Auditing SQL Server

Jonathan Allen

Jonathan Allen

- Working with SQL Server since 1999 / SQL 7.0
- 15+ years as full time DBA
- 5 years as Premier Field Engineer
- Founder of Data South West user group

Auditing options

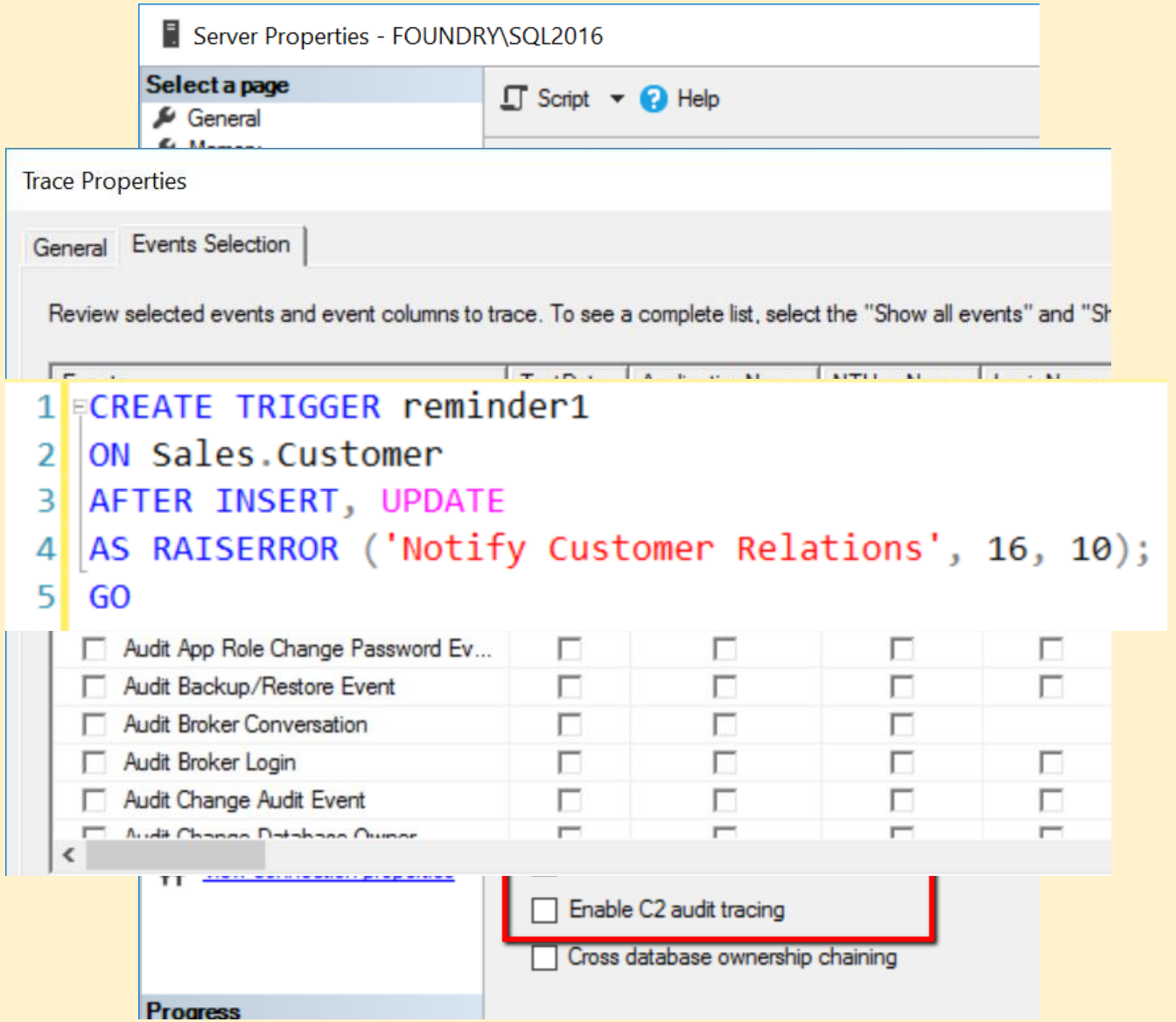
Login auditing

Common Criteria Compliance

C2 Audit

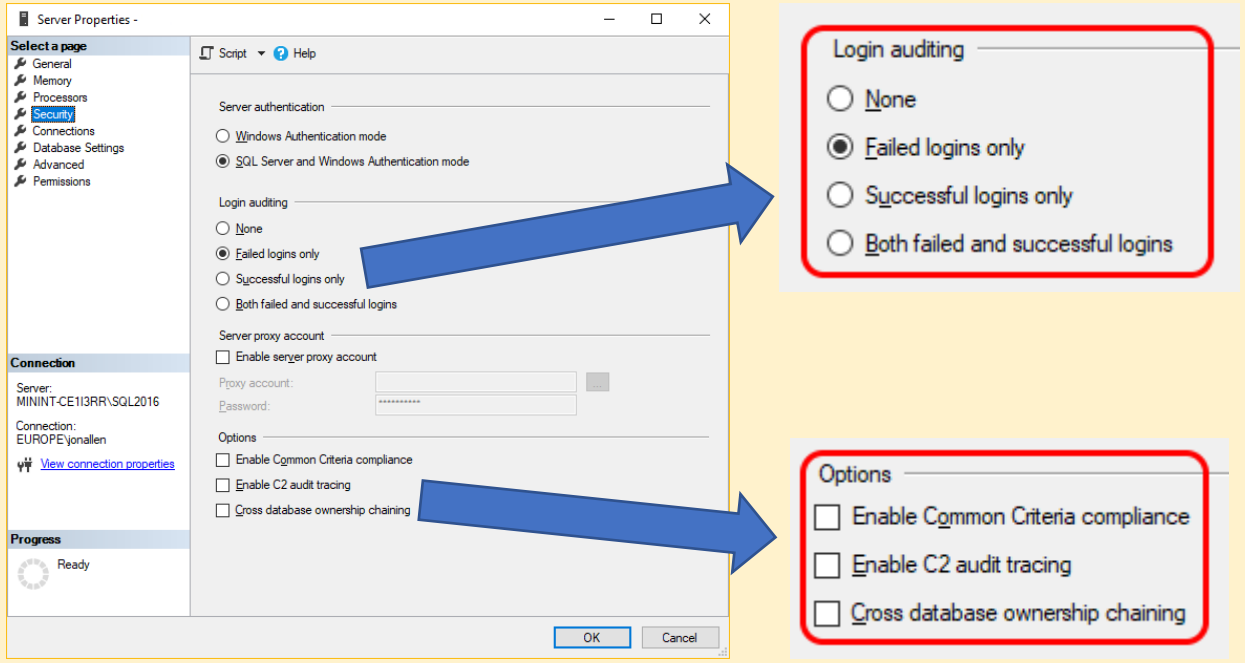
SQL Server Profiler Audit

Server / Database triggers



Auditing SQL Server

Default login auditing



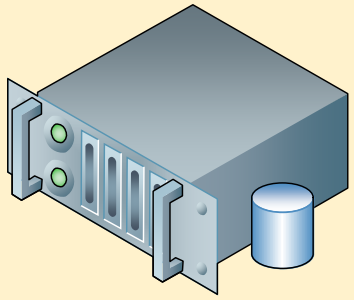
SQL Server – Server and Database Audits

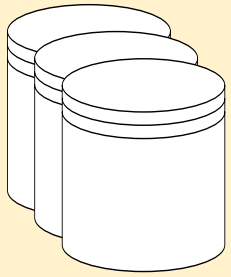
Server Audit

Server Audit Specification

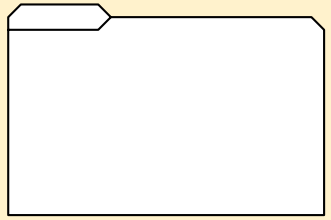
Database Audit Specification

Output





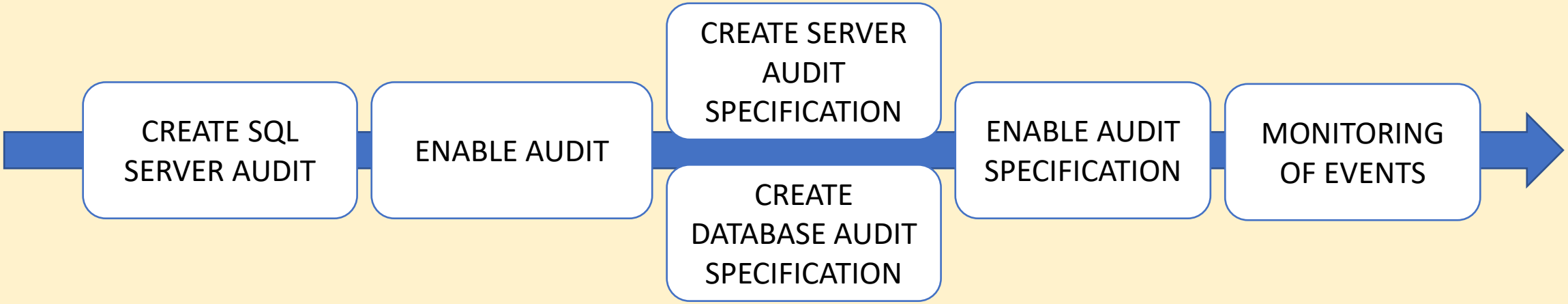
System Event Logs
Application or Security



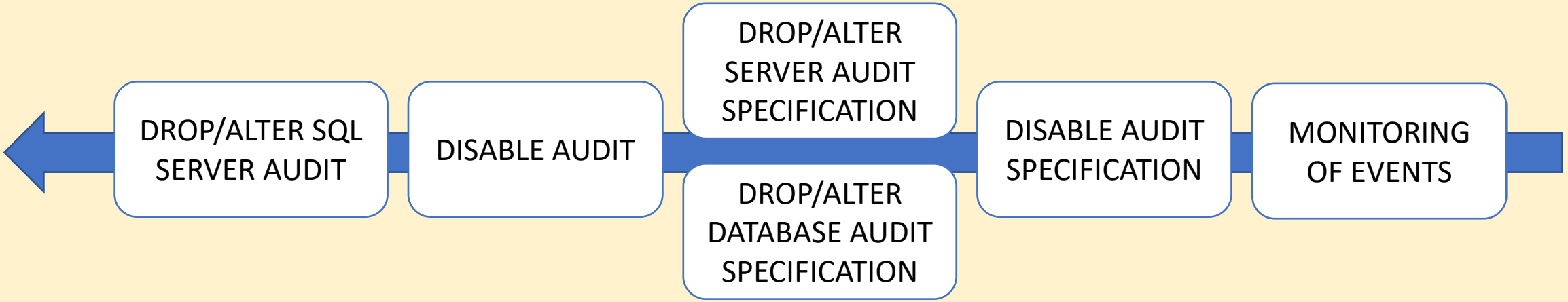
Folder location
Default is SQL Instance LOGS folder.

Audit properties
Name
Size
Roll-over options
etc

SQL Server Audit – creation workflow



SQL Server Audit – Drop/Alter workflow



Demo

So why SQL Server Audit?

For

- GUI for setup and management
- Easy to recreate via TSQL
- Very configurable
- Great for security
- Little/Zero penalty for usage

Against

- Can collect a lot of information
- Can have a severe effect on your server availability if you choose Stop Service option
- Can get complex to be very specific on event filter

Sponsors

Microsoft

POWER BI SENTINEL™

Governance, Disaster Recovery and Auditing for Power BI

dbWatch

redgate

Coeo

ADVANCING ANALYTICS

sqlbits

pyramid

Octopus Deploy

XTEN

CLOUD | DATA | XOPS

Simpson Associates

The Data Analytics Company

Thank you!
We couldn't do it without you.

DATA RELAY

References and more information

Demo code

https://github.com/fatherjack/Sessions/tree/master/20221007%20DataRelayBristol

SQL Server Audit

https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine

Action Groups and Actions

https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions

Audit Records

https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-records

EU General Data Protection Regulation (GDPR)

https://microsoft.sharepoint.com/sites/Infopedia_G01/Pages/Cards/TrustedCloud-GDPR.aspx

SQL Server and the GDPR

https://microsoft.sharepoint.com/sites/infopedia/pages/layouts/kcdoc.aspx?k=G01KC-1-26721