Лекція №18

Системний реєстр Windows XP

(c) Гроза П.М.

Навчальні питання

1. **Основні відомості**
2. **Логічна структура реєстру**
3. **Фізична організація реєстру**
4. **Робота з реєстром**
5. **Програмний інтерфейс доступу до реєстру**

Література

1. Язык програмирования С++. Лекция и упражнения. Учебник: Перевод с анг./Стивен Прата – СПб.: ООО «ДиаСофтЮП», 2005.-1104с.
2. Теренс Чан Системное програмирование на С++ для UNIX: пер. с англ. – К.: Издательская группа BHV, 1997. – 592с.
3. Вильямс А. Системное программирование в Windows 2000 для профессионалов — СПб: Питер, 2001. —624 с: ил.
4. Терес Чан Системное програмирование на С++ для Unix: Пер.с англ. – К.: Издательская группа BHV, 1997. – 592с / ISDN 5-7315-0013-4
5. Рихтер Дж. Windows для профессионалов: создание эффективных Win32 приложений с учетом специфики 64-разрядной версии Windows/Пер, англ - 4-е изд. - СПб; Питер; М.: Издательско-торговый дом "Русская Редакция", 2001. - 752 с.; ил.
6. Побегайло А.П. Системное программирование в Windows. – СПб.: БХВ-Петербург, 2006. – 1056с.:ил.

1. Основні відомості

Системний реєстр (registry)

- ієрархічно побудована, централізована база даних у складі ОС сімейства Microsoft Windows, що містить відомості для роботи ОС з користувачами, програмними продуктами і пристроями

Містить

- ✔ профілі всіх користувачів
- ✔ відомості про встановлене ПЗ
- ✔ відомості про типи файлів, що створюються кожною програмою
- ✔ інформація про властивості папок і значки додатків
- ✔ інформація про установлене устаткування і використовувані порти

Особливості використання реєстру

Замінив

- більшість **ini**-файлів в Windows 3.x
- файли конфігурації MS-DOS – приклад, **autoexec.bat** і **config.sys**

Звернення до Реєстру

- під час запуску ОС - до тисячі
- під час роботи протягом одного сеансу - до 10 тисяч

Проблеми з реєстром

- Некоректні настройки - поява всіляких «глюків» у роботі ОС
- Серйозні ушкодження – ОС завантажити неможливо
- Серйозні руйнування (втрата) файлів - при завантаженні поява BSOD

Рішення проблем з реєстром

1. Виправлення реєстру вручну або програмно
2. Відновлення з резервної копії
3. Обережне використання «чистильників» реєстру

Питання

2. Логічна структура реєстру

Логічні рівні реєстру

Рівні

1. Ключі (keys)
   - Характеризуються іменем і містять значення або інші ключі

2. Значення (values)
   - Характеризується
   - ✔ іменем, типом і даними, які воно містить
   - ✔ повним шляхом, що включає всі імена ключів, розташованих над ним

Кореневі каталоги реєстру

Папка/стандартний каталог	Опис
HKEY_CURRENT_USER	•Містить конфігураційні відомості для активного користувача: папки користувача, вибрані кольори екрана та параметри панелі керування •Скорочена назва "HKCU"
HKEY_USERS	•Підрозділ HKEY_USERS •Містить усі профілі користувачів •Скорочена назва "HKU"
HKEY_LOCAL_MACHINE	•Містить конфігураційні відомості комп'ютера •Скорочена назва "HKLM"
HKEY_CLASSES_ROOT	•Підрозділ розділу HKEY_LOCAL_MACHINE\Software •Забезпечує запуск відповідної програми, коли у провіднику відкривають файл •Скорочена назва "HKCR" •Починаючи з Windows 2000 ця інформація зберігається також у розділах HKEY_LOCAL_MACHINE і HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	•Містить відомості про конфігурацію обладнання ПК •Використовується при запуску системи •Скорочена назва "HKCC"

Особливості настроювань за умовчанням

- HKEY_LOCAL_MACHINE\Software\Classes - настройки за замовчуванням для усіх користувачів ПК
- Настройки HKEY_CURRENT_USER\Software\Classes - мають пріоритет над настройками за замовчуванням і застосовуються лише до активного користувача
- Щоб змінити настройки поточного користувача – внести зміни до розділу HKEY_CURRENT_USER\Software\Classes, а не до HKEY_CLASSES_ROOT

Приклад загальносистемного налагодження

HKLM\SYSTEM\CurrentControlSet\Services\Cdrom\Autorun типу REG_DWORD

- = 1 - вставлення нового диска у CD- дисковод приводить до автоматичного запуску застосування autorun.exe

HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0

- Ключ налагодження програмного продукту - містить значення конфігураційних параметрів версії продукту

64-розрядна версія ОС

- Реєстр складається з 32-х і 64-х розрядних розділів
- У 64-розрядній версії редактора реєстру 32-х розділи відображаються у вузлі HKEY_LOCAL_MACHINE\Software\WOW6432Node

Типи даних для використання в реєстрі

Назва	Тип даних	Опис
Двійковий параметр	REG_BINARY	Неформатовані двійкові дані Параметри відомостей про устаткування Відображається в редакторі реєстру в 16-му форматі
Параметр DWORD	REG_DWORD	Дані, представлені 4-байтовим числом (32-розрядним цілим) Параметри драйверів пристроїв і служб Відображається у 2-му, 16-му або 10-му форматі
Розширюваний рядковий параметр	REG_EXPAND_SZ	Рядок даних змінної довжини Змінні, які обчислюються для програм або служб
Мультирядковий параметр	REG_MULTI_SZ	Складний рядок Параметри, які містять списки декількох значень у формі, зручній для читання
Рядковий параметр	REG_SZ	Текстовий рядок фіксованої довжини
Двійковий параметр	REG_RESOURCE_LIST, REG_RESOURCE_REQUIREMENTS_LIST, REG_FULL_RESOURCE_DESCRIPTOR	Вкладені масиви Списки ресурсів для драйвера пристрою, яким він керує Записуються системою у структурі ResourceMap Відображаються в 16-му форматі як 2-й параметри
Невизначений	REG_NONE	Дані без типу Записуються до реєстру системою та додатками Відображаються в 16-му форматі як 2-й параметри
Посилання	REG_LINK	Рядок Юнікоду - позначає символічне посилання
Параметр QWORD	REG_QWORD	Дані, представлені 64-розрядним цілим числом Відображаються 2-м параметром З'явилися з Windows 2000

Максимальні розміри

Імені параметра

- Windows Server 2003, Windows XP та Windows Vista - 16383 знаки
- Windows 2000 - 260 знаків ANSI або 16383 знаків Юнікоду
- Windows Millennium Edition/Windows 98/Windows 95 - 255 знаків

Параметра

- Windows NT 4.0/Windows 2000/Windows XP/Windows Server 2003/Windows Vista - уся доступна пам'ять
- Windows Millennium Edition/Windows 98/Windows 95 - 16300 байт

!!!Примітка

Сукупний розмір усіх значень у розділі не перевищує 64 КБ

Питання

3. Фізична організація реєстру

Вулик реєстру

- Підмножину дерева ключів, починаючи із ключа другого рівня, називають вуликом (hive)

- **Вулик** (кущ) реєстру — це група розділів, підрозділів і параметрів реєстру, з якою пов'язано групу допоміжних файлів, де містяться резервні копії всіх цих даних

Фізичні дані реєстру - відповідають каталоги

- HKEY_LOCAL_MACHINE (HKLM) - інформацію про всю систему
- HKEY_USERS (HKU) — дані окремих користувачів

Важливі вулики ключа HKLM

HARDWARE

- ✔ інформація про поточну апаратну конфігурацію системи
- ✔ вміст формується динамічно і на диску не зберігається

SAM – БД облікових записів

- ✔ інформація про імена і паролі користувачів для реєстрації у системі

SOFTWARE

- ✔ налаштування ППЗ

SYSTEM

- ✔ інформація для запуску системи - список драйверів і служб, які необхідно завантажити і їх налаштування

Розміщення файлів реєстру

- Файли вуликів HKLM - папка %SystemRoot%\System32\Config
- Файли HKU - %SystemRoot%\Profiles\Username

Розширення імен файлів у папках

Кущ реєстру	Допоміжні файли
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	У Windows 98 файли реєстру мають імена User.dat і System.dat.

Питання

4. Робота з реєстром

Дії з реєстром

1. **Резервне копіювання реєстру**

2. Редагування реєстру

3. Використання інтерфейсу користувача Windows

4. Використання редактора реєстру

1. Резервне копіювання реєстру

- Перед редагування створіть резервну копію всього реєстру
- Використовується програма архівації
- Стан системи охоплює
  - ✔ реєстр
  - ✔ базу даних реєстрації класів COM
  - ✔ завантажувальні файли

2. Редагування реєстру

- для внесення змін до реєстру

- Адміністратор може використовувати
- ✔ редактор реєстру (Regedit.exe або Regedt32.exe)
- ✔ засоби "Групову політику"
- ✔ "Системну політику"
- ✔ файли реєстру (.reg)
- ✔ Сценарії

3. Використання інтерфейсу користувача Windows

- для зміни параметрів системи

- Для усунення проблему з продуктом
- ✔ необхідне редагування реєстру
- ✔ використовується база знань Microsoft Knowledge Base

4. Використання редактора реєстру

Дії

- ✔ пошук піддерева, розділу, підрозділуабо параметрів
- ✔ додати підрозділ або параметр
- ✔ змінити параметр
- ✔ видалити підрозділ або параметр
- ✔ перейменувати підрозділ або параметр

- При доступі до реєстру з віддаленого комп'ютера видимі розділи
- ✔ HKEY_USERS
- ✔ HKEY_LOCAL_MACHINE

Питання

5. Програмний інтерфейс доступу до реєстру

Можливості

1. **Зчитування інформації з реєстру**
2. **Створення нового ключа - RegCreateKeyEx( );**
3. **Створення нового значення - RegSetValueEx( );**

1. Зчитування інформації з реєстру

Виконання послідовно дій

1) Відкрити ключ зі значення - **RegOpenKeyEx( );**

2) Отримати дані - **RegQueryValueEx( );**

3) Закрити ключ- **RegCloseKey(hk);**

Функція RegOpenKeyEx( );

Опис

```
HKEY hk;
RegOpenKeyEx(
HKEY_LOCAL_MACHINE, // HKEY_CURRENT_USER тощо
"SYSTEM\CurrentControlSet\Services\Cdrom",
0,
KEY_READ,
&hk );
```

hk - покажчик на змінну для дескриптора ключа реєстру

Функція RegQueryValueEx( );

Опис

DWORD vsize, autorun;

RegQueryValueEx(

hk, // RegOpenKeyEx(.... ,&hk); **RegQueryValueEx( );** - передається відкритий дескриптор

"Autorun",

NULL,

NULL,

(LPBYTE) &autorun, // autorun містить 0 або 1

&vsize);

Приклад використання функцій

```
char myval[] = "my new data";
HKEY hknew;
RegCreateKeyEx(HKEY_LOCAL_MACHINE,
   "SOFTWARE\\myapp", 0, NULL, 0,0, NULL, &hknew,
   &res);
RegSetValueEx(hknew, "myval",0, REG_SZ,
   (LPBYTE)myval, sizeof(myval));
RegCloseKey(hk);
```

Програма для визначення списку драйверів

```
// Функція QueryKey()
#include  <windows.h>
#include  <stdio.h>
#include  <string.h>
#define MAX_VALUE_NAME 80
VOID QueryKey(HKEY hKey)
{
  CHAR achKey[MAX_PATH];
  CHAR achClass[MAX_PATH] = "";
  DWORD cchClassName = MAXPATH;
  DWORD cSubKeys;
  DWORD cbMaxSubKey;
  DWORD cchMaxClass;
  DWORD cValues;
  DWORD cchMaxValue;
  DWORD cbMaxValueData;
  DWORD cbSecurityDescriptor;
  FILETIME ftLastWriteTime;
  DWORD i, j;
  DWORD retCode, retValue;
  CHAR achValue[MAX_VALUE_NAME];
  DWORD cchValue = MA X_ VALUE_ NA M E;
  CHAR achBuff[80];
RegQueryInfoKey(hKeyachClass, &cchClassName, NULL , &cSubKays, &cbMaxSubKey, AcchMaxClass, &cValues, &cchMaxValue, &cbMaxValueData, &cbSecurityDescriptor, &ftLastWritolimo);
for (i = 0, retCode = ERROR_SUCCESS; retCode == ERROR_SUCCESS; i++)  {
  retCode = RegEnumKey(hKey i, acliKey, MAX_PATH);
  if (retCode == (DWORD)ERROR_SUCCESS)  printf ("%s\n", achKey);
  }
if (cValues) for (j = 0, retValue = ERROR_SUCCESS; j < cValues; j++)
  {
  cchValue = MAX_VALUE_NAME;
  achValue[0] = '\0';
  DWORD dwType;
  BYTE bcData[80];
  retValue = RegEnumValue(hKey j, achValue, &cchValue, NULL, &dwType, (PBYTE)achBuff, (DWORD*)bcData);
  if (retValue != (DWORD) ERROR_SUCCESS) continue;
  switch (dwType)   {
    case REG_DWORD:
    printf ("'\t\t%s = %d\n", achValue, *(DWORD*)achBuff);
    break;
    case REG_SZ;
    achBuff [*(DWORD*)bcData]=0;
  }
 printf ("\t\t%s = %s\n", achValue, achBuff);
 break;
  }
```

Програма для визначення списку драйверів

```
// Функція main()
 int main() {
  HKEY hkResult;
  LONG res1;
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SYSTEM       WCurrentControlSetWServices", 0, KEYREAD,
      &hkResult);
  if (res != ERROR_SUCCESS)  {
    printf ("Open Registry ErrorW);
    return 1;
  }
char buffer[256];
char path[256] = "SYSTEMWCurrentControlSet\\Services\\";
DWORD dwLen = strlen (path);
DWORD dwSize;
HKEY hkSubKey;
for (DWORD dwlndex = 0;  ; dwlndex++) {
   dwSize - sizeof (buffer);
   res = RegEnumKeyEx(hkResult, dwlndex, buffer, &dwSize, 0, 0, 0, 0);
   printf ("%s\n", buffer);
   if (buffer[0]=='{') continue;
   strcpy (path + dwLen, buffer);
   res1 = RegOpenKeyEx(HKEY_LOCA L_ MA CHINE, path, 0, KEY_READ, &hkSubKey);
   QueryKey(hkSubKey);
   res1 = RegCloseKey(hkSubKey);
   if (ERROR_NO_MORE_ITEMS == res) break;
 }
QueryKey (hkResult);
*res = RegCloseKey(hkResult );
return 0;
}
```

Питання