Міністерство освіти і науки України

Тернопільський Національний Економічний Університет

Факультет комп’ютерних інформаційних технологій

Лобораторна робота № 1

з дисципліни «Дослідження сучасних операційних систем»

Виконав: студент групи КСМм-51

Пилипчук Андрій

Перевірив: Мельник Г. М.

Тернопіль-2013

**Тема**: Засоби керування процесами та мережею в ОС Windows Server 2003.

**Мета:** Вивчити основні засоби контролю і керування процесами.  
**Засоби для виконання роботи:**

* апаратні: комп'ютер із установленою ОС Windows.
* програмні: застосування ВМ: Virtualbox; віртуальні машини: VM-1, VM-2.

**Теоретичні відомості**

Системна служба **Журнал подій**

Системна служба **Журнал подій** запускається за замовчуванням при завантаженні операційної системи й реєструє події в трьох журналах ( залежно від ролі сервера журналів може бути більше):

* *Приложение* (містить інформацію про зміну конфігурації в системі);
* *Система* (містить дані про системні події);
* *Безопасность* (містить записи про події входу в систему й про доступ до ресурсів).

Для моніторингу й оптимізації роботи комп'ютера в системах **Windows Server 2003** є кілька інструментів, що дозволяють адміністраторові стежити за роботою будь-яких компонентів системи й конфігурувати її оптимальним образом. Ці інструменти перераховані нижче.

* ***Task Manager (Диспетчер задач)*** служить для перегляду поточних даних про продуктивність системи. У цій утиліті основними є три індикатори: використання процесора, використання віртуальної пам'яті й запущені процеси й програми.
* ***Оснащення Event Viewer (Просмотр событий)*** дозволяє переглядати журнали подій, генерованих застосуваннями, службою безпеки й системою.
* ***Performance (Производительность)*** – містить у собі два компоненти: Activex-*Елемент System Monitor* і оснащення *Performance Logs and Alerts* (Оповещения и журналы безопасности). Графічні засоби *System Monitor* дозволяють візуально відслідковувати зміну продуктивності системи. За допомогою *System Monitor* можна одночасно переглядати дані з декількох комп'ютерів у вигляді динамічних діаграм, на яких відображається поточний стан системи й показання лічильників. Оснащення *Performance Logs and Alerts* дозволяє створювати звіти на основі поточних даних продуктивності або інформації з журналів. При перевищенні лічильниками заданого значення або зменшення нижче вказаного рівня дане оснащення за допомогою служби повідомлень (Messenger) посилає оповіщення користувачеві.

## Диспетчер задач

***Диспетчер задач*** можна використовувати для відстеження ключових індикаторів продуктивності комп'ютера, він дозволяє визначати статус запущених програм і завершувати застосування, які перестали відповідати на запити системи. За допомогою диспетчера задач можна відслідковувати активність запущених процесів по 25 параметрах і переглядати графіки використання процесора й пам'яті.

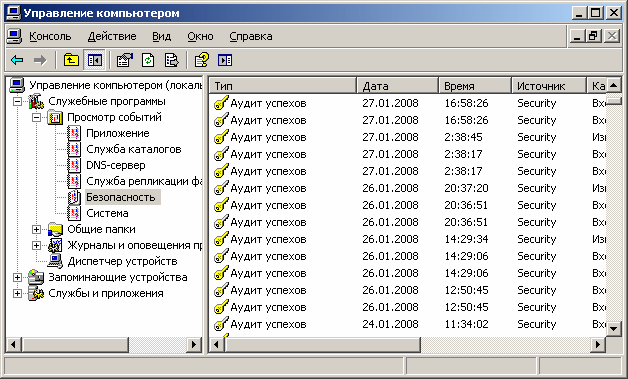
В **Windows Server 2003** диспетчер задач містить п'ять вкладок/індикаторів. Нижче перераховані ці вкладки й зазначене їхнє призначення.

* *Applications (Приложения)* – показує статус застосувань, запущених на комп'ютері.
* *Processes (Процессы)* – містить інформацію про процеси, запущені на комп'ютері.
* *Performance (Быстродействие)* – відображає динамічний стан продуктивності комп'ютера, включаючи ступінь використання пам'яті й процесора.
* *Networking (Сеть)* – показує ступінь завантаження мережі. Індикатор відображається тільки при наявності на комп'ютері мережної карти.
* *Users (Пользователи)* – містить список зареєстрованих користувачів. Ці користувачі можуть реєструватися локально (з консолі) або бути клієнтами служб *Terminal Services*, підключених з використанням технологій *Terminal Server, Remote Access* або *Remote Assistant*.

В операційних системах **Windows** подією називається будь-яка значна "подія" у роботі системи або застосування, про яку слід повідомити користувачів. У випадку виникнення критичних подій, таких як переповнення диска сервера або неполадки з електроживленням, на екран монітора буде виведено відповідне повідомлення. Інші події, які не вимагають негайних дій від користувача, реєструються в системних журналах. Служба реєстрації подій у системних журналах активізується автоматично при кожному запуску системи **Windows Server 2003**.

## Оснащення Event Viewer

У системі **Windows Server 2003** для перегляду системних журналів можна використовувати оснащення ***Event Viewer (Просмотр событий)*** (група ***Administrative Tools (Администрирование)*** на панелі керування). Це оснащення можна також запустити з вікна оснащення ***Computer Management (Управление компьютером)***. На рис. 1 показаний приклад вікна оснащення ***Event Viewer*** для контролера домена.

  
 *Рисунок. 1. Вікно оснащення Event Viewer.*

Оснащення ***Event Viewer*** можна також відкрити за допомогою команди ***Пуск/Программы/Администрирование/Просмотр событий***. За допомогою оснащення ***Event Viewer*** можна переглядати три типи стандартних (основних) журналів.

* *Журнал приложений(Application log)* — фіксує події, зареєстровані застосуваннями. Наприклад, текстовий редактор може зареєструвати в даному журналі помилку при відкритті файлу.
* *Журнал системы (System log)* — записує події, які реєструються системними компонентами **Windows Server 2003**. Наприклад, у системний журнал записуються такі події, як збій у процесі завантаження драйвера або іншого системного компонента при запуску системи.
* *Журнал безпеки (Security log)* — містить запису, пов'язані із системою безпеки. За допомогою цього журналу можна відслідковувати зміни в системі безпеки й ідентифікувати проломи в захисті. У даному журналі можна реєструвати спроби входу в систему. Для перегляду журналу необхідно мати права адміністратора. За замовчуванням реєстрація подій у журналі безпеки відключена.

Крім стандартних, на комп'ютері — у першу чергу на контролері домена — можуть бути й інші журнали, створювані різними службами (наприклад, ***Active Directory, DNS, File Replication Service*** і т.д.). Робота з такими журналами нічим не відрізняється від процедур перегляду стандартних журналів.

Журнал системи безпеки може переглядати тільки користувач із правами системного адміністратора. За замовчуванням реєстрація подій у даному журналі відключена. Для запуску реєстрації необхідно встановити політикові аудита.

**Типи подій, що реєструються в журналах:**

* *Error (Помилка)* — подія реєструється у випадку виникнення серйозної події (такого як втрата даних або функціональних можливостей). Подію даного типу буде зареєстровано, якщо неможливо завантажити який-небудь із сервісів у ході запуску системи.
* *Warning (Попередження)* — подія не є серйозною, але може привести до виникнення проблем у майбутньому. Наприклад, якщо недостатньо дискового простору, то буде зареєстроване попередження.
* *Information (Повідомлення)* — значима подія, яка свідчить про успішне завершення операції програмою, драйвером або сервісом. Така подія може, наприклад, зареєструвати мережний драйвер, що успішно завантажився.
* *Success Audit (Аудит успіхів)* — подія, пов'язана з безпекою системи. Прикладом такої події є успішна спроба реєстрації користувача в системі.
* *Failure Audit (Аудит відмов)* — подія пов'язане з безпекою системи. Наприклад, така подія буде зареєстрована, якщо спроба доступу користувача до мережного диска закінчилася невдачею.

**Хід роботи**

Завдання 1. Переглянути мережеві підключення до комп’ютера.

1. Підготувався до виконання завдання: запустив Windows Server 2008 на віртуальній машині VirtualBox. Створив на робочому столі папку My\_folder з документом Compname.doc з відомостями про IP-адресу та символьне ім’я комп’ютера.

2. Повернувся в віртуальну машину.

3. Запустив додаток Керування комп’ютером.

4. Розгорнув розділ Загальні ресурси.

5. Відключив загальний доступ до ресурсу My\_folder.

6. Відкрив розділ Сеанси.

7. Закрив відкритий файл Compname.doc.

Завдання 2. Відключити користувача з відправленням йому повідомлення.

1. Підготувався до виконання задання: відкрив файл Compname.doc, який розташований на віртуальній машині, на звичайному комп’ютері.

2. Повернувся в віртуальну машину.

3. Запустив додаток Керування комп’ютером.

4. Відкрив форму відправлення повідомлення консолі.

5. Ввів текст повідомлення та відправив його.

6. Закрив вікно відправлення повідомлення консолі.

7. За допомогою контекстного меню розділу Відкриті файли закрив всі відкриті файли.

8. Переглянув повідомлення, що надійшли.

Завдання 3. Переглянути відомості про процеси системи та її стан.

1. Переглянув інформацію про продуктивність системи (процеси, швидкодію, мережу та користувачів) за допомогою диспетчера задач.

2. За допомогою диспетчера задач зібрав наступну інформацію: кількість запущених програм, ім’я процесу, що використовує найбільше пам’яті, кількість виділеної пам’яті, імена зареєстрованих в системі користувачів.

3. Зберіг отриману інформацію в особистому каталозі.

Завдання 4. Викоати моніторинг мережевих підключень.

1. Запустив додаток Продуктивність.

2. Вилучив всі поточні лічильники.

3. Додав лічильник активних підключеньTCP.

4. Закрив діалогове вікно властивостей Системного монітору.

5. Змінив вид відображення інформації лічильників у текстовий режим.

6. Налаштував автоматичний збір інформації про завантаженість сервера в період з 8:00 до 17:00.

7. Налаштував сповіщення, якщо об’єм доступної пам’яті стане меншим, ніж 100 Мб.

Завдання 5. Переглянути інформацію про події.

1. Запустив додаток Керування комп’ютером.

2. Розгорнув підменю Перегляд подій.

3. Переглянув події служби безпеки.

4. Експортував список подій для розділу DNS-сервера у текстовий файл.

**Висновок**

На цій лабораторній роботі я ознайомився та навчився користуватися основними засобами контролю і керування процесами у Windows Server 2003.