7. Wprowadzenie do monitorowania w Windows Server

7.1. Rola monitorowania w zarządzaniu serwerem

Monitorowanie w Windows Server pełni kluczową rolę w zapewnieniu ciągłości działania, wydajności i bezpieczeństwa systemu. Administratorzy mogą dzięki niemu szybko identyfikować i rozwiązywać problemy, śledzić zużycie zasobów oraz analizować trendy i planować rozbudowę infrastruktury. Skuteczne monitorowanie pozwala również spełnić wymagania zgodności z przepisami i standardami.

7.2. Przegląd narzędzi dostępnych w Windows Server do monitorowania

Windows Server oferuje szereg narzędzi wbudowanych i opcjonalnych, umożliwiających monitorowanie systemu. Najważniejsze z nich to:

- Monitor zasobów (Resource Monitor) – narzędzie GUI pozwalające śledzić CPU, RAM, dyski i sieć w czasie rzeczywistym.
- Menedżer zadań (Task Manager) – szybki podgląd na działające procesy i użycie zasobów.
- Performance Monitor (PerfMon) – zaawansowane monitorowanie wydajności z możliwością tworzenia zestawów liczników.
- Event Viewer (Podgląd zdarzeń) – narzędzie do przeglądania dzienników systemowych, aplikacji i zabezpieczeń.
- Reliability Monitor – wykres stabilności systemu z historią błędów i ostrzeżeń.
- Server Manager – konsola do zarządzania rolami i funkcjami, zawiera także podgląd podstawowych alertów.
- Windows Admin Center – nowoczesne narzędzie centralne do zarządzania i monitorowania wielu serwerów z GUI.
- PowerShell + WMI/CIM – skrypty do automatyzacji monitorowania i zbierania danych.
- System Center Operations Manager (SCOM) – rozwiązanie klasy enterprise do centralnego monitorowania środowisk IT.

7.3. Monitorowanie wydajności serwera

Monitorowanie wydajności w Windows Server opiera się głównie na narzędziu Performance Monitor. Umożliwia ono tworzenie własnych zestawów liczników (Data Collector Sets), które mogą śledzić:

- Zużycie procesora (Processor Time, Queue Length)
- Pamięć RAM (Available MBytes, Pages/sec)
- Dyski (Disk Queue Length, Disk Read/Write Bytes/sec)
- Sieć (Bytes Total/sec, Packets/sec)
- Usługi i procesy (np. SQL Server, IIS)

Można tworzyć alerty, rejestrować dane do plików oraz analizować wydajność historycznie lub w czasie rzeczywistym.

Dodatkowo, polecenia PowerShell, takie jak Get-Counter, Measure-Command, Get-Process i Get-EventLog, umożliwiają zbieranie danych w sposób zautomatyzowany.

7.4. Monitorowanie logów systemowych

Podgląd zdarzeń (Event Viewer) to podstawowe narzędzie do analizy logów systemowych. Umożliwia przeglądanie dzienników takich jak:

- System – logi jądra systemu operacyjnego, sterowników, urządzeń.
- Application – logi z aplikacji i usług systemowych.
- Security – logi zdarzeń związanych z bezpieczeństwem, logowaniami, próbami nieautoryzowanego dostępu.
- Setup – logi instalacyjne ról, aktualizacji itp.
- Forwarded Events – logi z innych komputerów (subskrypcje).

Administratorzy mogą tworzyć widoki niestandardowe, filtry, a także eksportować logi do analizy offline lub do systemów SIEM.

W PowerShell logi można analizować np. za pomocą poleceń:
- Get-EventLog (dla starszych dzienników)
- Get-WinEvent (nowocześniejsze, bardziej wydajne)
- wevtutil (narzędzie CLI do eksportu/importu logów)

Podsumowanie

Skuteczne monitorowanie serwera to kluczowy element zarządzania systemem Windows Server. Dzięki zastosowaniu odpowiednich narzędzi, administratorzy mogą proaktywnie identyfikować problemy, utrzymywać wydajność i spełniać wymogi audytowe oraz bezpieczeństwa.