

Diagnostyka systemu Windows — dzienniki i wydajność

Czas: 2 × 45 min

praca indywidualna lub w parach

Cel: Wyszukiwanie przyczyn awarii i spowolnień Windows na podstawie dzienników zdarzeń, Monitora niezawodności i narzędzi wydajności oraz przygotowanie raportu z wnioskami.

Po zajęciach potrafisz:

- filtruje dzienniki System i Aplikacja w Podglądzie zdarzeń według poziomu, źródła i identyfikatora
- interpretuje typowe zdarzenia awarii (41, 6008, 7, 1001, 1000)
- korzysta z Monitora niezawodności, Menedżera zadań i Monitora zasobów
- mierzy czas uruchamiania systemu i wskazuje programy autostartu, które go wydłużają
- formułuje wnioski diagnostyczne i zalecenia

Sprzęt i materiały

- komputer stacjonarny (system szkolny lub Windows 11 z drugiego dysku)
- stoper (telefon)

Oprogramowanie

- **Podgląd zdarzeń (eventvwr.msc), Monitor niezawodności (perfmon /rel)** — wbudowane w Windows 11
- **Menedżer zadań, Monitor zasobów (resmon)** — wbudowane
- **PowerShell — Get-WinEvent** — filtrowanie dzienników z wiersza poleceń

Bezpieczeństwo

- Zadanie jest wyłącznie diagnostyczne: nie czyść dzienników, nie wyłączaj usług i nie usuwaj programów autostartu w systemie szkolnym — zmiany wolno wprowadzać tylko w Windows 11 z drugiego dysku.
- Dzienniki mogą zawierać nazwy użytkowników i komputerów — w sprawozdaniu zamaskuj je na zrzutach ekranu.
- Nie kończ w Menedżerze zadań procesów systemowych (np. `csrss.exe`, `wininit.exe`, `lsass.exe`) — spowoduje to natychmiastową awarię systemu.

Przebieg zadania

1 Podgląd zdarzeń

1. Uruchom `eventvwr.msc`. W Dzienniki systemu Windows → System użyj „Filtruj bieżący dziennik...”: poziom Krytyczny i Błąd, ostatnie 30 dni. Zapisz liczbę zdarzeń.
2. W tym samym filtrze wpisz identyfikatory `41,6008,7,1001`. Dla każdego znalezionej zdarzenia zapisz datę, źródło i krótki opis.
3. W dzienniku Aplikacja wyfiltruj zdarzenia o identyfikatorze `1000` (błąd aplikacji). Zapisz nazwy aplikacji, które uległy awarii.
4. Wykonaj to samo w PowerShell: `Get-WinEvent -FilterHashtable @{LogName='System'; Id=41,6008} -MaxEvents 10 | Format-Table TimeCreated, Id, ProviderName -AutoSize`. Porównaj z wynikiem Podglądu zdarzeń.
5. Utwórz widok niestandardowy „Awarie” (Akcja → Utwórz widok niestandardowy) z identyfikatorami 41, 6008, 1001 z dziennika System i zrób jego zrzut.

2 Monitor niezawodności

1. Uruchom `perfmon /rel`. Odczytaj indeks stabilności (1–10) i zapisz dni, w których spadał.
2. Kliknij dzień z czerwonym symbolem błędu i zapisz szczegóły dwóch zdarzeń (źródło, opis). Powiąż je ze zdarzeniami z Podglądu zdarzeń.
3. Kliknij „Wyświetl wszystkie raporty problemów” i zapisz, która aplikacja lub składnik systemu zgłaszała problemy najczęściej.

3 Czas uruchamiania i autostart

1. W Podglądzie zdarzeń otwórz Dzienniki aplikacji i usług → Microsoft → Windows → Diagnostics-Performance → Operacyjny i odszukaj zdarzenie 100. Zapisz czas rozruchu z ostatnich pięciu uruchomień. Jeśli dziennik jest niedostępny — zmierz stoperem czas od włączenia do pulpitu gotowego do pracy.
2. W Menedżerze zadań → Aplikacje autostartu posortuj według kolumny „Wpływ na uruchamianie”. Zapisz programy o wysokim wpływie.
3. Tylko w Windows 11 z drugiego dysku: wyłącz dwa programy autostartu o największym wpływie, uruchom ponownie i zmierz czas rozruchu jeszcze raz.

4 Wydajność w czasie pracy

1. Uruchom przeglądarkę z kilkoma kartami i dowolny program biurowy. W Menedżerze zadań → Procesy posortuj według CPU, Pamięci i Dysku — zapisz po dwa najbardziej obciążające procesy.
2. W `resmon` na karcie Dysk odczytaj, które procesy najwięcej zapisują i odczytują, a na karcie Pamięć — ile pamięci jest „W użyciu”, „Zmodyfikowane”, „W gotowości” i „Wolne”.
3. Jako administrator wykonaj `perfmon /report` (raport diagnostyki systemu, ok. 60 s). Zapisz ostrzeżenia z sekcji „Wyniki diagnostyki”.
4. Na podstawie wszystkich wyników przygotuj trzy wnioski diagnostyczne i trzy zalecenia dla użytkownika komputera.

W sprawozdaniu umieść

- ☐ tabela znalezionych zdarzeń awarii z interpretacją
- ☐ zrzut widoku niestandardowego i Monitora niezawodności (zamaskowane dane osobowe)
- ☐ czasy rozruchu przed i po wyłączeniu programów autostartu
- ☐ lista najbardziej obciążających procesów i programów autostartu
- ☐ wnioski i zalecenia
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Co oznacza zdarzenie 41 (Kernel-Power) i dlaczego samo w sobie nie wskazuje przyczyny awarii?
2. Czym różni się zdarzenie 6008 od zdarzenia 1001 (BugCheck)?
3. Co może oznaczać powtarzające się zdarzenie 7 ze źródła Disk i jakie narzędzie z wcześniejszych zadań wykorzystasz do dalszej diagnozy?
4. Dlaczego duża ilość pamięci „W gotowości” nie oznacza, że brakuje RAM-u?

Kryteria oceny

Kryterium	Punkty
Filtrowanie dzienników i interpretacja zdarzeń	6
Monitor niezawodności	3
Pomiar czasu rozruchu i analiza autostartu	4
Analiza wydajności, wnioski i zalecenia	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).