SQL Day

15 edycja konferencji SQLDay

8-10 maja 2023, WROCŁAW + ONLINE

Data Community

partner złoty

Future Processing

partner srebrny

Objectivity

summ-it

kursySQL.pl

VOLVO

partner brązowy

devart

Tomasz Libera & Michał Sadowski

Nowości w zakresie bezpieczeństwa w SQL Server 2022

AGENDA

- Intro
- SQL Ledger
- Uwierzytelnienie Azure AD
- Tabular Data Stream 8.0/Transport Layer Security 1.3
- Podsumowanie
- Linki

Microsoft

Michał Sadowski

Microsoft Technical Trainer

E-mail: Michal.Sadowski@Hotmail.com

LinkedIn: https://aka.ms/michal

- Były Microsoft MVP - Data Platform
- Ponad 15 lat doświadczenia w IT, pierwszy certyfikat w 2005
- Lider **Data Community** Kraków
- Prelegent na licznych konferencjach
- Zainteresowania:
  - Optymalizacja użycia infrastruktury
  - Migracje do najnwszych wersji oraz rozwiązań chmurowych

Microsoft Learn. Spark possibility.

TECHNOLOGY INNOVATION DATA KNOWLEDGE tidk

kursySQL.pl

Data Community

Tomasz Libera

Data Architect, TIDK

Microsoft MVP Data Platform, MCT

MVP Microsoft® Most Valuable Professional

/kursysql

/kursysql

/kursysql

POZNAJ NAS

Od 2009 roku **dostarczamy, projektujemy i wdrażamy** zaawansowane rozwiązania bazujące na danych w największych polskich organizacjach.

Zespół TIDK liczy ok. 50 osób i posiada wszystkie najważniejsze kompetencje techniczne oraz certyfikaty z obszaru Data & AI. Nieustannie podnosimy swoje kwalifikacje zarówno w technologiach chmurowych jak i on-premises.

Nad jakością projektów czuwają doświadczeni eksperci w dziedzinie projektowania i budowania najnowocześniejszych rozwiązań opartych o dane.

SPECIALIZATION
ANALYTICS
on Microsoft Azure

Łukasz Grala
Ekspert Data & AI,
Chief Execution Officer

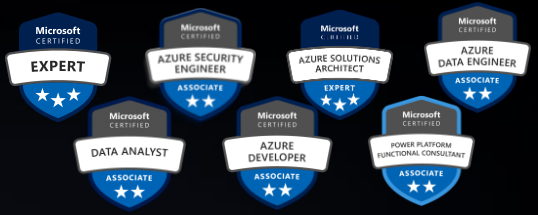
Grzegorz Stolecki
Mentor Data Platform,
Senior Data Architect

Tomasz Libera
Data Architect

Magdalena Biczkowska
Ekspert dziedzinowy,
Principal Data Architect

Jakub Wawrzyniak
Solution Architect,
Chief Technology Officer

dr Natalia Szóstak
Head of R&D



Materiały do sesji

Prezentacja, skrypty: https://www.kursysql.pl/sqlday

SQL Ledger

Tabele Updatable, widoki systemowe | Tabele Append-only

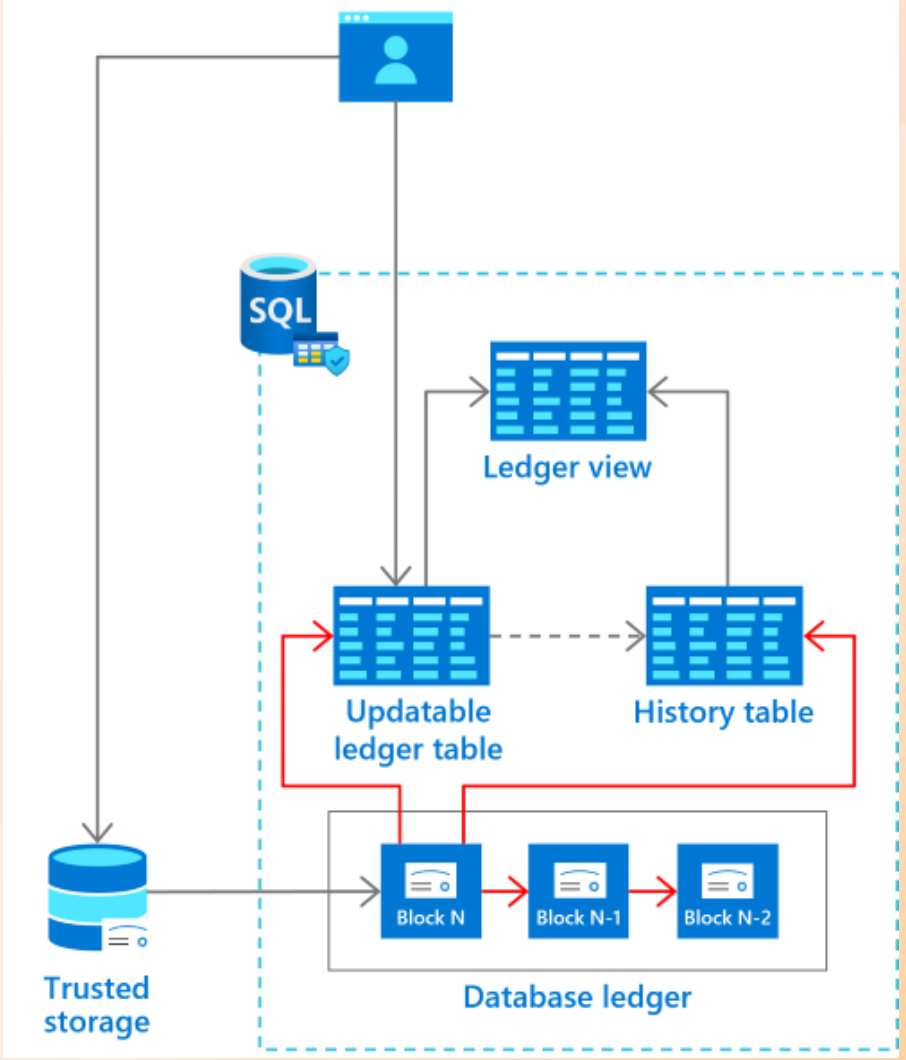
Baza danych Ledger | Digest management | Azure

Ledger

Zachowuje i daje możliwość przeglądania historii zmian

Zapewnia o nienaruszeniu danych, również przed osobami z wysokimi uprawnieniami (DBA)

Nie wymaga żadnych zmian po stronie aplikacji



https://docs.microsoft.com/en-us/sql/relational-databases/security/ledger/ledger-landing-sql-server

Tabela ledger (Updatable)

- Zapisuje wszystkie zmiany (UPDATE/ DELETE)
- Wraz z utworzeniem ledger table, automatycznie powstaje
  - tabela z historią zmian – zawierająca poprzednie (skasowane i zmodyfikowane) wersje wierszy
  - widok ledger
- Operacja TRUNCATE jest niewspierana

```
    JobTitle nvarchar(50),
    Rate money,
    PayFrequency tinyint
)
WITH
(
    SYSTEM_VERSIONING = ON,
    LEDGER = ON
)
```

Widok ledger (Ledger view)

ledger_transaction_id	ledger_sequence_number	ledger_operation_type	ledger_operati
5928	0	1	INSERT
5928	1	1	INSERT
5930	0	1	INSERT
5930	1	2	DELETE
5934	0	1	INSERT
5934	1	2	DELETE
5935	0	2	DELETE

Tworzony automatycznie dla każdej tabeli

Prezentuje dane z tabeli ledger

i powiązanej tabeli z historią. Kolumny:

- **ledger_transaction_id** – numer transakcji która utworzyła bądź skasowała wiersję wiersza
- **ledger_sequence_numer** – numer operacji w ramach transakcji
- **ledger_operation_type** – rodzaj operacji: 1 (INSERT) lub 2 (DELETE)
- **ledger_operation_type_desc** – opis rodzaju operacji (INSERT/ DELETE)

sys.database_ledger_transactions

Systemowy widok katalogowy, zawierający informacje o wszystkich transakcjach w tabelach typu ledger

- transaction_id – identyfikator transakcji w ramach bazy danych
- block_id – identyfikator wiersza
- commit_time – czas zatwierdzenia transakcji
- principal_name – nazwa loginu (ORIGINAL_LOGIN())
- table_hashes – zbiór klucz-wartość, zapisany jako dane binarne.

Klucze to identyfikatory tabel ledger (object_id), modyfikowanych przez transakcję.

Wartości to SHA-256 wszystkich wersji wierszy utworzonych lub skasowanych przez transakcję

	transaction_id	block_id	transaction_ordinal	commit_time	principal_name	table_hashes
1	5873	0	0	2022-09-03 13:56:19.1400000	KENOBI\kowalski	0x10148551031A51C8A2286FD192B656C5B091209795956C59D1A0E80667C37F3E2...
2	5883	0	1	2022-09-03 14:03:40.1233333	KENOBI\kowalski	0x9ECB9C4F7EAB1555F2DA7ED193328B05209623B6603543ABB3CFDF446A2E3A4...
3	5887	0	2	2022-09-03 14:03:40.1333333	KENOBI\kowalski	0x101485519E1E5EB47F61A8F07E6058FA6508E268194A985EE7D924A05E97054B9...
4	5890	0	3	2022-09-03 14:10:09.3800000	KENOBI\kowalski	0xBD0C8C65703B047C32E44DF58A1B2AE3A5C50696CEE5C6EF055CDC30EFEF4C...
5	5899	0	4	2022-09-03 14:10:48.5366667	KENOBI\kowalski	0x9ECB9C4F1DD58BB8B044A336A7274BDFA8C56819E5B98DD28190FD4ADD8577...
6	5901	0	5	2022-09-03 14:10:48.5466667	KENOBI\kowalski	0x101485517853B4E0DF40EBFAB100ACD8415DCF527617FD27CF72B588466E800D...

Tabela ledger (Append-only)

Nie pozwala na modyfikacje

wprowadzonych danych (tylko INSERT)

```
CREATE TABLE dbo.EmployeeBonus
(
    EmployeeBonusID int PRIMARY KEY IDENTITY,
    BusinessEntityID int,
    BonusAwarded money,
    BonusDate datetime DEFAULT GETDATE()
)
WITH (LEDGER = ON (APPEND_ONLY = ON))
```

```
UPDATE dbo.EmployeeBonus SET BonusAwarded = BonusAwarded*1.5 WHERE BusinessEntityID = 1
```

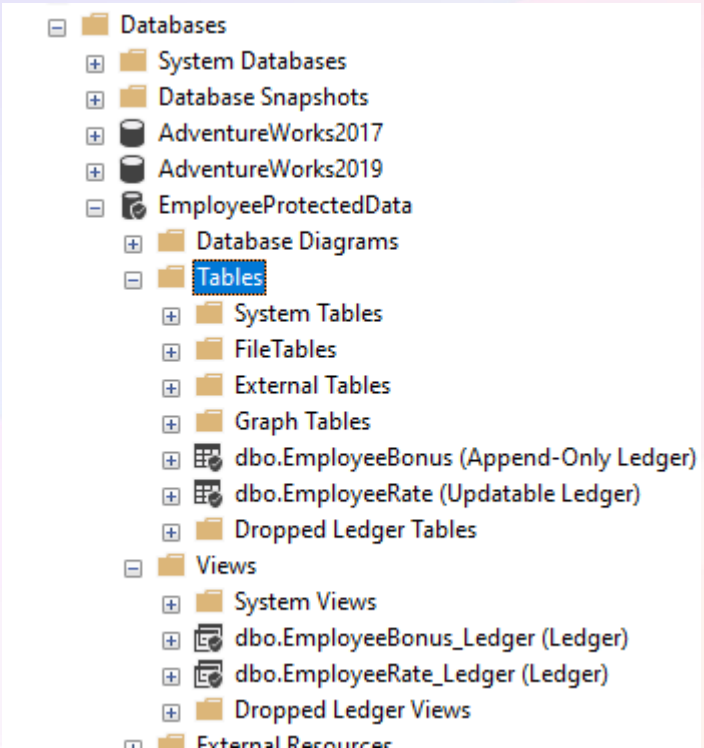
Messages

```
Msg 37359, Level 16, State 1, Line 144
Updates are not allowed for the append only Ledger table 'dbo.EmployeeBonus'.
```

Baza ledger

Wszystkie tabele muszą być typu ledger updatable (domyślnie) lub append-only

```
CREATE DATABASE EmployeeProtectedData
WITH LEDGER = ON
GO
```




```
CREATE TABLE dbo.RegularTable
(
    EmployeeBonusID int PRIMARY KEY IDENTITY,
    BusinessEntityID int,
    BonusAwarded money,
    BonusDate datetime DEFAULT GETDATE()
)
WITH (LEDGER = OFF)
```

51 %

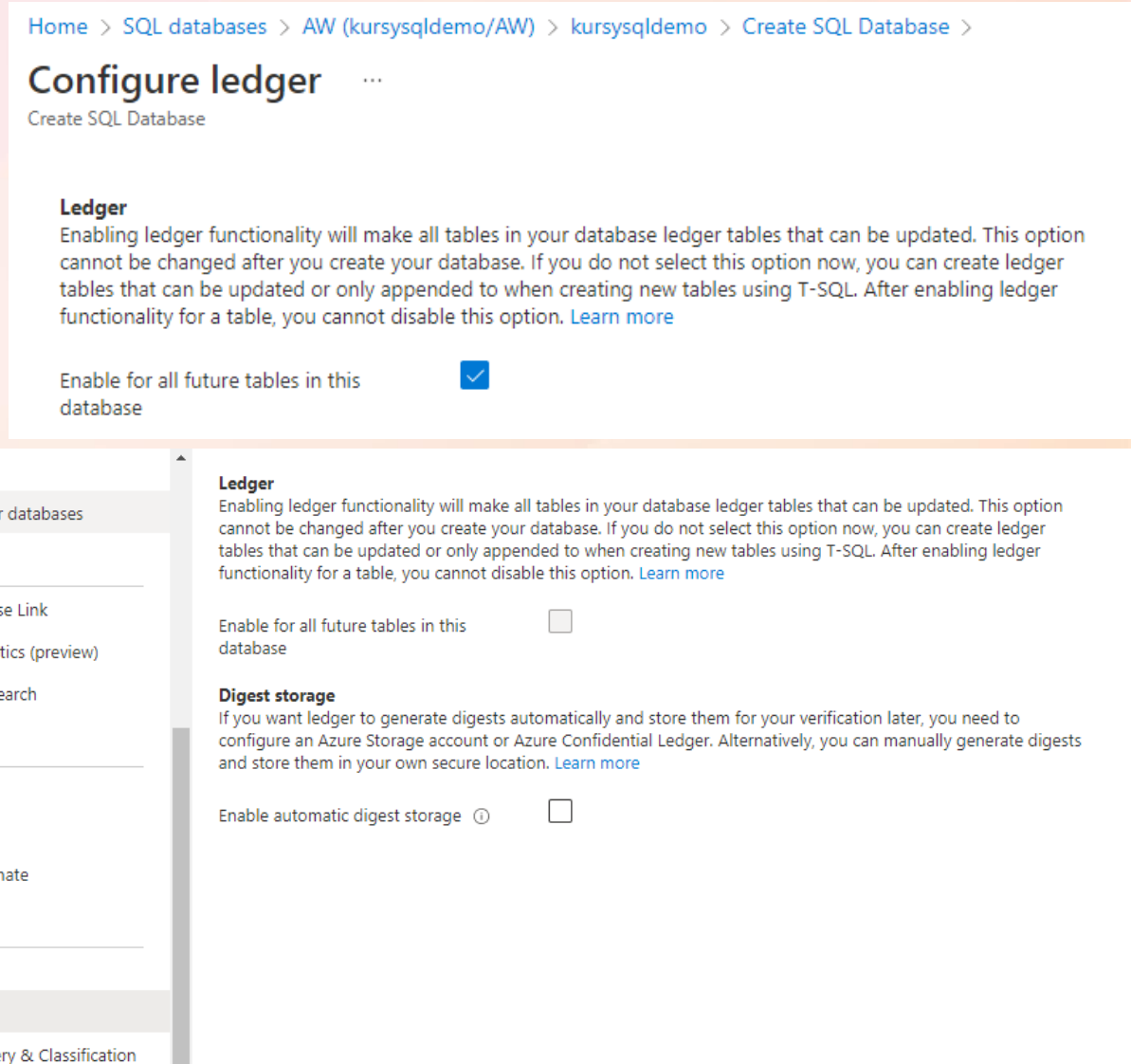
Messages

```
Msg 37420, Level 16, State 1, Line 74
LEDGER = OFF cannot be specified for tables in databases that were created with LEDGER = ON.
```

Baza ledger : Azure

Tworząc bazę w **Azure SQL** można skonfigurować Ledger na karcie Security

Po włączeniu/ wyłączeniu tej opcji – nie można jej zmienić po utworzeniu bazy



Digest management

Database digest – hash reprezentujący stan wszystkich tabel ledger w bazie.

Może być tworzony (generowany):

- Automatycznie (korzystając z Azure Blob Storage lub usługi Azure Confidential Ledger)
- Manualnie (na żądanie)

Udoskonalenia w zakresie bezpieczeństwa

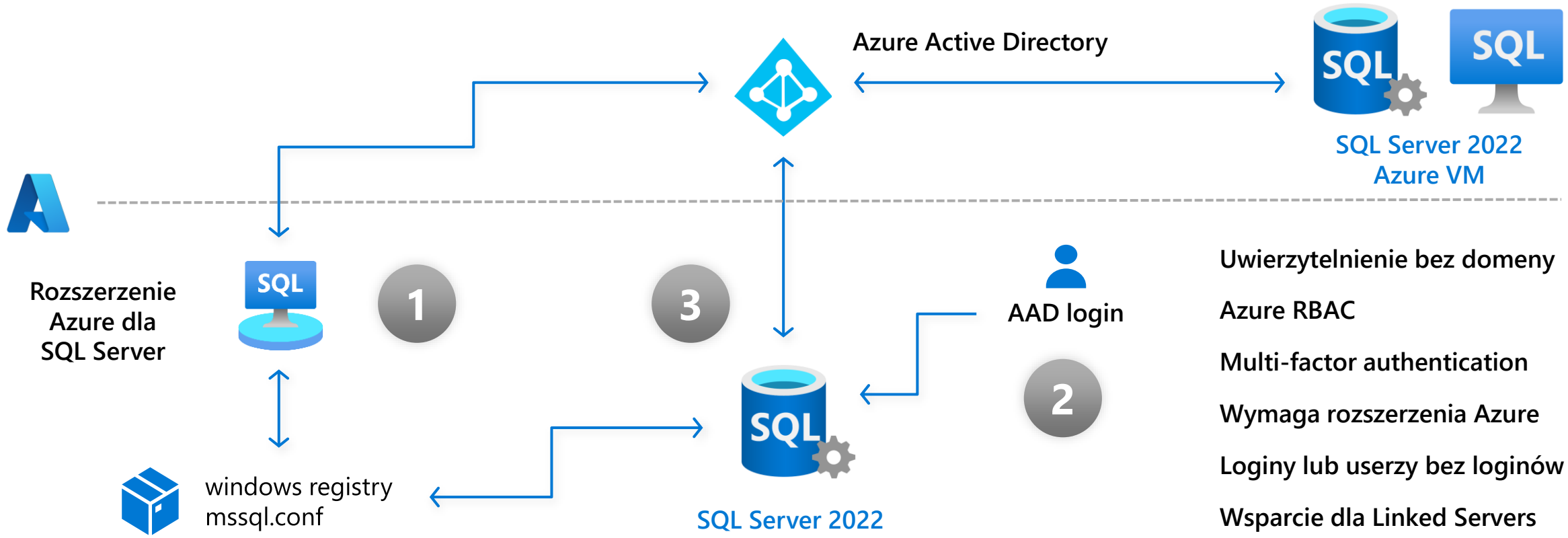
Udoskonalenia w zakresie bezpieczeństwa

- Uwierzytelnienie Azure Active Directory
- Rygorystyczne połączenie szyfrowane (TDS 8.0 and TLS 1.3)
- Wsparcie dla certyfikatów PFX
- Ulepszenia Always encrypted
- Nowe granularne wbudowane role serwerowe
- Ulepszenia Dynamic Data Masking

Uwierzytelnie Azure Active Directory

https://aka.ms/aadsqlserver

Wyzwanie: Alternatywa dla uwierzytelnienia typu SQL auth oraz domena Windows



Uwierzytelnienie bez domeny

Azure RBAC

Multi-factor authentication

Wymaga rozszerzenia Azure

Loginy lub userzy bez loginów

Wsparcie dla Linked Servers

Wsparcie dla Tabular Data Stream 8.0 oraz Transport Layer Security 1.3

Poprzednio (TDS 7.0/TLS 1.2):

- TCP handshake
- **TDS prelogin (jawny tekst) oraz response (jawny tekst)**
- TLS handshake
- **uwierzytelnienie (szyfrowane)**
- **wymiania danych (zaszyfrowane lub niezaszyfrowane)**

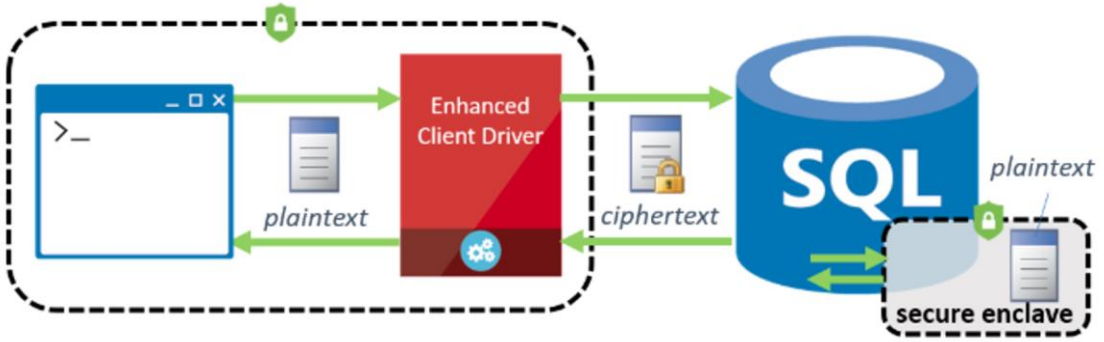
Obecnie (TDS 8.0/TLS 1.3):

- TCP handshake
- TLS handshake
- **TDS prelogin (zaszyfrowane) oraz response (zaszyfrowane)**
- **uwierzytelnienie (zaszyfrowane)**
- **wymiania danych (zaszyfrowane)**

TDS 8.0 oraz TLS 1.3 c.d.

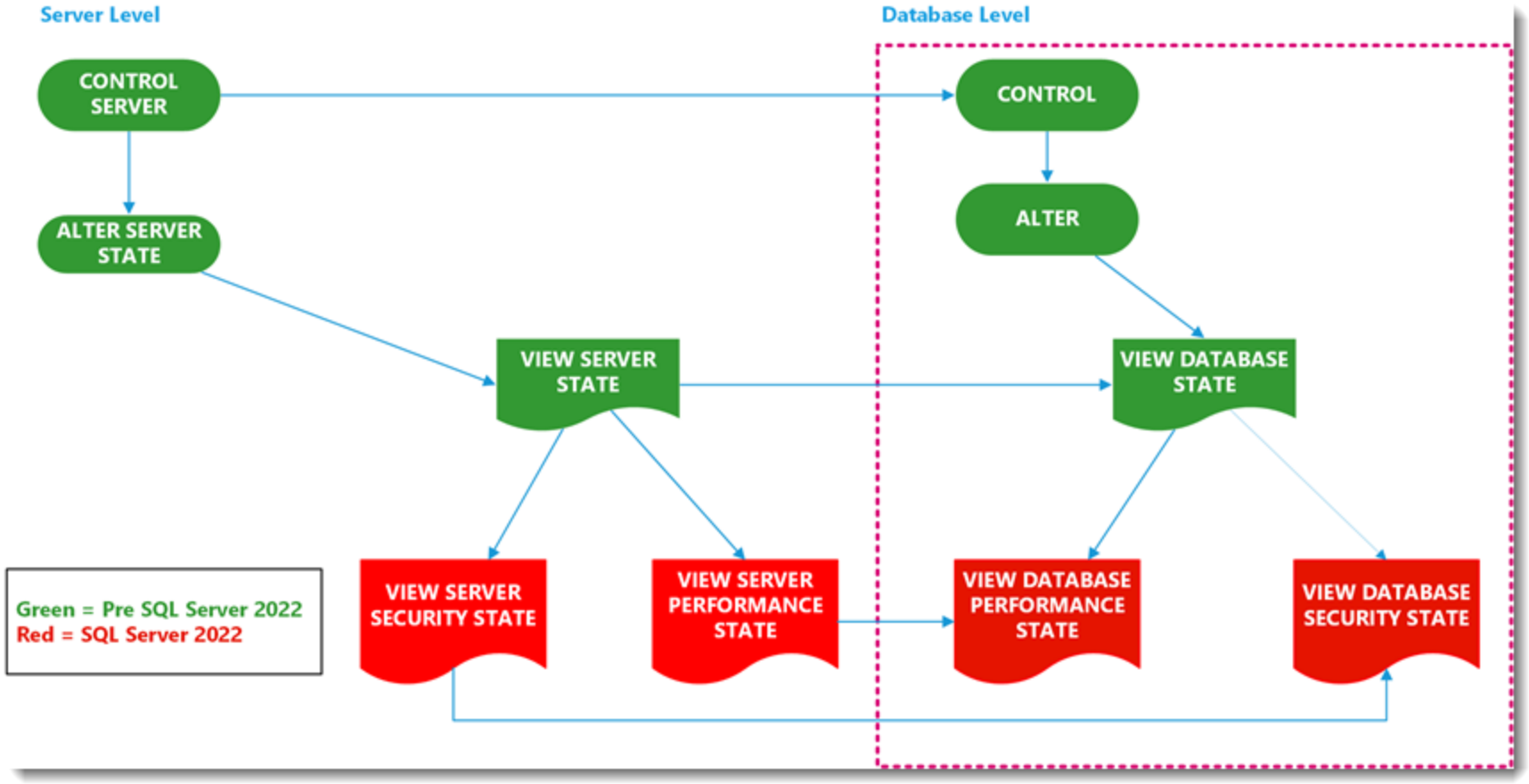
Algorytm	TLS 1.2	TLS 1.3
AES GCM/AES CCM	zabezpieczone	zabezpieczone
AES CBC	zależy od konfiguracji	N/A
Camellia GCM	zabezpieczone	N/A
Camellia CBC	zależy od konfiguracji	N/A
ARIA GCM	Zabezpieczone	N/A
ARIA CBC	zależy od konfiguracji	N/A
SEED CBC	zależy od konfiguracji	N/A
3DES EDE CBC	Niezabezpieczone	N/A
GOST 28147-89 CNT	Niezabezpieczone	N/A
ChaCha20-Poly1305	Zabezpieczone	zabezpieczone
RC4	Niezabezpieczone	N/A
Brak	Niezabezpieczone	N/A

Ulepszenia Always Encrypted



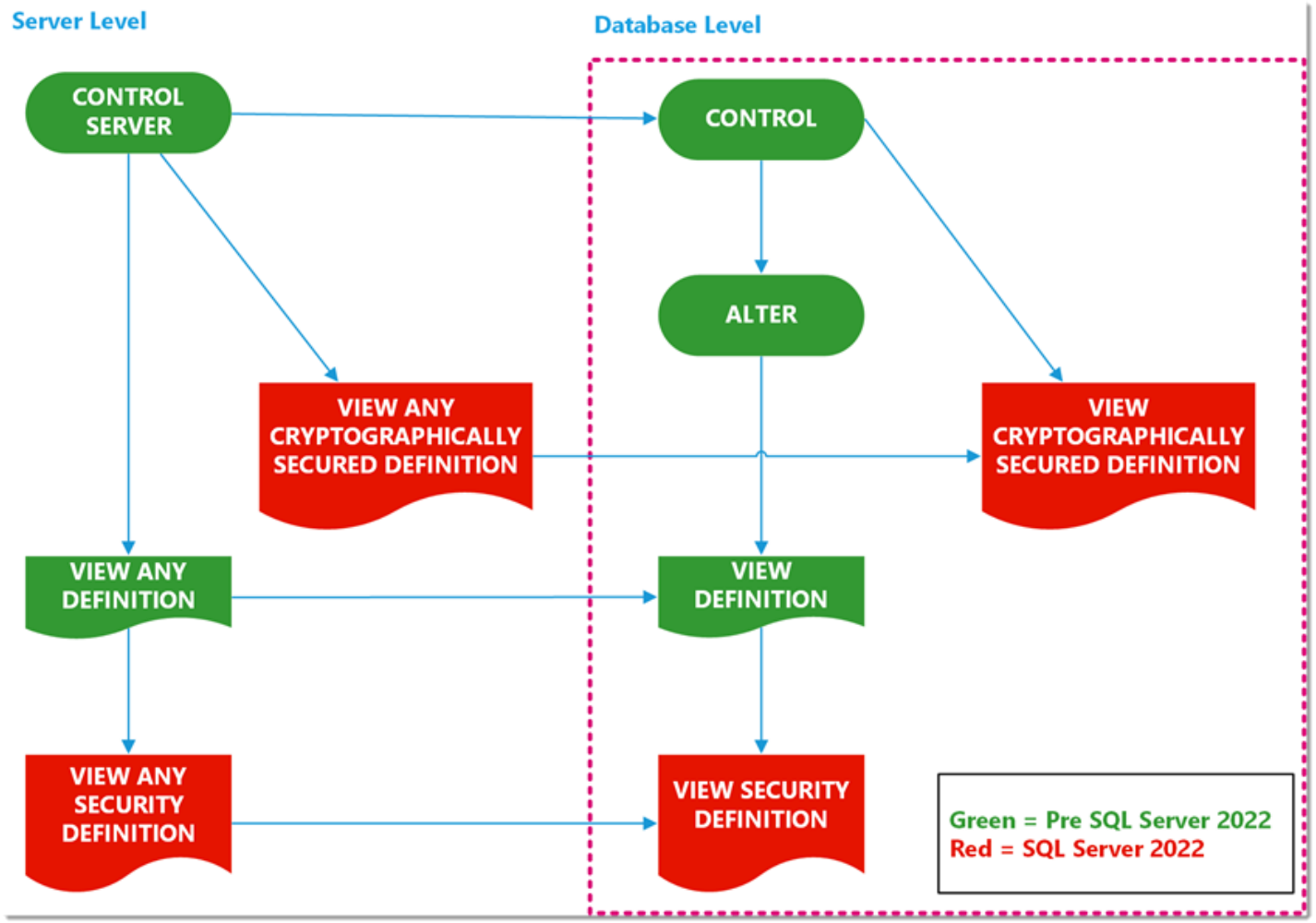
Operator	SQL Server 2019 (15.x)	SQL Server 2022 (16.x)	Azure SQL Database
Operatory porównania	Wspierane	Wspierane	Wspierane
BETWEEN (Transact-SQL)	Wspierane	Wspierane	Wspierane
IN (Transact-SQL)	Wspierane	Wspierane	Wspierane
LIKE (Transact-SQL)	Wspierane	Wspierane	Wspierane
DISTINCT	Wspierane	Wspierane	Wspierane
Joins	Tylko nested loop	Wspierane	Wspierane
SELECT - ORDER BY Clause (Transact-SQL)	Niewspierane	Wspierane	Wspierane
SELECT - GROUP BY- Transact-SQL	Niewspierane	Wspierane	Wspierane

Nowe granularne wbudowane role serwerowe



Źródło: https://techcommunity.microsoft.com/t5/azure-sql-blog/revamped-sql-permission-system-for-principle-of-least-privilege/ba-p/3639399

Nowe granularne wbudowane role serwerowe c.d.



Źródło: https://techcommunity.microsoft.com/t5/sql-server-blog/new-granular-permissions-for-sql-server-2022-and-azure-sql-to/ba-p/3607507

Ulepszenia Dynamic Data Masking

SQL Server 2016/2017/2019:

UNMASK na poziomie:

- podmiot bazy danych (database principal)

SQL Server 2022

UNMASK na poziomie:

- **bazy danych**
- **schematu**
- **tabeli**
- **kolumny**

Microsoft

Demo

Azure Active Directory (AAD)

Azure services

Create a resource
Azure Arc
Resource groups
Stream Analytics jobs
Event Hubs
Azure Active Directory
Virtual machines
App Services
Storage accounts
More services

Resources

Recent | Favorite

Name	Type

No resources have been favorited

Favorite resources to quickly navigate to them from the home page.

Select resources to favorite

Navigate

Subscriptions
Resource groups
All resources
Dashboard

Tools

In Seattle: May 23–25, 2023 | Online: May 23–24, 2023 PDT

Join us in Seattle for Microsoft Build!

Get ready to make your mark in this new era of AI. Be there as Microsoft leaders share exciting announcements and reveal the latest tech that will launch the next wave of developer innovation.

Register now

Showing 17 speakers

Satya Nadella

Chairman and CEO

Microsoft

Scott Guthrie

EVP, Cloud + AI

Microsoft

Amanda Silver

CVP, Head of Product, Developer Division

Microsoft

Kevin Scott

CTO and EVP, Technology & Research

Microsoft

Rajesh Jha

EVP, Experiences & Devices

Microsoft

Podsumowanie

- SQL Server 2022 wprowadził ważne usprawnienia w zakresie bezpieczeństwa, takie jak:
  - SQL Ledger
  - Uwierzytelnienie Azure Active Directory
  - Rygorystyczne połączenie szyfrowane (TDS 8.0 and TLS 1.3)
  - Wsparcie dla certyfikatów PFX
  - Ulepszenia Always encrypted
  - Nowe granularne wbudowane role serwerowe
  - Ulepszenia Dynamic Data Masking

Pytania?

Dziękujemy

SQL Day

15 edycja konferencji SQLDay

8-10 maja 2023, WROCŁAW + ONLINE

Data Community

partner złoty

Future Processing

partner srebrny

Objectivity

summ-it

kursySQL.pl

VOLVO

partner brązowy

devart