <Servernavn> :Navn (hvis named instans)

Efter connect fra anden server i samme domain, start ny Query

SELECT auth\_scheme FROM sys.dm\_exec\_connections WHERE session\_id = @@spid

Dette checker forbindelsestypen for den aktuelle session. Skal returnere: KERBEROS

# Klargør til Audit lognings:

1. Opret svd-sqla<servershort> (gMSA til at starte SQL agent) som sysadmin login på SQL Server instans
2. gpedit.msc Computer\windows\security\local Policies\user rights\log on as a batch job. Tilføj svd-sqla<servershort>

På MSSQL serverens logdisk (T:/S:) oprettes under Instansnavn en Auditlog folder:

På MSSQL serverens Backupdisk (U:) oprettes under Instansnavn en Audit folder:

På MSSQL serverens Backupdisk (U:) oprettes under Instansnavn\Audit en Logpoint folder:

Alle 3 må kun have følgende Security Permissions:

System: Full Control

Domæne\MSSQLServerAdms: Full Control (på dksund\ L-ORG-MSSQL-Sysadmin)

Domæne\ svd-sqla<servershort> : Full Control (SQL agenten starter)

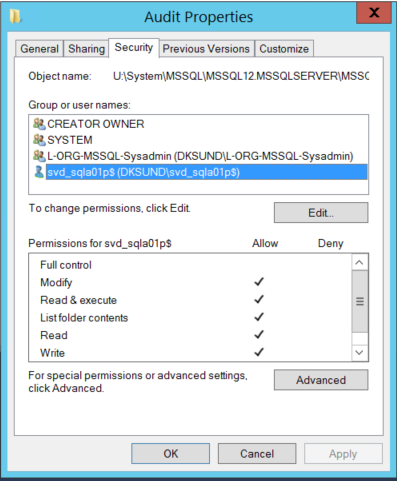
(Domæne\ svd-sqle<servershort> : Full Control) (SQL engine starter: nb. kun under auditlog)

Alle andre brugere skal fjernes via:

Properties\Security\Advanced

Replace all child object….. Disable inheritance Convert inherited….

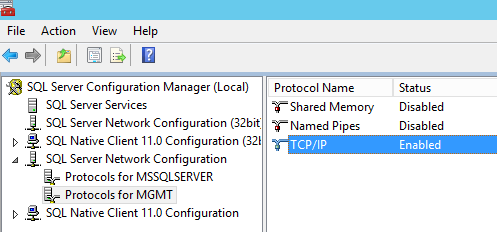
* Vælg og remove andre brugere.
* Add \ Select a principal \object types (tilføj service account)
* \ svd-sqla<servershort>; svd-sqle<servershort> svd-sqle… skal ikke tilføjes på u:
* Check Names
* Basic Permissions Full Control
* Ok



**Vent 10 dage, fjern gl serviceaccount & SecretServer password.**

# Bilag

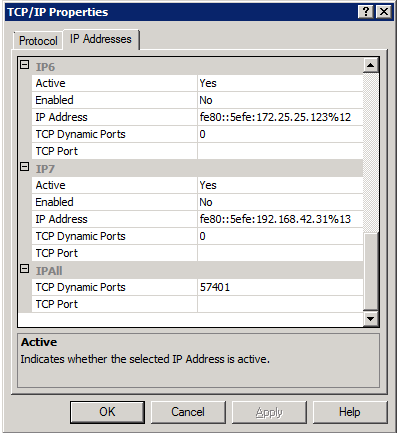
## Bilag 1:



Vælg SQL Server Network Configuration \ TCP/IP \ Properties

Vælg IP Addresses

Gå til bunden



Noter den dynamiske port som systemet har tildelt til den pågældende Named Instance for ALLip (her 57401)

Slet denne og tildel den faste port den samme nu frie port, og brug denne port ved prompten fra chk-gMSA.

Når man apply / ok for ændring fra dynamisk port til fast port får man at vide at det først virker når man har genstartet den navngivne service.

## Bilag 2: Audit opsætning

Opret Auditlog og parameter til samme, Maxsize X Max Rollover angiver max størrelse på disk, Filepath tilrettes efter auditlog folder.:

USE [master]

GO

CREATE SERVER AUDIT [AuditLog]

TO FILE

( FILEPATH = N'S:\System\MSSQL12.MSSQLSERVER\Auditlog'

,MAXSIZE = 50 MB

,MAX\_ROLLOVER\_FILES = 400

,RESERVE\_DISK\_SPACE = OFF

)

WITH

( QUEUE\_DELAY = 1000

,ON\_FAILURE = CONTINUE

)

ALTER SERVER AUDIT [AuditLog] WITH (STATE = ON)

GO

Angiv Parametre til logning:

NB. Hvis der ændres på hvad der logges, SKAL Logpoint have besked, da de skal normaliseres (opsamlings checkes)

CREATE SERVER AUDIT SPECIFICATION [AuditLogSpec]

FOR SERVER AUDIT [AuditLog]

ADD (SCHEMA\_OBJECT\_ACCESS\_GROUP),

ADD (DATABASE\_ROLE\_MEMBER\_CHANGE\_GROUP),

ADD (SERVER\_ROLE\_MEMBER\_CHANGE\_GROUP),

ADD (BACKUP\_RESTORE\_GROUP),

ADD (AUDIT\_CHANGE\_GROUP),

ADD (DATABASE\_PERMISSION\_CHANGE\_GROUP),

ADD (DATABASE\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SERVER\_OBJECT\_PERMISSION\_CHANGE\_GROUP),

ADD (SERVER\_PERMISSION\_CHANGE\_GROUP),

ADD (FAILED\_LOGIN\_GROUP),

ADD (SUCCESSFUL\_LOGIN\_GROUP),

ADD (DATABASE\_PRINCIPAL\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_CHANGE\_GROUP),

ADD (SERVER\_PRINCIPAL\_CHANGE\_GROUP),

ADD (DATABASE\_OWNERSHIP\_CHANGE\_GROUP),

ADD (DATABASE\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP),

ADD (SCHEMA\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP),

ADD (SERVER\_OBJECT\_OWNERSHIP\_CHANGE\_GROUP)

WITH (STATE = ON)

GO

(Højreklik Security\Audits\Auditlog og Enable Auditlog.) hvis det ikke kører

Herefter checkes om der kommer audit logs i auditlog folder:

## Konverteringsjob fra audit format til csv format.

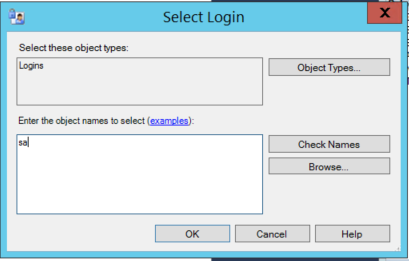
Kopier p:\anjet2\logpoint\auditexport.ps1 til Backupdisk (U:) Instansnavn\Audit folder: og ret til:

# ret AuditSourcedir & AuditExportdir til lokale disk navne.

# ret maxfilePerRun efter performance test.

Forbered Automatisk kørsel.

I SQL Server: \SQL Server Agent\Jobs Start New Job:



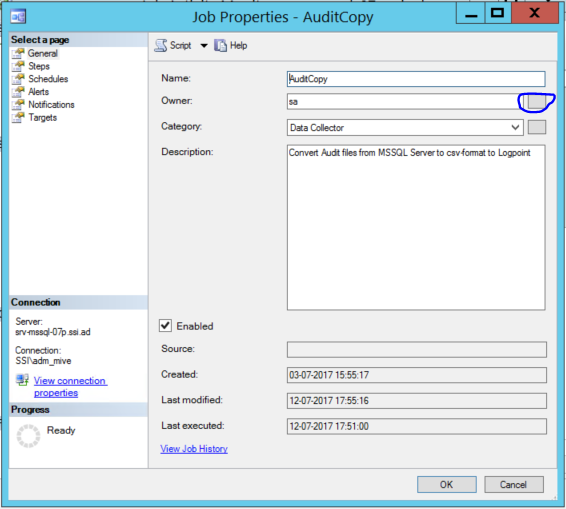
Owner:

(klik for select login,

skriv sa,

Check Names,

OK)

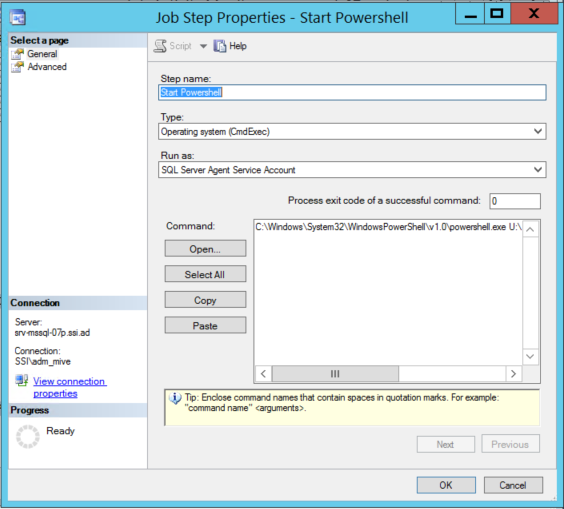


Name: AuditCopy

Category:

Data Collector

Description: Convert Audit files from MSSQL Server to csv-format to Logpoint

Steps: New

Step Name:

Start PowerShell

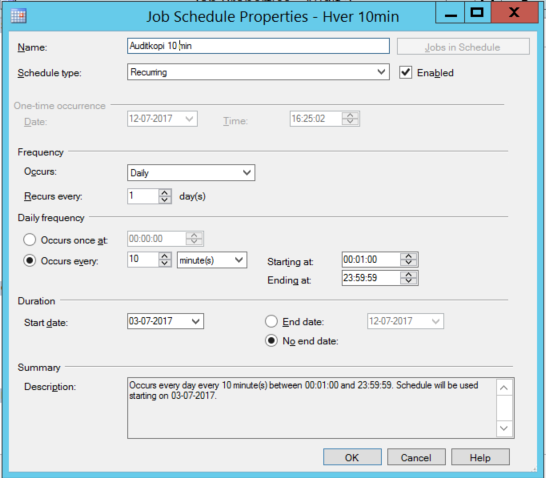
Type: Operating system (CmdExec)

Run as: SQL Server Agent Service Account

Command: (ombyt stien til -.ps1 filen med den aktuelle og indsæt under command som 1 linie)

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe T:\MSSQL12.MSSQLSERVER\MSSQL\Audit\auditexport.ps1

Tryk Ok

Schedules: New

Navn:

Auditkopi 10 min

Occours: Daily

Recours every 1 Days

Daily Frequency:

Occours every: 10 min.

Starting at 00:01:00

Start date: nu

No end date

Ok

Ok

## Logpoint opsætning:

NB.: man kan ikke redigere ”.conf” med notepad. (Kopier evt. til skrivebord, og åbn med wordpad)

1. Tilret C:\Program Files (x86)\nxlog\conf\nxlog.conf

Tilføj nederste linie:

include %CONFDIR%\Custom\_mssql.conf

<Output logcontents> sektion og <Output agentlog> sektion

Host logpoint rettes til ip-adresse se nedenfor

1. Tilret C:\Program Files (x86)\nxlog\conf\Custom\_mssql.conf

Basedir skal pege på u:…\audit\logpoint folderen

<Output out\_mssql> sektion

Host 192.168.39.16 rettes til nyeste (09t: Host 192.168.33.12)

1. Genstart nxlog service

Kontroller ved at åbne C:\Program Files (x86)\nxlog\data\nxlog (dobbeltklik)

Skal gerne slutte med noget der ligner:

2017-06-27 11:21:51 INFO nxlog-3.0.1714 started

2017-06-27 11:21:51 INFO connecting to 192.168.33.12:514

1. Hvis problem med nxlog service

Under installation: kontakt tskj

I drift: mail: [Support@logpoint.com](mailto:Support@logpoint.com)