Introduction

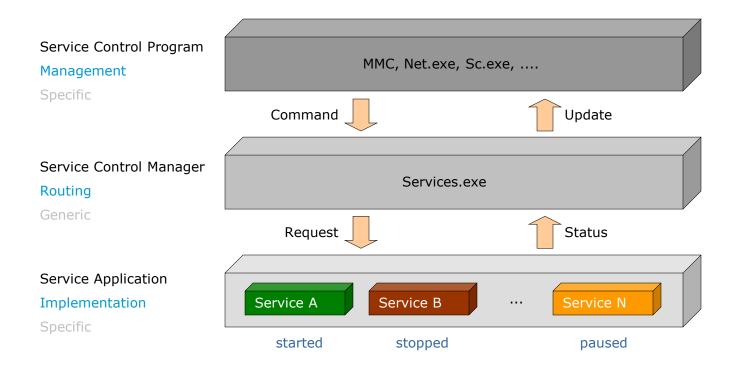
- Motivation
 - Implement server side solution (IIS, FTP, DNS, Print,...)
 - Perform background task (Antivirus, Event log...)
 - Perform privileged operations on behalf of less privileged user
- Definition
 - Background process (~daemon)
 - User-mode process
 - Win32 process with some additional code 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 controled by the system
 - RPC based mechanism
 - local and remote administration

Services Components – Logical View

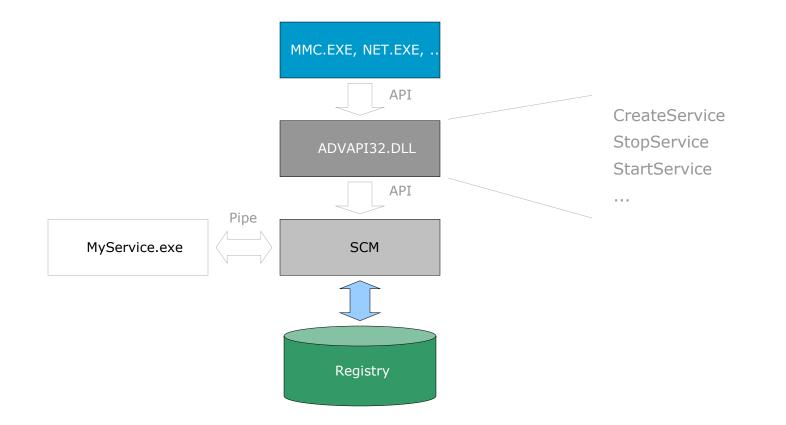
• Layered Architecture



@ochsenmeier | Marc Ochsenmeier | www.winitor.com

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

ile Options View Process Find Use			400 · · ·		1		
🚽 🗿 💻 🖹 🚟 🔊 😭 🗡	1 69	M		and an	- A		
rocess	PID	CPU	Description	User Name	Session	Command Line	Methods Jitt
System Idle Process	0	93.75		NT AUTHORITY\SYSTEM			
CSISS.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	
E Svchost.exe	796		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe + DcomLaunch	
svchost.exe	852		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe +k rpcss	
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\sychost.exe +k LocalServiceNetworkRest	
svchost.exe	1004		Host Process for Windows Services	NT AUTHORITY\SYSTEM	0	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestr	
E 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\sychost.exe +k LocalService	
SLsvc.exe	1200		Microsoft Software Licensing Service	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\svstem32\SLsvc.exe	
svchost.exe	1444		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\sychost.exe + 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 + LocalServiceNoNetwork	
sychost.exe	1104		Host Process for Windows Services	NT AUTHORITY\LOCAL SERVICE		C:\Windows\system32\sychost.exe +k bthsvcs	
svchost.exe	1884		Host Process for Windows Services	NT AUTHORITY\NETWORK SERVICE		C:\Windows\system32\sychost.exe + NetworkServiceNetworkR	
svchost exe	2064	3.13	Host Process for Windows Services	NT AUTHORITY\SYSTEM		C:\Windows\system32\sychost.exe +k LocalSystemNetworkRestri	
sychost.exe	2156		Host Process for Windows Services	NT AUTHORITY\SYSTEM		C:\Windows\System32\sychost.exe -k WerSycGroup	
wmpnetwk.exe	2576		Windows Media Player Network Sharing Service	NT AUTHORITY\NETWORK SERVICE		"C:\Program Files\Windows Media Player\wmpnetwk.exe"	
sass.exe	636		Local Security Authority Process	NT AUTHORITY\SYSTEM		C:\Windows\system32\lsass.exe	
Ism.exe	644		Local Session Manager Service	NT AUTHORITY\SYSTEM		C:\Windows\svstem32\lsm.exe	
Carss 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	i	winlogon.exe	
explorer.exe	2004		Windows Explorer	mox/marc		C:\Windows\Explorer.EXE	

Database

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

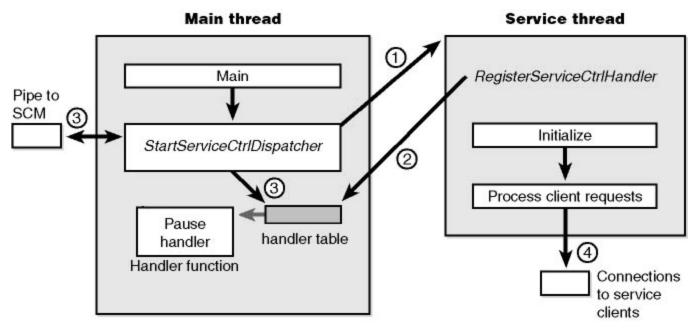
📸 Registry Editor				
File Edit View Favorites Help				
File Edit View Favorites Help P Termdd TermService P Themes P ThreMes P TrustedInstaller P TSDDD P Tunnel P Uagp35 P UGTHRSVC	•	Name (Default) Description DisplayName ErrorControl FailureActions Group TangePath ObjectName RequiredPrivileges Start Start Type	Type REG_SZ REG_SZ REG_DWORD REG_BINARY REG_SZ REG_EXPAND_SZ REG_SZ REG_MULTI_SZ REG_DWORD REG_DWORD	Data (value not set) @%SystemRoot%\System32\shsvcs.dll,-8193 @%SystemRoot%\System32\shsvcs.dll,-8192 0x0000001 (1) 80 51 01 00 00 00 00 00 00 00 00 30 00 00 14 00 00 00 10 00 00 60 ea 00 00 01 ProfSvc_Group %SystemRoot%\System32\svchost.exe -k netsvcs LocalSystem SeAssignPrimaryTokenPrivilege SeDebugPrivilege SeImpersonatePrivilege 0x0000002 (2) 0x00000020 (32)
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\S	Servi			III
Computer (INKET_LOCAL_IMACHINE(SYSTEM)(CuffentControlSet)3	Servi	cestmemes		

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

C:\Windows\system32\cmd.exe		
	soft Corpor	ation. All rights reserved.
C:\Users\marc>tasklist / 		
Image Name	PID	Services
system Idle Process	============== A	N/A
System fulle frocess System		N/A
mss.exe	396	
SPSS.exe	480	
ininit.exe	532	
SPSS.exe	540	
inlogon.exe	580	
ervices.exe	624	
sass.exe		SamSs
lsm.exe	644	
svchost.exe	796	DcomLaunch, PlugPlay
vchost.exe		RpcSs
vchost.exe		WinDefend
svchost.exe	976	Audiosrv, Dhcp, Eventlog, 1mhosts,
		p2pimsvc, WPCŠvc, wscsvc
svchost.exe	1004	AudioEndpointBuilder, CscService, EMDMgmt,
		Irmon, Netman, PcaSvc, TabletInputService,
		TrkWks, UxSms, WdiSystemHost, Wlansvc,
		WPDBusEnum State S

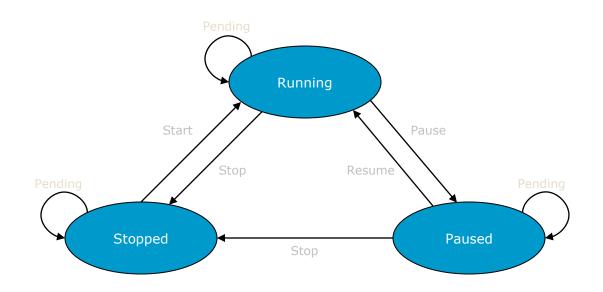
Recovery

- Motivation
 - Flexible and automatic healing and monitoring features

Themes Properties (Local Com	puter)	x					
General Log On Recovery	Dependenc	ies					
Select the computer's respons	e if this servio	e fails. <u>Help me set up recovery</u>					
First failure:	Restart the	Service 👻					
Second failure:	Restart the	Service 👻					
Subsequent failures:	Take No A	ction 💌					
Reset fail count after:	1	days					
Restart service after:	1	minutes					
Enable actions for stops w	ith errors.	Restart Computer Options					
Run program							
Program:							
		Browse					
Command line parameters:	Command line parameters:						
Append fail count to en	d of command	l line (/fail=%1%)					
	ОК	Cancel Apply					

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

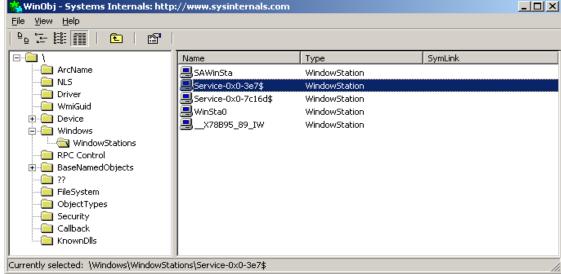
Security - Context

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

Windows Firewall Propert	ies (Local Computer)	X
General Log On Reco	very Dependencies	
Log on as:		
Local System accour Allow service to in	it teract with desktop	
This account:	Local Service	Browse
Password:	•••••	
Confirm password:	•••••	
Help me configure user a		
You can enable or disab	e this service for the hardware p	Service
Undocked Profile		Enabled
Troubleshooting using ha	ardware profiles. Enable	Disable
	OK Canc	el Apply

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

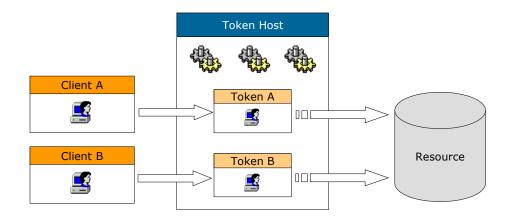
- Services are largest exposure to attack
 - buffer overflow, DOS, privilege escalation
- Use Discrete Account
 - LocalSystem has complete control of the system
 - Better security granularity LocalSystem cf. multiple users sharing the same user account and password
 - Better auditing (for most exposed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

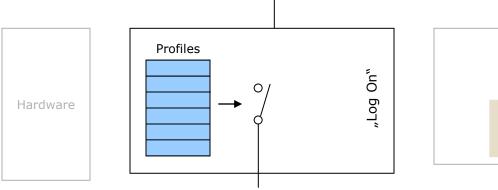
Droce	ess Explorer -	Sysinternal	10/10/	w.sysinternals.com					
	Process Handle			hisysmeethalsteem					ک ر
		<u> </u>							
Process		PID	CPU	Description	Owner	Session	Handles	Window Title	^
📃 System	Idle Process	0	96		<access denied=""></access>	0	0		
📃 Syst	tem	4	1		NT AUTHORITY\SYSTEM	0	146		
	smss.exe	284	0	Windows NT Session Manager	NT AUTHORITY\SYSTEM	0	19		
	CSISS.exe	340	0	Client Server Runtime Process	NT AUTHORITY\SYSTEM	0	351		
1	🍈 winlogon.exe	364	0	Windows NT Logon Application	NT AUTHORITY\SYSTEM	0	426		
	services.exe	408	0	Services and Controller app	NT AUTHORITY\SYSTEM	0	295		
	svchost.exe	e 584	0	Generic Host Process for Win32 Serv.	. NT AUTHORITY\SYSTEM	0	249		
	📩 svchost.exe	e 608	0	Generic Host Process for Win32 Serv	. NT AUTHORITY\SYSTEM	0	912		
	🔁 notepad	l.exe 1620	0	Notepad	MARC\Mathis	0	17	Untitled - Notepad	
	svchost.exe	e 728	0	Generic Host Process for Win32 Serv	. NT AUTHORITY\NETWORK SERVICE	0	67		
	📩 spoolsv.exe	e 764	0	Spooler SubSystem App	NT AUTHORITY\SYSTEM	0	159		
	ன msdtc.exe	800	0	MS DTC console program	NT AUTHORITY\NETWORK SERVICE	0	148		
	🗂 alg.exe	888	0	Application Laver Gateway Service	NT AUTHORITY\LOCAL SERVICE	0	125		
	defwatch.e	xe 908	0	Virus Definition Daemon	NT AUTHORITY\SYSTEM	0	30		
	🥅 mdm.exe	936	0	Machine Debug Manager	NT AUTHORITY\SYSTEM	0	71		
	📩 rtyscan.exe	976	1	Norton AntiVirus	NT AUTHORITY\SYSTEM	0	202		~
<			-			-			>
H A	Туре	Access	N :	ame					~
0x4	KeyedEvent	0x000F0003		rnelObjects\CritSecOutOfMemoryEvent					
0x4 0x8	Directory	0x000F0003		ownDlls					
0xc 0xC	File	0x00000003		windus VINDOWS					
oxc Ox10	File Mutant	0x00100020 0x00000001		CacheMutant					
0x10 0x14	Directory	0x00000001		ndows					_
0x14 0x1C	File	0x000F000F			lows.Common-Controls 6595b64144ccf1df	c o o o	1202470.		
0x1C 0x28	riie WindowStation	0x00100020		ndows\WindowStations\WinSta0	iuws.common-controis_6030064144ccr1dr	_0.0.0.0_X-V	ww_1362070a	1	
0x28 0v2C	Windowstation	0x000F037F							~
notepad.ex						Refresh I	Rate: 1 secon	nd	

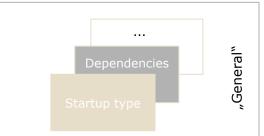
Services - Profiles

- 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

General Log On Re	covery Dependencies
Log on as:	
Local System acc Allow service to	punt p interact with desktop
• This account:	NT AUTHORITY\LocalService Browse
Password:	•••••
Confirm password	•••••
You can enable or dis	able this service for the hardware profiles listed below:
You can enable or dis Hardware Profile	able this service for the hardware profiles listed below:

Services - Management

• Microsoft Management Console (MMC)

ile Action V	iew Help				
Services (Loca	Name	Description	Status	Startup Type	Log On As
	Application Experience	Processes application compatibility cach	Started	Automatic	Local System
	Application Information	Facilitates the running of interactive appl	Started	Manual	Local System
	Application Layer Gateway Service	Provides support for 3rd party protocol p		Manual	Local Service
	Application Management	Processes installation, removal, and enu		Manual	Local System
	🔍 AVG7 Alert Manager Server		Started	Automatic	Local System
	AVG7 Resident Shield Service		Started	Automatic	Local System
	🔍 AVG7 Update Service		Started	Automatic	Local System
	🖗 Background Intelligent Transfer Service	Transfers files in the background using i	Started	Automatic (Delayed Start)	Local System
	🔍 Base Filtering Engine	The Base Filtering Engine (BFE) is a servic	Started	Automatic	Local Service
	🔍 Block Level Backup Engine Service	Engine to perform block level backup an		Manual	Local System
	🔍 Bluetooth Support Service			Disabled	Local Service
	🔍 Certificate Propagation	Propagates certificates from smart cards.		Manual	Local System

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
	AUG7 Alert Manager Server AUG7 Resident Shield Service AUG7 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

• > Sc

Services - Management

C:\Windo DESCRIPI	ows\system32>sc
DESCRIPT	SC is a command line program used for communicating with the
	Service Control Manager and services.
USAGE:	-
	sc <server> [command] [service name] <option1> <option2></option2></option1></server>
	The option <server> has the form "\\ServerName"</server>
	Further help on commands can be obtained by typing: "sc [command]"
	Commands:
	queryQueries the status for a service, or
	enumerates the status for types of services. queryexQueries the extended status for a service, or
	queryexqueries the extended status for a service, or enumerates the status for types of services.
	startStarts a service.
	pauseSends a PAUSE control request to a service.
	interrogateSends an INTERROGATE control request to a service.
	continueSends a CONTINUE control request to a service.
	stopSends a STOP request to a service. configChanges the configuration of a service (persistent).
	descriptionChanges the description of a service.
	failureChanges the actions taken by a service upon failure.
	failureflagChanges the failure actions flag of a service.
	sidtypeChanges the service SID type of a service.
	privsChanges the required privileges of a service. qcQueries the configuration information for a service.
	gcqueries the configuration information for a service.
	qfailureQueries the actions taken by a service upon failure.
	gfailureflagQueries the failure actions flag of a service.
	qsidtypeQueries the service SID type of a service.
	qprivsQueries the required privileges of a service.
	deleteDeletes a service (from the registry). createCreates a service. (adds it to the registry).
	controlSends a control to a service.
	sdshowDisplays a service's security descriptor.
	sdsetSets a service's security descriptor.
L	showsidDisplays the service SID string corresponding to an a
bitrary	
	GetDisplayNameGets the DisplayName for a service. GetKeyNameGets the ServiceKeyName for a service.
	EnumDependEnumerates Service Dependencies.
	The following commands don't require a service name:
	sc (server) (command) (option)
	boot(ok ¦ ĥad) Indicates whether the last boot should be saved as the last-known-good boot configuration
	LockLocks the Service Database
EVANDI E	QueryLockQueries the LockStatus for the SCManager Database
EXAMPLE:	: sc start MyService

Services - Management

> tasklist

as Administra	ator: Command	l Prompt						
C:\Windows	s\system32	>taskl:	ist /?					
TASKLIST	[/S system [/M [modulo	[/U u: e] /!	ername [/ VC /V]	⁄₽[p [∕F]	asswo filte	rd]]]] er] [/FO format] [/NH]		
	on: cool displa ^ a local d				tly r	unning processes on		
Parameter ⁄S	List: system		Specific	es th	e rem	ote system to connect to.		
∕U	[domain\]		Specifies the user context under which the command should execute.					
∕P	[password	Specific user con	Specifies the password for the given user context. Prompts for input if omitted.					
∕M	∕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			Display	ser	vices	hosted in each process.		
∕∪			Displays	ver	bose 1	task information.		
∕FI	filter		Display: given ci	Displays a set of tasks that match a given criteria specified by the filter.				
∕F0	∕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.							
/?						p message.		
Filters: Filter	• Name	Valid	Operators	3		Valid Value(s)		
STATUS		eq, no	,	-		RUNNING : NOT RESPONDING : UNKNOWN		
IMAGEN PID	IAME	eq, ne	e art 1t	(re	le	Image name PID value		
SESSIC)n Nname	eq, no	, gt, lt, , gt, lt,	ge,	le	Session number		
CPUTI		eq, no eq, no	: . gt, lt,	. ge,	le	Session name CPU time in the format		
			_	_		of hh:mm:ss. hh - hours,		
мтына	AF.					mm - minutes, ss - seconds		
MEMUSA Userna		eq, no eq, no	e, gt, lt, 9	.ge,	Te	Memory usage in KB User name in Edomain∖Juser format		
SERVIC		eq, ne				Service name		
WINDO MODULI	ATITLE ES	eq, no eq, no				Window title DLL name		
NOTE: "WIN a re	NDOWTITLE" mote mach:	and "S ine.	TATUS" f:	ilter	s are	not supported when querying		
Examples: TASKLI TASKLI TASKLI TASKLI TASKLI	IST IST /M IST /U /FO IST /SUC /1	CSU FO LISI						

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, <u>www.win2000mag.com</u>
- <u>www.sysinternals.com</u>

...

Mitre >

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