

Introduction

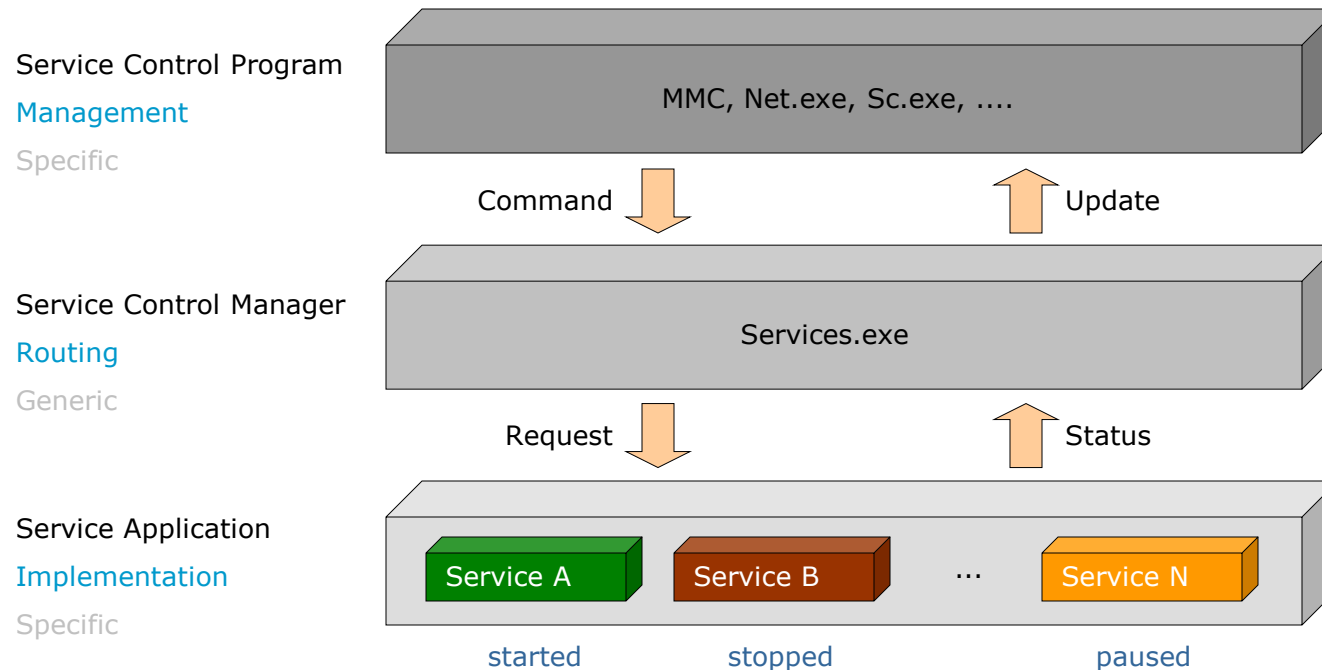
- Motivation
 - Implement server side solution (IIS, FTP, DNS, Print,...)
 - Perform background task (Antivirus, Event log...)
 - Perform privileged operations on behalf of less privileged user
- Definition
 - Background process (~daemon)
 - User-mode process
 - Win32 process with some additional code to interact with the SCM

Introduction

- Model
 - Typically start during boot process
 - Automatically started (dependency)
 - Once started never stop (when no more needed!)
 - Usually run when no user is logged
 - A host (often) contains several services
- Infrastructure
 - Services are controlled by the system
 - RPC based mechanism
 - local and remote administration

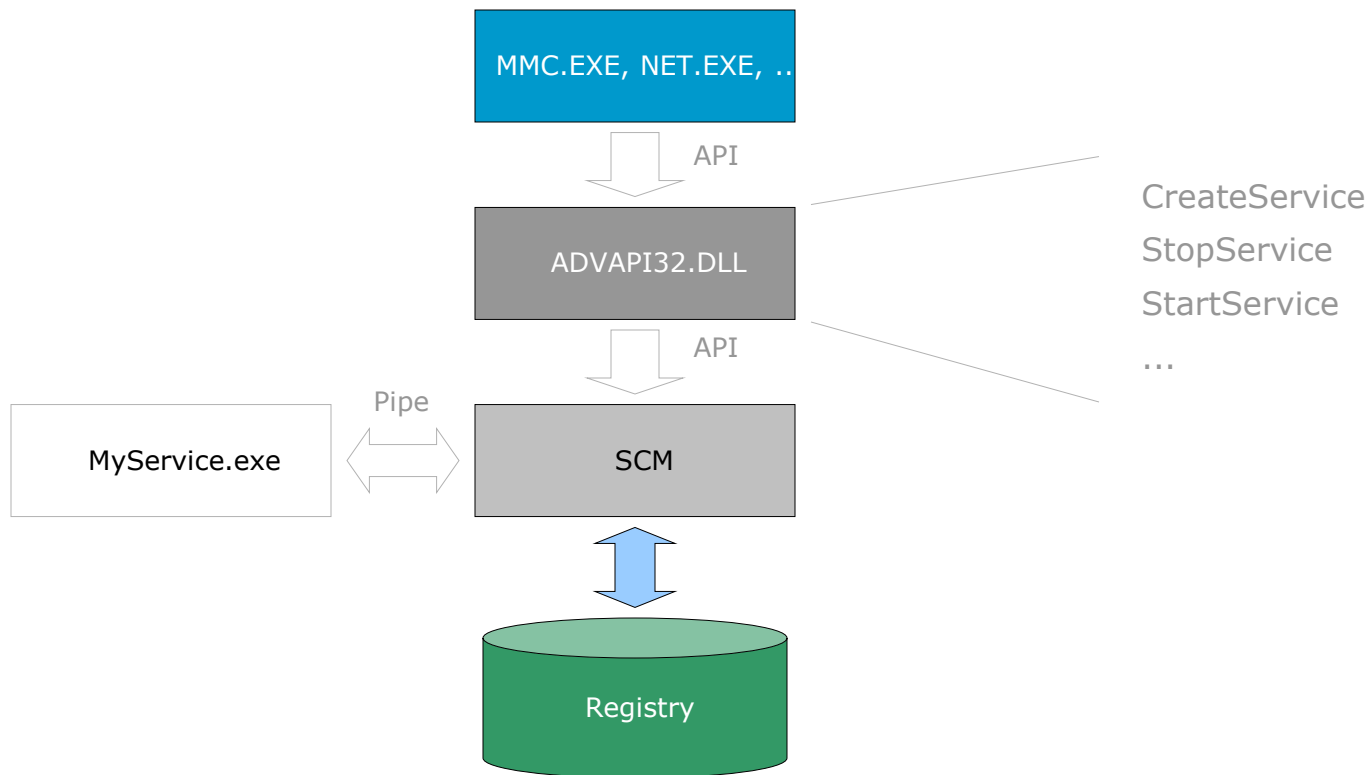
Services Components – Logical View

- Layered Architecture



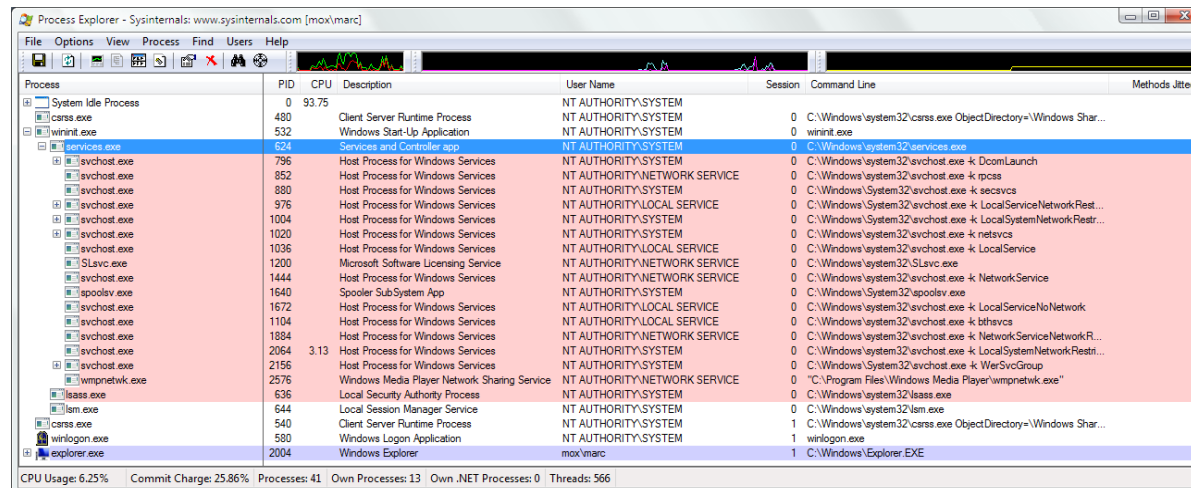
Service Control Program - SCP

- Layered Interfaces



Services Control Manager - SCM

- Owns all services
- Controls their lifetime
- Routes requests (install/start/stop/pause/delete)
- Maintains services database
 - HKLM\system\CurrentControlSet\Services

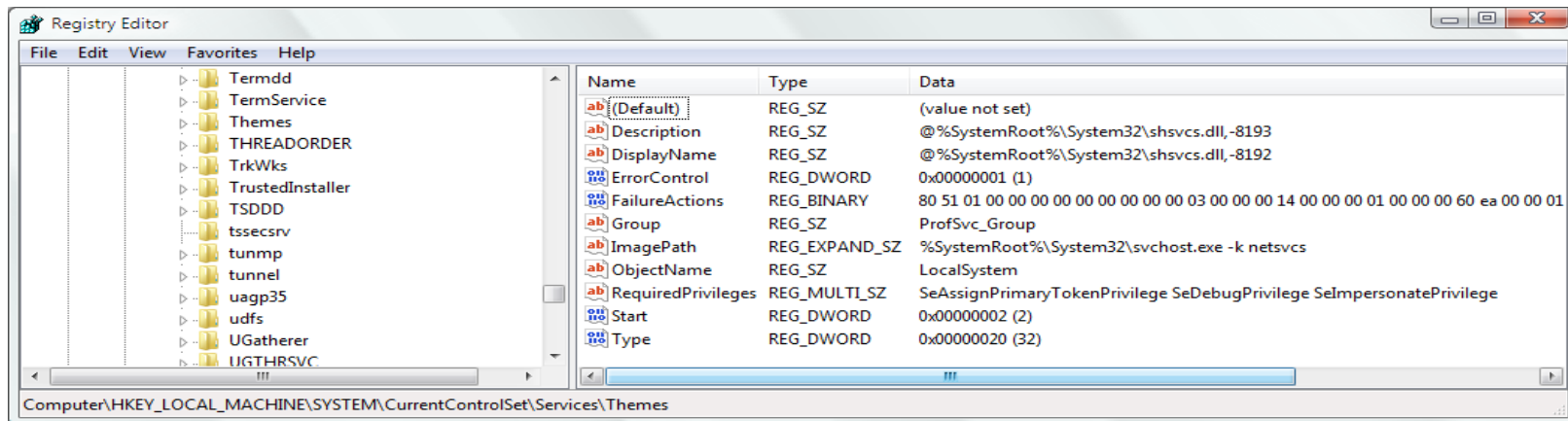


Process	PID	CPU	Description	User Name	Session	Command Line	Methods Jitted
System Idle Process	0	93.75		NT AUTHORITY\SYSTEM	0		
csrss.exe	480		Client Server Runtime Process	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\csrss.exe ObjectDirectory=\Windows Shar...	
wininit.exe	532		Windows Start-Up Application	NT AUTHORITY\SYSTEM	0	wininit.exe	
services.exe	624		Services and Controller app	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\services.exe	
svchost.exe	796		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k DcomLaunch	
svchost.exe	852		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k pssvc	
svchost.exe	880		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k secsvcs	
svchost.exe	976		Host Process for Windows Services	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestr...	
svchost.exe	1004		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestr...	
svchost.exe	1020		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k netsvcs	
svchost.exe	1036		Host Process for Windows Services	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k LocalService	
SLsvc.exe	1200		Microsoft Software Licensing Service	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\SLsvc.exe	
svchost.exe	1444		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k NetworkService	
spoolsv.exe	1640		Spooler SubSystem App	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\spoolsv.exe	
svchost.exe	1672		Host Process for Windows Services	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	
svchost.exe	1104		Host Process for Windows Services	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k bthsvcs	
svchost.exe	1894		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkR...	
svchost.exe	2064		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestr...	
svchost.exe	2156		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k WierSvcGroup	
wmipnetwk.exe	2576		Windows Media Player Network Sharing Service	NT AUTHORITY\NETWORK SERVICE	0	"C:\Program Files\Windows Media Player\wmipnetwk.exe"	
lsass.exe	636		Local Security Authority Process	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\lsass.exe	
lsim.exe	644		Local Session Manager Service	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\lsim.exe	
csrss.exe	540		Client Server Runtime Process	NT AUTHORITY\SYSTEM	1	C:\Windows\system32\csrss.exe ObjectDirectory=\Windows Shar...	
winlogon.exe	580		Windows Logon Application	NT AUTHORITY\SYSTEM	1	winlogon.exe	
explorer.exe	2004		Windows Explorer	mox\marc	1	C:\Windows\Explorer.EXE	

CPU Usage: 6.25% Commit Charge: 25.86% Processes: 41 Own Processes: 13 Own .NET Processes: 0 Threads: 566

Database

- Registration
 - CreateService(..) to register a service to the system
- Configuration
 - Name, startup, process type image file location, error reaction, description...

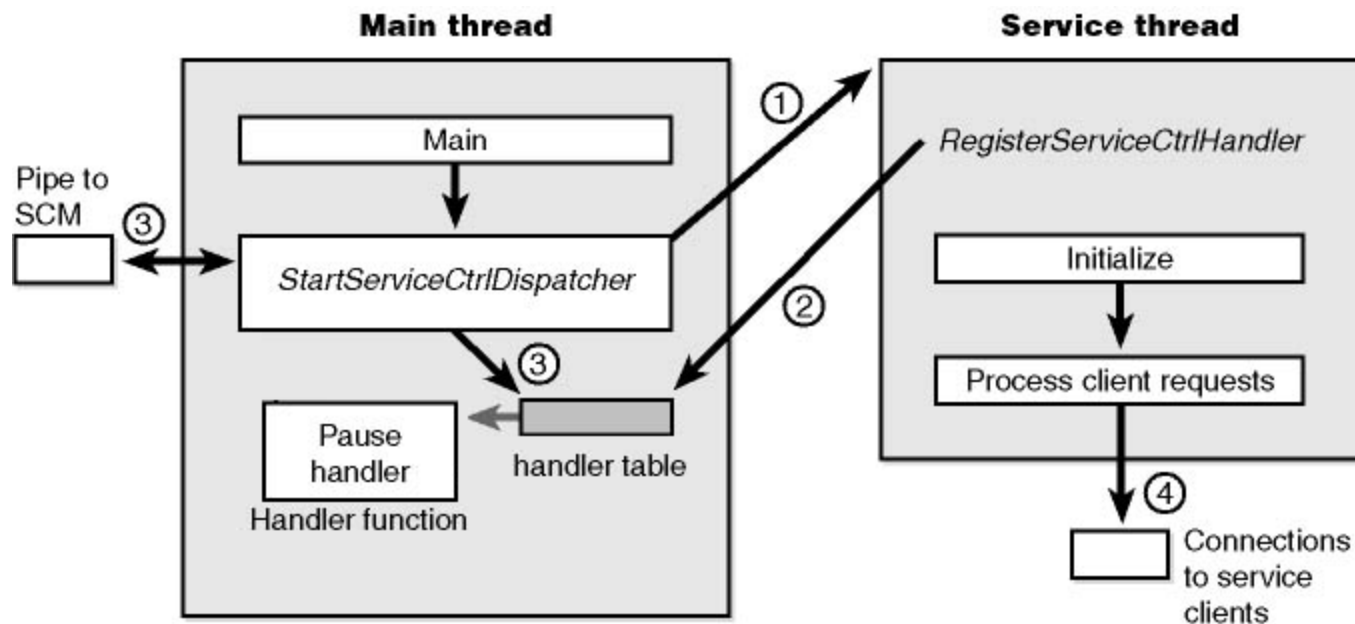


Internal Mechanism

- Types
 - SERVICE_WIN32_OWN_PROCESS
 - SERVICE_WIN32_SHARE_PROCESS
 - SERVICE_INTERACTIVE_PROCESS
- Interface
 - Interaction with the SCM
 - Receive commands
 - Send status feedback
 - Service receive SCM requests – WinMain(...)
 - Windows applications receive messages – WinMain(..)
 - Console applications receive keyboard input – Main(..)

Controls Flow

- Host have at least two threads



Windows Internals, Fifth Edition

Controls Steps

- SCM
 - Logon/Authenticate the user (LsaLogonUser)
 - Load user profile
 - Create service's process
 - Assign user's token to the process
 - Call Main(..)
- WinMain
 - Connect main thread to the SCM thread Dispatcher
 - Register service's function(s) - Collect service's entry point(s)
 - Start a thread for each service function and wait for them to terminate
 - Wait for any incoming request from the SCM (start/stop/pause/resume) and notify the appropriate thread
- Service Thread
 - Register Service's request handler

Multiple Hosted Services

- Motivation
 - Save resources
 - Boost performance
- Sample
 - Svchost.exe is the home of many Windows services

Multiple Hosted Services

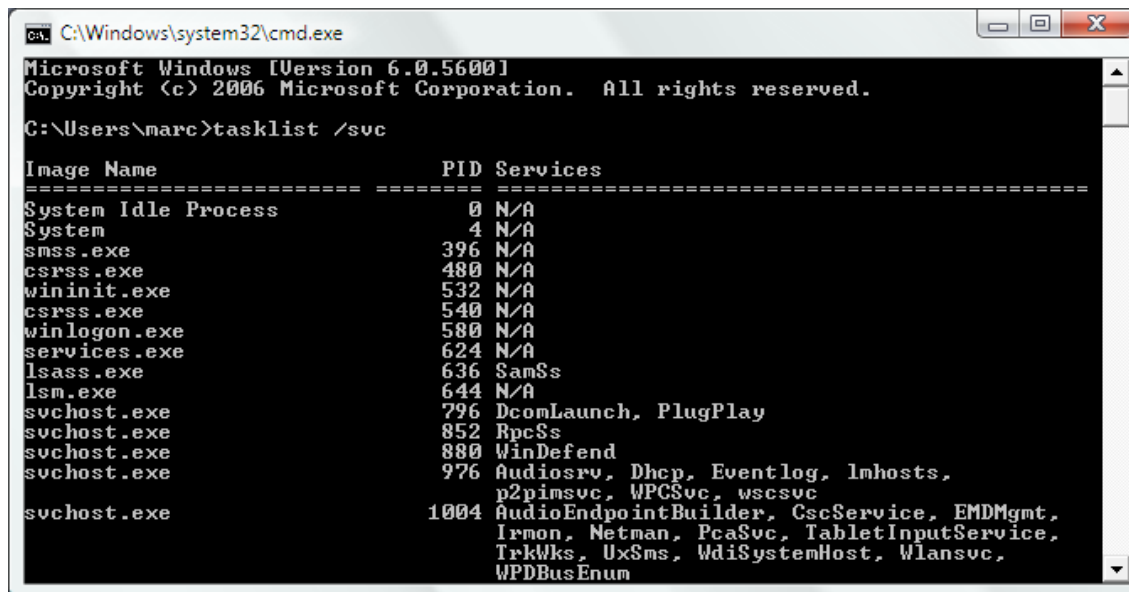
- Implications
 - Threads share same logon – Identity is the same
 - Threads share security context – Audit is difficult
 - One failure affects the host – Security is critical
 - One vulnerability compromises all hosted threads
- Best Practices
 - Services should only be consolidated if their security requirements exactly match

Windows Common Services

Server	Provides RPC, file, print and named pipe sharing (LanMan server)
Workstation	Provides network connections to RPC, file, print and named pipe sharing (LanMan client)
TCP/IP NetBios Helper	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution (LanMan host)
NetMeeting	Allows authorized users to remotely access the Windows desktop using NetMeeting
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files
Remote Registry	Allows remote registry administration (performance monitoring,...)
System Event	Tracks system events such as Windows logon, network and power events
SNMP	Monitor the activity and provide Management information
SNMP Trap	Receive traps generated by local or remote SNMP agents
Terminal Services	Provide multisession environment
Telnet	Allows a remote user to log on to the system and run console program using the command line
WWW	Provides Web connectivity
WINS	Naming service for NetBIOS network.

Hosting processes

- Many services are implemented as Libraries and must be therefore hosted
 - Hosted services share resources



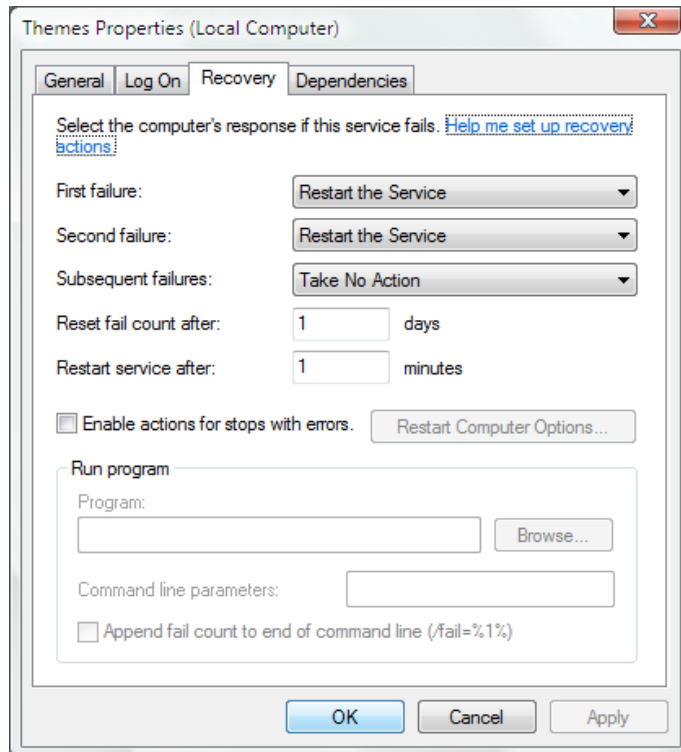
```
Microsoft Windows [Version 6.0.5600]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\marc>tasklist /svc

Image Name                      PID Services
=====
System Idle Process             0 N/A
System                          4 N/A
smss.exe                        396 N/A
csrss.exe                       480 N/A
wininit.exe                     532 N/A
csrss.exe                       540 N/A
winlogon.exe                    580 N/A
services.exe                   624 N/A
lsass.exe                       636 SamSs
lsm.exe                         644 N/A
svchost.exe                     796 DcomLaunch, PlugPlay
svchost.exe                     852 RpcSs
svchost.exe                     880 WinDefend
svchost.exe                     976 Audiosrv, Dhcp, Eventlog, lmhosts,
p2pimsvc, WPCSvc, wscsv
svchost.exe                    1004 AudioEndpointBuilder, CscService, EMDMgmt,
Irmon, Netman, PcaSvc, TabletInputService,
TrkWks, UxSms, WdiSystemHost, Wlansvc,
WPDBusEnum
```

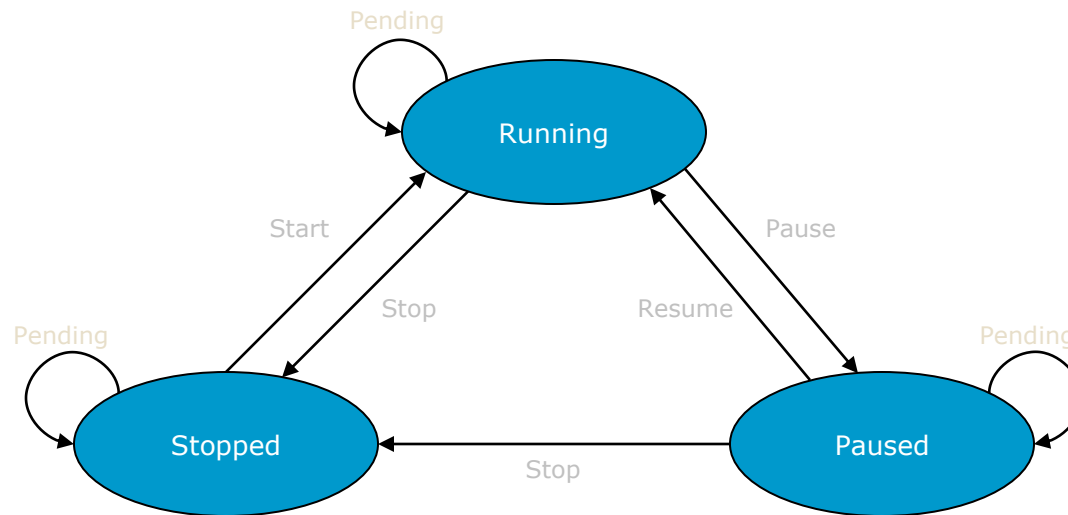
Recovery

- Motivation
 - Flexible and automatic healing and monitoring features



Services - Status

- Requests
- Transitions

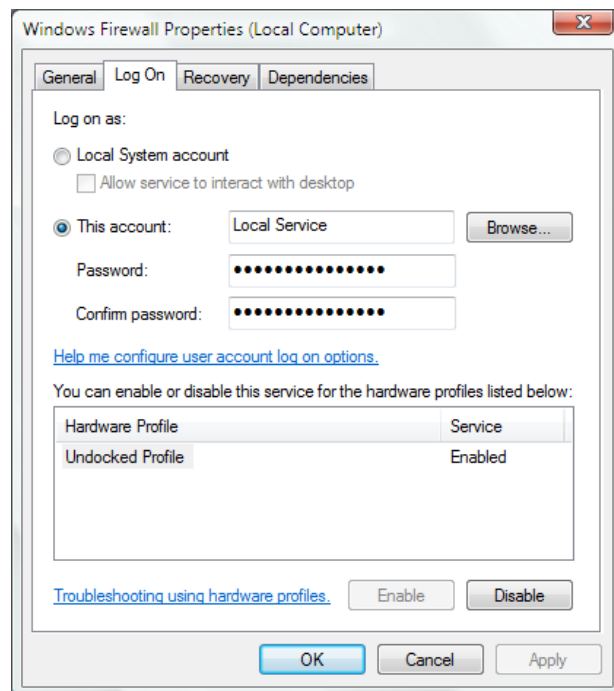


Security - Context

- Running a service under the Local System account
 - Advantages
 - Member of the local Administrators group
 - Owns virtually every defined privilege
 - Potential access to any local resource (SeTakeOwnership)
 - Only one window station is created – good for performance
 - Disadvantages
 - Only access to HKEY_CURRENT_USER\.Default
 - Service settings will be place in machine-specific registry area
 - No access to any other interactive users resources
 - Restricted access to network resource (printers, shares, named pipes that allow null session – connection without credential)
 - Very restricted access to WinSta0 (visible/interactive) window station
 - Only one window station is created – bad for security

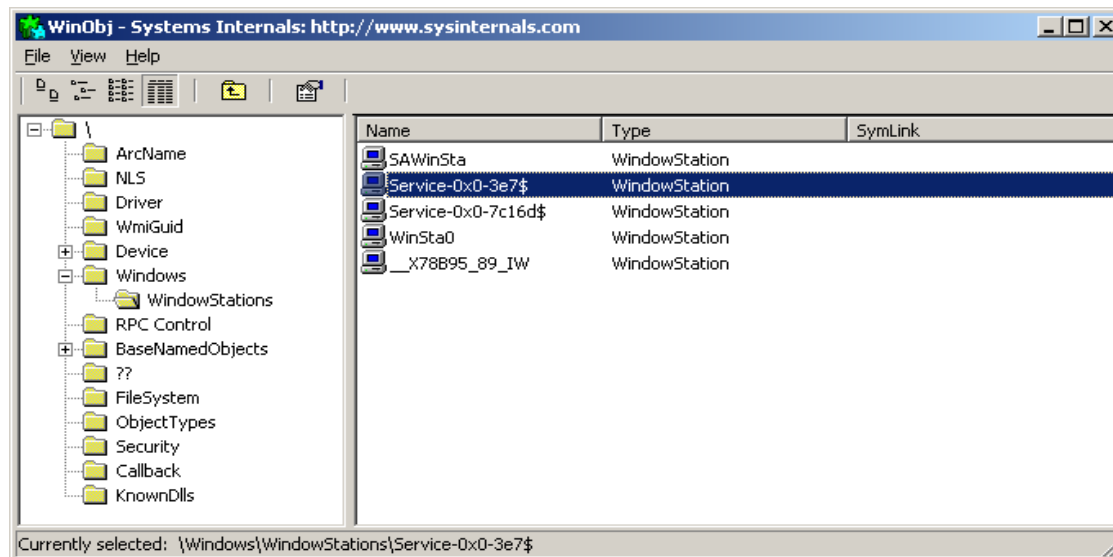
Security - Context

- Running an interactive service under the Local System account
 - Share user window station (desktop, clipboard,...)
 - SERVICE_INTERACTIVE_PROCESS



Security - Context

- Running a service under a specific user account
 - No access to WinSta0
 - Incompatible with any interactive usage
 - Access to HKEY_CURRENT_USER\sid profile (mapped drives, shares, printers...)



Security - Recommendations

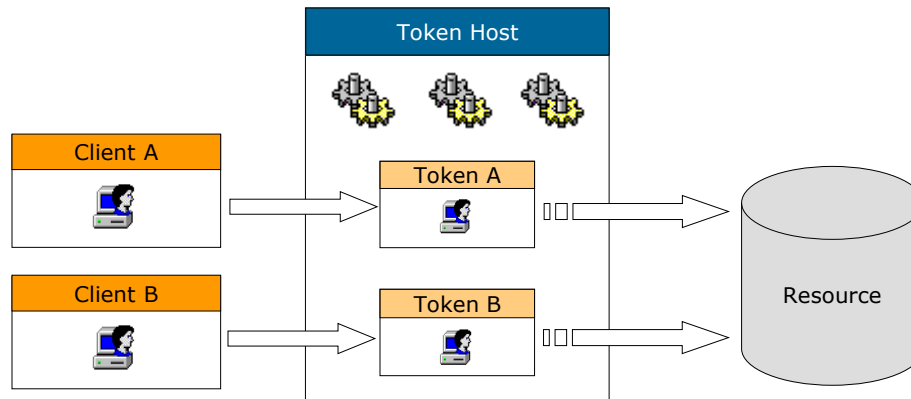
- Services are largest exposure to attack
 - buffer overflow, DOS, privilege escalation
- Use Discrete Account
 - LocalSystem has complete control of the system
 - Better security granularity – LocalSystem cf. multiple users sharing the same user account and password
 - Better auditing (for most exposed services)

Impersonation

- Definition
 - Take the identity of another user and perform a task in his security context
 - A thread is assigned a token different of its process
- Motivation
 - The reason why token exist at all!
 - Allow adjustable settings in a security context (privileges, ACL...)
 - Allow local customization without race condition on other parts of the application
 - Allow a thread to slip into a different security context
- Levels
 - Server creates a token with the trust indicated by the client
 - SecurityAnonymous: Client cannot be identified nor impersonated
 - SecurityIdentification: Client can be identified but not impersonated
 - SecurityImpersonation: Client can be used to open local objects

Impersonation

- Perform privileged operations on behalf of less privileged users

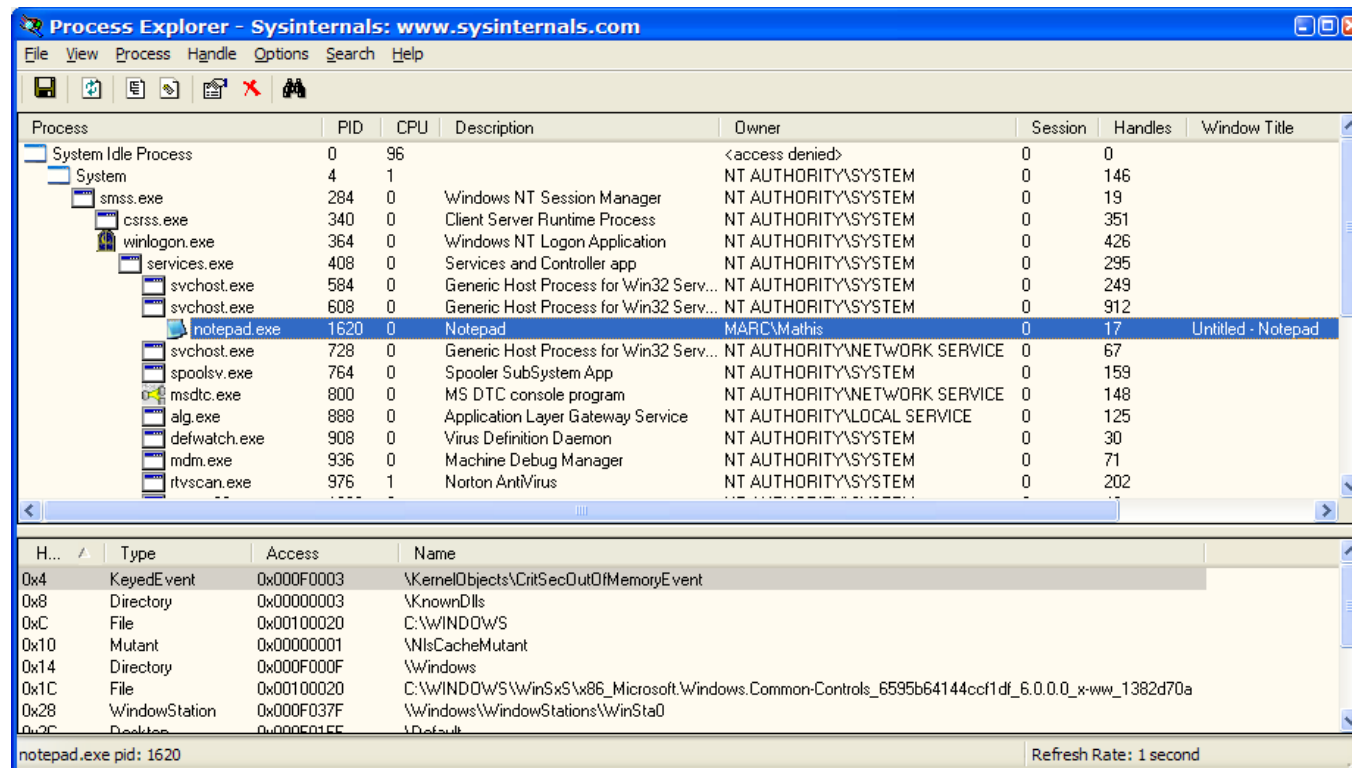


Impersonation

- Typically all threads within a process share (copy) the same token
 - In some situation a thread can have its own token
- A thread token overrides the host process token
 - There is no API to change a process token
 - There is an API to change a thread token

Impersonation

- Running a program with other credentials

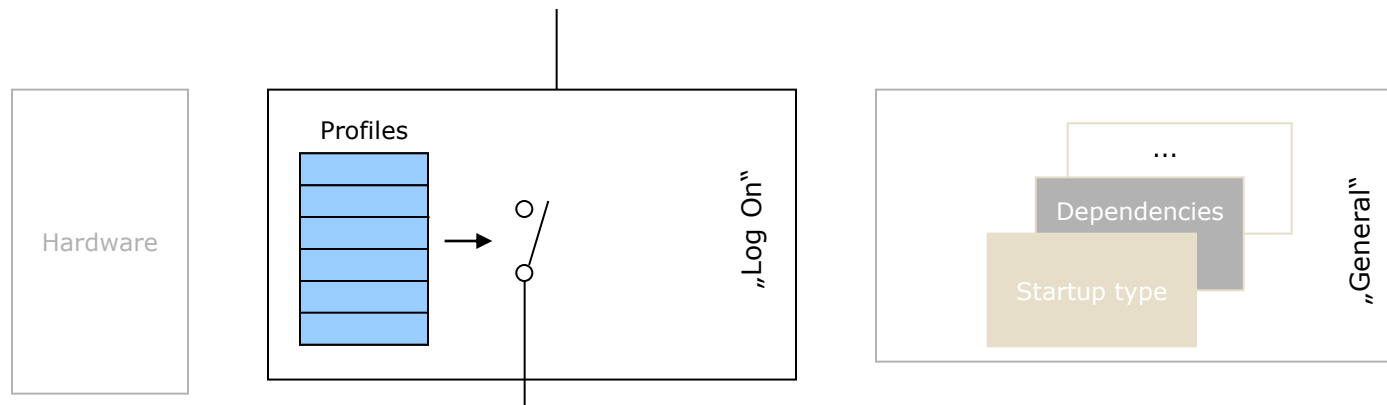


Services - Profiles

- Motivation
 - Some services are not necessary
 - „Computer Browser“ on a computer without a network interface
 - Some services should not run
 - „NetBIOS“ on a computer accessible over the Internet
 - Adjust services configuration...without taking too much risk

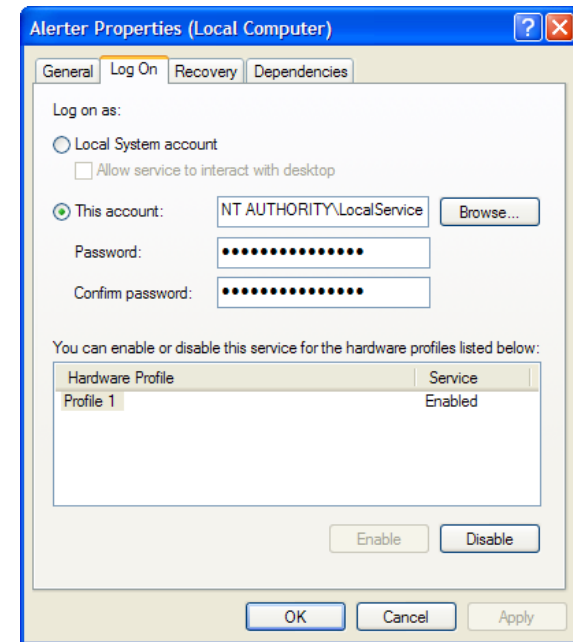
Services - Profiles

- Solution
 - Load services dependant to environment
 - Associate a service to a hardware profile



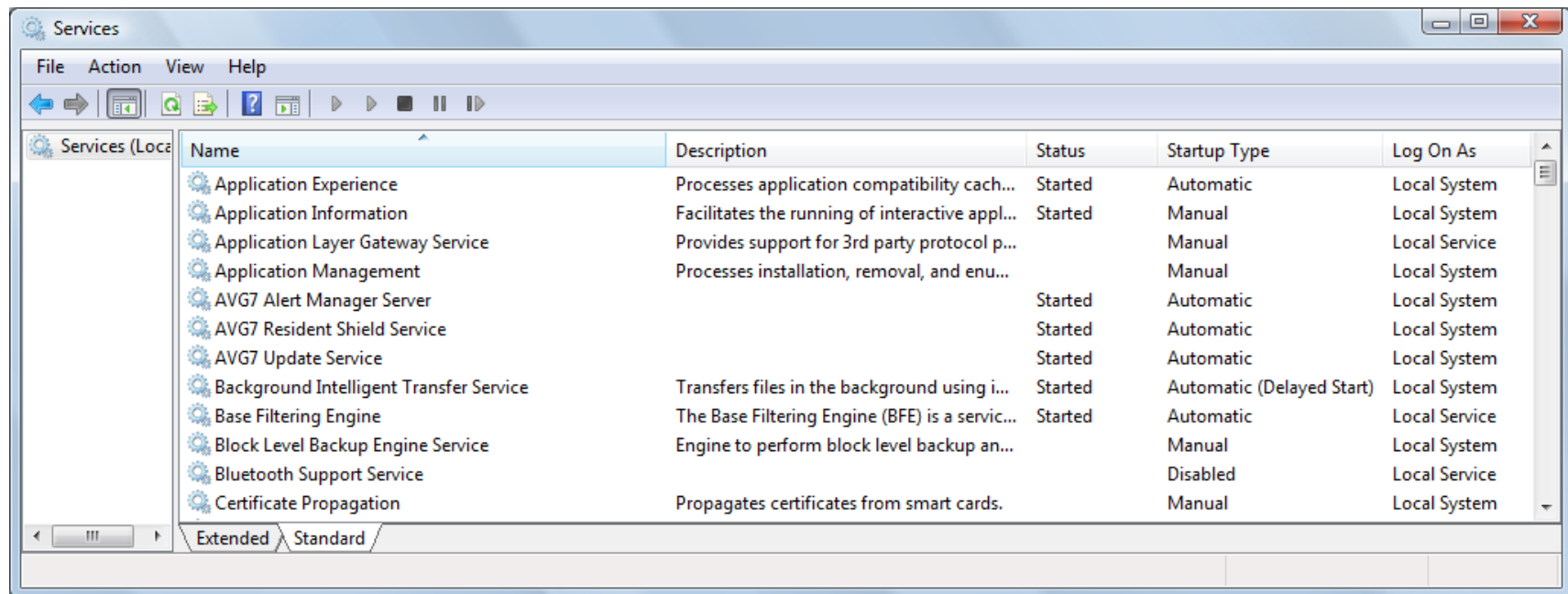
Hardware Profiles

- “General” settings affect
 - All hardware profiles
 - All users accounts
- “Log On” settings affect
 - All users accounts
- Some services cannot be disabled
 - “Event Log”
 - “PnP”
- On service should not be disabled
 - “RPC” - system unbootable



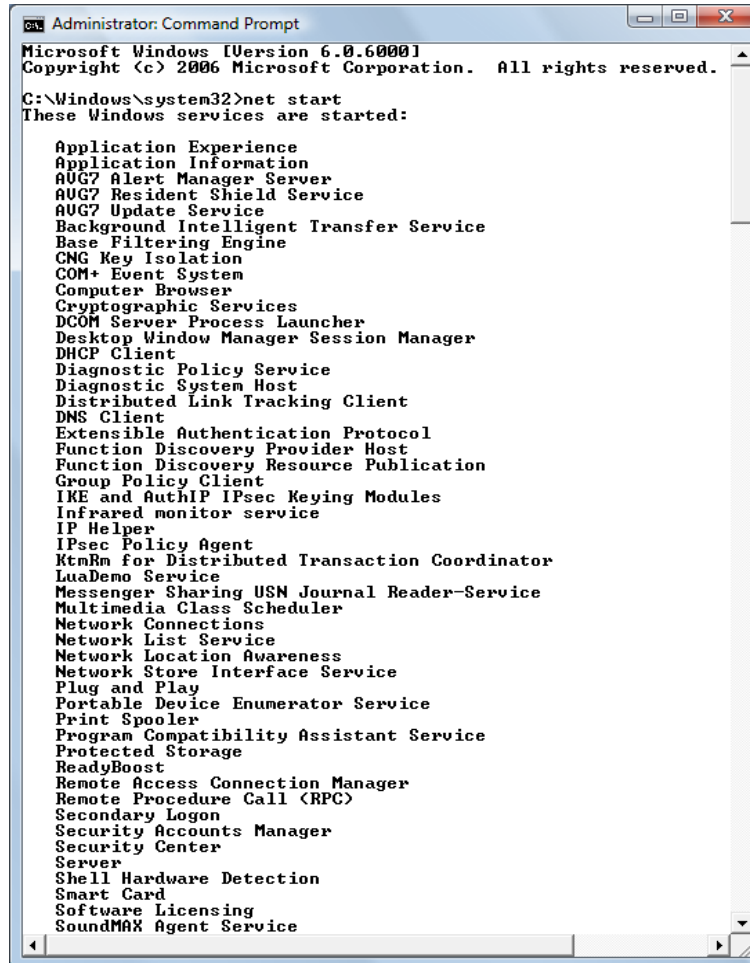
Services - Management

- Microsoft Management Console (MMC)



Services - Management

- > net



```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net start
These Windows services are started:

Application Experience
Application Information
AUG? Alert Manager Server
AUG? Resident Shield Service
AUG? Update Service
Background Intelligent Transfer Service
Base Filtering Engine
CNG Key Isolation
COM+ Event System
Computer Browser
Cryptographic Services
DCOM Server Process Launcher
Desktop Window Manager Session Manager
DHCP Client
Diagnostic Policy Service
Diagnostic System Host
Distributed Link Tracking Client
DNS Client
Extensible Authentication Protocol
Function Discovery Provider Host
Function Discovery Resource Publication
Group Policy Client
IKE and AuthIP IPsec Keying Modules
Infrared monitor service
IP Helper
IPsec Policy Agent
KtmRm for Distributed Transaction Coordinator
LuaDemo Service
Messenger Sharing USN Journal Reader-Service
Multimedia Class Scheduler
Network Connections
Network List Service
Network Location Awareness
Network Store Interface Service
Plug and Play
Portable Device Enumerator Service
Print Spooler
Program Compatibility Assistant Service
Protected Storage
ReadyBoost
Remote Access Connection Manager
Remote Procedure Call (RPC)
Secondary Logon
Security Accounts Manager
Security Center
Server
Shell Hardware Detection
Smart Card
Software Licensing
SoundMAX Agent Service
```

Services - Management

- > Sc

```
Administrator: Command Prompt - sc

C:\Windows\system32>sc
DESCRIPTION:
    SC is a command line program used for communicating with the
    Service Control Manager and services.
USAGE:
    sc <server> [command] [service name] <option1> <option2>...

The option <server> has the form "\\ServerName"
Further help on commands can be obtained by typing: "sc [command]"
Commands:
    query-----Queries the status for a service, or
                  enumerates the status for types of services.
    queryex-----Queries the extended status for a service, or
                  enumerates the status for types of services.
    start-----Starts a service.
    pause-----Sends a PAUSE control request to a service.
    interrogate---Sends an INTERROGATE control request to a service.
    continue----Sends a CONTINUE control request to a service.
    stop-----Sends a STOP request to a service.
    config-----Changes the configuration of a service <persistent>.
    description--Changes the description of a service.
    failure-----Changes the actions taken by a service upon failure.
    failureflag---Changes the failure actions flag of a service.
    sidtype-----Changes the service SID type of a service.
    privs-----Changes the required privileges of a service.
    qc-----Queries the configuration information for a service.
    qdescription--Queries the description for a service.
    qfailure-----Queries the actions taken by a service upon failure.
    qfailureflag--Queries the failure actions flag of a service.
    qsidtype-----Queries the service SID type of a service.
    qprivs-----Queries the required privileges of a service.
    delete-----Deletes a service (from the registry).
    create-----Creates a service. (adds it to the registry).
    control-----Sends a control to a service.
    sdshow-----Displays a service's security descriptor.
    sdset-----Sets a service's security descriptor.
    showsid-----Displays the service SID string corresponding to an ar
bitrary name.
    GetDisplayName--Gets the DisplayName for a service.
    GetKeyName-----Gets the ServiceKeyName for a service.
    EnumDepend-----Enumerates Service Dependencies.

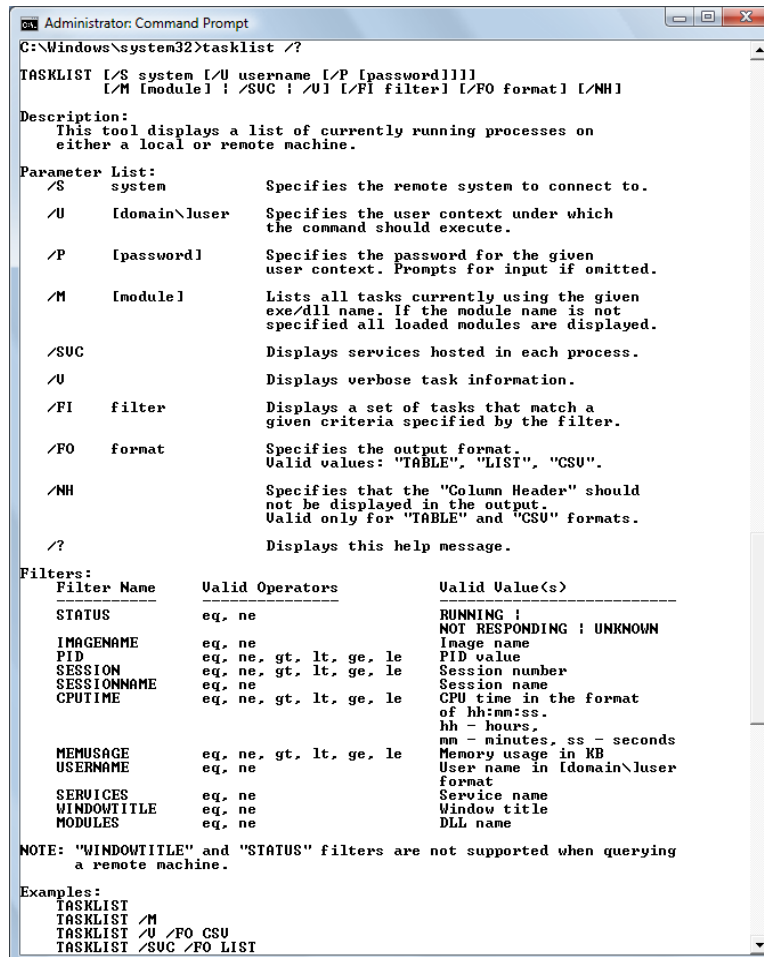
The following commands don't require a service name:
sc <server> <command> <option>
    boot-----<ok ! bad> Indicates whether the last boot should
                  be saved as the last-known-good boot configuration
    Lock-----Locks the Service Database
    QueryLock----Queries the LockStatus for the SCManager Database

EXAMPLE:
    sc start MyService

Would you like to see help for the QUERY and QUERYEX commands? [ y | n ]:
```

Services - Management

- > tasklist



```

Administrator: Command Prompt
C:\Windows\system32>tasklist /?

TASKLIST [/S system [/U username [/P [password]]]
          [/M [module] [/SUC [/U] [/FI filter] [/FO format] [/NH]

Description:
This tool displays a list of currently running processes on
either a local or remote machine.

Parameter List:
/S      system          Specifies the remote system to connect to.
/U      [domain\user]   Specifies the user context under which
                        the command should execute.
/P      [password]      Specifies the password for the given
                        user context. Prompts for input if omitted.
/M      [module]        Lists all tasks currently using the given
                        exe/dll name. If the module name is not
                        specified all loaded modules are displayed.
/SUC                      Displays services hosted in each process.
/U                      Displays verbose task information.
/FI     filter          Displays a set of tasks that match a
                        given criteria specified by the filter.
/FO     format          Specifies the output format.
                        Valid values: "TABLE", "LIST", "CSV".
/NH                      Specifies that the "Column Header" should
                        not be displayed in the output.
                        Valid only for "TABLE" and "CSV" formats.
/?                      Displays this help message.

Filters:
Filter Name      Valid Operators      Valid Value(s)
-----
STATUS          eq, ne          RUNNING !
                        NOT RESPONDING ! UNKNOWN
IMAGENAME        eq, ne          Image name
PID              eq, ne, gt, lt, ge, le  PID value
SESSION          eq, ne, gt, lt, ge, le  Session number
SESSIONNAME      eq, ne          Session name
CPU             eq, ne, gt, lt, ge, le  CPU time in the format
                        of hh:mm:ss.
                        hh - hours,
                        mm - minutes, ss - seconds
MEMUSAGE         eq, ne, gt, lt, ge, le  Memory usage in KB
USERNAME         eq, ne          User name in [domain\user
                        format
SERVICES         eq, ne          Service name
WINDOWTITLE      eq, ne          Window title
MODULES          eq, ne          DLL name

NOTE: "WINDOWTITLE" and "STATUS" filters are not supported when querying
a remote machine.

Examples:
TASKLIST
TASKLIST /M
TASKLIST /U /FO CSV
TASKLIST /SUC /FO LIST
  
```

Services - Management

- `OpenSCManager()`
- `CreateService()`
- `OpenService()`
- `ControlService()`
- `QueryServiceStatus()`
- `DeleteService()`

More

- NT Services, Wrox Press, Kevin Miller
- Programming NT Security, Addison-Wesley, Keith Brown
- Windows NT Security, R&D Books Miller Freeman, N.Okuntseff
- Windows NT Security Guide, Addison Wesley, Stephen A. Sutton
- Microsoft Windows Internals, Microsoft Press, Solomon, Russinovich
- Modern Operating Systems – Second Edition, Prentice Hall, Tanenbaum
- Inside Win32 Services, Mark Russinovich, www.win2000mag.com
- www.sysinternals.com

...

- Mitre >
 - T1035 - Service Execution
 - T1031 – Modifying existing Service
- Events >
 - Event 7036 – A service has started
 - Event 7045 – A service has been installed