T: <u>Oprogramowanie monitorujące lokalne sieci komputerowe.</u>

Polecenie do samodzielnego przeanalizowania:

```
at \\s04st01 10:11 /interactive cmd.exe
schtasks /create /S s04st01 ...
tasklist /svc
taskkill /S s04st01 /IM explorer.exe
sc config schedule start= demand
sc \\host create nazwa binpath= c:\nazwa.exe type= own start= auto
net start schedule
net stop mpssvc
apt-get install wavemon
watch -n 1 cat /proc/net/wireless
iwconfig wlan0
```

Do najważniejszych parametrów monitorowania sieci zaliczamy:
- sprawdzenie dostępności komputerów i urządzeń sieciowych,
- sprawdzenie dostępności usług sieciowych,
- sprawdzenie obciążenia łączy sieciowych,
- sprawdzenie obciążenia serwerów,
- kontrolowanie zdarzeń na urządzeniach sieciowych i serwerach.

Zadania związane z monitorowaniem wydajności:
- tworzenie wykresów danych dotyczących wydajności,
- tworzenie raportów danych dotyczących wydajności,
- tworzenie dzienników,
- tworzenie alertów.

Najważniejsze wskazówki dotyczące monitorowania wydajności:
- przygotowanie konfiguracji monitorowania,
- utrzymanie niskiego obciążenie związanego z monitorowaniem,
- konfiguracja rozmiarów plików i miejsca zajmowanego przez pliki dziennika,
- analiza wyników monitorowania wydajności i wyznaczanie poziomów odniesienia dla wydajności,
- ustawianie alertów,
- dostrajanie wydajności,
- planowanie z wyprzedzeniem.

Zalety stosowania monitoringu sieci:
- bieżąca kontrola parametrów sieci,
- wczesne wykrywanie problemów sieciowych pozwalające na podjęcie szybkich działań zapobiegawczych,
- możliwość wykorzystania wyników monitoringu do dokumentacji sprawozdawczej,
- i inne.

Zadanie1:

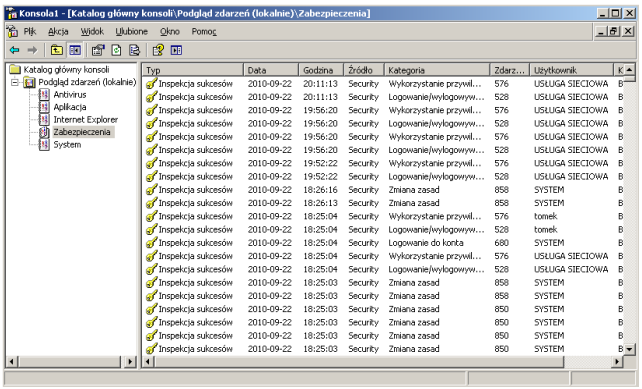
Zapoznaj się z zawartością systemowych dzienników zdarzeń przy twoim stanowisku komputerowym.

Usługa **Dziennik zdarzeń** jest uruchamiana automatycznie przy starcie systemu Windows i ze względów bezpieczeństwa nie można zmienić jej typu uruchamiania. Domyślnie komputer z systemem operacyjnym z rodziny Windows Server rejestruje zdarzenia w trzech rodzajach dzienników zdarzeń:
- **Dziennik aplikacji** zawiera zdarzenia zarejestrowane przez aplikacje lub programy. Na przykład program bazy danych może zarejestrować w nim błąd pliku. O tym, które zdarzenia są rejestrowane, decydują projektanci aplikacji.
- **Dziennik zabezpieczeń** rejestruje zdarzenia, takie jak prawidłowe i nieprawidłowe próby logowania, jak również zdarzenia związane z wykorzystaniem zasobów, na przykład tworzenie, otwieranie lub usuwanie

plików i innych obiektów. Na przykład jeśli włączono inspekcję logowania, w dzienniku zabezpieczeń będą rejestrowane próby zalogowania się do systemu.
- **Dziennik systemu** zawiera zdarzenia zarejestrowane przez składniki systemu Windows. Zapisywane są w nim, na przykład, niepowodzenia podczas procesu ładowania sterownika lub innego składnika systemu w czasie autostartu. Typy zdarzeń rejestrowanych przez składniki systemu są wstępnie określone przez serwer.

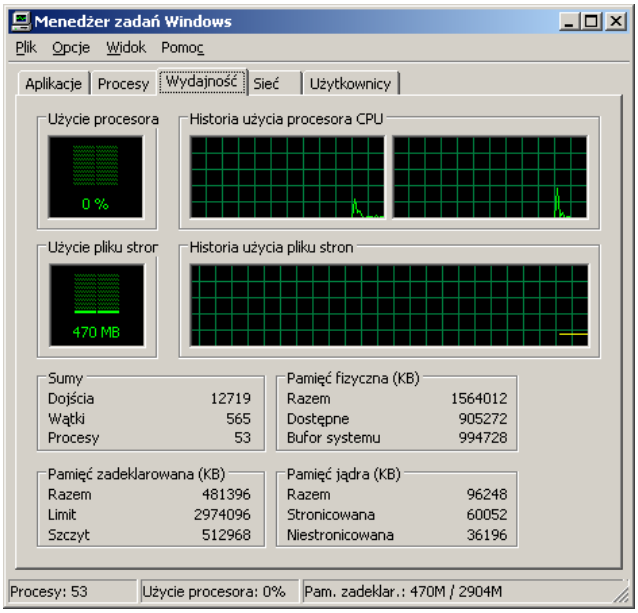
Komputer z systemem operacyjnym z rodziny Windows Server, skonfigurowany jako kontroler domeny, rejestruje zdarzenia w dwóch dodatkowych dziennikach:
- **Dziennik usługi katalogowej** zawiera zdarzenia zarejestrowane przez usługę Active Directory systemu Windows. Zapisywane są w nim, na przykład, problemy z połączeniem serwera z katalogiem globalnym.
- **Dziennik usługi replikacji plików** zawiera zdarzenia zarejestrowane przez usługę replikacji plików systemu Windows. Rejestrowane są w nim, na przykład, niepowodzenia replikacji plików i zdarzenia występujące podczas aktualizowania kontrolerów domeny za pomocą informacji o zmianach w woluminie systemowym.

Komputer z uruchomionym systemem Windows, skonfigurowany jako serwer DNS (Domain Name System), rejestruje zdarzenia w dodatkowym dzienniku:
- **Dziennik serwera DNS** zawiera zdarzenia zarejestrowane przez usługę DNS systemu Windows.



W zależności od usług zainstalowanych na komputerze mogą być na nim dostępne inne typy zdarzeń i inne dzienniki. Odczytywanie dzienników zdarzeń umożliwia nam konsola administracyjna Podgląd zdarzeń (`eventvwr.msc` lub Panel sterowania => Narzędzia administracyjne => Zarządzanie komputerem).

Menedżer zadań udostępnia informacje o programach i procesach uruchomionych na komputerze. Wyświetla także najczęściej używane miary wydajności procesów.
Menedżer zadań może być używany do monitorowania kluczowych wskaźników wydajności komputera. Można zapoznać się ze stanem uruchomionych programów i zakończyć te programy, które przestały odpowiadać. Można także szacować aktywność uruchomionych procesów przy użyciu piętnastu parametrów oraz oglądać wykresy i dane dotyczące użycia procesora CPU i pamięci.
Ponadto, jeśli użytkownik jest połączony z siecią, może wyświetlić stan sieci i sprawdzić, jak ona działa.
Jeśli z komputerem jest połączony więcej niż jeden użytkownik, można sprawdzić, którzy użytkownicy są połączeni i co robią; można także wysłać do nich wiadomość.



Menedżer zadań możemy uruchomić poprzez kliknięcie kombinacji klawiszy Alt+Ctrl+Del i wybraniu w wyświetlonym oknie przycisku Menedżer zadań. Inną metodą jest uruchomienie programu c:\windows\system32\taskmgr.exe.

Karta **Aplikacje** przedstawia stan programów działających na komputerze. Za pomocą tej karty można uruchomić lub zakończyć program, a także przejść do innego programu.

Karta **Procesy** przedstawia informacje dotyczące procesów uruchomionych na komputerze.
Ta karta pozwala na przykład wyświetlić informacje dotyczące użycia procesora i pamięci, błędy stron, liczbę dojść, a także wiele innych parametrów.

Na karcie **Wydajność** jest dynamicznie wyświetlany przegląd wydajności komputera, w tym:
- wykresy przedstawiające użycie procesora i pamięci;
- całkowita liczba dojść, wątków i procesów działających na komputerze;
- całkowita wielkość pamięci fizycznej, pamięci jądra i pamięci zadeklarowanej w kilobajtach.

Na karcie **Sieć** jest wyświetlana graficzna ilustracja wydajności sieci. Jest to prosty wskaźnik jakościowy, obrazujący stan sieci działających na komputerze. Karta Sieć jest wyświetlana tylko wówczas, gdy w komputerze znajduje się karta sieciowa.
Na karcie tej można przeglądać informacje dotyczące jakości i dostępności połączenia sieciowego oraz sprawdzić, czy użytkownik jest połączony z jedną czy z wieloma sieciami.

Na karcie **Użytkownicy** są wyświetlani użytkownicy, którzy mogą uzyskiwać dostęp do komputera, oraz stany i nazwy sesji. **Nazwa klienta** (jeśli występuje) określa nazwę komputera klienckiego korzystającego z sesji. **Sesja** to nazwa służąca do wykonywania takich zadań jak wysyłanie wiadomości do innego użytkownika lub łączenie się z sesją innego użytkownika. Karta **Użytkownicy** jest wyświetlana tylko w przypadku pracy na komputerze autonomicznym lub należącym do grupy roboczej, który ma włączoną funkcję szybkiego przełączania użytkowników. Karta **Użytkownicy** jest niedostępna na komputerach należących do domeny sieciowej.

Narzędzia Monitor systemu oraz Dzienniki wydajności i alerty obsługują szczegółowe monitorowanie wykorzystania zasobów systemu operacyjnego.

Aby utworzyć niestandardową konsolę monitorowania:
- Otwórz program Microsoft Management Console (MMC).
- W menu Plik kliknij polecenie Dodaj/Usuń przystawkę.
- Na karcie Autonomiczna kliknij przycisk Dodaj.
- Na liście przystawek kliknij pozycję Formant ActiveX, a następnie kliknij przycisk Dodaj.
- W kreatorze Wstawianie formantu ActiveX kliknij przycisk Dalej. Następne okno dialogowe pojawia się z pewnym opóźnieniem; jest to normalne.
- W polu Kategoria formantu kliknij opcję Wszystkie kategorie.
- W polu Typ formantu kliknij opcję Formant monitora systemu.
- Kliknij przycisk Dalej. Formant monitora systemu udostępnia funkcje Monitora systemu.
- W polu Wybierz nazwę dla formantu ActiveX wpisz nazwę formantu, a następnie kliknij przycisk Zakończ.

Uwagi:
- Aby otworzyć konsolę MMC, kliknij przycisk Start, kliknij polecenie Uruchom, a następnie wpisz polecenie mmc.
- Utworzenie konsoli niestandardowej jest użyteczne, jeśli Monitor systemu ma być obsługiwany w tej samej konsoli, co Podgląd zdarzeń lub inne narzędzie.

Uruchomienie **Monitora systemu** polega na wybraniu Start => Programy => Narzędzia administracyjne => Wydajność. Uruchomienie Monitora systemu ze wskazaniem pliku, w którym zostaną zarejestrowane pomiary:
Start => Uruchom => **perfmon.exe nazwa_pliku**

Przy użyciu narzędzia **Monitor systemu** można mierzyć wydajność własnego komputera lub innych komputerów w sieci:
- Zbierać i przeglądać w czasie rzeczywistym dane dotyczące wydajności komputera lokalnego lub kilku komputerów zdalnych: W systemach z rodziny Windows Server została zmodyfikowana funkcjonalność. Na przykład można usunąć wiele liczników naraz i wyświetlić stronę właściwości danych dla licznika bezpośrednio z okna listy. Wybrane dane z pliku dziennika wydajności lub bazy danych SQL można zapisać w nowym pliku na potrzeby późniejszej analizy.
- Nowością w systemach z rodziny Windows Server są także dwie nowe grupy zabezpieczeń, gwarantujące, że tylko zaufani użytkownicy będą mieli dostęp do poufnych danych dotyczących wydajności, aby nimi operować. Są to grupy Użytkownicy dzienników wydajności i Użytkownicy monitora wydajności.

- Przeglądać dane zbierane na bieżąco lub zarejestrowane w dzienniku liczników. W systemach z rodziny Windows Server możliwe jest teraz jednoczesne przeglądanie danych z wielu plików dziennika.
- Prezentować dane wykresie, histogramie lub raporcie, które można wydrukować.
- Włączać funkcje Monitora systemu do aplikacji obsługujących formanty ActiveX, na przykład strony sieci Web, a także programu Microsoft Word i innych aplikacji pakietu Microsoft Office.
- Tworzyć strony HTML z widoków wydajności. Widoki przechowywane w formacie HTML mogą być wyświetlane przez przeglądarkę.
- Tworzyć konfiguracje monitorowania wielokrotnego użytku, które można instalować na innych komputerach przy użyciu konsoli Microsoft Management Console (MMC).

Przy użyciu Monitora systemu można zbierać i przeglądać wiele różnych danych dotyczących wykorzystania zasobów sprzętowych i aktywności usług systemowych na administrowanych komputerach. Można określić następujące sposoby zbierania żądanych danych przez Monitor systemu:

- Typ danych. Aby wybrać dane, które mają być zbierane, należy określić obiekty wydajności, liczniki wydajności i wystąpienia obiektów wydajności. Niektóre obiekty dostarczają danych o zasobach systemu (takich jak pamięć); inne dostarczają danych o działaniu aplikacji (na przykład usług systemowych).
- Źródło danych. Monitor systemu może zbierać dane z komputera lokalnego lub z innych komputerów w sieci, dla których użytkownik ma poświadczenia administracyjne. Domyślnie poświadczenia administracyjne są wymagane. Ponadto można uwzględniać dane w czasie rzeczywistym lub dane zebrane uprzednio przy użyciu dzienników liczników. W systemach z rodziny Windows Server można teraz przeglądać dane dotyczące wydajności, które zostały wcześniej zebrane i zapisane w bazie danych SQL przez usługę Dzienniki wydajności i alerty.
- Parametry próbkowania. Monitor systemu obsługuje próbkowanie ręczne (na żądanie) lub próbkowanie automatyczne w okresach wyznaczonych przez użytkownika. Funkcja ta dotyczy wyłącznie danych czasu rzeczywistego. Przeglądając zarejestrowane dane, można również wybrać moment uruchomienia i zatrzymania, co pozwala przeglądać dane z określonego zakresu czasu.

Poza opcjami określania zawartości danych, Monitor systemu oferuje dużą elastyczność, jeśli chodzi o projektowanie wyglądu widoków danych:

- Typ wyświetlania. Monitor systemu obsługuje widoki wykresu, histogramu i raportu. Widok wykresu jest widokiem domyślnym; oferuje on najwięcej ustawień opcjonalnych.
- Parametry wyświetlania. Dla każdego z trzech widoków można określić, jakie kolory i czcionki mają być wyświetlane. W widokach wykresu i histogramu można wybierać spośród wielu różnych opcji wyświetlania danych o wydajności:
  - Podawanie tytułu wykresu lub histogramu i etykiety dla osi pionowej.
  - Ustawianie zakresów wartości przedstawianych na wykresie lub histogramie.
  - Dostosowywanie cech wykreślanych linii i słupków wskazujących wartości liczników za pomocą koloru, szerokości, stylu i innych funkcji graficznych.

Przy użyciu narzędzia **Dzienniki wydajności i alerty** można automatycznie zbierać dane dotyczące wydajności komputerów lokalnych i zdalnych. Zarejestrowane dane liczników można oglądać za pomocą Monitora systemu lub można je eksportować do programów arkuszy kalkulacyjnych lub baz danych w celu analizy lub wygenerowania raportu. Poniższy wykaz opisuje możliwości narzędzia Dzienniki wydajności i alerty:

- Nowością w rodzinie systemów Microsoft® Windows Server 2003 jest możliwość uruchamiania kolekcji dzienników w ramach różnych kont. Na przykład, jeżeli są potrzebne dane dziennika z komputera zdalnego, który wymaga poświadczeń administracyjnych, można podać konto, które ma niezbędne poświadczenia.
- Nowością w systemach z rodziny Windows Server 2003 są także dwie nowe grupy zabezpieczeń, gwarantujące, że tylko zaufani użytkownicy będą mieli dostęp do poufnych danych dotyczących wydajności, aby nimi operować. Są to grupy Użytkownicy dzienników wydajności i Użytkownicy monitora wydajności.
- Systemy z rodziny Windows Server 2003 obsługują pliki dziennika o rozmiarze większym niż 1 GB, a dzięki nowemu formatowi pliku dziennika dane dotyczące wydajności można obecnie dołączać do istniejącego pliku dziennika.
- Usługa Dzienniki wydajności i alerty zbiera dane w formacie tekstu rozdzielanego przecinkiem lub tabulatorem, co pozwala je łatwo importować do programów arkuszy kalkulacyjnych. Dostępny jest

również binarny format pliku dziennika służący do rejestrowania cyklicznego lub do rejestrowania wystąpień, takich jak wątki lub procesy, które mogą zaczynać się po rozpoczęciu zbierania danych przez dziennik. (Rejestrowanie cykliczne jest procesem ciągłego rejestrowania danych w jednym pliku, przy czym stare dane są zastępowane nowymi.)
- Możliwe jest również zbieranie danych w formacie bazy danych SQL. Opcja ta definiuje nazwę istniejącej bazy danych SQL i zestawu dzienników w bazie danych, w której będą zapisywane lub z której będą odczytywane dane dotyczące wydajności. Ten format pliku jest użyteczny przy zbieraniu i analizowaniu danych dotyczących wydajności na poziomie przedsiębiorstwa, a nie na poziomie komputera. Dane mogą być rejestrowane bezpośrednio w bazie danych SQL przy użyciu standardu ODBC (Open Database Connectivity).
- Dane liczników zebrane przez usługę Dzienniki wydajności i alerty można przeglądać zarówno w trakcie ich zbierania, jak i po zatrzymaniu zbierania.
- Ponieważ rejestrowanie jest uruchamiane jako usługa, zbieranie danych odbywa się bez względu na to, czy jakiś użytkownik jest zalogowany na monitorowanym komputerze.
- Można określić moment uruchomienia i zatrzymania, nazwy plików, rozmiary plików i inne parametry w celu automatycznego generowania dzienników.
- Można zarządzać wieloma sesjami rejestrowania z jednego okna konsoli.
- Można ustawić alert dla licznika, określając, że gdy wartość wybranego licznika wzrośnie powyżej lub spadnie poniżej określonej wartości progowej, ma zostać wysłany komunikat, uruchomiony program, wykonany wpis do dziennika zdarzeń aplikacji albo uruchomiony dziennik.

Zagadnienia do samodzielnego przeanalizowania:
- msconfig.exe,
- konsola administracyjna services.msc,
- konsola administracyjna perfmon.msc,
- klucze rejestru run i runservices,
- sysdm.cpl => Zaawansowane => Wydajność => Ustawienia => Dopasuj dla uzyskania najlepszej wydajności.

Zadanie2:

Odszukaj w zasobach Internetu informacje na temat oprogramowania The Dude, Nagios, Nmap, Wireshark.

The Dude – aplikacja służąca do zarządzania i kontrolowania sieci lokalnej. Program odnajdzie każdego typu urządzenia dostępne w danej podsieci takie jak: drukarki, routery, przełączniki, czy też serwer DNS, serwer FTP, serwer IMAP4, serwer NTP, SMTP, WWW. Program wszystko przedstawia w przejrzystej, miłej dla oka wersji graficznej z możliwością zapisu do pliku graficznego bądź PDF-a.

Oprogramowanie Nagios umożliwia monitorowanie następujących parametrów:
- dostępności hostów i urządzeń,
- działających usług sieciowych na zdalnych systemach,
- statusu drukarek,
- stanu urządzeń sieciowych,
- stanu wybranego parametru wskazanego systemu operacyjnego,
- podstawowy monitoring systemów,
- ważności certyfikatów SSL,
- i inne.

Zadanie3:

Odszukaj w serwisie internetowym dobreprogramy.pl informacje na temat dostępnych programów w kategorii Narzędzia > Narzędzia sieciowe.

Zadanie4:

Odszukaj w zasobach Internetu informacje na temat oprogramowania NetTools.

NetTools Pro to pełna wersja aplikacji przeznaczonej do administrowania sieciami, niedawno uczyniona całkowicie bezpłatną. W skład programu wchodzi 10 narzędzi pozwalającymi m. in. na skanowanie sieci w poszukiwaniu wszystkich komputerów na niej działających, wy listowanie wszystkich przychodzących i wychodzących połączeń z komputera, skanowanie portów i serwerów (HTTP, POP3, MS SQL, Oracle i 50 innych) oraz narzędzie TCP/IP workshop, które pozwala uzyskać niskopoziomowe połączenie TCP i UDP w celu testowania i wykrywania problemów z serwisami sieciowymi. Oprócz powyższych, aplikacja zwiera także inne popularne narzędzia, takie jak: graficzny Ping, Trace, Lookup, Local info czy Bindwidth.