

# SQL SERVER | BACKUP I RESTORE PRAKTYCZNY PRZEWODNIK DBA



*Od zielonego joba do realnej strategii odtwarzania*

MARCIN PYTLIK | SQLMANIAK | WYDANIE 2026

**BEZPŁATNY FRAGMENT**

# **SQL Server Backup i Restore - Praktyczny Przewodnik DBA**

Od zielonego joba do realnej strategii odtwarzania

Nie chcę, aby ktokolwiek kupował kota w worku. Dlatego w tej próbce znajdziesz pełny spis treści oraz wybrany, kompletny fragment publikacji.

Możesz sprawdzić styl, poziom szczegółowości oraz praktyczny charakter materiału przed podjęciem decyzji o zakupie.

## Spis treści

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Licencja użytkowania.....                                          | 2  |
| Disclaimer.....                                                    | 2  |
| Wstęp.....                                                         | 8  |
| 1. Backup to nie strategia.....                                    | 8  |
| 2. RPO, RTO i odpowiedzialność DBA.....                            | 8  |
| 3. Rodzaje backupów SQL Server.....                                | 9  |
| 4. Recovery model: SIMPLE, FULL, BULK_LOGGED.....                  | 10 |
| 4.1. SIMPLE recovery model.....                                    | 10 |
| 4.2. FULL recovery model.....                                      | 10 |
| 4.3. Test: SIMPLE -> FULL i pierwszy backup LOG.....               | 11 |
| 4.4. BULK_LOGGED recovery model.....                               | 12 |
| 4.5. Skrypt kontrolny recovery model.....                          | 12 |
| 5. LSN i łańcuch logów transakcyjnych.....                         | 12 |
| 5.1. Historia backupów i LSN.....                                  | 12 |
| 5.2. Ciągłość backupów LOG.....                                    | 13 |
| 5.3. DIFF i jego baza różnicowa.....                               | 14 |
| 6. Co dzieje się podczas FULL, DIFF i backupu LOG.....             | 14 |
| 6.1. Rozpoczęcie pełnej kopii zapasowej.....                       | 14 |
| 6.2. Uruchomienie różnicowej kopii zapasowej.....                  | 15 |
| 6.3. Uruchomienie backupu LOG.....                                 | 15 |
| 6.4. Monitoring aktualnie trwających backupów.....                 | 16 |
| 7. FULL backup a transakcje wykonywane w trakcie backupu.....      | 17 |
| 7.1. Transakcja zakończona przed zakończeniem pełnego backupu..... | 17 |
| 7.2. Transakcja zakończona po zakończeniu pełnego backupu.....     | 17 |
| 7.3. Czy backup jest spójny na 20:00 czy 21:30?.....               | 17 |
| 7.4. Co dzieje się podczas RESTORE?.....                           | 18 |
| 7.5. Praktyczne konsekwencje dla planu odtwarzania.....            | 18 |
| 8. Restore na konkretną godzinę.....                               | 19 |
| 8.1. Przykładowa oś czasu.....                                     | 19 |
| 8.2. Zapytanie budujące plan odtwarzania z msdb.....               | 19 |
| 8.3. Przykładowy RESTORE z STOPAT.....                             | 21 |
| 8.4. Ograniczenia planu odtwarzania z bazy msdb.....               | 21 |
| 8.5. Checklista restore point-in-time.....                         | 21 |
| 9. Strategie backupu dla różnych środowisk.....                    | 23 |
| 9.1. Firma A - ERP i CRM pracujące od 8:00 do 16:00.....           | 23 |
| 9.2. Bank - aplikacja przelewy działająca 24/7.....                | 24 |
| 9.3. Duże bazy i VLDB.....                                         | 25 |
| 9.4. Środowiska DEV/TEST.....                                      | 25 |
| 10. Bazy systemowe SQL Server.....                                 | 26 |

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| 10.1. Baza master.....                                                             | 26 |
| 10.2. Baza msdb.....                                                               | 26 |
| 10.3. Baza model.....                                                              | 26 |
| 10.4. Baza tempdb.....                                                             | 27 |
| 10.5. Baza SSISDB i dodatkowe bazy funkcji SQL Server.....                         | 27 |
| 11. Harmonogramy i checklisty strategii backupu.....                               | 28 |
| 12. Wydajność backupu: model przepływu danych.....                                 | 28 |
| 12.1. Model przepływu.....                                                         | 28 |
| 12.2. Najczęstsze wąskie gardła.....                                               | 29 |
| 12.3. Zasada bezpiecznego tuningu.....                                             | 29 |
| 13. COMPRESSION i CHECKSUM.....                                                    | 29 |
| 13.1. COMPRESSION.....                                                             | 29 |
| 13.2. CHECKSUM.....                                                                | 30 |
| 14. MAXTRANSFERSIZE i BUFFERCOUNT.....                                             | 30 |
| 14.1. MAXTRANSFERSIZE.....                                                         | 30 |
| 14.2. BUFFERCOUNT.....                                                             | 31 |
| 14.3. Czego unikać.....                                                            | 31 |
| 15. Backup do wielu plików.....                                                    | 31 |
| 15.1. Przykład backupu do czterech plików.....                                     | 31 |
| 15.2. Restore z backupu do wielu plików.....                                       | 32 |
| 15.3. Kiedy wiele plików pomaga.....                                               | 32 |
| 16. Pomiar, testy i dobór profilu wydajnościowego.....                             | 33 |
| 16.1. Macierz testów.....                                                          | 33 |
| 16.2. Pomiar historii backupów.....                                                | 33 |
| 16.3. Monitoring aktualnie trwającego backupu.....                                 | 34 |
| 16.4. Profile dla generatora backupów.....                                         | 35 |
| 17. Planowanie pojemności (Capacity planning): backupy, dane, logi i retencja..... | 35 |
| 17.1. Trzy osobne prognozy.....                                                    | 35 |
| 17.2. backup_size vs compressed_backup_size.....                                   | 35 |
| 17.3. Dlaczego backup FULL nie jest równy rozmiarowi plików danych.....            | 36 |
| 18. Analiza wzrostu FULL backupów.....                                             | 36 |
| 18.1. Wzrost dzień do dnia.....                                                    | 36 |
| 18.2. Średni i maksymalny dzienny przyrost.....                                    | 37 |
| 18.3. Prognoza rozmiaru pojedynczego FULL backupu.....                             | 37 |
| 19. Szacowanie retencji FULL, DIFF i LOG.....                                      | 38 |
| 19.1. Przykład obliczeniowy.....                                                   | 38 |
| 19.2. Raport FULL + DIFF + LOG z msdb.....                                         | 38 |
| 19.3. Interpretacja wyniku.....                                                    | 40 |
| 20. Szacowanie miejsca dla danych i logów.....                                     | 40 |
| 20.1. Aktualny rozmiar plików.....                                                 | 40 |
| 20.2. Zajęte i wolne miejsce w plikach bazy.....                                   | 40 |

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 20.3. Własna historia rozmiaru baz.....                             | 40 |
| 20.4. Prognoza miejsca na dane.....                                 | 41 |
| 21. Alerty pojemnościowe.....                                       | 41 |
| 21.1. Checklista capacity planning.....                             | 41 |
| 22. TDE i szyfrowanie backupów.....                                 | 42 |
| 22.1. Co szyfruje TDE.....                                          | 42 |
| 22.2. Hierarchia kluczy TDE.....                                    | 42 |
| 22.3. Czy zwykły backup bazy TDE jest szyfrowany.....               | 43 |
| 22.4. TDE a Backup Encryption.....                                  | 43 |
| 23. Certyfikaty, klucze i ich backup.....                           | 44 |
| 23.1. Backup certyfikatu TDE.....                                   | 44 |
| 23.2. Backup master key.....                                        | 44 |
| 23.3. Gdzie przechowywać certyfikaty.....                           | 44 |
| 23.4. Inwentaryzacja baz z TDE.....                                 | 45 |
| 24. Restore zaszyfrowanej bazy na innym serwerze.....               | 45 |
| 24.1. Procedura restore krok po kroku.....                          | 45 |
| 24.2. Typowy błąd przy braku certyfikatu.....                       | 46 |
| 25. Backup Encryption jako dodatkowa warstwa.....                   | 46 |
| 25.1. Przygotowanie certyfikatu dla backup encryption.....          | 47 |
| 25.2. Backup z opcją ENCRYPTION.....                                | 47 |
| 25.3. Kiedy używać Backup Encryption.....                           | 48 |
| 26. Checklista bezpieczeństwa TDE i backupów.....                   | 48 |
| 26.1. Checklista przed włączeniem TDE.....                          | 48 |
| 26.2. Checklista miesięczna.....                                    | 48 |
| 26.3. Zasada retencji certyfikatów.....                             | 48 |
| 27. Uprawnienia do backupów i zasada minimalnych uprawnień.....     | 48 |
| 27.1. Minimalne uprawnienie SQL do backupu.....                     | 49 |
| 27.2. Czego nie dawać do backupu.....                               | 49 |
| 27.3. SQL permission a NTFS permission.....                         | 49 |
| 27.4. Backup jako ryzyko wycieku danych.....                        | 49 |
| 28. Projekt kont SQL Server: usługi, DBA, aplikacje i migracje..... | 50 |
| 28.1. Minimalny zestaw kont i grup.....                             | 50 |
| 28.2. Trzy konta dla aplikacji.....                                 | 50 |
| 28.3. Monitoring bez uprawnienia db_owner.....                      | 51 |
| 29. Konta per klaster i gMSA.....                                   | 51 |
| 29.1. Przykład dla trzech klastrów.....                             | 51 |
| 29.2. Dlaczego nie jedno konto dla wszystkich klastrów.....         | 51 |
| 29.3. Dlaczego gMSA jest lepsze od zwykłego konta domenowego.....   | 51 |
| 29.4. Foldery backupowe per klaster.....                            | 52 |
| 30. SPN, Kerberos i problem double-hop.....                         | 52 |
| 30.1. Co to jest double-hop.....                                    | 52 |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 30.2. Jak sprawdzić schemat uwierzytelnienia na SQL Server.....         | 52 |
| 30.3. Przykładowe SPN dla SQL Server.....                               | 53 |
| 31. Delegacja: unconstrained, constrained i RBCD.....                   | 53 |
| 31.1. Unconstrained delegation.....                                     | 53 |
| 31.2. Constrained delegation.....                                       | 53 |
| 31.3. Resource-Based Constrained Delegation.....                        | 54 |
| 31.4. Czy gMSA rozwiązuje problem unconstrained delegation.....         | 54 |
| 32. Audyt kont, ról i delegacji.....                                    | 54 |
| 32.1. Audyt ról serwerowych.....                                        | 54 |
| 32.2. Audyt db_owner i db_backupoperator we wszystkich bazach.....      | 55 |
| 32.3. Audyt unconstrained delegation w domenie.....                     | 56 |
| 32.4. Inwentaryzacja kont usług SQL Server.....                         | 56 |
| 33. Checklista least privilege dla backupów i restore.....              | 56 |
| 33.1. Konta usług.....                                                  | 56 |
| 33.2. Backupy.....                                                      | 57 |
| 33.3. Aplikacje i migracje.....                                         | 57 |
| 33.4. Kerberos i delegacja.....                                         | 57 |
| 34. Monitoring backupów - dlaczego zielony job nie wystarcza.....       | 58 |
| 34.1. Co trzeba monitorować.....                                        | 58 |
| 34.2. Podstawowy raport stanu backupów.....                             | 58 |
| 34.3. Monitorowanie wieku backupu LOG.....                              | 59 |
| 35. Alerty operacyjne dla backupów i łańcucha logów transakcyjnych..... | 60 |
| 35.1. Minimalny zestaw alertów.....                                     | 60 |
| 35.2. Backup podejrzenie mały.....                                      | 61 |
| 35.3. Backup trwa zbyt długo.....                                       | 62 |
| 36. RESTORE VERIFYONLY, test restore i ich ograniczenia.....            | 62 |
| 36.1. RESTORE VERIFYONLY.....                                           | 63 |
| 36.2. Prawdziwy test restore.....                                       | 63 |
| 37. Automatyczny test restore krok po kroku.....                        | 63 |
| 37.1. Minimalny proces automatycznego testu.....                        | 63 |
| 37.2. Przykładowy restore test FULL backupu.....                        | 63 |
| 37.3. Tabela wyników testów restore.....                                | 64 |
| 37.4. PowerShell jako warstwa automatyzacji.....                        | 65 |
| 38. DBCC CHECKDB po restore i walidacja spójności.....                  | 65 |
| 38.1. Przykład DBCC CHECKDB.....                                        | 65 |
| 38.2. Kiedy wykonywać CHECKDB.....                                      | 65 |
| 38.3. CHECKDB a okno czasowe.....                                       | 66 |
| 39. Raport walidacji backupów i dokumentacja testu.....                 | 66 |
| 39.1. Co powinien zawierać raport.....                                  | 66 |
| 39.2. Zapytanie raportowe z historii walidacji.....                     | 66 |
| 39.3. Minimalny raport dla audytu.....                                  | 67 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 40. Checklista monitoringu i testów restore.....                          | 67 |
| 40.1. Codziennie.....                                                     | 67 |
| 40.2. Tygodniowo.....                                                     | 67 |
| 40.3. Miesięcznie.....                                                    | 67 |
| 40.4. Po każdej zmianie.....                                              | 67 |
| 41. Procedury awaryjne - od backupu do działania po incydencie.....       | 69 |
| 41.1. Zasada pierwsza: zatrzymaj eskalację szkody.....                    | 69 |
| 41.2. Minimalny formularz decyzji restore.....                            | 69 |
| 41.3. Kolejność myślenia w awarii.....                                    | 69 |
| 42. Tail-log backup - ostatnia szansa na minimalizację utraty danych..... | 69 |
| 42.1. Kiedy tail-log backup ma sens.....                                  | 70 |
| 42.2. Kiedy tail-log backup może się nie udać.....                        | 70 |
| 42.3. Przykład tail-log backupu przed restore.....                        | 70 |
| 42.4. Przykład tail-log backupu dla uszkodzonej bazy.....                 | 70 |
| 43. Scenariusz awaryjny: przypadkowe usunięcie danych.....                | 70 |
| 43.1. Cel.....                                                            | 71 |
| 43.2. Przykład osi czasu.....                                             | 71 |
| 43.3. Dwa warianty działania.....                                         | 71 |
| 43.4. Restore pomocniczy do punktu sprzed błędu.....                      | 71 |
| 43.5. Checklista przed skopiowaniem danych z bazy pomocniczej.....        | 72 |
| 44. Scenariusz awaryjny: uszkodzenie bazy danych.....                     | 72 |
| 44.1. Czego nie robić w pierwszej kolejności.....                         | 72 |
| 44.2. Minimalna diagnostyka.....                                          | 72 |
| 44.3. Zalecany kierunek.....                                              | 73 |
| 45. Scenariusz awaryjny: awaria pamięci masowej lub utrata serwera.....   | 73 |
| 45.1. Co musi istnieć poza plikami BAK/TRN.....                           | 73 |
| 45.2. Odtworzenie na nowym serwerze - kolejność.....                      | 73 |
| 45.3. Kontrola orphaned users.....                                        | 74 |
| 46. Scenariusz awaryjny: baza chroniona TDE po awarii.....                | 74 |
| 46.1. Minimalny zestaw potrzebny do restore.....                          | 74 |
| 46.2. Odtworzenie certyfikatu na nowym serwerze.....                      | 74 |
| 46.3. Test kontrolny certyfikatów.....                                    | 75 |
| 47. Scenariusz awaryjny: ransomware lub podejrzenie kompromitacji.....    | 75 |
| 47.1. Zasady postępowania.....                                            | 75 |
| 47.2. Restore w izolacji.....                                             | 75 |
| 48. Runbook restore - szablon operacyjny.....                             | 76 |
| 48.1. Sekcja decyzyjna.....                                               | 76 |
| 48.2. Sekcja techniczna.....                                              | 76 |
| 48.3. Minimalny szablon komend restore.....                               | 76 |
| 49. Dokumentacja po incydencie restore.....                               | 77 |
| 49.1. Co powinno znaleźć się w raporcie.....                              | 77 |

|                                                  |    |
|--------------------------------------------------|----|
| 49.2. Najważniejsze pytania po awarii.....       | 77 |
| 50. Checklista procedur awaryjnych.....          | 78 |
| 50.1. Przed awarią.....                          | 78 |
| 50.2. W czasie awarii.....                       | 78 |
| 50.3. Po awarii.....                             | 78 |
| 51. Checklista końcowa standardu DBA.....        | 78 |
| 51.1 Backupy.....                                | 78 |
| 51.2 Restore.....                                | 79 |
| 51.3 Bezpieczeństwo.....                         | 79 |
| 51.4 Pojemność i monitoring.....                 | 79 |
| 52. Plan wdrożenia standardu backup/restore..... | 79 |
| 53. Źródła i podstawa opracowania.....           | 80 |
| 54. Zakończenie.....                             | 81 |
| Załącznik A. Spis załączników i skryptów.....    | 82 |
| Słownik pojęć.....                               | 83 |



# Wstęp

Materiał jest przeznaczony dla administratorów SQL Server, osób utrzymujących systemy Windows z bazami SQL Server, developerów odpowiedzialnych za środowiska produkcyjne oraz trenerów, którzy chcą pokazać backup i restore nie jako zbiór poleceń, ale jako kompletny standard operacyjny.

Najważniejsza myśl tego przewodnika jest prosta: backup nie jest celem samym w sobie. Backup jest tylko środkiem do osiągnięcia celu, którym jest skuteczne odtworzenie danych i działania systemu po awarii, błędzie użytkownika, uszkodzeniu bazy, utracie serwera albo incydencie bezpieczeństwa.

Dokument łączy trzy perspektywy: oficjalną dokumentację SQL Server, praktykę administracyjną oraz scenariusze laboratoryjne, które można samodzielnie powtórzyć. Dlatego obok wyjaśnień znajdują się zapytania T-SQL, checklisty, runbooki i przykłady decyzji projektowych dla różnych typów środowisk.

Celem tego materiału nie jest opisanie każdej opcji polecenia BACKUP i RESTORE. Celem jest pokazanie, jak myśleć o strategii backupu i odtwarzania tak, jak powinien myśleć DBA odpowiedzialny za produkcję: przez RPO, RTO, łańcuch logów transakcyjnych, test restore, bezpieczeństwo certyfikatów, uprawnienia, monitoring oraz procedury awaryjne.

Ten przewodnik powstał z bardzo praktycznego powodu: w wielu środowiskach SQL Server backup istnieje, job świeci się na zielono, ale nikt nie ma pewności, czy w sytuacji awarii da się odtworzyć bazę szybko, poprawnie i do właściwego punktu w czasie.

## 1. Backup to nie strategia

Backup jest tylko jednym z elementów bezpieczeństwa danych. Strategia zaczyna się dopiero wtedy, gdy jesteśmy w stanie odpowiedzieć na pytanie: jak odtworzyć bazę, na jaki moment, z jakich plików i w jakim czasie.

Zielony status joba SQL Server Agent oznacza wyłącznie, że konkretna operacja zakończyła się sukcesem. Nie oznacza, że plik istnieje, że jest kompletny, że mamy wymagany łańcuch LOG, że mamy certyfikat TDE ani że restore został kiedykolwiek przetestowany.

## 2. RPO, RTO i odpowiedzialność DBA

RPO określa, ile danych firma może maksymalnie stracić. RTO określa, jak szybko system musi wrócić po awarii. Harmonogram backupów powinien wynikać z tych dwóch wartości, a nie z wygody administratora.

DBA nie odpowiada tylko za wykonanie backupu. Odpowiada za możliwość odtworzenia środowiska w akceptowalnym czasie i do akceptowalnego punktu.

### 3. Rodzaje backupów SQL Server

Podstawowe typy backupów w SQL Server to FULL, DIFFERENTIAL oraz LOG. Dodatkowo istnieją backupy COPY\_ONLY, file/filegroup oraz partial. W praktyce produkcyjnej najczęściej projektujemy łańcuch: FULL + DIFF + LOG.

FULL daje punkt startowy, DIFF skraca drogę od FULL-a, a LOG pozwala dojść do konkretnego punktu w czasie.

| Typ  | Najważniejsza funkcja              | Uwagi DBA                                                                                            |
|------|------------------------------------|------------------------------------------------------------------------------------------------------|
| FULL | Pełny punkt startowy restore       | Zwykły FULL resetuje bazę dla DIFF. COPY_ONLY nie resetuje.                                          |
| DIFF | Zmiany od ostatniego zwykłego FULL | DIFF rośnie do kolejnego FULL. Nie jest przyrostowy względem poprzedniego DIFF.                      |
| LOG  | Fragment logu transakcyjnego       | Wymaga FULL/BULK_LOGGED i aktywnego łańcucha logów transakcyjnych. Umożliwia point-in-time recovery. |

# To dopiero fragment

Pełna publikacja zawiera rozbudowane wyjaśnienia, skrypty T-SQL, checklists, runbooki i scenariusze do wykorzystania jako podstawa własnego standardu DBA.

## W pełnej wersji znajdziesz m.in.:

- RPO, RTO oraz projektowanie strategii backupu
- FULL, DIFF, LOG, LSN i point-in-time restore
- wydajność backupu i restore dla dużych baz
- capacity planning i retencja
- TDE, szyfrowanie, certyfikaty i least privilege
- testy restore, DBCC CHECKDB i procedury awaryjne



Zeskanuj i zobacz pełną wersję

**Kup pełną publikację**

<https://cart.easy.tools/checkout/sqlmaniak/sql-server-backup-i-restore-praktyczny-przewodnik-dba>