Case: Wielopoziomowe problemy z wydajnością w sieci korporacyjnej

Opis sytuacji:

W średniej wielkości instytucji użytkownicy zaczęli zgłaszać pogorszenie wydajności sieci, szczególnie w godzinach porannych oraz popołudniowych, czyli w okresach największego obciążenia. Problem ma charakter ogólny i obejmuje zarówno aplikacje wewnętrzne, jak i zewnętrzne systemy (np. platformy zgłoszeniowe czy usługi działające w chmurze).

Do najczęściej obserwowanych symptomów należą:

- znaczne spowolnienie w ładowaniu stron internetowych oraz odczuwalne opóźnienia podczas pracy na mapowanych dyskach sieciowych,
- duże opóźnienia podczas pracy z serwerem plików w centrali,
- sporadyczne, lecz wyraźne „zamrożenia" aplikacji biznesowych korzystających z zasobów sieciowych,
- zwiększona liczba aktywnych sesji TCP na interfejsach brzegowych, przy czym klasyczne systemy monitoringu (np. Zabbix) nie wskazują istotnych przekroczeń przepustowości ani zużycia pasma.

Wstępna diagnoza sugeruje, że problem nie wynika wyłącznie z ograniczeń łącza, lecz ma charakter bardziej złożony – może być powiązany z obciążeniem poszczególnych komponentów infrastruktury, nierównomiernym rozłożeniem ruchu lub specyfiką aplikacji działających w różnych porach dnia.

Źródło problemu

Środowisko korzysta z jednego, wydajnego serwera fizycznego, który współdzielony jest przez wiele wewnętrznych aplikacji oraz baz danych. W godzinach największego obciążenia („godzinach szczytu") obserwowane są okresowe przeciążenia zasobów systemowych. Charakterystyka problemu jest zmienna – w zależności od dnia inne komponenty wywołują nadmierne obciążenie poszczególnych podsystemów, takich jak:

- **warstwa storage** – opóźnienia w dostępie do danych i zwiększone kolejki operacji I/O,
- **zasoby procesora** – intensywne wykorzystanie mocy obliczeniowej skutkujące spadkiem responsywności,

- **sesje użytkowników i aplikacji** – obserwowana jest znacząca liczba aktywnych sesji równoległych.

Wstępna analiza wskazuje, że obciążenie nie ma stałego wzorca – każdy dzień charakteryzuje się innym profilem wykorzystania zasobów. To sugeruje brak jednoznacznego źródła problemu i konieczność przeprowadzenia bardziej szczegółowych badań, w tym:

- identyfikacji aplikacji i procesów generujących największe obciążenie,
- korelacji zdarzeń z harmonogramem prac i aktywności użytkowników,
- analizy trendów w dłuższym horyzoncie czasowym w celu wykrycia powtarzalnych wzorców.

Docelowe rozwiązanie (co ma powstać na hackathon):

Projektowane rozwiązanie ma na celu stworzenie kompleksowego mechanizmu monitorowania i analizy incydentów wydajnościowych, który umożliwi zarówno szybką reakcję w momencie wystąpienia problemu, jak i identyfikację jego źródeł w dłuższym horyzoncie czasowym.

1. **Alertowanie w czasie rzeczywistym**
    a. Opracowanie alertu opartego na wskaźniku RTT (Round Trip Time), który natychmiast poinformuje o wystąpieniu problemu.
    b. Dzięki temu możliwe będzie szybkie reagowanie, jeszcze zanim degradacja usług stanie się zauważalna dla użytkowników końcowych.
2. **Interaktywne dashboardy diagnostyczne**
    a. Stworzenie 2–3 interaktywnych dashboardów, które po uruchomieniu alertu pozwolą szczegółowo wskazać przyczynę problemu.
    b. Dashboardy będą agregować dane z wielu systemów monitorujących i analitycznych, takich jak Zabbix czy Splunk, wykorzystując zapytania API.
    c. Funkcjonalności obejmą m.in.:
        i. identyfikację procesów i usług najbardziej obciążających serwer,
        ii. prezentację TOP 10 URL-i obsługiwanych w danym momencie,
        iii. powiązanie obciążenia infrastruktury z ruchem sieciowym i logami aplikacyjnymi.
    d. Analiza codziennych danych pokazuje, że przyczyny przeciążeń różnią się w zależności od dnia, co potwierdza brak jednoznacznego i powtarzalnego źródła problemu.
3. **Raportowanie i analiza trendów**

a. Automatyczne generowanie raportów dziennych obejmujących okresy największego obciążenia (tzw. godziny szczytu).
b. Raporty będą wskazywały:
    i. jak często występowały problemy,
    ii. które komponenty odpowiadały za przeciążenia,
    iii. w jakich okolicznościach pojawiały się nieprawidłowości.
c. Analiza raportów w cyklu tygodniowym i miesięcznym umożliwi precyzyjne określenie przyczyn oraz wybór optymalnych działań korygujących.

Efektem końcowym będzie narzędzie, które łączy detekcję w czasie rzeczywistym z analizą długoterminową, umożliwiając zarówno bieżące rozwiązywanie problemów, jak i strategiczne planowanie działań optymalizacyjnych.