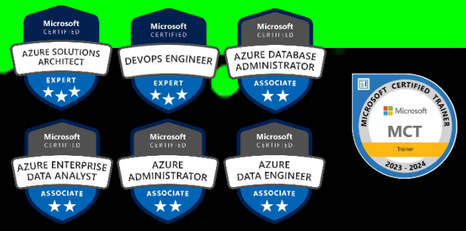
unit it

René F Jensby Kristiansen
Dataplatform Architect



Audit og Sikkerhed i dit SQL setup

Strategisk

DATA & CLOUD DAGEN VEST
Aarhus
28. september

Agenda

01 Hvorfor Audit

02 Audit SQL on-prem

03 Audit SQL i Azure

04 Best practices

05 Spørgsmål og afslutning

Hvorfor Audit!?

Hvorfor Audit

Audit:

Overvågning og opsamling af database aktiviteter for at sikre overensstemmelse med krav, opdage brud på sikkerhed og identificere uberettiget adgang til data

- Vi vil overholde gældende krav..
- Der kræves bevis for at vi gør det..

Krav kan komme fra forskellige steder

- **GDPR**
  - Tilgang til data
- **ISO-27001**
  - Registrering af systemændringer
- **Interne Audit**
- ....

Audit SQL on-prem

Eget miljø

Ejerskab over underliggende miljø

Skal selv opbygge audit evt. med 3.part software

Fuld kontrol over data

Mange komponenter skal konfigureres sammen

Skal selv vedligeholde

Selv ansvarlig

Stor opstartsudgift

Hostet miljø/Azure

Underliggende komponenter styret af leverandør

Nem opsætning

Fleksibilitet

Nem administration

Rigtig mange detaljer

Eksterne afhængigheder

Pladsomkostninger

Begrænsninger i tilpasningsmuligheder

Audit muligheder

Server niveau	Database niveau	Forklaring
SERVER_PRINCIPAL_CHANGE_GROUP	DATABASE_PRINCIPAL_CHANGE_GROUP	Skift i brugere fx opret bruger & nedlæg bruger
SERVER_ROLE_MEMBER_CHANGE_GROUP	DATABASE_ROLE_MEMBER_CHANGE_GROUP	Skift i bruger rolle medlemskab, henholdsvis server roller og database roller
SERVER_PERMISSION_CHANGE_GROUP	DATABASE_PERMISSION_CHANGE_GROUP	Object niveau rettigheder, som fx View Server State, og Select på en enkel tabel
FAILED_LOGIN_GROUP	FAILED_DATABASE_AUTHENTICATION_GROUP	Login forsøg der fejler, på databasen er det kun hvis man køre contained databaser
SERVER_STATE_CHANGE_GROUP		Start & Stop af SQL Serveren
SERVER_OBJECT_CHANGE_GROUP	DATABASE_OBJECT_CHANGE_GROUP	Alle underliggende objecter, som fx Opret & nedlæg af en database, eller opret eller nedlæg af en tabel på database niveau
	DATABASE_CHANGE_GROUP	Oprettelse og nedlæggelser af databaser
AUDIT_CHANGE_GROUP		Ændringer i hvad der bliver auditeret

Ledger til audit

- Trigger på tabel/database gemmer informationer i Ledger database / Tabel
- Ledger teknologien sikrer historik som ikke kan slettes heller ikke af DBA
- Understøttes både on-prem (SQL 2022) og i Azure

Audit SQL i Azure

Destination

Storage

Log Analytics

Eventhub

Alarmer / dokumentation

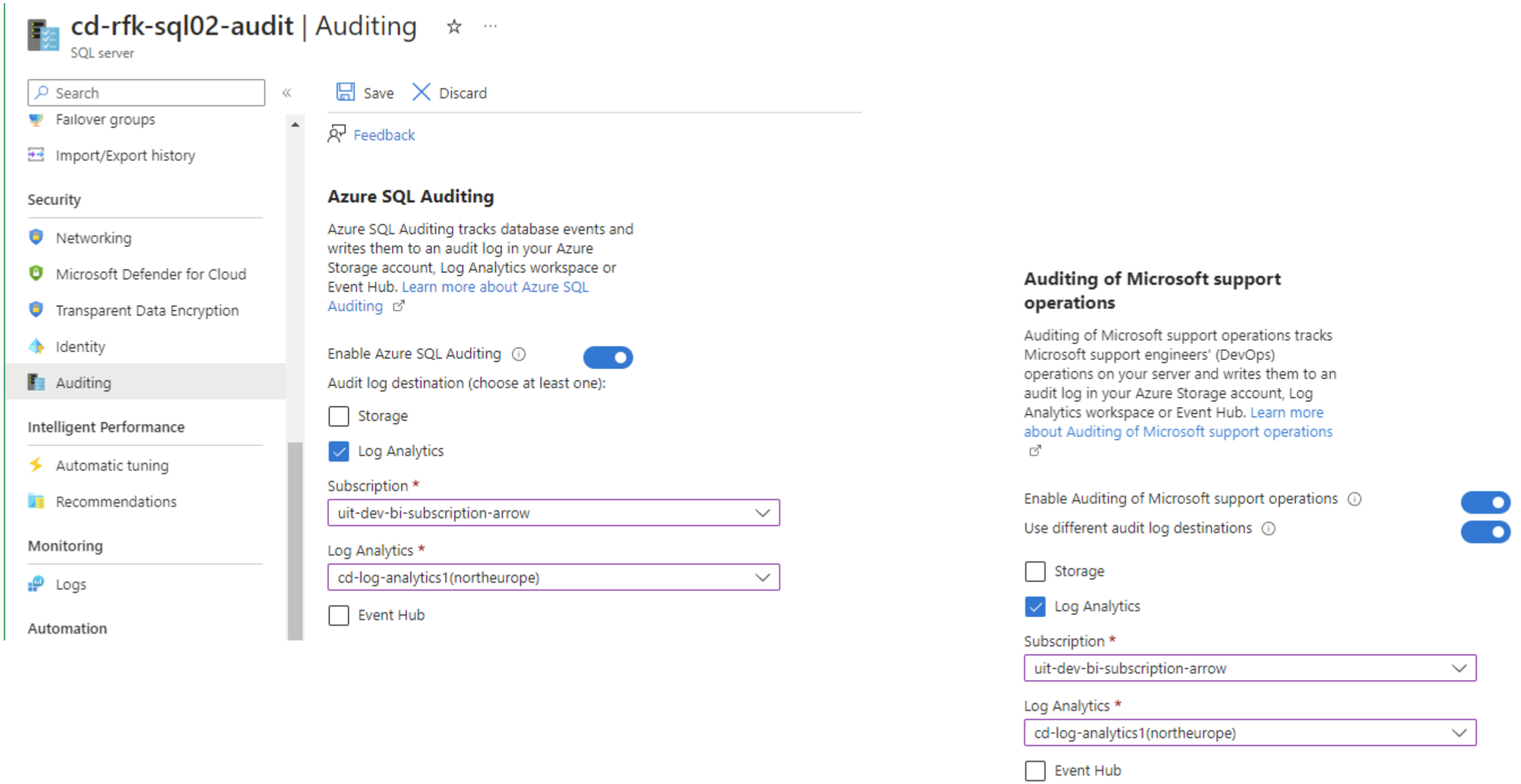
- Enorme mængder af data hvis man har flere servere eller mange målepunkter
- Skal data benyttes til alarmer og hvor vigtigt
- Er det bare log
- Hvor længe skal data gemmes

DEMO

OPRET SQL AUDIT

TILPAS AUDIT KONFIGURATION

QUERY AUDIT LOGS


cd-rfk-sql02-audit | Auditing
SQL server
Search
Failover groups
Import/Export history
Security
Networking
Microsoft Defender for Cloud
Transparent Data Encryption
Identity
Auditing
Intelligent Performance
Automatic tuning
Recommendations
Monitoring
Logs
Automation
Save
Discard
Feedback
Azure SQL Auditing
Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Azure SQL Auditing
Enable Azure SQL Auditing
Audit log destination (choose at least one):
Storage
Log Analytics
Subscription *
uit-dev-bi-subscription-arrow
Log Analytics *
cd-log-analytics1(northeurope)
Event Hub
Auditing of Microsoft support operations
Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Auditing of Microsoft support operations
Enable Auditing of Microsoft support operations
Use different audit log destinations
Storage
Log Analytics
Subscription *
uit-dev-bi-subscription-arrow
Log Analytics *
cd-log-analytics1(northeurope)
Event Hub

TESTDB2 (cd-rfk-sql02-audit/TESTDB2) | Auditing

SQL database

Search

Azure Synapse Link
Stream analytics (preview)
Add Azure Search

Power Platform

Power BI
Power Apps
Power Automate

Security

Auditing
Ledger
Data Discovery & Classification
Dynamic Data Masking
Microsoft Defender for Cloud
Identity

Save | Discard | View audit logs

Feedback

If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings.

View server settings

Server-level Auditing: **Enabled**

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Azure SQL Auditing

Enable Azure SQL Auditing

Turn on Microsoft Defender for SQL to receive security alerts upon suspicious events.

Logs

cd-log-analytics1

New Query 1*

Feedback | Queries

cd-log-analytics1 | Select scope | Run | Time range : Last 7 days | Save | Share | New alert rule | Export | Pin to

Tables | Queries | Functions

Search

Filter | Group by: Solution

Collapse all

Favorites

You can add favorites by clicking on the ☆ icon

LogManagement

```
AzureDiagnostics
| where Category == 'SQLSecurityAuditEvents'
| where ResourceId like '/SUBSCRIPTIONS/C0285559-FFF3-4C3E-8C53-7B66FD167F71/RESOURCEGROUPS/CLOUD-DAG-RFK/PROVIDERS/MICROSOFT.SQL/SERVERS/CD-RFK-SQL02-AUDIT/DATABASES/'
| project
    event_time_t,
    statement_s,
    succeeded_s,
    affected_rows_d,
    server_principal_name_s,
    client_ip_s,
    application_name_s,
    additional_information_s,
    data_sensitivity_information_s,
    ResourceId
| order by event_time_t desc
| take 100
```

Results | Chart

event_time_t [UTC]	statement_s	succeeded_s	affected_rows_d	server_principal
9/27/2023, 1:02:42.304 PM	INSERT INTO [dbo].[TestTBL] ([i]...	true	1	rfk@unit-it.dk
9/27/2023, 1:02:42.304 PM	INSERT INTO [dbo].[TestTBL] ([i]...	true	1	rfk@unit-it.dk
9/27/2023, 1:02:42.257 PM	USE [TESTDB2]	true	0	rfk@unit-it.dk
9/27/2023, 1:02:42.257 PM	USE [TESTDB2]	true	0	rfk@unit-it.dk
9/27/2023, 1:02:40.085 PM	exec sp_executesql N'SELECT cl...	true	1	rfk@unit-it.dk

Best practices

Tilpas Audit

Overvej nødvendigheden af data

Hvor meget kan egentlig behandles

Hvordan skal information benyttes

Kan det kræve ændringer på database/applikations niveau

Start et sted og tilpas derfra..

Eksterne krav skal helt sikkert overholdes

- GDPR
  Adgang til sensitiv data
- ISO 27001
  Hvilke ændringer er der sket

Spørgsmål !?

Tak for opmærksomheden

Næste session her starter kl. 11.30
DevOps: Få styr på udvikling og drift i dit dataprojekt

Muligheder:

Lokale M1 - **Byg en Azure dataplatform**
Lokale M5+M6 - **360 grader med Awareness**