Services, Events, Registry

http://www.cs.vsb.cz/navrat

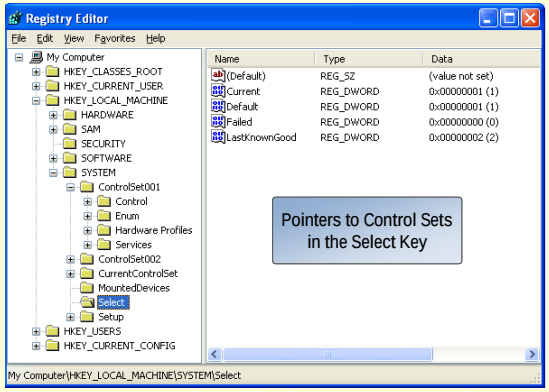
Jan Žák

Agenda

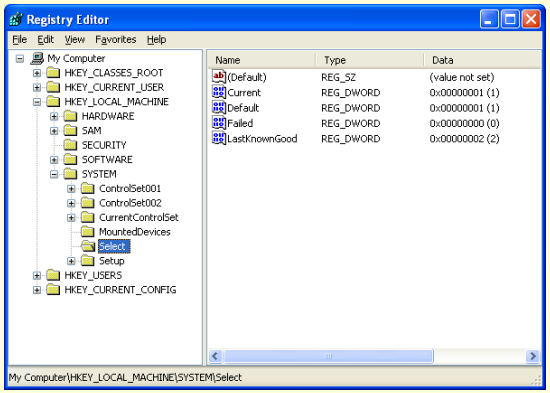
- Services
- Events
- Registry editor
- WSUS
- PKI/CA (if time permits ☺)

Services

Examining Control Sets



Examining the Select Subkey



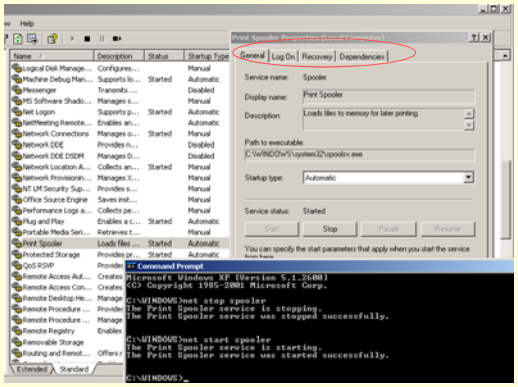
About Services

- The **service control manager** (SCM) maintains a database of installed services and driver services, and provides a unified and secure means of controlling them. The database includes information on how each service or driver service should be started. It also enables system administrators to customize security requirements for each service and thereby control access to the service.

Service status

- service is a file system driver.
- service is a device driver.
- service runs in its own process.
- service shares a process with other services.
- service can/can not interact with the desktop.
- service continue is pending.
- service pause is pending.
- service is paused.
- service is running.
- service is starting.
- service is stopping.
- service is not running.

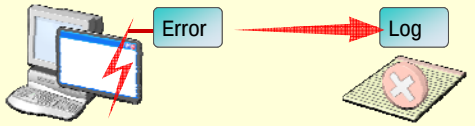
Services



- You are able to manage services remotely with MMC!

Events

Introduction to Event Logs



- System logs contain events logged by system components in Windows XP Professional
- Application logs contain events logged by applications or programs

Types of Events

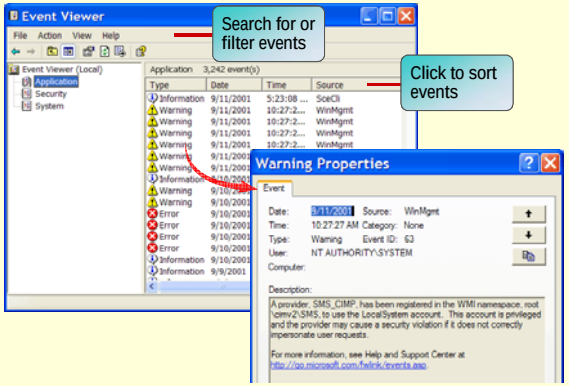
Types of system and application events

- Information
- Warning
- Error

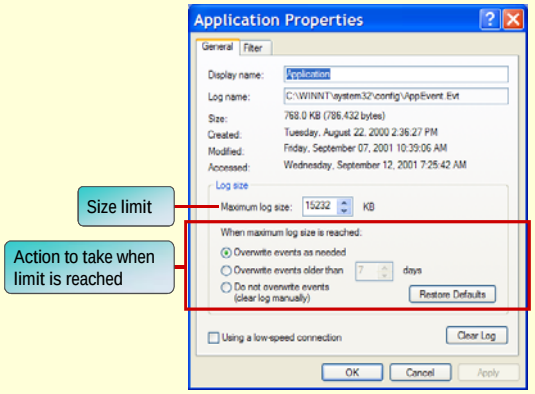
Types of security events

- Success audit
- Failure audit

Viewing Event Logs



Limiting the Size of Log Files



Archiving Event Logs

- Archive event logs to:
  - Track trends to determine resource usage
  - Track use of resources
  - Keep records when required by law
- Select a file format to view archived logs in other applications:
  - Log-file format (.evt)
  - Text-file format (.txt)
  - Comma-delimited text-file format (.csv)

Registry

What is Windows registry?

- **Windows registry** is a database which stores settings and options for Microsoft operating system (32, 64 bits versions and also for Windows Mobile).
- Registry contains information and settings for all the hardware, software, users, and preferences.
- Whenever a user makes changes to "Control Panel" settings, or file associations, system policies, or installed software, the changes are reflected and stored in the registry.
- The Windows Registry was introduced to tidy up the profusion of per-program INI files that had previously been used to store configuration settings for Windows programs. These files tended to be scattered all over the system, which made them difficult to keep track of.

Registry structure

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

HKEY_CLASSES_ROOT

- Abbreviated HKCR, HKEY_CLASSES_ROOT stores information about registered applications, including associations from file extensions and OLE object class ids to the applications used to handle these items.
- On Windows 2000 and above, HKCR is a compilation of HKCU\Software\Classes and HKLM\Software\Classes. If a given value exists in both of the subkeys above, the one in HKCU\Software\Classes is used

HKEY_CURRENT_USER

- Abbreviated HKCU, HKEY_CURRENT_USER stores settings that are specific to the currently logged in user. HKCU mirrors the current user's subkey of HKEY_USERS.

HKEY_LOCAL_MACHINE

- Abbreviated HKLM, HKEY_LOCAL_MACHINE stores settings that are general to all users on the computer. This key is found within the file %SystemRoot%\System32\Config\system on NT-based versions of Windows. Information about system hardware is located under the SYSTEM key.

HKEY_USERS

- Abbreviated HKU, HKEY_USERS contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user registered on the machine.

HKEY_CURRENT_CONFIG

- Abbreviated HKCC, HKEY_CURRENT_CONFIG contains information gathered at runtime; information stored in this key is not permanently stored on disk, but rather regenerated at boot time.

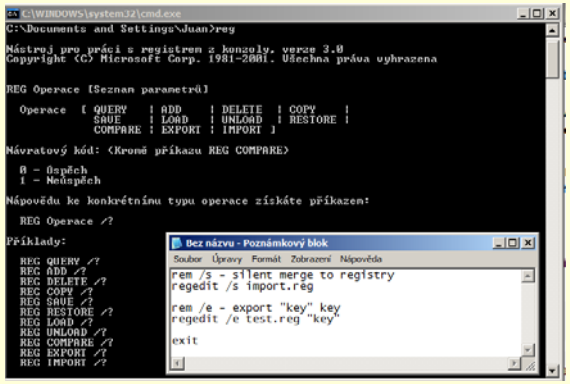
Registry values

- String Value
- Binary Value (0 and 1's)
- DWORD Value, a 32 bit unsigned integer (numbers between 0 and 4,294,967,295 [232 – 1])
- Multi-String value
- Expandable String Value

Registry editing tools

- REGEDIT.EXE had a left-side tree view that began at "My Computer" and listed all loaded hives. REGEDT32.EXE had a left-side tree view, but each hive had its own window, so the tree displayed only keys.
- REGEDIT.EXE represented the three components of a value (its name, type, and data) as separate columns of a table. REGEDT32.EXE represented them as a list of strings.
- REGEDIT.EXE supported right-clicking of entries in a tree view to adjust properties and other settings. REGEDT32.EXE required all actions to be performed from the top menu bar.
- Because REGEDIT.EXE was directly ported from Windows 95, it did not support permission editing (permissions do not exist on Windows 9x). Therefore, the only way to access the full functionality of an NT registry was with REGEDT32.EXE.
- REGEDIT.EXE only supported string (REG_SZ), binary (REG_BINARY), and DWORD (REG_DWORD) values. REGEDT32.EXE supports those, plus expandable string (REG_EXPAND_SZ) and multi-string (REG_MULTI_SZ). **Attempting to edit unsupported key types with REGEDIT.EXE on Windows 2000 or Windows NT 4 will result in registry corruption and, possibly, an unbootable system.**
- Windows XP was the first system to integrate these two programs into one, adopting the old REGEDIT.EXE interface and adding the REGEDT32.EXE functionality. The differences listed above are not applicable on Windows XP and newer systems; REGEDIT.EXE is the improved editor, and REGEDT32.EXE simply invokes REGEDIT.EXE.

Command line registry editing



Where are my registry?

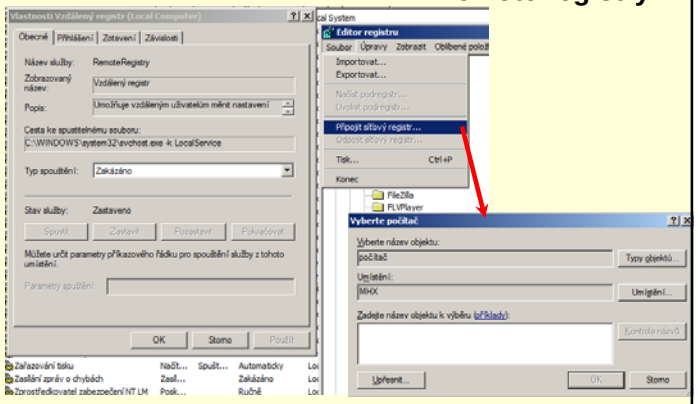
Windows NT, 2000, XP, and Server 2003

- The following Registry files are stored in %SystemRoot%\System32\Config\:
- **Sam** - HKEY_LOCAL_MACHINE\SAM
- **Security** - HKEY_LOCAL_MACHINE\SECURITY
- **Software** - HKEY_LOCAL_MACHINE\SOFTWARE
- **System** - HKEY_LOCAL_MACHINE\SYSTEM
- **Default** - HKEY_USERS\.DEFAULT
- **Userdiff**
- The following file is stored in each user's profile folder:
- NTUSER.DAT

Windows 95, 98, and Me

- The registry files are named **User.dat** and **System.dat** and are stored in the C:\WINDOWS\ directory. In Windows Me **Classes.dat** was added.

Remote registry



Windows Software Update Services

What Is Microsoft Update?

Microsoft Update is a Microsoft Web site that includes:

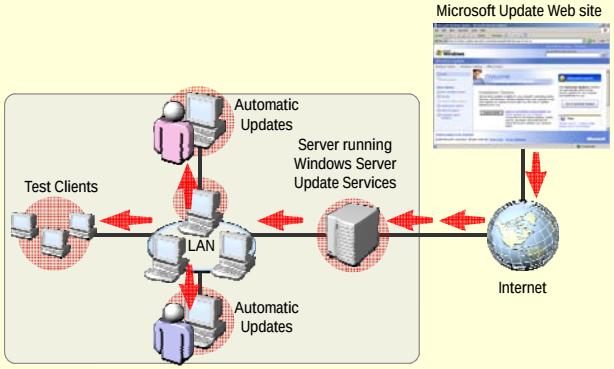
- Updates for Microsoft Windows operating systems, software, and device drivers
- Updates for Microsoft applications
- New content that is added to the site regularly

What Is Automatic Updates?

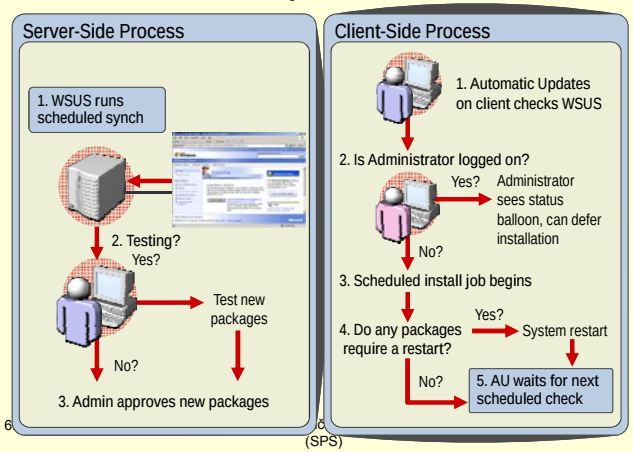
Automatic Updates is client software that:

- Communicates with Microsoft Update or WSUS
- Automatically downloads updates
- Notifies users of update availability

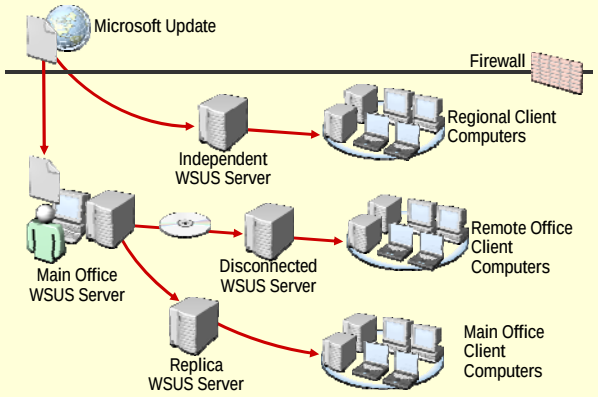
What Is Windows Server Update Services?



Windows Server Update Services Process



WSUS Deployment Scenarios



Server Requirements for Windows Server Update Services

- Hardware requirements
  - Pentium III 1GHz or higher
  - 1 GB of RAM
  - 30 GB of hard disk space
- Software requirements
  - Windows 2000 Server or Windows Server 2003
  - IIS 5.0 or later
  - BITS
  - Microsoft .NET Framework 1.1 SP1
  - Internet Explorer 6.0 SP1 or later

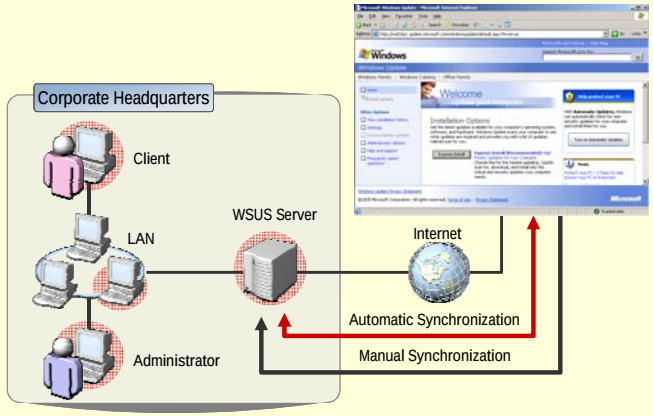
Automatic Updates Configuration

- Configure Automatic Updates by using Group Policy
- Requires updated wuau.adm administrative template
- Requires:
  - Windows 2000 SP3
  - Windows XP SP1
  - Windows Server 2003

Windows Server Update Services Administration Web Site

- Review status information
- Review and approve updates
- Generate reports
- Manage computer groups
- Configure WSUS options

How Synchronization Works



Managing Computer Groups

- Computers are automatically added
- Default computer groups
  - All Computers
  - Unassigned Computers
- Client-side targeting

Approving Updates

- Approve updates to initiate an action
  - Detection
  - Installation
  - Removal
- Decline updates
- Automate approvals

Using Reports

The reports page offers:

- Status of Updates
- Status of Computers
- Synchronization Results
- Settings Summary