Demystifying the “SVCHOST.EXE” Process and Its Command Line Options

nasbench.medium.com/demystifying-the-svchost-exe-process-and-its-command-line-options-508e9114e747

September 26, 2020

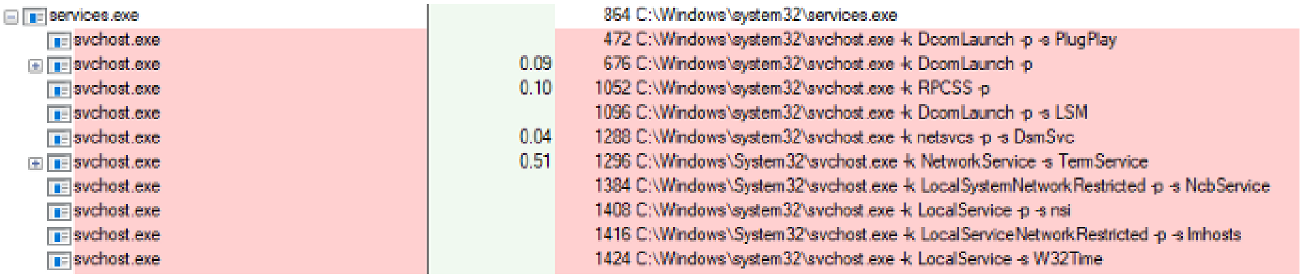
Nasreddine Bencherchali

Sep 26, 2020

·

5 min read

·



```
services.exe                                  864 C:\Windows\system32\services.exe
  svchost.exe                                 472 C:\Windows\system32\svchost.exe -k DcomLaunch -p -s PlugPlay
  svchost.exe                         0.09    676 C:\Windows\system32\svchost.exe -k DcomLaunch -p
  svchost.exe                         0.10   1052 C:\Windows\system32\svchost.exe -k RPCSS -p
  svchost.exe                                1096 C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
  svchost.exe                         0.04   1288 C:\Windows\system32\svchost.exe -k netsvcs -p -s DsmSvc
  svchost.exe                         0.51   1296 C:\Windows\System32\svchost.exe -k NetworkService -s TermService
  svchost.exe                                1384 C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
  svchost.exe                                1408 C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
  svchost.exe                                1416 C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
  svchost.exe                                1424 C:\Windows\system32\svchost.exe -k LocalService -s W32Time
```

Family Group Photo

The Service Host process or *“svchost.exe”* is one the most notorious processes out there. It got a bad reputation for being “malicious” due to mostly two factors, one is malware impersonating it and the other is good old “Task Manager”.

Because of the way task manager was designed in the old days (and to some extent today), it never gave much details into processes on the system and especially “special” processes like *“svchost.exe”*. So by using the task manager to see what processes are opened, you’ll get a bunch of *“svchost.exe”* processes with the description “Host Process for Windows Services”. Without any information about the services that are hosted in it. So it only took malware two additional steps to make itself look legitimate.

First, name the malware *“svchost.exe”* and second, give it the description *“Host Process for Windows Services”* and you’ll be indistinguishable from the legitimate *“svchost.exe”* process as far as the old task manager is concerned.

You could of course use the *“Tasklist”* command with the *“/SVC”* flag or tools like *“Process Explorer” or* even the new task manager in windows 10 to view the list of services hosted inside the *“svchost.exe”* process . But this is not the purpose of this blog post.

Instead, let's take a deeper look and try to answer how services get launched, what is the relationship between *"services.exe"* and *"svchost.exe"*, what type of services are hosted inside an *"svchost.exe"* process and what is the meaning behind the flags in an *"svchost.exe"* command line.

The Service Control Manager (SERVICES.EXE)

The service control manager or SCM for short is a system process that runs the image *"services.exe"* from the *"System32"* folder on disk. In short it is the one process responsible for running and managing services on the system.

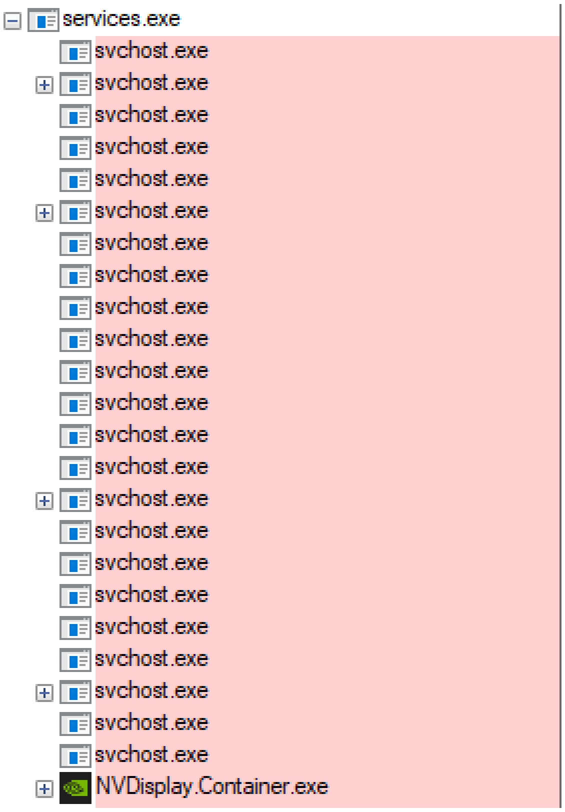
It keeps track of all the services that are installed via a key in the registry called the SCM database, which is located in the following path.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

When the SCM starts at system boot, it launches all the services that are marked with *"auto-start"* and all other dependencies needed to run the services.

All those services and others will be spawned as children of the *"services.exe"* process and when looking at the *"services.exe"* process we'll see two kinds of processes.

Processes that are hosting their own services and multiple "svchost.exe" instances.



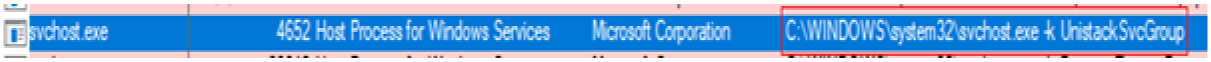
```
⊟ services.exe
    svchost.exe
  ⊞ svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
  ⊞ svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
  ⊞ svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
    svchost.exe
  ⊞ svchost.exe
    svchost.exe
    svchost.exe
  ⊞ NVDisplay.Container.exe
```

The Service Host (SVCHOST.EXE)

From the Microsoft documentation, here a small description of the “*svchost.exe*” process.

> The Service Host (svchost.exe) is a shared-service process that serves as a shell for loading services from DLL files — Microsoft Docs

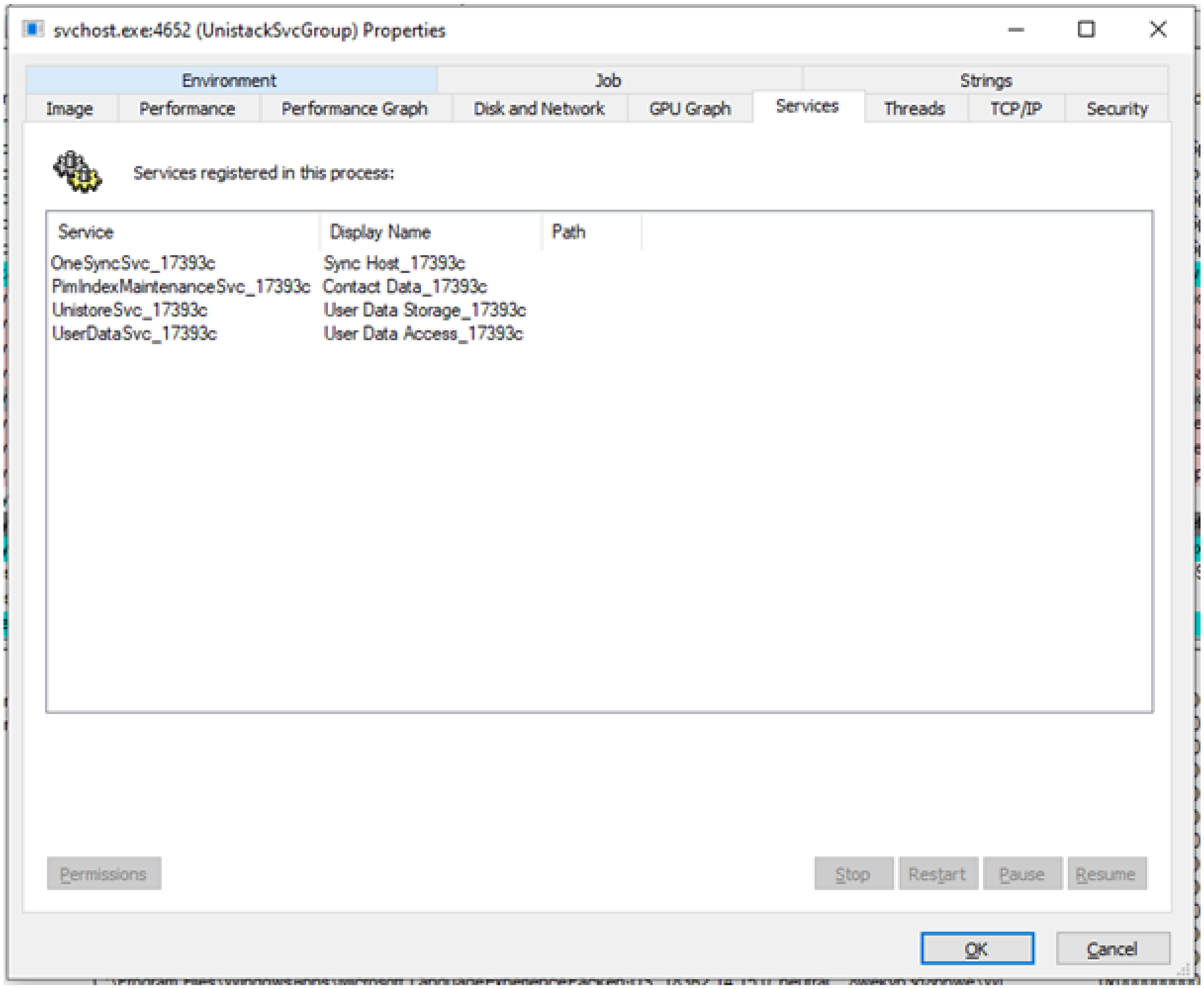
If we take a look at a running *“svchost.exe”* instance and check its command line, we’ll see something similar to the following:



```
svchost.exe    4652 Host Process for Windows Services    Microsoft Corporation    C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
```

As previously discussed the command line doesn't give much insight on what service is hosted inside this process.

Inspecting the process with a tool like process explorer reveals that this instance is actually hosting four services.



svchost.exe:4652 (UnistackSvcGroup) Properties

Services registered in this process:

Service	Display Name	Path
OneSyncSvc_17393c	Sync Host_17393c	
PimIndexMaintenanceSvc_17393c	Contact Data_17393c	
UnistoreSvc_17393c	User Data Storage_17393c	
UserDataSvc_17393c	User Data Access_17393c	

So the question to answer is how does this simple command line arguments reference multiple services. To explain this let us take a look at the arguments and what they mean.

The “K” Flag

When *“svchost.exe”* uses the *“-k”* flag, a request will be made to the following registry key.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

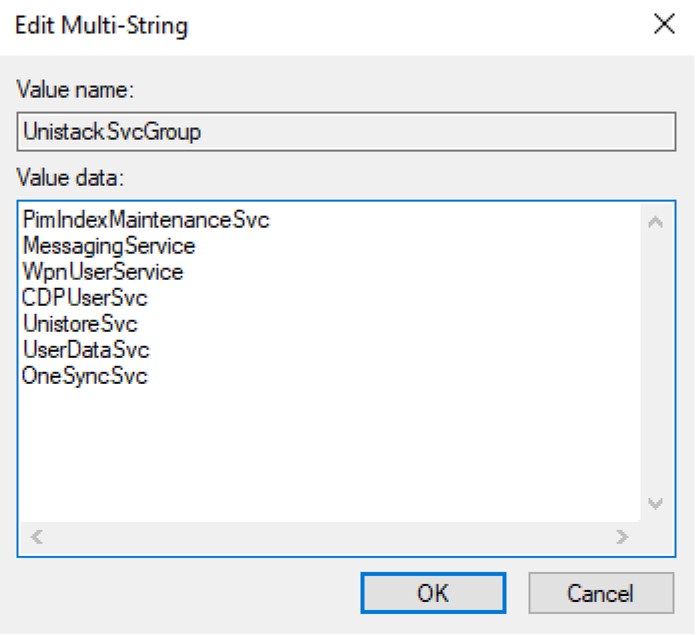
Where it will try to locate the value corresponding to the one sent via the *“-k”* flag.

This registry key defines values for Service Host Groups. Each value will contain a string that contains references to the services to launch once the *“-k”* flag is used.

In our example when the *“svchost.exe”* process used the **“***-k UnistackSvcGroup”*, it’ll look inside the registry and find the corresponding value (on my machine).

Once its reads these values and no other flag was specified, it will go and load each service referenced inside form its corresponding registry key

And that’s how you get multiple services on a single *“svchost.exe”* process.



Edit Multi-String

Value name:

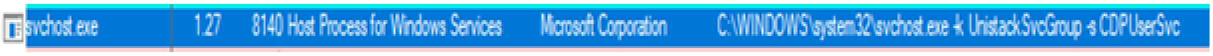
UnistackSvcGroup

Value data:

```
PimIndexMaintenanceSvc
MessagingService
WpnUserService
CDPUserSvc
UnistoreSvc
UserDataSvc
OneSyncSvc
```

The “S” Flag

The “svchost.exe” process in addition of being launched with the –“k” flag, can sometimes uses the “-s” flag, like the example below.



```
svchost.exe    1.27    8140 Host Process for Windows Services    Microsoft Corporation    C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
```

When the “-s” flag is used, this will tell the *“svchost.exe”* process to load only the service specified by the flag from the selected group.

In our example its only requesting the *“CDPUserSvc”* service inside the *“UnistackSvcGroup”* registry key and loading that.

The “P” Flag

For me, the “-p” flag was one of those mysterious flags in the service host process. Fortunately, I’ve recently read a blog post by which shed some light on this. I’ll share with you the TL;DR.

> **The “P” flag enforces different policies: DynamicCodePolicy, BinarySignaturePolicy and ExtensionPolicy**

I highly suggest you go read the full blog post to get a better understanding on how he reached this conclusion.

Exploration of svchost.exe /P flag

Hey there! In this blog post, we are gonna take a look at the mysterious "/P" flag of svchost.exe. TL;DR: P flag…

pusha.be

Conclusion

With this we conclude this small tour of the service host process, i hope you learnt something along the way.

If you liked this and want to know more about Windows and its internals than there is no better resource than the book : **“Windows Internals, Part 1: System architecture, processes, threads, memory management, and more, 7th Edition”.**

Delve inside Windows architecture and internals - and see how core components work behind the scenes. This classic…