ERPOLOGIA • RUNBOOK

Pierwsze 60 minut incydentu enova365

Dowody, oś czasu i decyzje przed pierwszą zmianą

5	60	1
ETAPÓW	MINUT	PAKIET DOWODOWY

wersja pilotażowa 1.0 | 1 września 2026

KARTA SZYBKIEGO DZIAŁANIA

Godzina, która zachowuje dowody

Runbook zaczyna się w chwili potwierdzenia incydentu. Jeżeli zagrożone jest bezpieczeństwo, integralność danych albo ciągłość kluczowego procesu, zastosuj właściwą procedurę krytyczną organizacji.

Czas	Działanie	Rezultat
00–15	Ogranicz wpływ	Potwierdź zakres, czas i krytyczność. Wstrzymaj zmiany, które mogłyby usunąć ślady.
15–30	Zapisz kontekst	Wersja, baza, operator, interfejs, host, kroki, oczekiwany i rzeczywisty rezultat.
30–45	Sprawdź zdrowie	Procesy, healthcheck, logi, metryki, trace, dostępność SQL i zależności sieciowe.
45–55	Zbuduj oś czasu	Połącz zdarzenia WEB, Server, Scheduler, CommHub i SQL w jednym oknie czasu.
55–60	Wybierz test	Test ma potwierdzić albo wykluczyć konkretną hipotezę i posiadać punkt powrotu.

Zasada

Restart jest działaniem diagnostycznym tylko wtedy, gdy wcześniej zapisano stan, wiadomo co restart ma sprawdzić i istnieje sposób oceny rezultatu.

KROK 1

Karta przyjęcia incydentu

Nie zapisuj „program nie działa”. Zapisz zdarzenie tak, aby druga osoba mogła je odtworzyć bez rozmowy z autorem zgłoszenia.

Numer incydentu	
Data i dokładny czas	
Zgłaszający / operator	
Baza / środowisko	
Wersja enova365	
Interfejs	□ okienkowy □ WEB □ API □ mobilny
Host / stanowisko	
Zakres wpływu	□ jedna osoba □ grupa □ wszyscy □ proces automatyczny
Kroki odtworzenia	
Oczekiwany rezultat	
Rzeczywisty rezultat	
Zmiany przed incydentem	
Osoba prowadząca	

KROK 2

Sprawdź warstwy, nie tylko proces

Jedna warstwa może działać, gdy inna nie obsługuje ruchu. Zacznij od mapy zależności i przejdź w kierunku bazy danych.

Warstwa	Dowód	Przykładowy stan
WEB / WebApi	żądanie, kod odpowiedzi, czas, trace	healthy / degraded / unhealthy
Router	aktywny endpoint i routing	serving / not serving
Server	sesja, logika biznesowa, komunikacja SQL	serving / not serving
Scheduler	zadanie, kolejka, czas wykonania	serving / not serving
CommHub	kanał, subskrypcja, komunikacja	serving / not serving
SQL Server	połączenie, blokady, czas, Reads, plan	własny monitoring SQL

Kontrola healthcheck

□ Czy healthcheck był skonfigurowany przed incydentem?

□ Jaki stan zwraca każda instancja?

□ Czy stan zmienia się w czasie?

□ Czy monitoring widzi tę samą instancję, którą obsługuje użytkownik?

□ Czy dashboard jest dostępny tylko dla uprawnionych osób?

Źródła: Systemowe, s. 619, 624, 626, 635 i 720–721.

KROK 3

Zbierz minimalny, spójny zestaw dowodów

Zbieraj tylko dane potrzebne do diagnozy. Każdy plik oznacz środowiskiem, źródłem, zakresem czasu i strefą czasową.

Rodzaj	Zakres	Ochrona
Opis	formularz incydentu	brak sekretów
Konfiguracja	wartość efektywna i źródło nadpisania	usuń hasła, tokeny i klucze
Logi	WEB, Server, Scheduler, CommHub, Event Log	ogranicz zakres czasu
Trace	trace_id, span_id, czasy operacji	pełny SQL tylko po świadomej decyzji
Metryki	CPU, RAM, liczba żądań, kolejki	zapisz jednostkę i interwał
SQL	Duration, Reads, plan, blokady, indeksy	najpierw odczytowo
Zrzut	PID, czas, warunek wyzwolenia	dane wrażliwe; kontroluj dostęp

Ryzyko telemetrii

Ustawienie CollectFullSqlStatement może umieścić pełną treść SQL w trace. Dokumentacja ostrzega o możliwym wycieku danych wrażliwych; domyślna wartość jest wyłączona.

Źródła: Systemowe, s. 655–656.

KROK 4

Zbuduj oś czasu w LogCenter

Celem nie jest zgromadzenie największej liczby plików. Celem jest pokazanie kolejności zdarzeń prowadzących do objawu użytkownika.

Czas	Źródło	Zdarzenie	Status
10:14:08.114	WEB	żądanie rozpoczęte; trace 7f9a...	fakt
10:14:08.391	Server	otwarcie sesji i rozpoczęcie operacji	fakt
10:14:08.612	SQL	zapytanie; rośnie Reads	fakt
10:14:43.804	WEB	odpowiedź błędu po 35,7 s	fakt
10:14:43.900	Analiza	podejrzenie nieoptymalnego planu	hipoteza

Kontrola osi czasu

□ Wszystkie źródła używają tej samej strefy czasowej.

□ Rozbieżność zegarów została zmierzona.

□ Zdarzenia mają identyfikator źródła i procesu.

□ Fakty i hipotezy są oznaczone osobno.

□ Filtry użyte w analizie są zapisane w pakiecie.

TOR SQL

Duration to nie jedyny sygnał

Analiza jest odczytowa. Zmianę indeksu, statystyk lub planu wykonuj dopiero na kopii i po ustaleniu testu porównawczego.

□ Policz wszystkie zapytania w badanym oknie.

□ Wskaż najdłuższe zapytanie i jego Reads.

□ Sprawdź, czy najwyższy Duration ma również najwyższe Reads.

□ Zgrupuj podobne zapytania i policz ich powtarzalność.

□ Policz zapytania przekraczające uzgodniony próg czasu.

□ Zapisz plan wykonania dla kandydatów do dalszej analizy.

□ Sprawdź stan indeksów, statystyki i page_count.

Nie stosuj automatycznej recepty

Indeks przyspiesza odczyt, ale zwiększa koszt dodawania, modyfikacji i usuwania. Zły plan może zależeć od parametrów, statystyk, indeksów i cache. Zmiana wymaga kontekstu i pomiaru przed/po.

Obserwacja	Wniosek roboczy	Następny dowód
wysoki Duration, niski Reads	możliwe oczekiwanie lub blokada	waits, blocking, oś czasu
wysoki Duration i Reads	kosztowny odczyt	plan, selektywność, indeksy
wiele podobnych zapytań	problem powtarzalności	źródło wywołań i cache

Źródła: Systemowe, s. 459, 463, 465–466, 1141 i 1151–1153.

TOR PROCESU

Kiedy potrzebny jest zrzut pamięci

Zrzut jest materiałem szczególnie wrażliwym. Wykonuj go na podstawie uzgodnionej procedury i przechowuj tylko tak długo, jak wymaga analiza.

Objaw	Metoda	Metadane
Nieobsłużony wyjątek	ProcDump przed operacją; zrzut na zdarzeniu	PID, czas, wersja, kroki
Narastające użycie RAM	2–4 zrzuty przy kolejnych progach	zużycie pamięci i odstępy
Zawieszenie	seria zrzutów w trakcie zjawiska	czas każdego zrzutu
Szybki jednorazowy zapis	Task Manager lub Process Explorer	ograniczona wartość diagnostyczna

Najczęstszy błąd

Polecenie przechwytywania należy przygotować przed badaną operacją. Zrzut wykonany dopiero po pojawieniu się okna błędu może nie zawierać chwili powstania problemu.

□ Zweryfikowano właściwy PID.

□ Katalog docelowy ma wystarczająco dużo miejsca.

□ Dostęp do pliku jest ograniczony.

□ Plik otrzymał znacznik czasu i sumę SHA-256.

□ Ustalono termin bezpiecznego usunięcia.

Źródła: Systemowe, s. 454–457.

KROK 5

Wybierz najmniejszy test rozróżniający hipotezy

Test ma mieć oczekiwany rezultat, miernik i punkt powrotu. Nie łącz kilku zmian w jednym kroku.

Decyzja	Kiedy	Warunek
Obserwuj	wpływ niski, stan stabilny	zbierz dodatkowy cykl danych
Testuj na kopii	hipoteza dotyczy konfiguracji, SQL lub dodatku	porównaj przed/po
Restartuj komponent	dowody wskazują konkretny proces	zapisz stan i sprawdź healthcheck
Wycofaj zmianę	incydent koreluje z wdrożeniem	użyj zatwierdzonego rollback
Eskaluje	brak narzędzi, ryzyko danych lub awaria producenta	przekaż pakiet dowodowy

Hipoteza	
Test	
Oczekiwany rezultat	
Miernik	
Punkt powrotu	
Zatwierdził	

PAKIET ESKALACYJNY

Przekaż dowody, nie przypadkowy katalog logów

Odbiorca powinien zrozumieć problem, odtworzyć oś czasu i zobaczyć, które hipotezy zostały już sprawdzone.

□ Karta incydentu z dokładnym czasem i strefą czasową.

□ Wersja enova365, SQL Server, systemu i dodatków.

□ Diagram komponentów i portów używanych w środowisku.

□ Status healthcheck każdej istotnej instancji.

□ Logi ograniczone do uzgodnionego przedziału czasu.

□ Trace lub identyfikator korelacji, jeśli występuje.

□ Wyniki odczytowej analizy SQL i użyte filtry.

□ Zrzuty pamięci wraz z PID i warunkiem przechwycenia.

□ Lista wykonanych testów oraz ich rezultatów.

□ Lista usuniętych lub zamaskowanych danych wrażliwych.

□ Manifest plików i sumy SHA-256.

Plik	Źródło	Zakres czasu	SHA-256

PO INCYDENCIE

Zmień zdarzenie w trwałą poprawę

Przegląd nie służy szukaniu winnego. Ma zmniejszyć ryzyko powtórzenia oraz skrócić czas detekcji i diagnozy.

1. Co dokładnie było skutkiem dla użytkowników i procesu biznesowego?

2. Kiedy incydent rozpoczął się, został wykryty, ograniczony i zakończony?

3. Które dowody były dostępne od razu, a których brakowało?

4. Która hipoteza została potwierdzona i na jakiej podstawie?

5. Jakie działanie przywróciło usługę, a jakie usunęło przyczynę?

6. Który monitoring, alert albo runbook należy zmienić?

7. Kto jest właścicielem działania, jaki jest termin i test odbioru?

Definicja zamknięcia incydentu

Usługa działa, przyczyna lub granica wiedzy jest udokumentowana, działania następcze mają właścicieli, a pakiet dowodowy jest przechowywany zgodnie z zasadami bezpieczeństwa.

ŹRÓDŁA I ODPOWIEDZIALNOŚĆ

Materiał wersjonowany

Runbook został przygotowany dla niezależnego programu ERPologia. Nie jest oficjalną instrukcją producenta ani zamiennikiem procedur bezpieczeństwa organizacji.

□ Systemowe, s. 619, 624, 626 i 631 - komponenty serwera, komunikacja i cykl życia.

□ Systemowe, s. 635 - healthcheck backendu i front-endu.

□ Systemowe, s. 637 i 642 - priorytety konfiguracji i serwer logiki biznesowej.

□ Systemowe, s. 655–656 - telemetria, OTLP i bezpieczeństwo pełnego SQL.

□ Systemowe, s. 720–721 - Orchestrator Dashboard, dzienniki i ślady.

□ Systemowe, s. 454–457 - zrzuty pamięci i ProcDump.

□ Systemowe, s. 459, 463, 465–466 - indeksy i plany zapytań.

□ Systemowe, s. 1141, 1144 i 1151–1153 - metodyka analizy wydajności.

Ważne

Nazwy ustawień, możliwości komponentów i zalecenia mogą zależeć od wersji enova365. Przed użyciem procedury potwierdź ją na zainstalowanej wersji i w dokumentacji właściwej dla środowiska.