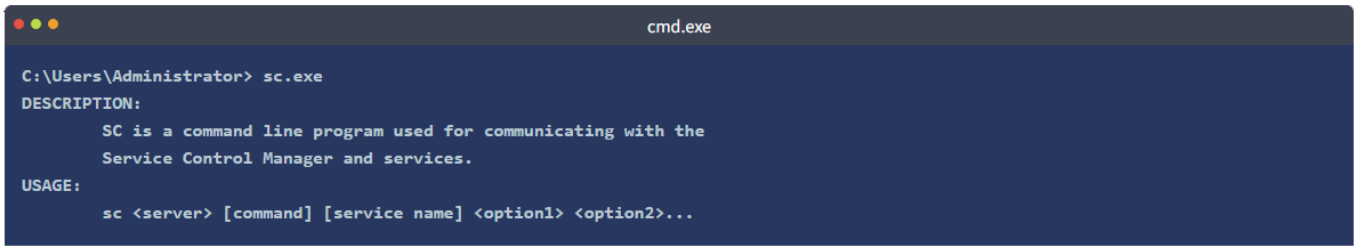
5 - wininit.exe > services.exe

Task 7 ○ wininit.exe > services.exe

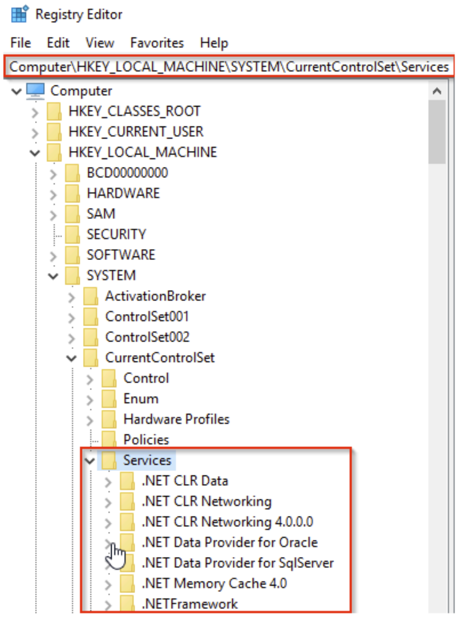
The next process is the **Service Control Manager** (SCM) or **services.exe**. Its primary responsibility is to handle system services: loading services, interacting with services and starting or ending services. It maintains a database that can be queried using a Windows built-in utility, `sc.exe`.



cmd.exe

```
C:\Users\Administrator> sc.exe
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>...
```

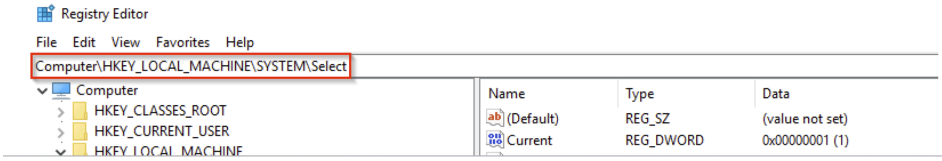
Information regarding services is stored in the registry, `HKLM\System\CurrentControlSet\Services`.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

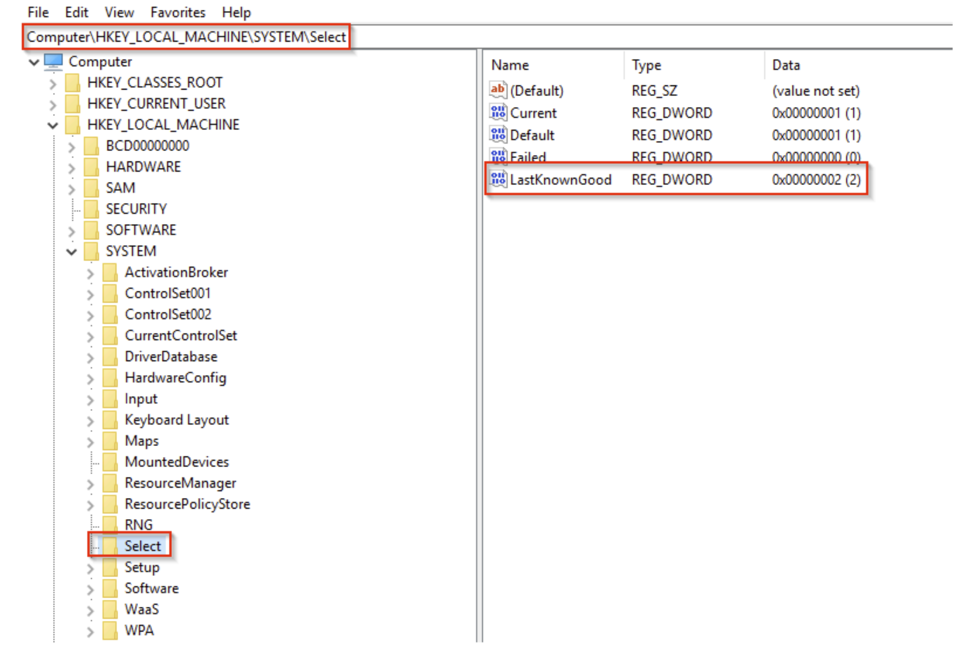
This process also loads device drivers marked as auto-start into memory.

When a user logs into a machine successfully, this process is responsible for setting the value of the Last Known Good control set (Last Known Good Configuration), `HKLM\System\Select\LastKnownGood`, to that of the CurrentControlSet.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)



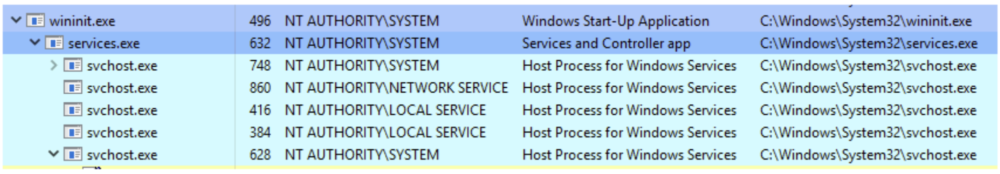
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Select

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - BCD00000000
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
    - SYSTEM
      - ActivationBroker
      - ControlSet001
      - ControlSet002
      - CurrentControlSet
      - DriverDatabase
      - HardwareConfig
      - Input
      - Keyboard Layout
      - Maps
      - MountedDevices
      - ResourceManager
      - ResourcePolicyStore
      - RNG
      - Select
      - Setup
      - Software
      - WaaS
      - WPA

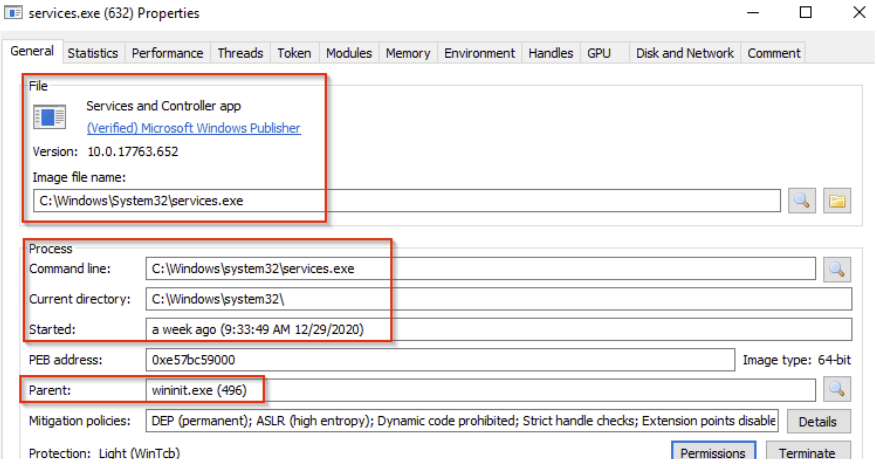
Name	Type	Data
(Default)	REG_SZ	(value not set)
Current	REG_DWORD	0x00000001 (1)
Default	REG_DWORD	0x00000001 (1)
Failed	REG_DWORD	0x00000000 (0)
LastKnownGood	REG_DWORD	0x00000002 (2)

This process is the parent to several other key processes: svchost.exe, spoolsv.exe, msmpeng.exe, and dllhost.exe, to name a few. You can read more about this process here.



wininit.exe	496	NT AUTHORITY\SYSTEM	Windows Start-Up Application	C:\Windows\System32\wininit.exe
services.exe	632	NT AUTHORITY\SYSTEM	Services and Controller app	C:\Windows\System32\services.exe
svchost.exe	748	NT AUTHORITY\SYSTEM	Host Process for Windows Services	C:\Windows\System32\svchost.exe
svchost.exe	860	NT AUTHORITY\NETWORK SERVICE	Host Process for Windows Services	C:\Windows\System32\svchost.exe
svchost.exe	416	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Services	C:\Windows\System32\svchost.exe
svchost.exe	384	NT AUTHORITY\LOCAL SERVICE	Host Process for Windows Services	C:\Windows\System32\svchost.exe
svchost.exe	628	NT AUTHORITY\SYSTEM	Host Process for Windows Services	C:\Windows\System32\svchost.exe

What is normal?



services.exe (632) Properties

File

Services and Controller app

(Verified) Microsoft Windows Publisher

Version: 10.0.17763.652

Image file name: C:\Windows\System32\services.exe

Process

Command line: C:\Windows\system32\services.exe

Current directory: C:\Windows\system32\

Started: a week ago (9:33:49 AM 12/29/2020)

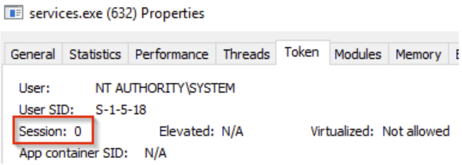
PEB address: 0xe57bc59000 Image type: 64-bit

Parent: wininit.exe (496)

Mitigation policies: DEP (permanent); ASLR (high entropy); Dynamic code prohibited; Strict handle checks; Extension points disable

Protection: Light (WinTcb)

Protection: Light (WinTcb)



services.exe (632) Properties

User: NT AUTHORITY\SYSTEM

User SID: S-1-5-18

Session: 0 Elevated: N/A Virtualized: Not allowed

App container SID: N/A

Image Path: %SystemRoot%\System32\services.exe
Parent Process: wininit.exe
Number of Instances: One
User Account: Local System
Start Time: Within seconds of boot time

What is unusual?

- A parent process other than wininit.exe
- Image file path other than C:\Windows\System32
- Subtle misspellings to hide rogue processes in plain sight
- Multiple running instances
- Not running as SYSTEM