

Rozdział 8: Monitorowanie i optymalizacja wydajności systemu Windows 2000

Spis treści

Przegląd zagadnień	1
Monitorowanie dzienników zdarzeń	2
Wykorzystanie programu Task Manager do monitorowania zasobów systemowych	11
Laboratorium A: Korzystanie z programów Task Manager i Event Viewer	17
Wykorzystanie programu System Monitor do śledzenia wydajności systemu	27
Alerty	33
Laboratorium B: Monitorowanie aktywności systemu	35
Optymalizacja wydajności	42
Podsumowanie	53



Zastrzega się prawo wprowadzania zmian do treści niniejszego dokumentu bez uprzedniego powiadomienia. Wszelkie nazwy firm, nazwiska i imiona osób oraz inne dane wykorzystywane w przykładach są fikcyjne, o ile nie zaznaczono, że jest inaczej. Odpowiedzialność za przestrzeganie wszelkich praw autorskich ponosi użytkownik. Niniejszego dokumentu ani jego części nie wolno powielać w żadnej formie, ani przekazywać za pomocą jakichkolwiek nośników elektronicznych lub mechanicznych, z wyjątkiem przypadków, gdy uzyskano na to pisemną zgodę firmy Microsoft Corporation. Jeżeli użytkownik ma dostęp do tego dokumentu wyłącznie w formie elektronicznej, zezwala się na wydrukowanie jednego egzemplarza tego dokumentu.

Firma Microsoft może mieć patenty lub rozpoczęte postępowania patentowe, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, które odnoszą się do treści zawartej w tym dokumencie. Otrzymanie tego dokumentu nie oznacza udzielenia licencji na patenty, znaki towarowe, prawa autorskie lub inne prawa związane z własnością intelektualną, z wyjątkiem wyraźnie określonych przypadków zawartych w pisemnych umowach licencyjnych firmy Microsoft.

© 2000 Microsoft Corporation. Wszelkie prawa zastrzeżone.

Microsoft, Active Desktop, Active Directory, ActiveX, BackOffice, DirectX, FrontPage, JScript, MS-DOS, NetMeeting, PowerPoint, Visual Basic, Visual Studio, Windows, Windows Media, and Windows NT są zastrzeżonymi znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Microsoft Corporation zarejestrowanymi w USA i/lub w innych krajach.

Wszelkie inne nazwy firm i produktów wymienione w niniejszym dokumencie mogą być znakami towarowymi zarejestrowanymi przez ich właścicieli.

Project Lead: Rick Selby

Instructional Designers: Kelly Bowen, Victoria Fodale (ComputerPREP),
H. James Toland III (ComputerPREP), Kathryn Yusi (Independent Contractor),
Barbara Pelletier (S&T Onsite)

Lead Program Manager: Andy Ruth (Infotec Commercial Systems)

Program Manager: Chris Gehrig (Infotec Commercial Systems),
Joern Wettern (Wettern Network Solutions)

Graphic Artist: Kimberly Jackson (Independent Contractor)

Editing Manager: Lynette Skinner

Editor: Kelly Baker (The Write Stuff)

Copy Editor: Kathy Toney (S&T Consulting)

Online Program Manager: Debbi Conger

Online Publications Manager: Arlo Emerson (Aditi)

Online Support: David Myka (S&T Consulting)

Multimedia Development: Kelly Renner (Entex)

Courseware Test Engineers: Jeff Clark, H. James Toland III (ComputerPREP)

Testing Developer: Greg Stemp (S&T OnSite)

Compact Disc Testing: Data Dimensions, Inc.

Courseware Testing: Data Dimensions, Inc.

Production Support: Carolyn Emory (S&T Consulting)

Manufacturing Manager: Rick Terek (S&T OnSite)

Manufacturing Support: Laura King (S&T OnSite)

Lead Product Manager, Development Services: Bo Galford

Lead Product Manager: Gerry Lang

Group Product Manager: Robert Stewart

Simulation and interactive exercises were built with Macromedia Authorware

Opracowanie wersji polskiej: DC Edukacja Sp. z o.o. Sopot

Współpraca: DC Edukacja Kielce, P.S.I. Sp. z o.o. Kielce

Zespół tłumaczy: Przemysław Dąbkowski, Sylwester Nowicki, Marcin Sworzyński

Konsultacja: Waldemar Pierścioneek, Witold Stajura, Piotr Zejer

Uwagi dla wykładowcy

Prezentacja:
45 minut

Laboratoria:
60 minut

W tym rozdziale przedstawiono wiadomości i działania niezbędne do monitorowania wydajności komputerów. Obejmują one korzystanie z dzienników, konfigurację mechanizmów obsługi danych i monitorowanie systemu w celu optymalizacji wydajności.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Przeglądać dzienniki zdarzeń i wyszukiwać informacje o pracy systemu.
- Wykorzystywać program Task Manager do monitorowania zasobów systemowych.
- Wykorzystywać program System Monitor do kontroli wydajności systemu.
- Wykorzystywać alerty do powiadamiania użytkowników lub administratora, gdy niektóre kryteria nałożone na system nie są spełnione lub przekroczone.
- Optymalizować wydajność, dzięki odpowiedniemu doborowi obserwowanych wskaźników.

Materiały i sposób przygotowania

W sekcji tej opisano sposób przygotowania wykładowcy oraz materiały niezbędne do właściwej prezentacji rozdziału.

Wymagane materiały

Do przedstawienia tego rozdziału wykładowcy potrzebne będą następujące materiały:

- Plik Microsoft® PowerPoint® 2152B_08.ppt.

Sposób przygotowania

Aby przygotować się do przedstawienia tego rozdziału, należy:

- Przeczytać wszystkie materiały związane z tym rozdziałem.
- Wykonać ćwiczenia.
- Przeanalizować pytania podsumowujące i przygotować alternatywne odpowiedzi.
- Zastanowić się, jakie pytania mogą zadać uczestnicy kursu. Zapisać je wraz z odpowiedziami.

Strategia przedstawienia rozdziału

Wskazówki dotyczące prezentacji rozdziału:

- Monitorowanie dzienników zdarzeń

W tej sekcji zawarte są informacje o różnych typach dzienników zdarzeń i danych, jakie zawierają. Należy omówić różne typy zdarzeń, generowanych przez system i aplikacje, które są zapisywane w dziennikach. Zaprezentować możliwości przeglądania dzienników zdarzeń. Można w tym celu wykorzystać dowolny dziennik. Nadmienić, że można przeszukiwać dzienniki, w celu wyszukania konkretnego zdarzenia lub zdarzeń. Po przejrzaniu dzienników, zaprezentować, jak można ograniczyć ich rozmiar. Podkreślić, że w sieciach o wysokim stopniu bezpieczeństwa, należy archiwizować dzienniki zdarzeń. Na zakończenie omówić zarządzanie dziennikami zdarzeń. Zademonstrować zapisywanie dzienników do pliku i ich ręczne czyszczenie.

- Wykorzystanie programu Task Manager do monitorowania zasobów systemowych

Na początku tej sekcji, należy upewnić się, że uczestnicy wiedzą, co to jest proces. Następnie, zaprezentować informacje na temat monitorowania programów poprzez kartę **Application**. Upewnić się, że na komputerze instruktora jest uruchomiony jakiś proces, który można wykorzystać do demonstracji zamykania procesów. Następnie, zaprezentować informacje na temat monitorowania procesów poprzez kartę **Processes**. Upewnić się, że uczestnicy wiedzą, czym jest przestrzeń adresowa. Na zakończenie, omówić monitorowanie wydajności poprzez kartę **Performance**. Zademonstrować sposób sprawdzania czasu procesu i trybu jądra.

- Wykorzystanie programu System Monitor do śledzenia wydajności systemu

Na wstępie, należy omówić obiekty Monitora systemu i wyjaśnić, jak są ze sobą powiązane. Zaznaczyć, że obiekty monitora systemu nie są powiązane z obiektami usług katalogowych Active Directory™. Następnie zaprezentować, jak dodaje się liczniki. Zaakcentować, że dane liczników zbierane są przez cały czas, dodanie licznika powoduje dodatkowo wyświetlanie zebranych dla niego danych. Zaprezentować różne sposoby przeglądania danych liczników, np. histogram, raport lub wykres.

- Alerty

Na wstępie, należy omówić wykorzystanie alertów. Zaznaczyć, że mogą być używane do ostrzegania użytkowników i administratorów, gdy kryteria nałożone na system nie są spełniane. Można konfigurować różne typy alertów. Należy zademonstrować ustawianie alertu.

- Optymalizacja wydajności

Na wstępie, należy zaprezentować proces optymalizacji systemu. Podkreślić, że analiza wydajności nie jest pojedynczą czynnością, ale rozwijającym się zadaniem. Zaprezentować informacje o testowaniu wydajności pamięci, łącznie z ustanawianiem bazy, wykorzystaniem liczników i testowaniem pliku stronicowania. Omówić testowanie wydajności procesora. Jeżeli wystarczy czasu zaprezentować liczniki % Processor Time i Processor Queue Length. Omówić monitorowanie wydajności dysku, łącznie z odpowiednimi licznikami. Na zakończenie zaprezentować testowanie wydajności sieci. Zaznaczyć, że dzięki programowi Performance Monitor można śledzić wydajność komponentów sieciowych na innych serwerach i przepływ danych przez sieć.

Informacje uzupełniające

W sekcji tej opisane są wymagania dotyczące instalacji laboratorium dla tego rozdziału oraz zmiany w konfiguracji, które zachodzą na komputerach słuchaczy w trakcie realizacji laboratorium. Informacje te będą pomocne w powielaniu lub dostosowywaniu materiałów szkoleniowych MOC (Microsoft Official Curriculum).

Ważne Aby możliwe było wykonanie laboratorium, zawartego w tym rozdziale, konieczne jest odpowiednie skonfigurowanie pracowni, zgodnie z uwagami znajdującymi się w sekcji Informacje uzupełniające, zamieszczonej w rozdziale Przygotowanie pracowni do kursu 2244A, *Wdrażanie systemów operacyjnych Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*.

Przygotowanie laboratorium

Aby przygotować komputery słuchaczy do laboratorium w tym rozdziale, należy ukończyć rozdział 1, „Instalacja lub uaktualnianie do Windows 2000” kursu 2244A, *Wdrażanie systemów operacyjnych Microsoft Windows 2000 Professional i Microsoft Windows 2000 Server*.

Rezultaty laboratorium

Wykonanie ćwiczeń z tego rozdziału nie spowoduje żadnych zmian w konfiguracji komputerów słuchaczy:

Przegląd zagadnień

Cel slajdu

Przedstawienie tematów i celów rozdziału.

Wprowadzenie

W tym rozdziale przedstawione zostaną zagadnienia, związane z monitorowaniem i optymalizacją systemu. Windows 2000.

- **Monitorowanie dzienników zdarzeń**
- **Wykorzystanie programu Task Manager do monitorowania zasobów systemowych**
- **Wykorzystanie programu System Monitor do śledzenia aktywności systemu**
- **Alerty**
- **Optymalizacja wydajności**

Do zadań administratora należy monitorowanie zasobów systemowych, w celu oceny poziomu ich wykorzystania, obserwowania zmian i trendów w ich użytkowaniu i diagnozowania problemów.

W systemie Microsoft® Windows® 2000 znajdują się narzędzia, przeznaczone do monitorowania zasobów systemowych. Task Manager pozwala śledzić aktualny stan uruchomionych programów i procesów, a także wykorzystanie pamięci i procesora. W programach System Monitor i Performance Logs and Alerts, można uzyskać szczegółowe dane na temat wykorzystania zasobów przez poszczególne komponenty systemu operacyjnego i komputera.

Po zrealizowaniu tego rozdziału słuchacz będzie potrafił:

- Przeglądać dzienniki zdarzeń i wyszukiwać informacje o pracy systemu.
- Wykorzystywać program Task Manager do monitorowania zasobów systemowych.
- Wykorzystywać program System Monitor do kontroli wydajności systemu.
- Wykorzystywać alerty do powiadamiania użytkowników lub administratora, gdy niektóre kryteria nałożone na system nie są spełnione lub przekroczone.
- Optymalizować wydajność, dzięki odpowiedniemu doborowi obserwowanych wskaźników.

◆ Monitorowanie dzienników zdarzeń

Cel slajdu

Zestawienie zagadnień związanych z monitorowaniem dzienników zdarzeń.

Wprowadzenie

W systemie Windows 2000 można monitorować różnego rodzaju aktywność i zdarzenia.

- Wprowadzenie do dzienników zdarzeń
- Typy zdarzeń systemowych i aplikacji
- Przeglądanie dzienników zdarzeń
- Ograniczanie rozmiaru pliku dziennika
- Zarządzanie dziennikami zdarzeń

Zdarzenia są to działania użytkownika, notowane w oparciu o założenia systemowe, a także wszystkie znaczące wydarzenia, jakie występują podczas pracy systemu i aplikacji. Monitoruje się je w celu obserwacji skuteczności zabezpieczeń, wykorzystania zasobów lub powstawania błędów systemowych i aplikacji. Zdarzenia dotyczące bezpieczeństwa systemu, odnoszące się do założeń systemowych, przechowywane są w dzienniku bezpieczeństwa. Zdarzenia systemowe, automatycznie wykonywane przez system operacyjny, zapisywane są w dzienniku systemowym. Zdarzenia określone przez projektantów aplikacji, zapisywane są w dzienniku aplikacji.

Zdarzenia zapisywane w tych dziennikach powinny być następnie przeglądane i analizowane w celu wykrycia takich, które mogą wymagać interwencji administratora. W oparciu o analizę dzienników można wykryć naruszenia zabezpieczeń, błędne zachowanie systemu lub przemieszczenie zasobów. Może to wymusić zmiany w założeniach systemowych, konfiguracji zabezpieczeń, aplikacji lub systemu.

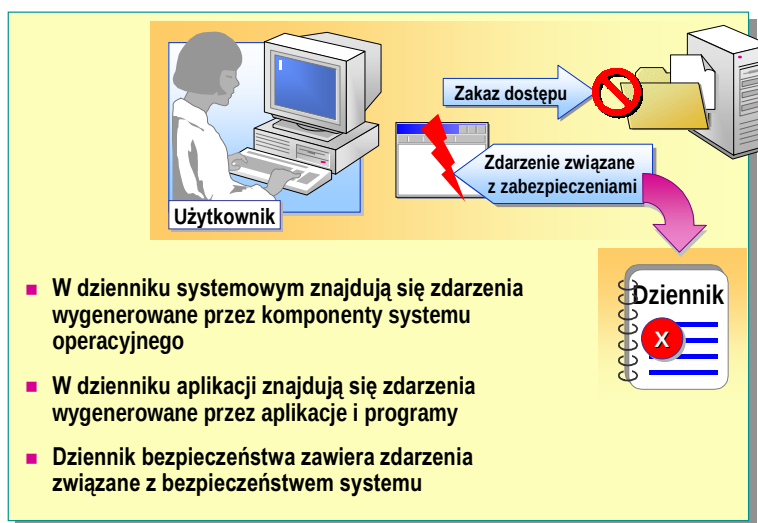
Wprowadzenie do dzienników zdarzeń

Cel slajdu

Zilustrowanie przykładowych czynności związanych z dziennikami zdarzeń.

Wprowadzenie

Dzięki dziennikom zdarzeń można zbierać informacje o sprzęcie, oprogramowaniu, niewłaściwej konfiguracji systemu i zabezpieczeniach.



Zagadnienia kluczowe

W systemie Windows 2000 zdarzenia zapisywane są w trzech dziennikach: dzienniku bezpieczeństwa, dzienniku systemowym i dzienniku aplikacji.

Wyjaśnij, że w zależności od usług, jakie są uruchomione na danym komputerze, mogą być dostępne dodatkowe dzienniki.

Dzienniki zdarzeń umożliwiają zbieranie informacji o sprzęcie, oprogramowaniu, niewłaściwych zachowaniach systemu i zabezpieczeniach. Przeglądanie tych dzienników umożliwia obserwację aktywności systemu i zdarzeń wymagających reakcji administratora. Dzienniki mogą być także użyte do gromadzenia archiwalnych informacji o pracy systemu.

Zdarzenia w systemie Windows 2000 są zapisywane w trzech dziennikach:

- *Dziennik systemowy (system log)*. W dzienniku tym zapisywane są zdarzenia generowane przez komponenty systemu operacyjnego, na przykład, uszkodzenie sterownika lub składnika systemu podczas rozruchu. Zdarzenia, które mają być zapisywane, są z góry określone w systemie.
- *Dziennik aplikacji (application log)*. Dziennik przeznaczony dla zdarzeń generowanych przez aplikacje. Na przykład, program bazy danych zapisuje w nim wykrycie błędów w pliku. Programiści decydują, które zdarzenia będą zapisywane. Zdarzenia generowane przez aplikację Dr. Watson również są przechowywane w tym dzienniku. Program Dr. Watson, dla systemu Windows 2000, jest programem przeznaczonym do analizy wystąpienia błędów. Gdy wystąpi błąd w aplikacji, program Dr. Watson generuje plik (Drwtsn32.log) opisujący to zdarzenie.
- *Dziennik bezpieczeństwa (security log)*. Jest to dziennik zawierający zdarzenia związane z zabezpieczeniami systemu, takimi jak próby logowania, dostęp do zasobów, tworzenie, otwieranie i usuwanie plików. Administrator określa szczegółowo, które zdarzenia mają być w nim zapisywane, na przykład, jeżeli zostanie włączona obserwacja prób logowania, wszystkie takie próby będą zapisywane w tym dzienniku.

Uwaga Wszyscy użytkownicy mogą przeglądać dzienniki aplikacji i systemowy, ale dziennik bezpieczeństwa dostępny jest tylko dla administratora systemu.

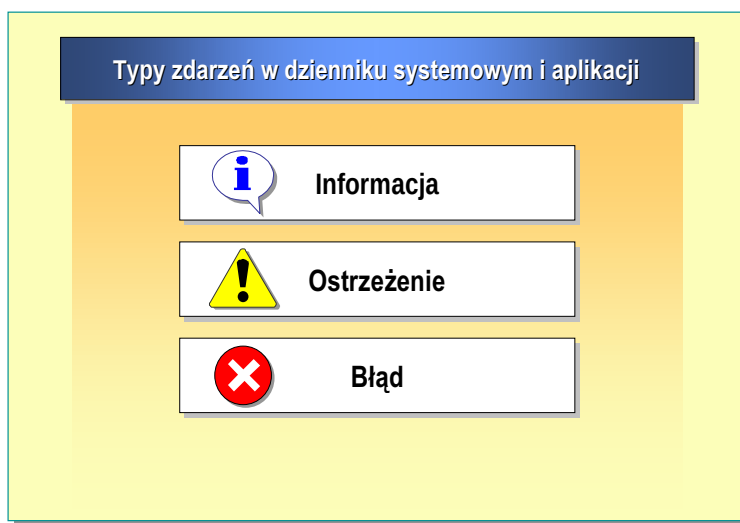
Typy zdarzeń systemowych i aplikacji

Cel slajdu

Zilustrowanie typów zdarzeń systemowych i aplikacji.

Wprowadzenie

Typy zdarzeń systemowych i aplikacji to: informacja, ostrzeżenie i błąd.



Występują trzy typy zdarzeń zapisywanych w dzienniku systemowym i aplikacji: informacja, ostrzeżenie i błąd. Do każdego zdarzenia dołączane są szczegółowe informacje, takie jak typ zdarzenia i usługa z nim związana. Można je wykorzystać do dokładnej identyfikacji zdarzenia i dzięki temu odpowiednio zareagować. Zdarzenia generowane przez system operacyjny zapisywane są w dzienniku systemowym. Zdarzenia generowane przez aplikacje zapisywane są w dzienniku aplikacji. Programiści tworzący system i aplikacje decydują, które zdarzenia mają być zapisywane.

Opisz każdy typ zdarzenia.

Typy zdarzeń aplikacji i systemowych opisano w poniższej tabeli.

Typ zdarzenia	Opis
Informacja	Udana operacja przeprowadzona przez aplikację, sterownik lub usługę, na przykład, udane uruchomienie znaczącej usługi, takiej jak dziennik zdarzeń.
Ostrzeżenie	Zdarzenie, które nie ma dużego znaczenia dla funkcjonalności systemu, ale w przyszłości może powodować utrudnienia, na przykład, mała dostępna wolna przestrzeń na dysku. Programy antywirusowe mogą zapisywać informację o wykryciu wirusa.
Błąd	Znaczący problem w wykonaniu operacji systemowej, taki jak utrata danych lub funkcjonalności, na przykład, niemożność uruchomienia usługi podczas rozruchu systemu

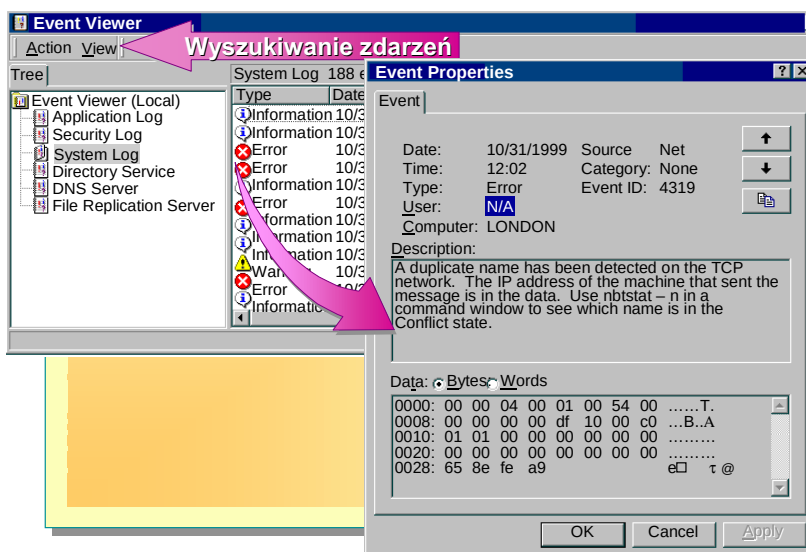
Przeglądanie dzienników zdarzeń

Cel slajdu

Prezentacja interfejsu do przeglądania dzienników zdarzeń.

Wprowadzenie

Korzystając z przeglądarki zdarzeń można przeglądać dzienniki, które mogą być wykorzystane do monitorowania sprzętu, oprogramowania, problemów z systemem i zabezpieczeniami.



Zdarzenia związane z aktywnością systemu i aplikacji zapisywane są w dziennikach chronologicznie, od najstarszych do najmłodszych. Pliki dzienników zawierają wiele informacji o każdym zdarzeniu. Można je przeglądać przy pomocy przeglądarki zdarzeń, w celu wyszukiwania informacji o sprzęcie, oprogramowaniu, nieprawidłowym działaniu systemu i zabezpieczeniach. Dla ułatwienia tego zadania, specyficzne zdarzenia mogą być wyszukiwane.

Lokalne przeglądanie dzienników

Wskazówka

Zademonstruj działanie przeglądarki zdarzeń. Wybierz przykładowe zdarzenie do omówienia.

Poprzez przeglądarkę zdarzeń można uzyskać szczegółowe informacje. Aby ją uruchomić należy rozwinąć menu **Start**, następnie **Programs**, **Administrative Tools** i wybrać polecenie **Event Viewer**. Następnie, w drzewie konsoli należy wybrać dziennik, który ma być przeglądany. W panelu szczegółów wyświetlane są zapisane zdarzenia i szczegółowe informacje na ich temat. Aby uzyskać pełny opis zdarzenia, należy otworzyć jego okno szczegółów.

Uwaga Poza możliwością przeglądania dzienników na lokalnym komputerze, można je przeglądać także na komputerach zdalnych. Aby to zrobić, należy w przeglądarce zdarzeń prawym przyciskiem myszy wskazać **Event Viewer (Local)**. Z menu kontekstowego wybrać polecenie **Connect**. Wskazać domenę, w której znajduje się zdalny komputer, a następnie wskazać komputer, do którego należy podłączyć się.

Właściwości zdarzenia

Poza datą, czasem i identyfikatorem zdarzenia, można również przeglądać jego właściwości, które zostały opisane w poniższej tabeli.

Właściwość	Opis
Source	Komponent systemu, aplikacja lub zdarzenie związane z zabezpieczeniami, które wygenerowało zdarzenie.
Category	Definicja zdarzenia, do wykorzystania przez programistów.
Type	Typ zdarzenia: informacja, ostrzeżenie, błąd.
User	Nazwa użytkownika, jeżeli zdarzenie było powiązane z konkretnym kontem.
Computer	Nazwa komputera, na którym wystąpiło zdarzenie.
Description	Opis zdarzenia, tworzony przez jego źródło.
Data	Dane binarne, wygenerowane przez zdarzenie.

Wskazówka

Zademonstruj wyszukiwanie specyficznych grup zdarzeń.

Wyszukiwanie zdarzeń

Dostępny w przeglądarce mechanizm wyszukiwania konkretnych zdarzeń pozwala identyfikować trendy lub łatwo odszukiwać potrzebne informacje. Dostępne są następujące typy wyszukiwania:

- Wyszukiwanie konkretnego zdarzenia poprzez polecenie **Find** z menu **View**. Na przykład, jakieś zdarzenie wydaje się być związane z niewłaściwym działaniem systemu. Można wtedy wyszukać inne wystąpienia tego zdarzenia, aby ocenić częstość jego występowania.
- Wyszukiwanie grup zdarzeń poprzez filtrację dziennika. Na przykład, jeżeli wydaje się, że jakiś składnik sprzętowy jest przyczyną złego działania systemu, należy przefiltrować dziennik systemowy tak, aby wyświetlane były tylko zdarzenia wygenerowane przez ten składnik. Aby użyć filtrowania, należy prawym przyciskiem myszy wybrać **Security Log**, **System Log** lub **Application Log**, wskazać **View**, a następnie **Filter**.

Do szczegółowego filtrowania można wykorzystać właściwości zdarzeń, zgodnie z poniższym opisem.

Właściwość	Opis
Event types	Typ zdarzenia.
Event source	Aplikacja lub składnik, który wygenerował zdarzenie.
Category	Kategoria zdarzenia, np. logowanie, wylogowanie.
Event ID	Identyfikator zdarzenia. Pomocny przy kontakcie z obsługą techniczną producenta programu.
User	Nazwa użytkownika.
Computer	Nazwa komputera.
From: To:	Okres czasu, w którym wystąpiły zdarzenia.

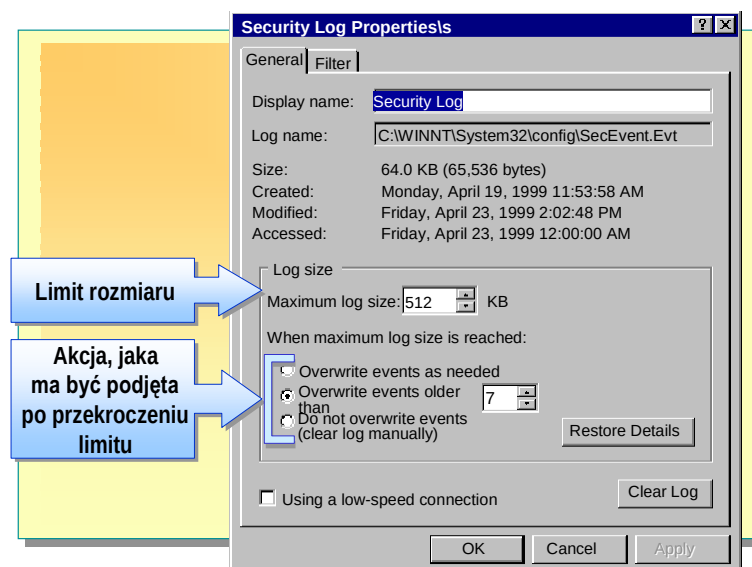
Ograniczanie rozmiaru plików dziennika

Cel slajdu

Ilustracja interfejsu do ograniczania rozmiaru plików dziennika.

Wprowadzenie

Można kontrolować rozmiar dzienników i określić reakcję systemu na przekroczenie tego rozmiaru.



Zagadnienie kluczowe

Jeżeli wymagany jest duży poziom bezpieczeństwa, można archiwizować stare zdarzenia przed nadpisaniem ich nowymi.

W przypadku problemów z ilością wolnego miejsca na dysku, można ograniczyć wielkość plików dzienników zdarzeń i nadpisywać stare zdarzenia nowymi. Nadpisywanie zdarzeń jest nazywane *event log wrapping*. Po włączeniu opcji **Event log wrapping** stare wpisy są tracone. Jeżeli wymagany jest duży poziom bezpieczeństwa i zachowywanie historii zdarzeń, można zapisywać dzienniki przed ich nadpisaniem.

Aby skonfigurować rozmiar dziennika, należy wskazać dziennik w przeglądarce zdarzeń i otworzyć okno dialogowe **Properties** tego dziennika. W oknie tym, dla każdego dziennika można skonfigurować:

- Rozmiar pliku od 64 kilobajtów (KB) do 4 giabajtów (GB). Domyślny rozmiar wynosi 512 KB.
- Reakcję systemu na przekroczenie rozmiaru dziennika. W poniższej tabeli opisano możliwości konfiguracji opcji **Event log wrapping**.

Opcja	Opis
Overwrite events as needed	Gdy plik się przepełni część informacji może być utracona przed jego zarchiwizowaniem. Jednak takie ustawienie jest łatwiejsze w obsłudze. Należy z niego korzystać, jeżeli dzienniki są często przeglądane, co pozwoli zauważyć zdarzenia przed usunięciem informacji z dzienników. Dopuszczalne również w sieciach o niskim wymaganym poziomie bezpieczeństwa.
Overwrite events older than x days	Należy wprowadzić ilość dni. Po przepełnieniu dziennika, informacje są nadpisywane, jednak tylko te, które wystąpiły określoną ilość dni wcześniej. Z tego ustawienia można korzystać przy stosunkowo częstym przeglądaniu dzienników.

(ciąg dalszy)

Opcja	Opis
Do not overwrite events (clear log manually)	Dziennik musi być czyszczony ręcznie. Po zapełnieniu dziennika system przestaje zapisywać nowe zdarzenia. Dzięki temu stare nie zostaną nadpisane. Opcja przeznaczona jest dla sieci o dużym wymaganym poziomie bezpieczeństwa.

Przekaż poniższą uwagę.

Ważne Przy wybranej opcji **Do not overwrite events (clear log manually)** konieczne jest ręczne, okresowe archiwizowanie i czyszczenie dzienników. Gdy dziennik zostanie zapełniony, wyświetlany jest komunikat systemowy, informujący o tym. System Windows 2000 można tak skonfigurować, aby w takiej sytuacji nastąpiło jego automatyczne zamknięcie. Zapobiega to nadpisywaniu dziennika bezpieczeństwa w celu ukrycia działań narażających bezpieczeństwo sieci. Ważne jest również takie ustawienie rozmiaru dziennika, aby w założonym okresie archiwizowania był w stanie pomieścić zebrane informacje.

Zarządzanie dziennikami zdarzeń

Cel slajdu

Zestawienie niektórych zadań związanych z zarządzaniem dziennikami zdarzeń.

Wprowadzenie

Należy archiwizować dzienniki zdarzeń, aby móc analizować trendy i porównywać różne okresy.

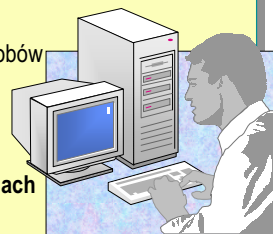
■ Archiwizacja dzienników w celu:

- Śledzenia trendów wykorzystania zasobów
- Wykrywania nieautoryzowanego użycia zasobów
- Przechowywania informacji ze względów regulaminowych

■ Wybór formatu plików dla dzienników, które mają być analizowane w innych aplikacjach

- Format dziennika (.evt)
- Format tekstowy (.txt)
- Format tekstowy z separatorem (.csv)

■ Ręczne czyszczenie dzienników, jeżeli zdarzenia nie mogą być nadpisywane



Zarządzanie dziennikami zdarzeń wymaga wykonywania różnego rodzaju czynności. Możliwe jest ich archiwizowanie, z określeniem formatu zapisu danych. W niektórych przypadkach konieczne jest ręczne czyszczenie dzienników.

Archiwizacja dzienników zdarzeń

Wskazówka

Zademonstruj archiwizowanie, przeglądanie i czyszczenie dziennika.

Archiwizowanie dzienników pozwala analizować historię działania systemu i porównywać dzienniki z różnych okresów, w celu analizy trendów. Analiza taka pozwala określić wykorzystanie zasobów i zaplanować rozbudowę systemu. Pozwala również wychwytywać nieautoryzowany dostęp do zasobów. Wiele firm wymusza archiwizowanie dzienników w określonych odstępach czasu. Niektóre organizacje rządowe i banki są zobligowane prawnie do archiwizowania dzienników.

Zwróć uwagę, że opcja jest dostępna podczas archiwizowania dziennika.

Do archiwizacji i przeglądania zarchiwizowanych dzienników służy aplikacja Event Viewer. W tym celu, z menu **Action** należy wybrać jedną z opisanych poniżej opcji.

Aby	Należy
Zarchiwizować dziennik	Wybrać Save Log File As i wpisać nazwę pliku.
Przeglądać zarchiwizowany dziennik	Wskazać New , a następnie wybrać Log View . W oknie dialogowym Add Another Log View wybrać Saved i podać ścieżkę dostępu do dziennika.

Wybór formatu pliku

Dzienniki zdarzeń można zapisywać w różnych formatach, co pozwala przeglądać je w różnych aplikacjach. Do zarządzania takimi dziennikami można, na przykład, wykorzystywać arkusz kalkulacyjny Microsoft Excel. Dostępne formaty:

- Format dziennika (.evt). Zarchiwizowane dzienniki można przeglądać ponownie w przeglądarce zdarzeń.
- Format tekstowy (.txt). Informacje można przeglądać w dowolnym edytorze tekstu.
- Format tekstowy z separatorami (.csv). Dane można przeglądać w arkuszach kalkulacyjnych i aplikacjach baz danych.

Zagadnienie kluczowe

W formacie tekstowym lub formacie tekstowym z separatorami nie można zapisywać danych binarnych, umieszczanych w dzienniku. Niektóre informacje są wtedy tracone.

Ważne Dzienniki zapisywane w formacie tekstowym lub formacie tekstowym z separatorami nie zawierają danych binarnych. Dane te mogą zawierać dodatkowe informacje, pomocne w rozwiązywaniu problemów.

Ręczne czyszczenie dzienników zdarzeń

Po wybraniu opcji **Do not overwrite events (clear log manually)** w oknie dialogowym **Properties** aktywnego dziennika, konieczne jest jego okresowe ręczne czyszczenie w sytuacji, gdy zbliża się do rozmiaru granicznego lub wyświetlany jest komunikat, że dziennik został zapełniony.

Aby wyczyścić dziennik zdarzeń należy:

1. W drzewie konsoli zaznaczyć dziennik, który ma być wyczyszczony.
2. Z menu **Action** wybrać **Clear all Events**.
3. Wybrać **Yes**, aby zapisać dziennik przed wyczyszczeniem.

-lub-

Wybrać **No**, co spowoduje utratę aktualnego zestawu zdarzeń i umożliwi zapisywanie nowych.

Wskazówka

Otwórz przeglądarkę zdarzeń i zaprezentuj, gdzie można wyczyścić dziennik, ale nie czyść go.

◆ Wykorzystanie programu Task Manager do monitorowania zasobów systemowych

Cel slajdu

Prezentacja zagadnień związanych z zarządzaniem zasobami systemowymi w programie Task Manager.

Wprowadzenie

W programie Task Manager można uzyskać informacje o programach i procesach uruchomionych na komputerze.

- Monitorowanie programów
- Monitorowanie procesów
- Monitorowanie wydajności

Upewnij się, że uczestnicy wiedzą, co to jest proces.

W programie Task Manager można uzyskać aktualne informacje o aplikacjach pracujących w systemie, procesach oraz statystyki wydajności procesora i pamięci.

Można, na przykład, wykorzystać program Task Manager do odszukania aplikacji, wykorzystujących nieproporcjonalnie dużo zasobów systemowych. Dodatkowo, w programie tym można uzyskać wyniki pomiarów aktywności systemu i programów.

Ważne Proces jest programem pierwszoplanowym lub uruchomionym w tle, pracującym w wyznaczonej przestrzeni pamięci i wykonującym konkretne zadanie. Może być częścią aplikacji, wykonującej jednocześnie wiele procesów. Przykładowymi procesami są: Winword.exe i Services.exe.

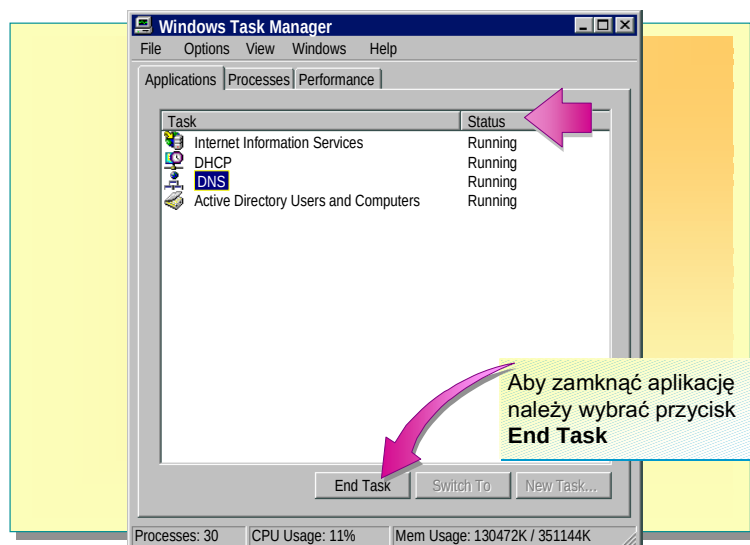
Monitorowanie programów

Cel slajdu

Ilustracja interfejsu monitorowania aplikacji w programie Task Manager.

Wprowadzenie

W celu sprawdzenia statusu uruchomionych aplikacji, należy użyć karty Applications.



Wyjaśnij, że na karcie aplikacji wyświetlane są aplikacje uruchomione w aktualnym kontekście użytkownika.

Na karcie **Applications** programu Task Manager, można przeglądać status aplikacji uruchomionych na komputerze oraz identyfikować powiązane z nimi procesy. Dodatkowo, można na niej zamykać niewłaściwie działające programy.

Na karcie **Application** można wykonać następując czynności:

- Przeglądać wszystkie aktualnie pracujące aplikacje i ich status.
- Zamykać nie działające aplikacje. Aby to zrobić, należy wcisnąć kombinację klawiszy CTRL+ALT+DELETE, wybrać **Task Manager** i wskazać kartę **Applications**. Następnie wskazać zawieszony program i wybrać przycisk **End Task**.

Wskazówki

Zademonstruj zamykanie aplikacji. Potrzebna będzie do tego uruchomiona aplikacja.

Zademonstruj identyfikację procesów powiązanych z daną aplikacją.

Uwaga Wszystkie wprowadzone dane i zmiany wykonane w aplikacji, które nie zostały zapisane, zostaną utracone.

- Identyfikować procesy związane z aplikacjami. Aby to zrobić, należy wskazać prawym przyciskiem myszy aplikację i wybrać polecenie **Go To Process**. Zostanie wyświetlona karta **Processes**, z wyróżnionymi procesami, z których korzysta aplikacja.

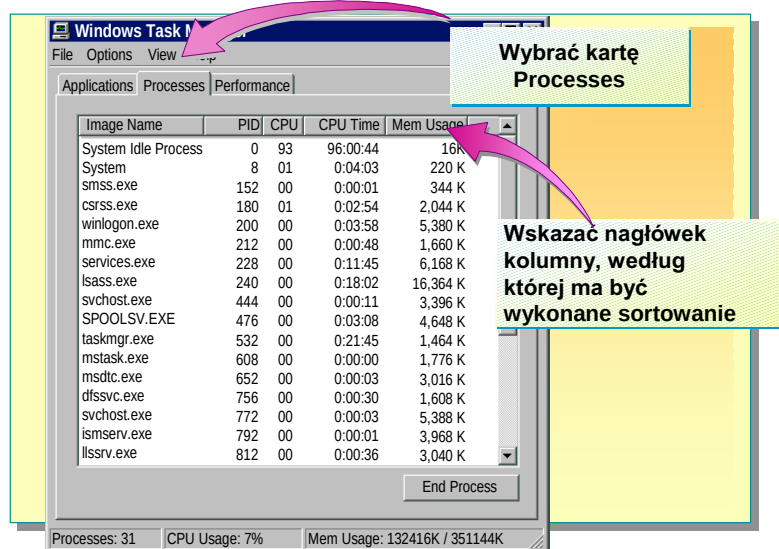
Monitorowanie procesów

Cel slajdu

Ilustracja interfejsu monitorowania procesów w Menedżerze zadań.

Wprowadzenie

Na karcie **Processes** można odczytać informacje o aktualnie uruchomionych procesach i programach.



Upewnij się, że słuchacze wiedzą, co to jest przestrzeń adresowa.

Na karcie **Processes** można przeglądać listę uruchomionych procesów i ich liczników. Należą do nich pomiary wartości związanych z procesem, takich jak całkowity czas procesora, rozmiar używanej pamięci. Lista, wyświetlana na karcie **Processes**, zawiera wszystkie procesy pracujące we własnej przestrzeni adresowej, łącznie z aplikacjami i usługami systemowymi. Zarówno użytkownik jak i system mogą zainicjalizować proces, ale użytkownik może zakończyć tylko procesy użytkownika.

Przeglądanie pomiarów procesów

Wyjaśnij, że w programie Task Manager dostępne są 23 liczniki dla procesów. W tabeli przedstawiono najczęściej używane.

Niektóre liczniki dla procesów, dostępne na karcie **Processes**, opisano w poniższej tabeli.

Właściwość	Opis
CPU	Aktualne wykorzystanie czasu procesora. Jeżeli system nie przetwarza żadnego konkretnego procesu aktywny jest System Idle Process , który pozwala odczytać procentowo czas, przez jaki komputer nie wykonuje żadnych zadań. Przy małym wykorzystaniu systemu może osiągnąć 100 procent.
CPU Time	Całkowity czas procesora, w sekundach, przez jaki przetwarzał procesy od momentu uruchomienia.
Mem Usage	Rozmiar pamięci, w kilobajtach, wykorzystanej przez procesy.
I/O Read Bytes	Ilość bajtów odczytywana w operacjach wejścia/wyjścia (I/O), generowanych przez procesy wykorzystujące pliki, sieć i inne urządzenia wejścia/wyjścia.
I/O Write Bytes	Ilość bajtów zapisywana w operacjach wejścia/wyjścia (I/O), generowanych przez procesy wykorzystujące pliki, sieć i inne urządzenia wejścia/wyjścia.

Aby wyświetlić inne liczniki, należy wybrać polecenie **View**, a następnie **Select Columns**. Zaznaczyć żądane liczniki i wybrać przycisk **OK**.

Zwróć uwagę, że dzięki sortowaniu procesów, administrator może odnaleźć procesy o dużych wymaganiach.

Użycie pomiarów procesów do określenia wykorzystania zasobów

W programie Task Manager, na karcie **Process** można odczytać wykorzystanie zasobów przez programy. Po zidentyfikowaniu aplikacji najbardziej wykorzystującej czas procesora, niektóre z nich można przenieść na inne komputery. Dane w kolumnach można sortować rosnąco lub malejąco.

Aby zidentyfikować aplikację w dużym stopniu wykorzystującą czas procesora, należy zaznaczyć kolumnę **CPU**. Po pierwszym jej zaznaczeniu, wartości zostaną posortowane rosnąco. Kolejne zaznaczenie tej samej kolumny, posortuje jej zawartość malejąco. Do sortowania można wykorzystywać tylko jedną kolumnę jednocześnie.

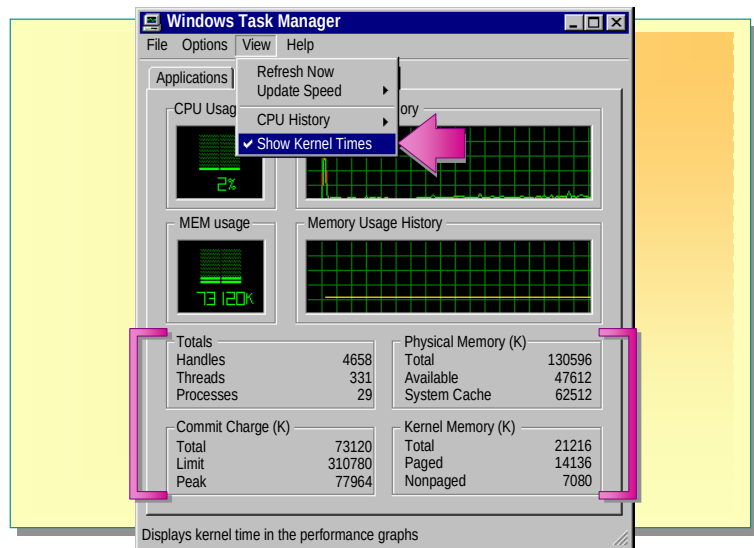
Monitorowanie wydajności

Cel slajdu

Ilustracja interfejsu do monitorowania wydajności w programie Task Manager.

Wprowadzenie

Na karcie **Performance** wyświetlane są dynamiczne zmiany wydajności komputera.



Karta **Performance** umożliwia monitorowanie wydajności systemu. Wyświetlane są na niej, na bieżąco odświeżane, informacje o wydajności systemu, łącznie z graficznymi i cyfrowymi wskaźnikami użycia procesora i pamięci.

W tabeli przedstawiono przegląd pomiarów, dostępnych na karcie **Performance**. Omów w skrócie niektóre z nich.

Wyjaśnij, że plik stronicowania i pamięć wirtualna będą omówione później.

Pomiary dla procesów

Niektóre pomiary dla procesów, dostępne na karcie **Performance**, opisano w poniższej tabeli.

Pomiar	Opis
Totals	Ilość uchwytów (<i>handle</i>), wątków i procesów uruchomionych na komputerze. <i>Uchwyt</i> jest zmienną, używaną do dostępu do urządzenia lub obiektu takiego jak plik, okno lub okno dialogowe. <i>Wątek</i> jest jednostką wykonywalną w procesie.
Physical Memory	Total: Rozmiar fizycznej pamięci RAM, w kilobajtach, zainstalowanej w komputerze. Available: Rozmiar fizycznej pamięci, w kilobajtach, dostępnej dla procesów. System Cache: Wielkość fizycznej pamięci, w kilobajtach, udostępnianej na żądanie jako pamięć podręczna dla plików.

(ciąg dalszy)

Pomiar	Opis
Commit Charge	Total: Rozmiar pamięci wirtualnej, w kilobajtach, wykorzystywanej przez wszystkie procesy. <i>Pamięć wirtualna</i> jest to przestrzeń na dysku, wykorzystywana przez system operacyjny i obsługiwana jako pamięć RAM. Limit: Rozmiar pamięci wirtualnej, w kilobajtach, jaka może być wykorzystana przez wszystkie procesy, bez konieczności zwiększania pliku stronicowania. Poprzez <i>plik stronicowania</i>, strony pamięci są przenoszone pomiędzy dyskiem twardym i fizyczną pamięcią RAM. Peak: Maksymalny rozmiar pamięci wirtualnej, w kilobajtach, do wykorzystania w danej sesji. Może zostać powiększony poprzez zwiększenie limitu.
Kernel Memory	Total: Sumaryczny rozmiar, w kilobajtach, stronicowanej i nieostronicowanej pamięci. Paged: Rozmiar stronicowanych zasobów, w kilobajtach, zarezerwowanych dla systemu operacyjnego. Nonpaged: Rozmiar niestronicowanych zasobów, w kilobajtach, zarezerwowanych dla systemu operacyjnego.

Czas procesora

Wskazówka
Zademonstruj
obserwowanie czasu
procesora w trybie jądra.

Na karcie **Performance** programu Task Manager można odczytać wielkość zasobów systemowych, które wykorzystuje system operacyjny lub aplikacja i sprawdzić procentowe wykorzystanie czasu procesora w trybie jądra. *Jądro* jest rdzeniem systemu operacyjnego, zarządzającym pamięcią, plikami i urządzeniami zewnętrznymi; obsługuje też liczniki daty i czasu, uruchamia aplikacje i rezerwuje zasoby systemowe.

Aby sprawdzić procentowe wykorzystanie czasu procesora w trybie jądra, należy z menu **View** wybrać polecenie **Show Kernel Times**.

Czas procesora w trybie jądra wyświetlany jest na wykresie na czerwono. Jest to pomiar czasu, przez jaki aplikacje wykorzystują usługi systemu operacyjnego. Pozostały czas, wyświetlany na zielono, nazywany jest trybem użytkownika. Jest to czas, przez który aplikacja przetwarza własny kod.

Laboratorium A: Korzystanie z programów Task Manager i Event Viewer

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W tym laboratorium zostaną użyte programy Task Manager i Event Viewer do obserwacji pracy systemu i zarządzania dziennikami zdarzeń.



Wyjaśnij cel laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Monitorować pracę aplikacji w programie Task Manager.
- Zamykać aplikacje poprzez program Task Manager.
- Monitorować aktywność komputera poprzez program Event Viewer.
- Zarządzać dziennikami zdarzeń.
- Odszukiwać informacje w dziennikach zdarzeń.

Wymagania wstępne

Przed rozpoczęciem laboratorium należy:

- Zapoznać się z zabezpieczeniami plików w systemie Windows 2000.
- Zapoznać się z informacjami o monitorowaniu zabezpieczeń w systemie Windows 2000.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Windows 2000 Advanced Server, skonfigurowany jako serwer członkowski w domenie nwtraders.msft.
- Domenowe konto użytkownika o nazwie Adminx (gdzie x jest numerem komputera słuchacza).
- Domenowe konto użytkownika, które nie posiada praw administratorskich. Jeśli takie nie istnieje należy je utworzyć.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Monitorowanie pracy aplikacji w programie Task Manager

Scenariusz

Zarządzasz serwerem pracującym w systemie Windows 2000. Do twoich zadań należy monitorowanie pracy serwera i skuteczności zabezpieczeń. W ostatnim czasie wydajność serwera znacznie spadła. Przypuszczasz, że jedna z pracujących na nim aplikacji wykorzystuje nieproporcjonalnie dużo zasobów systemowych. Musisz sprawdzić, która to aplikacja i podjąć działania mające na celu poprawienie wydajności.

Cel

W tym ćwiczeniu uruchomisz kilka aplikacji i wykorzystasz program Task Manager, aby określić, jakie zasoby systemowe są przez nie wykorzystywane. Następnie użyjesz programu Task Manager do zamknięcia aplikacji.

Zadanie	Szczegółowe kroki
1. Zaloguj się do domeny nwtraders jako Adminx (gdzie x jest numerem Twojego stanowiska) z hasłem domain , a następnie uruchom Lab08a1.cmd z folderu C:\MOC\Win2152b\Labfiles\Lab08.	a. Zaloguj się, wykorzystując poniższe informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. W programie Windows Explorer odszukaj folder C:\MOC\Win2152b\Labfiles\Lab08 i uruchom Lab08a1.cmd . c. Zamknij program Windows Explorer.
2. Użyj programu Task Manager do określenia, która aplikacja w największym stopniu wykorzystuje zasoby systemowe i jakie są to zasoby.	a. Naciśnij kombinację klawiszy CTRL+ALT+DELETE i uruchom program Task Manager . b. Na karcie Applications przejrzyj uruchomione programy.
Czy na liście znajdują się jakieś procesy systemu operacyjnego? Dlaczego? Nie. Lista nie zawiera procesów systemu operacyjnego, ponieważ na karcie Applications znajdują się tylko procesy uruchomione w kontekście aktualnego użytkownika.	
2. (ciąg dalszy)	c. Wybierz kartę Performance .

(ciąg dalszy)

Zadania	Szczegółowe kroki
? Jakie zasoby systemowe są wykorzystywane w największym stopniu? Moc procesora wykorzystana jest prawie w 100 procentach.	
2. (ciąg dalszy)	d. Przejdź na kartę Processes .
? Który proces wykorzystuje w największym stopniu moc procesora? Czy może to powodować problemy? Aplikacja App1-5. Może to powodować problemy, ponieważ wysoki stopień wykorzystania mocy procesora może utrudniać pracę innym programom.	
? Który proces od startu komputera w największym stopniu wykorzystał czas procesora? Czy to może powodować problemy? Dlaczego? W największym stopniu czas procesora wykorzystany był przez proces System Idle Process. Nie powoduje to żadnych problemów, ponieważ czas wyświetlany dla tego procesu jest czasem, przez który procesor nie był wykorzystywany.	
2. (ciąg dalszy)	e. Z menu View wybierz polecenie Select Columns. f. W oknie dialogowym Select Columns zaznacz pola opcji I/O Read Bytes i I/O Write Bytes, a następnie wybierz przycisk OK. g. Przesuń ramkę okna programu Task Manager w prawo, aż będą widoczne wszystkie kolumny.

(ciąg dalszy)

Zadania	Szczegółowe kroki
 Czy aplikacja App1-5 w dużym stopniu wykorzystuje przestrzeń dysku twardego? Nie.	
3. Zamknij programy App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe i App1-5.exe, wykorzystując program Task Manager.	a. Zaznacz App1-5.exe i wybierz przycisk End Process. b. W oknie dialogowym Task Manager Warning przeczytaj ostrzeżenie i wybierz przycisk Yes. c. Zamknij w ten sam sposób aplikacje App1-1.exe, App1-2.exe, App1-3.exe i App1-4.exe, a następnie zamknij program Task Manager.

Ćwiczenie 2

Obserwowanie aktywności komputera poprzez program Event Viewer

Scenariusz

Aby upewnić się, że komputer pracuje bez żadnych nieprawidłowości, regularnie korzystasz z programu Event Viewer do sprawdzania pracy komputera podczas ostatniego tygodnia. Wymagania bezpieczeństwa twojej firmy nakazują również regularne archiwizowanie dzienników zdarzeń z każdego tygodnia.

Cel

W tym ćwiczeniu dokonasz przeglądu plików dzienników systemu Windows 2000, skonfigurujesz archiwizację dzienników i zarchiwizujesz je.

Zadania	Szczegółowe kroki
1. Skorzystaj z programu Event Viewer, aby określić, kiedy twój komputer był ostatnio uruchomiony.	a. Uruchom program Event Viewer z menu Administrative Tools . b. W drzewie konsoli wskaż System Log , jeśli to konieczne. c. W oknie szczegółów odszukaj najnowsze zdarzenie i otwórz okno jego opis.
 Uwaga: W systemie Windows 2000, usługa dzienników zdarzeń uruchamiana jest automatycznie przy starcie komputera. Czas uruchomienia usługi jest w przybliżeniu czasem uruchomienia komputera.	
1. <i>(ciąg dalszy)</i>	d. Wybierz przycisk OK , aby zamknąć okno dialogowe Event Properties . e. Przejrzyj typy zdarzeń występujące w każdym z dzienników. f. Nie zamykaj programu Event Viewer.

Ćwiczenie 3

Archiwizacja dziennika aplikacji

Scenariusz

Bezpieczeństwo twojej firmy wymaga, abyś przeglądał i archiwizował dzienniki zdarzeń raz na tydzień.

Cel

W tym ćwiczeniu zarchiwizujesz dziennik aplikacji Twojego komputera.

Zadania	Szczegółowe kroki
1. Zapisz dziennik aplikacji w pliku yyyy-mm-dd.evt (gdzie yyyy jest aktualnym rokiem, mm to dwie pierwsze litery nazwy bieżącego miesiąca, a dd to aktualna data) w folderze C:\MOC\Win2152b\Labfiles\Lab08, a następnie wyczyść dziennik aplikacji.	a. W drzewie konsoli Event Viewer wskaż Application Log. b. Z menu Action wybierz Save Log File As. c. W oknie dialogowym Save "Application Log" As, w polu Save in odzyskaj folder C:\MOC\Win2152b\Labfiles\Lab08, a następnie zapisz dziennik aplikacji w pliku o nazwie yyyy-mm-dd.evt (gdzie yyyy jest aktualnym rokiem, mm jest aktualnym miesiącem, a dd jest aktualnym dniem). d. Z menu Action wybierz polecenie Clear all Events. e. W oknie komunikatu Event Viewer wybierz przycisk No, aby wyczyścić zdarzenia bez ich zapisywania.

Ćwiczenie 4

Wyszukiwanie określonych zdarzeń w zapisanym dzienniku

Scenariusz

Dział bezpieczeństwa twojej firmy przypuszcza, że nastąpiło naruszenie bezpieczeństwa w sieci firmowej. Otrzymałeś zadanie przejrzenia i zarchiwizowanych dzienników bezpieczeństwa, aby odszukać potencjalne ślady takiego naruszenia. Dział bezpieczeństwa potrzebuje informacji o wszystkich wypadkach nieautoryzowanych prób dostępu do zasobów w folderze Projects.

Cel

W tym ćwiczeniu dokonasz filtracji dziennika bezpieczeństwa w celu odśledzenia przypadków dostępu do folderu Projects.

Zadania	Szczegółowe kroki
1. Otwórz zapisany w pliku C:\MOC\Win2152b\Labfiles\Lab08\Lab08A.evt dziennik bezpieczeństwa i sprawdź pierwsze zdarzenie.	a. W drzewie konsoli prawym przyciskiem myszy wskaż Event Viewer (Local) , a następnie wybierz polecenie Open Log File . b. W oknie dialogowym Open , w polu Look in odśledź folder C:\MOC\Win2152b\Labfiles\Lab08, jeśli będzie to konieczne, a następnie wybierz plik Lab08A.evt . c. W polu Log Type wskaż Security i wybierz przycisk Open . d. Otwórz pierwsze zdarzenie w dzienniku. e. Przeczytaj informacje na temat tego zdarzenia i wybierz przycisk ze strzałką w dół, aby przejść do kolejnego zdarzenia.
? Czy sprawdzanie każdego zdarzenia jest najwydajniejszą metodą poszukiwania konkretnych informacji? Nie. Przy dużej ilości zdarzeń w dzienniku potrzebny jest jakiś sposób, aby odfiltrować te, które nie są istotne przy bieżących poszukiwaniach. 	
1. <i>(ciąg dalszy)</i>	f. Wybierz przycisk Cancel , aby zamknąć okno dialogowe Event Properties .
2. Przefiltruj zdarzenia w dzienniku tak, aby zostały tylko zakończone niepowodzeniem, a następnie posortuj je pod względem kategorii.	a. W drzewie konsoli wskaż prawym przyciskiem myszy Saved Security Log , wybierz polecenie View , a następnie Filter . b. W oknie dialogowym Saved Security Log Properties , w sekcji Event types wyczyść wszystkie pola opcji, poza Failure audit i wybierz przycisk OK . c. Wskaż nagłówek kolumny Category , aby posortować zdarzenia.

(ciąg dalszy)

Zadania	Szczegółowe kroki
3. Odszukaj w zapisanym dzienniku zdarzenia nieautoryzowanych prób dostępu do folderu E:\Projects. Sprawdź, który użytkownik podjął próby dostępu do tego folderu i czy była to tylko jednokrotna próba.	a. Wskaż prawym przyciskiem myszy Saved Security Log, a następnie rozwiń menu View i wybierz polecenie Find. b. W oknie dialogowym Find in local Saved Security Log, w sekcji Event Types wyczyść wszystkie pola opcji, z wyjątkiem Failure audit. c. W polu Event ID wpisz 560.
 Uwaga: Zdarzenie o numerze 560 opisuje nieudaną próbę dostępu do zasobów, takich jak plik lub folder.	
3. (ciąg dalszy)	d. W polu Description wpisz e:\projects i wybierz przycisk Find Next, aby przeszukiwać zdarzenia.  <i>Najbliższe zdarzenie, spełniające kryteria wyszukiwania, jest podświetlane. Ponieważ dziennik był zapisywany na komputerze nie należącym do sieci znajdującej się w pracowni, w systemie Windows 2000 nie będzie możliwe rozpoznanie, do jakiego użytkownika należy identyfikator bezpieczeństwa (SID). W kolumnie User będzie wyświetlony tylko SID.</i> e. Przesuń okno dialogowe Find in local Saved Security Log, jeśli to konieczne, a następnie otwórz podświetlone zdarzenie.
 W oparciu o informacje opisujące zdarzenie, należy odczytać, jaka jest nazwa użytkownika, który próbował uzyskać dostęp do folderu? User1.	
3. (ciąg dalszy)	f. Wybierz przycisk Cancel, aby zamknąć okno Event Properties. g. Wybierz prawym przyciskiem myszy Saved Security Log, a następnie rozwiń menu View i wybierz polecenie All Records. h. Wskaż prawym przyciskiem myszy Saved Security Log, a następnie rozwiń menu View i wybierz polecenie Find. i. W oknie dialogowym Find in local Saved Security Log, w sekcji Event types wyczyść wszystkie pola opcji, z wyjątkiem Failure audit. j. Sprawdź, czy w polu Event ID wpisane jest 560. k. W polu Description wpisz User1 i wybierz przycisk Find Next. l. Wybieraj przycisk Find Next, aż zostanie wyświetlona informacja, że przeszukano wszystkie zdarzenia. m. W oknie dialogowym Event Viewer wybierz przycisk No, aby nie kontynuować przeszukiwania od początku dziennika.

(ciąg dalszy)

Zadania	Szczegółowe kroki
 Czy była to jednokrotna próba uzyskania dostępu do zasobów? Użytkownik User1 próbował dostać się do folderu kilkakrotnie, ponieważ wystąpiło kilka zdarzeń z tym związanych.	
4. Przeszukaj zdarzenia w celu stwierdzenia, czy użytkownik User1 uzyskał dostęp do folderu E:\Projects.	a. W oknie dialogowym Find in local Saved Security Log, w sekcji Event types, wyczyść wszystkie pola opcji, z wyjątkiem Success audit. b. Sprawdź, czy w polu Event ID znajduje się wartość 560. c. Sprawdź, czy w polu Description wpisane jest User1, a następnie wybierz przycisk Find Next. d. Otwórz opis podświetlonego zdarzenia. e. Zapoznaj się z dostępnymi informacjami na temat zdarzenia i wybierz przycisk OK, aby zamknąć okno dialogowe Event Properties. f. Wybierz przycisk Close, aby zamknąć okno dialogowe Find in local Saved Security Log.

Ćwiczenie 5

Zapisywanie dzienników zdarzeń do plików o wybranym formacie

Scenariusz

Dział bezpieczeństwa firmy wymaga zapisywania zdarzeń naruszenia bezpieczeństwa na jednym z serwerów. Dane mają być zapisane w formacie pliku tekstowego z separatorami, aby mogły być importowane do programu Microsoft Excel w celu dalszej analizy.

Cel

W tym ćwiczeniu zapiszesz wcześniej zachowany dziennik bezpieczeństwa w formacie pliku tekstowego z separatorami.

Zadania	Szczegółowe kroki
1. Zapisz dziennik bezpieczeństwa z pliku Lab08A.evt w formacie tekstowym z separatorami jako C:\MOC\Win2152b\Labfiles\Lab08\Seclog.csv, a następnie przejrzyj go przy pomocy Notatnika.	a. W drzewie konsoli, prawym przyciskiem myszy wskaż Saved Security Log i wybierz polecenie Save Log File As. b. W oknie dialogowym Save "Saved Security Log" As, w polu Look in odszukaj, jeśli to konieczne, folder C:\MOC\Win2152b\Labfiles\Lab08, a następnie w polu File name wpisz Seclog c. W polu Save as type wybierz CSV (Comma delimited) (*.csv), a następnie przycisk Save. d. Zamknij program Event Viewer. e. Otwórz menu Start i wybierz polecenie Run. f. W polu Open wpisz Notepad.exe C:\MOC\Win2152b\Labfiles\Lab08\Seclog.csv i wybierz przycisk OK. g. Odtwórz okno programu Notepad. h. Z menu Edit wybierz polecenie Find. i. W polu Find what wpisz e:\projects i wybierz przycisk Find Next. j. W oknie dialogowym Find wybierz przycisk Cancel. k. Zamknij program Notepad i wyloguj się.

◆ Wykorzystanie programu System Monitor do śledzenia wydajności systemu

Cel slajdu

Zestawienie zagadnień związanych z wykorzystaniem programu Task Manager do monitorowania zasobów systemowych.

Wprowadzenie

Jeżeli potrzeba więcej szczegółowych informacji, niż można uzyskać w programie Task Manager, należy użyć programu System Monitor. Dzięki niemu, można uzyskać zestawienie informacji na temat komputera, jak też innych komputerów w sieci.

- Obiekty, egzemplarze i liczniki
- Dodawanie liczników
- Przeglądanie danych

Jeżeli w programie Task Manager nie można uzyskać wystarczającej ilości szczegółowych informacji, można w tym celu wykorzystać program System Monitor. Dostępny jest on w sekcji Performance, konsoli MCC (Microsoft Management Console). Dzięki niemu, można zbierać w czasie rzeczywistym, lub przeglądać zebrane wcześniej informacje, na temat pamięci, dysku, procesora i aktywności w sieci. Informacje te pozwalają stwierdzić, jak funkcjonują aplikacje i zoptymalizować system. Na przykład, można wykryć zbyt małą ilość wolnego miejsca na dysku twardym.

Informacje zebrane w programie System Monitor mogą być przeglądane w postaci wykresu, histogramu (wykres słupkowy) lub raportu. Dane te mogą być przeglądane i drukowane także po zapisaniu ich w formacie HTML (Hypertext Markup Language).

Obiekty, instancje i liczniki

Cel slajdu

Ilustracja obiektów, liczników i instancji w programie System Monitor.

Wprowadzenie

Zrozumienie, jak powiązane są ze sobą obiekty, instancje i liczniki, jest bardzo ważne dla skutecznego posługiwania się programem System Monitor.

- **Obiekty programu System Monitor, to główne komponenty lub podsystemy systemu komputerowego**
- **Instancje, to wielokrotne wystąpienia jednego obiektu**
- **Liczniki:**
 - Pomiar różnych cech obiektu
 - Ciągłe zbieranie danych o obiekcie
 - Dane o wszystkich instancjach obiektu
 - Mogą być wyświetlane w programie System Monitor

Podaj definicję obiektu, instancji i licznika.

Upewnij się, że słuchacze rozumieją różnicę pomiędzy obiektami występującymi w programie System Monitor i w usłudze Active Directory.

Zrozumienie, jak powiązane są ze sobą obiekty, instancje i liczniki ma podstawowe znaczenie dla skutecznego wykorzystania programu System Monitor.

- **Obiekty.** Obiekty w programie System Monitor, to główne komponenty lub podsystemy systemu komputerowego. Może to być sprzęt, taki jak dysk twardy lub element programowy, taki jak proces. W systemie Windows 2000 ilość obiektów jest stała.

Ważne Obiekty Monitora systemu nie wiążą się w żaden sposób z obiektami usługi Active Directory™.

- **Instancje.** Instancje, to wielokrotne wystąpienia obiektu tego samego typu. Na przykład, w systemach wieloprocesorowych typ obiektu Processor występuje w wielu egzemplarzach.
- **Liczniki.** Liczniki pozwalają zbierać dane o różnych cechach obiektów. Na przykład, dla obiektu Process, poprzez liczniki gromadzone są dane o czasie procesu i czasie użytkownika. Liczniki są wbudowane w system operacyjny i zbierają dane w sposób ciągły, niezależnie od tego, czy uruchomiony jest Monitor systemu, czy nie. Jeżeli dany obiekt występuje wiele razy, dane zbierane są, poprzez liczniki, dla każdej instancji z osobna lub tworzone jest jedno podsumowanie dla wszystkich.

W programie System Monitor można określić, które liczniki mają być brane pod uwagę.

Uwaga W programie Task Manager również występują liczniki, ale użytkownik nie ma wpływu na to, co jest wyświetlane.

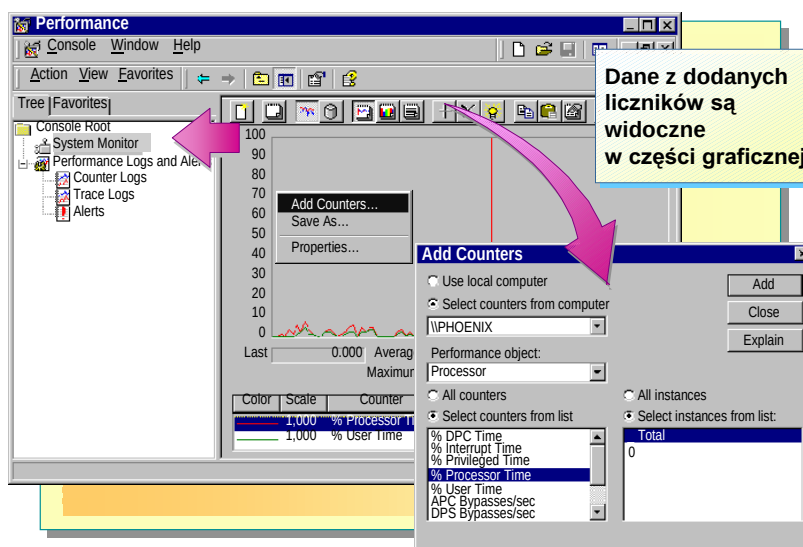
Dodawanie liczników

Cel slajdu

Zilustrowanie interfejsu do monitorowania wydajności systemu Windows 2000.

Wprowadzenie

W konsoli Performance znajdują się dwa narzędzia: System Monitor i Performance Logs and Alerts.



Wskazówka

Podczas opisywania Monitora systemu otwórz okno Performance i dodaj licznik. Zaznacz, że dla każdego obiektu istnieje kilka liczników i wybierz obiekt występujący przynajmniej w dwóch egzemplarzach.

Ponieważ liczniki zbierają dane o pracy systemu w sposób ciągły, dodawanie liczników w monitorze systemu oznacza tylko konfigurację wyświetlania zebranych danych. Pozwala to śledzić wydajność systemu.

Uwaga Dla monitorowania wydajności w konsoli MCC (Microsoft Management Console) przeznaczone są dwa komponenty: System Monitor i Performance Logs and Alerts.

Aby dodać licznik w programie System Monitor, należy:

1. Rozwinąć menu start **Start, Programs**, następnie **Administrative Tools** i wybrać polecenie **Performance**.
Po pierwszym uruchomieniu, w oknie programu System Monitor wyświetlany jest pusty wykres.
2. Prawym przyciskiem myszy wskazać panel szczegółów programu System Monitor i z menu podręcznego wybrać polecenie **Add Counters**.
3. Z listy **Performance object** wybrać obiekt do obserwacji.

W programie System Monitor występuje ponad 350 liczników. Lista dostępnych liczników znajduje się w sekcji Server Operations Guide publikacji *Microsoft Windows 2000 Server Resource Kit*.

Dostępne obiekty są zdefiniowane w oparciu o usługi i aplikacje, zainstalowane na danym komputerze. Dla jednego obiektu można wybrać kilka różnych liczników. W poniższej tabeli opisano główne obiekty systemu Windows 2000, dostępne w programie System Monitor.

Nazwa obiektu	Opis
Cache	Obszar pamięci fizycznej, przechowujący ostatnio używane dane.
Memory	Pamięć RAM, wykorzystywana do przechowywania kodu programów i danych.
Objects	Niektóre obiekty oprogramowania systemowego.
Paging File	Plik używany do przechowywania pamięci wirtualnej.

(ciąg dalszy)

Nazwa obiektu	Opis
Physical Disk	Dysk fizyczny (macierz lub urządzenie typu RAID).
Process	Obiekt programowy, reprezentujący uruchomiony program.
Processor	Jednostka fizyczna, wykonująca instrukcje programu.
Server	Usługa obsługująca żądania pobrania danych, przychodzące od klientów sieciowych.
System	Liczniki dla sprzętu i oprogramowania systemowego.
Thread	Część procesu wykorzystująca procesor.

Po wybraniu obiektu, powiązane z nim liczniki zostaną wyświetlone na liście.

Uwaga Wybierz przycisk **Explain**, aby obejrzeć opis licznika wskazanego w oknie dialogowym **Add Counters**.

- Wybrać przycisk **All counters** lub **Select counters from list**, aby wybrać konkretny licznik.
- Jeżeli obiekt występuje w wielu instancjach, należy wybrać **All instances** lub **Select instances from list**, aby wybrać konkretny egzemplarz.
- Wybrać przycisk **Add**, a następnie **Close**, aby zamknąć okno dialogowe **Add Counters**.

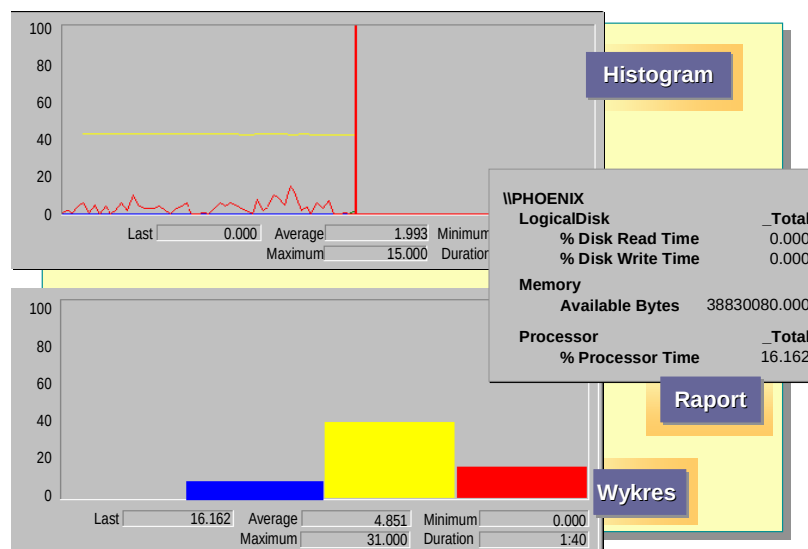
Przeglądanie danych

Cel slajdu

Zilustrowanie trzech sposobów przeglądania danych w programie System Monitor.

Wprowadzenie

Po dodaniu liczników, dane można przeglądać na trzy sposoby.



Po dodaniu liczników, można przeglądać zebrane przez nie dane w czasie rzeczywistym. Dane mogą być wyświetlane na trzy sposoby:

Zagadnienia kluczowe

Administrator może przeglądać dane zebrane przez liczniki na jeden z trzech sposobów: histogram, raport lub wykres.

- **Wykres.** Dane wyświetlane są w postaci wykresu liniowego. Przydatne do monitorowania danych w czasie rzeczywistym.
- **Raport.** Dane wyświetlane są jako zestaw liczb w kolumnach. Jest to przydatne przy zbieraniu danych, które mają być eksportowane, na przykład, do arkusza kalkulacyjnego.
- **Histogram.** Dane wyświetlane są na wykresie słupkowym. Jest to użyteczna metoda przy obserwacji wielu liczników.

Zmiany i dostosowania sposobu wyświetlania informacji, można dokonać po wskazaniu prawym przyciskiem myszy okna szczegółów i wybraniu polecenia **Properties**. Szczegółowe informacje na temat zmiany ustawień można znaleźć w sekcji Server Operations Guide *Windows 2000 Server Resource Kit*.

Wspomnij, że administrator może zapisywać zebrane dane w formacie HTML.

Wskazówka Jeśli wyświetlanych jest kilka liczników, może być trudne odszukanie danych z konkretnego licznika. Aby wyróżnić słupki lub linię dla wybranego licznika na białą (domyślnie) lub czarną (dla jasnego tła), należy na pasku narzędzi wybrać przycisk **Highlight** lub nacisnąć CTRL+H.

Dane można zapisać w pliku w formacie HTML i przeglądać przy pomocy programu Microsoft Internet Explorer lub innej przeglądarki witryn internetowych. Można również drukować tak zapisane dane. Aby zapisać dane w formacie HTML, należy w programie System Monitor, prawym przyciskiem myszy wskazać panel szczegółów i podać nazwę pliku.

Uwaga Dane można również zbierać w programie Performance Logs and Alerts, w postaci dzienników do późniejszego przeglądania. Istnieją dwa typy dzienników. Dane z liczników, zapisywane w dziennikach, odnoszą się do zasobów sprzętowych i usług systemowych. Dzienniki liczników wykorzystuje się do śledzenia trendów.

Więcej informacji o licznikach, śledzeniu trendów i ich konfiguracji można znaleźć w pomocy systemu Windows 2000.

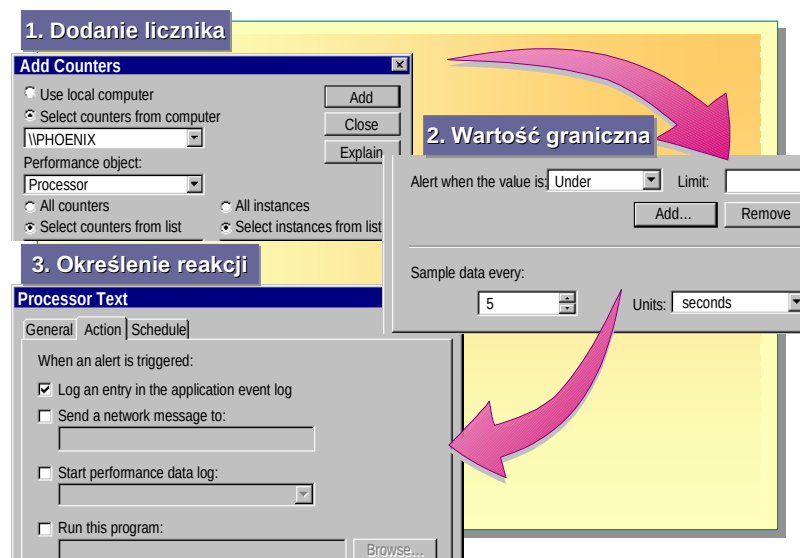
Alerty

Cel slajdu

Prezentacja procesu ustawiania alertów.

Wprowadzenie

Ustawianie alertu jest procesem trzystopniowym.



Zagadnienie kluczowe

Alerty mogą być używane do ostrzegania użytkowników lub obsługi, gdy kryteria nałożone na system zostaną przekroczone.

Alerty wykorzystuje się do informowania użytkowników i administratorów, gdy wskaźniki przekroczą wartości graniczne. Dodatkowo, dzienniki aktywności można wykorzystać do zbierania danych o zasobach sprzętowych, usługach systemowych i wydajności.

Alerty

Alerty są przydatne, jeżeli administrator nie monitoruje w sposób ciągły poszczególnych liczników, ale chce być powiadamiany, jeżeli któryś z nich przekroczy określoną wartość, aby móc określić powody takiego zdarzenia i podjąć odpowiednie kroki. Można, na przykład, skonfigurować alert w sytuacji przekroczenia wykorzystanej przestrzeni dysku powyżej 80 procent lub gdy ilość nieudanych logowań przekroczy określoną wartość. Aby ustawić alert należy wykonać trzy czynności:

1. Wybrać odpowiedni licznik do śledzenia.
2. Ustawić dla niego graniczną wartość.
3. Określić czynność, jaka ma być wykonana, gdy zostanie przekroczona wartość graniczna:
 - Send a network message.
 - Run a program.
 - Start a log.

Wskazówka

Zademonstruj ustawianie alertu.

Uwaga Aby uruchomić program Performance Logs and Alerts, konieczne jest prawo uruchamiania i konfiguracji usług systemowych. Domyślnie, prawo takie posiada administrator.

Ustawianie alertu

Alerty ustawia się w konsoli Performance, w programie Performance Logs and Alerts. Aby ustawić alert należy:

1. W drzewie konsoli, otworzyć **Performance Logs and Alerts** i wybrać **Alerts**.
2. W panelu szczegółów, wskazać prawym przyciskiem myszy **New Alert Setting** i podać nazwę dla alertu.
3. Na karcie **General**, w polu **Comment** wprowadzić krótki opis.
4. W oknie dialogowym **Add Counters** wybrać przycisk **Add** w celu wskazania obiektów, liczników lub instancji.
5. Po dodaniu liczników, na karcie **General** określić interwał próbkowania i wartość graniczną.
6. Upewnić się, że na karcie **Action** wybrana jest opcja **Log an entry in the application event log**. Można również określić wiadomość, jaka będzie wysłana przez komputer generujący alert.
7. Na karcie **Schedule**, w polach **Start scan** i **Stop scan** zdefiniować parametry początkowe i końcowe dziennika, a następnie wybrać przycisk **OK**.

Laboratorium B: Monitorowanie aktywności systemu

Cel slajdu

Omówienie laboratorium.

Wprowadzenie

W tym ćwiczeniu monitorowana będzie aktywność systemu i ustawiane alerty, z wykorzystaniem liczników.



Wyjaśnij cel laboratorium.

Cele laboratorium

Po zrealizowaniu tego laboratorium słuchacz będzie potrafił:

- Monitorować aktywność systemu w programie System Monitor.
- Ustawiać i przeglądać alerty.
- Tworzyć i przeglądać dzienniki wydajności.

Wymagania wstępne

Przed rozpoczęciem laboratorium należy:

- Zapoznać się z głównymi elementami sprzętowymi, które wchodzi w skład komputera z zainstalowanym systemem Windows 2000.
- Znać obsługę programu Internet Explorer.

Przygotowanie laboratorium

Do wykonania tego laboratorium niezbędne są:

- Komputer pracujący w systemie Windows 2000 Advanced Server, skonfigurowany jako serwer członkowski w domenie nwtraders.msft.
- Domenowe konto użytkownika o nazwie Adminx (gdzie x jest numerem stanowiska).
- Domenowe konto użytkownika, które nie posiada praw administratorskich. Jeśli takie nie istnieje, należy je utworzyć.
- Drukarka o nazwie Color Printer.

Przewidywany czas ukończenia laboratorium: 30 minut

Ćwiczenie 1

Monitorowanie aktywności w programie System Monitor

Scenariusz

Do twoich obowiązków należy kontrolowanie, czy serwer pracuje wydajnie i ustawianie alertów, ostrzegających o wystąpieniu sytuacji awaryjnych. Musisz też mieć możliwość analizy problemów, które zgłaszają użytkownicy. Obawiasz się wpływu, jaki może mieć defragmentacja dysku na wydajność twojego komputera. Decydujesz, że defragmentacja musi być przeprowadzona, gdy użytkownicy nie wykorzystują zasobów twojego serwera.

Cel

W tym ćwiczeniu uruchomisz program System Monitor i ustawisz w nim kilka liczników do monitorowania pracy procesora, pamięci i wykorzystania dysku.

Zadania	Szczegółowe kroki
1. Zaloguj się jako Adminx (gdzie x jest numerem Twojego stanowiska), z menu Administrative Tools uruchom program Performance, a następnie dodaj liczniki Processor\% Processor Time, Memory\Available Bytes, PhysicalDisk\% Disk Read Time i PhysicalDisk\%Disk Write Time.	a. Zaloguj się, wykorzystując poniższe informacje: User name: Adminx (gdzie x jest numerem Twojego stanowiska) Password: domain Log on to: nwtraders b. Z menu Administrative Tools otwórz program Performance. c. W drzewie konsoli sprawdź, czy jest wybrany System Monitor. d. Prawym przyciskiem myszy wskaż panel szczegółów i wybierz polecenie Add Counters.  <i>Domyślnie, w części Select counters from list, wybrany jest licznik % Processor. Jest to najczęściej używany licznik.</i> e. W oknie dialogowym Add Counters wybierz przycisk Explain i przeczytaj opis licznika % Processor Time. f. W polu poniżej opcji Select instances from list upewnij się, że jest wybrana pozycja _Total, a następnie wybierz przycisk Add. g. Z listy Performance object wybierz Memory i na liście Select counters from list wskaż licznik Available Bytes, a następnie wybierz przycisk Add. h. Z listy Performance object wybierz PhysicalDisk i na liście Select counters from list wskaż licznik % Disk Read Time, a następnie wybierz przycisk Add. i. Na liście Select counters from list wskaż licznik % Disk Write Time, a następnie wybierz przycisk Add. j. Wybierz przycisk Close aby zamknąć okno dialogowe Add Counters, a następnie zminimalizuj okno Performance.
2. Korzystając z programu System Monitor przejrzyj analizę defragmentacji dysku.	a. Z menu Administrative Tools wybierz polecenie Computer Management. b. W kontenerze Storage wybierz Disk Defragmenter. c. W panelu szczegółów wybierz przycisk Analyze. d. Po zakończeniu analizy defragmentacji dysku wybierz przycisk Close, aby zamknąć okno Analysis Complete.

Zadania	Szczegółowe kroki
2. (ciąg dalszy)	e. Zamknij program Computer Management i przywróć okno Performance. f. W panelu szczegółów wybierz przycisk Freeze Display (czerwone koło z białym znakiem X). g. Na dole panelu szczegółów, w sekcji Counter, sprawdź czy jest wybrany % Processor Time. h. Wciśnij klawisz CTRL, a następnie H, aby wyróżnić aktualnie wybrany licznik. i. Korzystając z przycisków ze strzałkami w górę i w dół, dokonaj przeglądu innych liczników.
? Z których zasobów systemowych korzysta, przede wszystkim, program Disk Defragmenter? Disk Defragmenter wykorzystuje %Processor Time i %Disk Read Time. Można również dostrzec operacje zapisu na dysku.	
2. (ciąg dalszy)	j. Na dole panelu szczegółów, w sekcji Object, wskaż prawym przyciskiem myszy Memory i wybierz polecenie Properties. k. W oknie dialogowym System Monitor Properties, na karcie Data, w sekcji Counters sprawdź, czy jest wybrany \\server\Memory\Available Bytes (gdzie <i>server</i> jest nazwą Twojego komputera). l. W polu Scale wybierz najmniejszą dostępną wartość i wybierz przycisk OK.
? Czy użycie pamięci zmieniło się znacznie po uruchomieniu programu Disk Defragmenter? Nie.	
2. (ciąg dalszy)	m. Wskaż prawym przyciskiem myszy panel szczegółów i wybierz przycisk Save As. n. W oknie Save As, w polu Save in odszukaj Desktop. o. W polu File name wpisz System Overview i wybierz przycisk Save. p. Zminimalizuj okno Performance. q. Otwórz na pulpicie System Overview.htm. r. Przejrzyj informacje zapisane w postaci strony sieci Web i zamknij okno programu Internet Explorer.

Ćwiczenie 2

Ustawianie alertów

Scenariusz

Chcesz mieć możliwość szybkiego reagowania na problemy z drukarką. W tym celu konfigurujesz alert, który będzie generowany, gdy w kolejce drukarki będzie zbyt wiele dokumentów. Duża ilość dokumentów w kolejce drukarki wskazuje zazwyczaj na jej niewłaściwą pracę.

Cel

W tym ćwiczeniu skonfigurujesz alert informujący o oczekiwaniu w kolejce wydruku więcej niż pięciu dokumentów.

Zadania	Szczegółowe kroki
1. Odłącz drukarkę.	a. Rozwiń menu Start, następnie Settings i wybierz polecenie Printers. b. W folderze Printers, prawym przyciskiem myszy wskaż Color Printer i wybierz polecenie Use Printer Offline. c. Zamknij folder Printers.
2. Ustaw alert wysyłający wiadomość do twojego komputera, gdy użycie procesora przekroczy 90 procent i zapisujący to zdarzenie do dziennika zdarzeń.	a. Przywróć okno Performance. b. W drzewie konsoli rozwiń Performance Logs and Alerts, prawym przyciskiem myszy wskaż Alerts i z menu podręcznego wybierz polecenie New Alert Settings. c. W oknie dialogowym New Alert Settings wpisz Print Queue i wybierz przycisk OK. d. W oknie Print Queue, w polu Comment, wpisz More than 5 documents in the print queue i wybierz przycisk Add. e. W oknie dialogowym Select Counters, w polu Performance object wybierz Print Queue, a następnie upewnij się, że na liście Select counters from list wybrana jest pozycja Jobs. f. Z listy Select instances from list wybierz Color Printer. g. Wybierz przycisk Add, a następnie przycisk Close. h. Z listy Alert when the value is, wybierz Over, a w polu Limit wpisz 5. i. W sekcji Sample data entry, w polu Interval wpisz 10 i upewnij się, że w polu Units wyświetlona jest jednostka miary seconds. j. Upewnij się, że na karcie Action jest zaznaczone pole opcji Log an entry in the application event log. k. Zaznacz pole opcji Send a network message to i wpisz Server (gdzie Server jest nazwą Twojego komputera). l. Upewnij się, że na karcie Schedule, w sekcji Start scan jest wybrana opcja At i wybierz przycisk OK. m. Zminimalizuj okno Performance.

(ciąg dalszy)

Zadania	Szczegółowe kroki
3. Zainicjuj skonfigurowany alert poprzez uruchomienie wygaszacza ekranu OpenGL. Następnie, przejrzyj dziennik aplikacji, w celu odszukania alertu.	a. Otwórz Notatnik i wydrukuj pusty dokument sześć razy. Zamknij Notatnik.  Zostanie wyświetlone okno dialogowe Messenger Service z informacją, że ilość zleceń wydruku przekroczyła limit. b. Przywróć okno Performance. c. W drzewie konsoli wybierz Alerts, w panelu szczegółów, prawym przyciskiem myszy wybierz Print Queue, następnie polecenie Stop i zminimalizuj okno Performance. d. Zamknij wszystkie okna komunikatów Messenger Service. e. Z menu Administrative Tools uruchom Computer Management. f. W kontenerze System Tools rozwiń Event Viewer i wybierz dziennik Application. g. W panelu szczegółów otwórz zdarzenie, którego źródłem jest SysmonLog. h. W oknie dialogowym Event Properties przeczytaj opis zdarzenia i wybierz przycisk OK. i. Zamknij program Computer Management.

Ćwiczenie 3

Zapisywanie aktywności systemu w dziennikach liczników

Scenariusz

Do twoich obowiązków należy monitorowanie pracy serwera. Ostatnio otrzymujesz od użytkowników raporty, że serwer często pracuje bardzo wolno. Nie można tego wychwycić podczas przeglądania danych w programie Monitor System. Decydujesz się utworzyć dziennik licznika, w którym zapisywana będzie praca kilku komponentów systemu. W dzienniku będą zbierane dane z dłuższego okresu czasu.

Cel

W tym ćwiczeniu utworzysz dziennik licznika i przejrzysz zebrane w nim dane.

Zadania	Szczegółowe kroki
1. Utwórz dziennik licznika, wykorzystując ustawienia zapisane podczas pracy z programem System Monitor we wcześniejszej części tego laboratorium i zainicjuj zapisywanie.	a. Przywróć okno Performance. b. W drzewie konsoli wskaż prawym przyciskiem myszy kontener Counter Logs i wybierz polecenie New Log Settings From. c. W oknie dialogowym Open, w polu Look in odszukaj pulpit, wskaż plik System Overview, a następnie wybierz przycisk Open. d. W oknie dialogowym Performance Logs and Alerts wybierz przycisk OK. e. W oknie dialogowym New Log Settings wpisz Long-term monitoring i wybierz przycisk OK. f. W oknie dialogowym Long-term monitoring, w polu Counters upewnij się, że wszystkie liczniki, które dodałeś w poprzednim laboratorium wciąż są wyświetlane. g. Sprawdź, czy w polu Interval wyświetlana jest 1, a w polu Units jednostka miary seconds. h. Wybierz przycisk OK. i. W oknie komunikatu Long-term monitoring wybierz Yes, aby utworzyć folder Perflogs. j. W drzewie konsoli wybierz Counter Logs, w panelu szczegółów wskaż prawym przyciskiem myszy Long-term monitoring i wybierz polecenie Start. k. Zminimalizuj okno Performance.
2. Uruchom na krótko wygaszacz ekranu OpenGL.	a. Wskaż prawym przyciskiem myszy pulpit i wybierz polecenie Properties. b. Na karcie Screen Saver, w polu Screen Saver wybierz 3D Pipes (OpenGL) i wybierz przycisk Preview. c. Nie dotykaj myszy i nie używaj klawiatury przez około 10 sekund. Następnie przesunij mysz w celu zatrzymania wygaszacza. d. Wybierz przycisk Cancel, aby zamknąć okno dialogowe Display Properties.

(ciąg dalszy)

Zadania	Szczegółowe kroki
3. Zatrzymaj dziennik aktywności i przejrzyj go przy pomocy Monitora systemu.	a. Przywróć okno Performance. b. W panelu szczegółów wskaż prawym przyciskiem myszy Long term monitoring i wybierz polecenie Stop . c. W drzewie konsoli wybierz System Monitor . d. W panelu szczegółów wybierz przycisk View Log File Data .
i Uwaga: Aby odszukać właściwy przycisk umieść na nim wskaźnik myszy i poczekaj na wyświetlenie etykiety.	
3. (ciąg dalszy)	e. W oknie dialogowym Select Log File , w polu Look in odzyskaj folder C:\Perflogs. f. Wskaż plik Long-term monitoring_000001.blg i wybierz przycisk Open .  Zebrane dane zostaną wyświetlone w oknie programu System Monitor.
? Które zasoby były wykorzystywane w największym stopniu? Procesor. 	
i Uwaga: Wygaszacz ekranu OpenGL bardzo mocno wykorzystuje moc procesora. Nawet jego podgląd może powodować gwałtowny wzrost użycia procesora. Wygaszacze takie nigdy nie powinny być konfigurowane na serwerach.	
3. (ciąg dalszy)	g. Zamknij okno Performance i wyloguj się.

◆ Optymalizacja wydajności

Cel slajdu

Przedstawienie zagadnień związanych z optymalizacją wydajności systemu.

Wprowadzenie

Zwiększenie wydajności powoduje lepsze i łatwiejsze wykorzystanie zasobów systemowych przez aplikacje.

- Proces optymalizacji wydajności
- Testowanie pracy pamięci
- Testowanie pracy procesora
- Testowanie pracy dysku
- Testowanie pracy sieci

Zdefiniuj pojęcie bazy i podaj informację z ramki **Ważne**.

Optymalizacja wydajności skutkuje lepszym wykorzystaniem zasobów systemowych przez aplikacje i system operacyjny. Poziom wydajności systemu, który można uznać za zadowalający, gdy uruchomione są niezbędne usługi i podczas wykonywania typowych zadań, nazywany jest *bazą*. Wydajność bazowa jest subiektywnym standardem, określonym przez administratora, w oparciu o pracę systemu w trakcie wykonywania typowych zadań. Baza może być użyteczną miarą do ustalenia zakładanej wydajności systemu.

Aby utworzyć bazę, zalecane jest monitorowanie podstawowych zasobów systemowych, takich jak:

- Pamięć.
- Aktywność procesora.
- Aktywność dysków.
- Aktywność sieci.

Ważne Podczas optymalizacji systemu, konieczne jest rozważenie wielu kwestii. Ta sekcja jest ich krótkim przeglądem. Więcej informacji na temat monitorowania i usprawniania pracy pamięci, procesora, dysków systemowych i komponentów sieciowych znajduje się w rozdziałach o optymalizacji, w sekcji Performance Monitoring in the Server Operations Guide w *Microsoft Windows 2000 Server Resource Kit*.

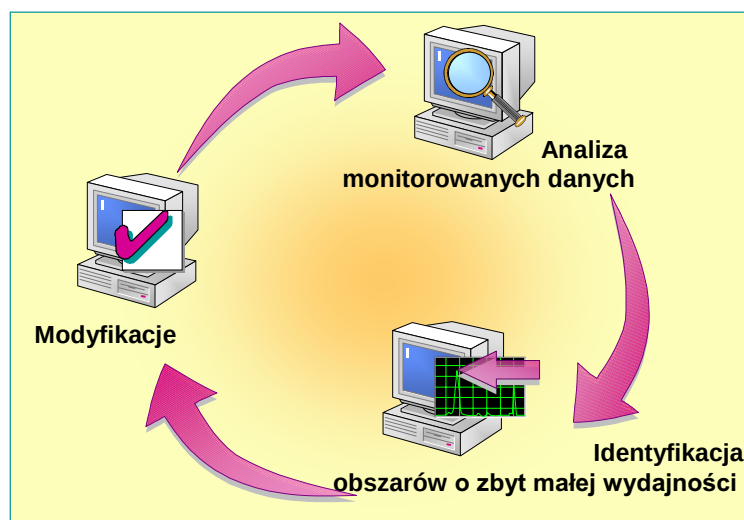
Proces optymalizacji wydajności

Cel slajdu

Zilustrowanie procesu optymalizacji wydajności.

Wprowadzenie

Optymalizacja wydajności jest stałym cyklem pomiarów i testów, rozwiązywania problemów i dokonywania zmian.

**Zagadnienie kluczowe**

Wyjaśnij, że analiza wydajności nie jest jednoznacznie określoną czynnością, ale stale ewoluującym procesem.

W procesie optymalizacji określa się działania, jakie należy podjąć, aby zwiększyć wydajność systemu. Proces optymalizacji rozpoczyna się od przemyślanego i zorganizowanego zbierania danych.

Do procesu optymalizacji należą następujące zadania:

- Analiza i monitorowanie danych. Analiza monitorowanych danych polega na sprawdzaniu danych, zebranych w licznikach podczas wykonywania przez system różnych operacji. Podczas tego procesu należy określić:
 - Który proces wykazuje się największą aktywnością i które programy lub wątki zawłaszczają zasoby systemowe.
 - Czy nadmierne wykorzystanie niektórych zasobów sprzętowych powoduje spadek wydajności systemu.
 - Czy wydajność któregoś elementu sprzętowego nie jest zbyt mała, w porównaniu do innych. Na przykład, system zaczyna pracować wolniej przy dużym wzroście aktywności dysku. Może to świadczyć o problemach z dyskiem twardym lub o niewystarczającej ilości pamięci RAM do obsługi aplikacji i systemu operacyjnego.

Dzięki takiej analizie, można przewidzieć zachowanie systemu przy zakładanym obciążeniu w normalnych warunkach pracy.

- Rozpoznawanie obszarów zbyt małej wydajności. W efekcie takiej analizy można stwierdzić, że dany system w niektórych warunkach spełnia wymagania, a w innych nie. Zatem decyzja, czy system działa wystarczająco wydajnie jest subiektywnym osądem jego pracy w różnorodnym środowisku użytkownika. Wartości, które zostaną przyjęte jako bazowe, są najlepszą podstawą do porównań. Należy jednak pamiętać, że aktywność systemu zmienia się w czasie. Porównania powinny obejmować różne okresy działania systemu.
- Wprowadzanie zmian. W zależności od przyczyny zmian i ich skali, można je wprowadzić na bieżąco lub odłożyć ich przeprowadzenie, jeżeli wymaga to uprzedniego zaplanowania. W niektórych przypadkach, zmiany mogłyby być tak niewielkie, że nie odniosą zbyt dużego wpływu na działanie systemu.

Testowanie pracy pamięci

Cel slajdu

Zebranie zagadnień związanych z optymalizacją pracy pamięci.

Wprowadzenie

Praca pamięci jest najważniejszym czynnikiem, mającym wpływ na wydajność systemu.

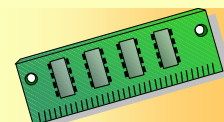
- **Ustanowienie podstawy, zakresu normalnych wartości, w celu analizy trendów i problemów**

- **Wykorzystanie liczników do testowania pamięci**

- Licznik Pages per second
- Licznik Available Bytes

- **Testowanie pliku stronicowania**

- Częste stronicowanie oznacza zbyt małą ilość pamięci
- Sprawdzanie wielkości pliku stronicowania
- Liczniki pozwalające monitorować rozmiar pliku stronicowania



Zagadnienia kluczowe

Mała ilość pamięci może spowolnić działanie aplikacji i usług systemowych, co źle wpłynie na wydajność całego systemu.

Zła praca pamięci może spowalniać pracę aplikacji i usług systemowych, co negatywnie odbija się na wydajności zasobów systemowych.

Ustanawianie bazy

Aby ustawić bazę dla pamięci fizycznej, należy przetestować jej wykorzystanie w normalnych warunkach pracy. Baza jest zazwyczaj graniczną wartością zakresu, w którym zmienia się wykorzystanie pamięci, a która zapewnia jeszcze zadowalającą wydajność systemu. Bazę wykorzystuje się do analizy trendów zmian, takich jak zwiększenie zapotrzebowania na pamięć fizyczną lub identyfikacji problemów, które pojawiają się po wprowadzeniu zmian.

Wskazówka

Jeżeli czas pozwoli, zaprezentuj liczniki Pages/sec i Available Bytes programu System Monitor.

Wykorzystanie liczników do testowania pamięci

Wszelkiego rodzaju przetwarzanie odbywa się z wykorzystaniem pamięci, a zatem bardzo ważne jest upewnienie się, że jest jej wystarczająco dużo aby system był w stanie wykonywać swoje bieżące zadania. Liczniki opisane w poniższej tabeli są bardzo przydatne przy testowaniu pamięci.

Licznik	Opis
Pages/sec	Ilość potrzebnych stron pamięci, które nie były od razu dostępne w fizycznej pamięci RAM i konieczne było odczytanie ich z dysku lub zapisanie innych na dysku, aby zwolnić miejsce. Jeżeli w systemie często zdarzają się takie sytuacje, wartość wskazywana przez licznik będzie wysoka.
Available bytes	Ilość wolnej pamięci fizycznej, nie przydzielonej żadnemu procesowi i nie wykorzystanej jako pamięć podręczna.

Jeżeli wartość licznika Available Bytes jest ciągle poniżej zdefiniowanej dla systemu wartości granicznej, oznacza to, że jest jej zbyt mało dla potrzeb systemu.

Zagadnienia kluczowe

Jedną z oznak zbyt małej pamięci systemowej jest częsta wymiana stron.

Testowanie pliku stronicowania

Jedną z oznak zbyt małej ilości pamięci w systemie, jest częsta wymiana stron pamięci pomiędzy pamięcią fizyczną i plikiem stronicowania na dysku.

Stronicowanie

Stronicowanie jest procesem przenoszenia stron wirtualnej pamięci pomiędzy pamięcią fizyczną i dyskiem. Gdy komputer ma mało pamięci fizycznej, stronicowanie występuje bardzo często, co powoduje spowolnienie pracy.

W procesie stronicowania, w dużym stopniu wykorzystywany jest dysk, tak więc częsta wymiana stron utrudnia korzystanie z dysku innym zadaniom. Procesor natomiast jest wykorzystywany w małym stopniu, ponieważ nie wykonuje żadnych czynności w trakcie realizacji odwołania do dysku lub reaguje na wywołanie przerwać podczas błędów stronicowania. (Błąd stronicowania ma miejsce, gdy system nie może zlokalizować wymaganych danych w pamięci fizycznej, dostępnej dla danego procesu). Skutek ostateczny, to spowolnienie pracy aplikacji i usług.

Uwaga Ponieważ nadmierne stronicowanie może powodować częste korzystanie z dysku, możliwe jest pomylenie problemów z pamięcią z problemami z dyskiem, które są skutkiem stronicowania.

Wskazówka

Odnajdź plik Pagefile.sys i porównaj jego rozmiar z wartościami ustawionymi w programie **System** w Panelu sterowania.

Rozmiar pliku stronicowania

Aby sprawdzić czy rozmiar pliku stronicowania zbliża się do swojej granicznej wartości, należy porównać rozmiar pliku z wartością maksymalnego rozmiaru pliku stronicowania ustawioną w programie **System** z Panelu sterowania. Jeżeli te dwie wartości są podobne, należy rozważyć zwiększenie początkowego rozmiaru pliku stronicowania lub uruchamiać mniej programów.

Uwaga Jeżeli plik stronicowania osiągnie maksymalny rozmiar, zostanie wyświetlone ostrzeżenie i może dojść do wstrzymania pracy komputera.

Plik stronicowania znajduje się na dysku, na którym zainstalowano system Windows 2000. Aby sprawdzić jego wielkość należy w programie Windows Explorer sprawdzić rozmiar pliku Pagefile.sys. Jeżeli jest dostępna wolna przestrzeń na dysku, można zwiększyć rozmiar pliku wymiany. Zalecany rozmiar pliku stronicowania to 150 procent fizycznej pamięci RAM, dostępnej dla systemu.

Liczniki i monitorowanie rozmiaru pliku stronicowania

Aby monitorować rozmiar pliku Pagefile.sys, można również wykorzystać liczniki opisane poniżej.

Licznik	Rozmiar pliku stronicowania należy zwiększyć, gdy:
Paging File\ % Usage	Wartość zbliża się do maksymalnej ustawionej dla pliku wymiany.
Paging File\ % Usage Peak (bytes)	Wartość zbliża się do 100 procent ustawionego limitu.

Testowanie pracy procesora

Cel slajdu

Zebranie zagadnień związanych z testowaniem pracy procesora.

Wprowadzenie

Podczas testowania pracy procesora, należy brać pod uwagę rolę, jaką pełni komputer i zadania, jakie ma wykonywać.

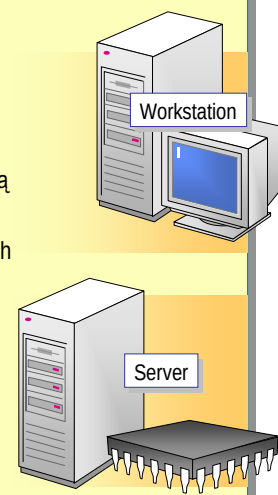
■ Wykorzystanie liczników do testowania aktywności procesora

■ Sprawdzenie wskaźników wykorzystania zasobów na stacji roboczej

- Duże wykorzystanie może oznaczać wydajną pracę
- Konieczne jest zebranie dodatkowych danych

■ Sprawdzenie wykorzystania zasobów wskaźników na serwerze

- Niedopuszczalne wysokie wykorzystanie
- Wysokie wykorzystanie może doprowadzić do wystąpienia zatorów



Podczas testowania pracy procesora, należy brać pod uwagę, jakie zadania spełnia komputer. W zależności od tego, przy tych samych pomiarach, może się okazać, że system pracuje efektywnie albo jest znacznie przeciążony. Jeżeli jednak przynajmniej kilka procesów wymaga większego dostępu do procesora, zainstalowanie szybszego może poprawić wydajność.

Wskazówka

Jeżeli czas pozwoli, zaprezentuj w programie System Monitor liczniki % Processor Time i Processor Queue Length.

Korzystanie z liczników przy testowaniu procesora

Przydatne przy testowaniu procesora liczniki opisano w poniższej tabeli.

Obiekt	Licznik	Opis
Processor	% Processor Time	Procentowo przedstawiony czas, przez jaki procesor zajęty jest przetwarzaniem zadań. Wartość powyżej 80 procent świadczy zazwyczaj o zatorach.
System	Processor Queue Length	Ilość wątków oczekujących na przetwarzanie. Kolejka dwóch lub więcej wątków na jednoprocessorowym komputerze oznacza wystąpienie zatoru.

Sprawdzanie odpowiednich danych na stacji roboczej

Jeżeli monitorowana jest stacja robocza pracująca w systemie Windows 2000, wysokie współczynniki wykorzystania mogą oznaczać, że system skutecznie radzi sobie z wysokimi wymaganiami. Na przykład, uruchamiana aplikacja wykorzystuje w 100 procentach czas procesora. Może to jednak również spowalniać pracę innych aplikacji na danym komputerze, więc konieczne jest zebranie dalszych informacji. Jeżeli niektóre programy mają jednak problem z prawidłowym działaniem, można spróbować przenieść je na inny komputer lub zmienić rolę komputera.

Sprawdzanie odpowiednich danych na serwerze

Wykorzystanie procesora w około 100 procentach, w przypadku serwera, może spowalniać odpowiedzi na wezwania klientów, które muszą oczekiwać w kolejce i utrudniać klientom pracę. System serwera jest przeładowany i nie nadąża z obsługą klientów, natomiast systemy klienckie nie są w pełni wykorzystane, gdyż do kontynuowania pracy muszą oczekiwać na odpowiedź przeładowanego podsystemu. Dłuższe utrzymywanie się takiego stanu na serwerze jest niedopuszczalne.

Testowanie pracy dysku

Cel slajdu

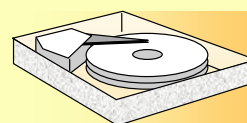
Zebranie zagadnień związanych z testowaniem pracy dysku.

Wprowadzenie

Pracę dysku monitoruje się w celu wykrycia niewydajnych dysków i zrównoważenia obciążenia serwerów.

■ Monitorowanie dysków fizycznych i logicznych**■ Dzięki licznikom można określić:**

- Procentowo wolny obszar na dysku
- Ilość operacji wejścia/wyjścia
- Prędkość przenoszenia danych
- Transfer danych
- Ilość odczytów i zapisów na sekundę



Monitorowanie pracy dysków ma na celu wykrycie niewydajnych systemów dyskowych, co pozwala zlikwidować problemy z obsługą danych.

Wskazówka Podczas monitorowania pracy dysków, dane powinny być zapisywane do dzienników umieszczonych na innym dysku lub komputerze, aby pomiary odpowiadały rzeczywistej pracy systemu.

Monitorowanie dysków fizycznych i logicznych

W systemie Windows 2000 występują liczniki do monitorowania aktywności dysków fizycznych (łącznie z dyskami wymiennymi), jak również logicznych partycji i woluminów. W obiekcie PhysicalDisk znajdują się liczniki do testowania dysków fizycznych. W obiekcie LogicalDisk znajdują się liczniki do testowania dysków logicznych i woluminów. W programie System Monitor, dyski oznaczane są numerami, począwszy od 0, a dyski logiczne literami alfabetu.

Liczniki przeznaczone do testowania pracy dysków

W poniższej tabeli znajduje się opis liczników z obiektów LogicalDisk i PhysicalDisk, przydatnych przy testowaniu dysków.

Obiekt	Licznik	Opis
LogicalDisk	% Free Space	Procentowa wielkość wolnego miejsca na dysku.
LogicalDisk PhysicalDisk	Avg. Disk Bytes/Transfer	Pomiar wydajności operacji wejścia/wyjścia. Dysk jest wydajny, jeżeli potrafi przesyłać stosunkowo dużą ilość danych w krótkim czasie.

(ciąg dalszy)

Obiekt	Licznik	Opis
LogicalDisk PhysicalDisk	Avg. Disk sec/Transfer	Szybkość przenoszenia danych (w sekundach). Jest to pomiar średniego czasu transferu danych, niezależnie od ilości zapisywanych lub odczytywanych danych. Wysoka wartość, wskazywana przez ten licznik, może oznaczać powtarzające się zlecenia, jeżeli kolejka jest stosunkowo długa lub rzadziej błędy w obsłudze dysku.
LogicalDisk PhysicalDisk	Disk Bytes/sec	Szybkość transferu danych. Jest to podstawowy licznik, oceniający przepustowość dysku. Im większa wartość tym lepsza wydajność.
LogicalDisk PhysicalDisk	Disk Transfers/sec	Ilość pełnych operacji odczytu lub zapisu na sekundę, niezależnie od ilości przetwarzanych w ten sposób danych. Jest to wskaźnik wykorzystania dysku. Jeżeli wartość przekroczy 50 (dla dysku fizycznego w przypadku macierzy), mogą wystąpić problemy.

Testowanie pracy sieci

Cel slajdu

Zebranie zagadnień związanych z testowaniem pracy sieci.

Wprowadzenie

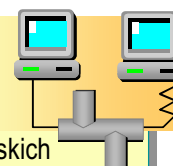
Korzystanie z sieci może mieć wpływ nie tylko na wydajność komputerów, które z niej korzystają, ale również na system jako całość.

■ Performance Monitor:

- Monitorowanie aktywności serwerów członkowskich
- Do wykorzystania liczniki danych o aktywności serwerów sieciowych, łącznie z informacją o przepływie i długości wysyłanych pakietów

■ Network Monitor:

- Monitorowanie strumieni danych
- Wymagana instalacja Network Monitor Driver i Network Monitor Tools



Od wydajności sieci zależy nie tylko wydajność jej poszczególnych komponentów, ale całego systemu. Po przetestowaniu i zoptymalizowaniu komputerów użytkowników i zasobów serwerów sieciowych, należy przetestować pracę sieci. W systemie Windows 2000, dostępne są dwa podstawowe narzędzia do monitorowania pracy sieci: Performance Monitor i Network Monitor. Po zebraniu i przeanalizowaniu danych, należy określić obszary potencjalnych problemów i podjąć czynności zapobiegawcze.

Wykorzystanie programu Performance Monitor

Dzięki programowi Performance Monitor można monitorować wydajność komponentów sieciowych na serwerze. W poniższej tabeli znajduje się opis obiektów i liczników przydatnych przy testowaniu aktywności sieciowej serwerów członkowskich.

Obiekt	Licznik	Opis
Network Interface	Output Queue Length	Długość kolejki wysyłanych pakietów. Kolejki z jednym lub dwoma zleceniami pozwalają utrzymać wydajność na zadowalającym poziomie. Dłuższe kolejki oznaczają, że karta sieciowa oczekuje na możliwość nadawania i nie nadąża z odpowiedziami na wezwania serwera.
Network Interface	Packets Outbound Discarded	Licznik wykorzystywany do określenia, czy sieć jest przeciążona i może wskazywać, że sieć jest tak zajęta, że bufor sieciowe nie radzą sobie z przetrzymywaniem pakietów.
Network Interface	Bytes Total/sec	Licznik wykorzystywany do testowania kart sieciowych. Wysoka wartość oznacza dużą ilość udanych transmisji. Jeżeli wartość jest równa lub zbliżona do pojemności sieci oznacza to pełne wykorzystanie sieci.

(ciąg dalszy)

Obiekt	Licznik	Opis
Transmission Control Protocol (TCP)	Segments Received/sec Segments Retransmitted/sec Segments/sec Segments Sent/sec	Monitorowanie aktywności warstwy transportowej.
Internet Protocol (IP)	Datagrams Forwarded/sec Datagrams Received/sec Datagrams/sec Datagrams Sent/sec	Monitorowanie aktywności warstwy sieciowej.

Korzystanie z programu Network Monitor

Wykorzystując program Network Monitor można monitorować w sieci przepływ strumienia, w którym znajdują się wszystkie przesyłane dane. Komponenty, których instalacja jest wymagana to:

- Sterowniki Network Monitor Drivers do przechwytywania danych.
- Narzędzia programu Network Monitor Tools, które umożliwiają przeglądanie danych. Dane podzielone są na mniejsze fragmenty, nazywane ramkami lub pakietami. Ponieważ z sieci wychwytywane są ramki, statystyki dotyczące ramek wyświetlane są w oknie Network Monitor Capture.

Więcej informacji na temat programu Network Monitor i instalacji jego komponentów znajduje się w rozdziale 15, "Troubleshooting Windows 2000 Network Services", kursu 2153A, *Implementing a Networking Infrastructure Using Microsoft Windows 2000*.

Podsumowanie

Cel slajdu

Podsumowanie celów rozdziału poprzez przypomnienie zagadnień kluczowych.

Wprowadzenie

Kilka pytań pozwoli podsumować główne idee omawiane w bieżącym rozdziale.

- Monitorowanie dzienników zdarzeń
- Wykorzystanie programu Task Manager do monitorowania zasobów systemowych
- Wykorzystanie programu System Monitor do śledzenia aktywności systemu
- Alerty
- Optymalizacja wydajności

1. Użytkownik nie może połączyć się z serwerem pocztowym. Informuje, że podczas uruchamiania komputera wyświetlany jest komunikat informujący o tym, że przynajmniej jeden z serwisów nie został uruchomiony. Który dziennik zdarzeń należy przejrzeć, w celu odszukania zdarzenia, które spowodowało wyświetlenie tego komunikatu? Jaki typ zdarzeń należałoby przeszukać?

Należy przeszukać dziennik systemowy na komputerze, na którym wystąpił problem i przejrzeć zdarzenia oznaczone czerwonym kółkiem z literką X.

2. Użytkownik twierdzi, że program Internet Explorer nie odpowiada. Z jakiego narzędzia należy skorzystać, aby sprawdzić, czy aplikacja wciąż pracuje?

Należy uruchomić program Task Manager, wskazać kartę Application i sprawdzić status aplikacji uruchomionych na komputerze użytkownika. Jeżeli aplikacja nie odpowiada, można ją zamknąć.

3. Użytkownik twierdzi, że jego komputer pracuje ostatnio wolniej. Po sprawdzeniu wydajności procesora przy pomocy programu Task Manager, nie można stwierdzić żadnej przyczyny takiego zachowania. Jakie inne narzędzie można wykorzystać, w celu dalszej diagnozy problemu?

Program System Monitor. Można dzięki niemu obserwować wiele liczników dla różnych obiektów systemowych.

4. W serwerze wydruku znajduje się dysk o małej ilości wolnego miejsca. Jego administrator chce zostać powiadomionym, gdy poziom wolnego miejsca spadnie poniżej założonej wartości. Jak można to zrobić?

Wykorzystać dzienniki wydajności i alerty, w celu wysłania ostrzeżenia, gdy ilość wolnego miejsca na dysku spadnie poniżej założonego poziomu.

5. Jakie trzy czynności składają się na proces optymalizacji? Czy jest to proces wykonywany jednokrotnie?

Trzy czynności składające się na proces optymalizacji to:

- **Analiza monitorowanych danych**
- **Identyfikacja obszarów o zbyt małej wydajności**
- **Modyfikacje**

Proces ten powinien być powtarzany, aż do uzyskania satysfakcjonującego poziomu wydajności.