**BAT批处理文件 sfc,takeown,icacls命令介绍**

**sfc/?(2019.5.5)**

Microsoft ® Windows ® Resource Checker 6.0 版  
版权所有 © Microsoft Corporation。保留所有权利。

扫描所有保护的系统文件的完整性，并使用正确的 Microsoft 版本替换不正确的版本。

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]  
[/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory> [/OFFLOGFILE=<log file path>]]

| **参数** | **作用** |
| --- | --- |
| /SCANNOW | 扫描所有保护的系统文件的完整性，并尽可能修复有问题的文件。 |
| /VERIFYONLY | 扫描所有保护的系统文件的完整性。不会执行修复操作。 |
| /SCANFILE | 扫描引用的文件的完整性，如果找到问题，则修复文件。 指定完整路径 <file> |
| /VERIFYFILE | 验证带有完整路径<file> 的文件的完整性。不会执行修复操作。 |
| /OFFBOOTDIR | 对于脱机修复，指定脱机启动目录的位置 |
| /OFFWINDIR | 对于脱机修复，指定脱机 Windows 目录的位置 |
| /OFFLOGFILE | 对于脱机修复，通过指定日志文件路径选择性地启用记录 |

示例:

sfc /SCANNOW

sfc /VERIFYFILE=c:\windows\system32\kernel32.dll

sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows

sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt

sfc /VERIFYONLY

**扫描并修复Windows10系统文件**

当 Windows 10 还可正常启动运行时，如下命令将对计算机上受保护的系统文件进行扫描并尽可能修复有问题的文件：

1 点击 Windows + X 快捷键 – 选择「命令提示符（管理员）」

2 在 CDM 窗口中执行如下命令：

sfc /scannow

* 1

3 一旦扫描完成后，如果没问题，命令行会有提示。如果有问题，会进行提示并输出日志路径。

**查看SFC扫描结果详细信息**

SFC 扫描结果会存储在 CBS.Log 日志文件当中，大家可用如下步骤进行查看：

1 点击 Windows + X 快捷键 – 选择「命令提示符（管理员）」

2 为保证不破坏原有日志文件，在 CDM 窗口中执行如下命令：

findstr /c:"[SR]" %windir%\Logs\CBS\CBS.log > "C:\sfclogs.txt"

* 1

3 此时便可以在 C 盘根目录下找到转出来的 sfclogs.txt 日志文件。

CBS.log

注意：CBS.Log 日志只适用于能正常登录的 Windows 10，脱机命令行不支持该日志。

**如何脱机扫描并修复Windows 10**

在 Windows 10 运行过程中，有很多受保护的系统文件会被加载到内存中，此时就无法直接进行修复替换，此时就需要进行 SFC 脱机修复。

1 与进入 Windows 10 安全模式的步骤类似，先在设置 – 更新和安全 – 恢复里面的高级启动中点击立即重启

2 系统重启之后点击疑难解答 – 高级选项 – 命令提示符

3 使用你的用户名和密码进行登录

4 在 Windows 环境外执行 SCF 修复时，必需要告诉它哪个是 Windows 安装盘和系统保留分区，在命令行中执行如下命令可以查看 Windows 系统分区的盘符：

wmic logicaldisk get deviceid, volumename, description

* 1

从上图中我们可以看到 C 盘成了保留分区、E 盘是光驱，所以 Windows 分区就是 D 盘了。

5 此时我们可以执行如下命令开始修复：

sfc /scannow /offbootdir=C:\ /offwindir=D:\Windows

* 1

/offboodir 参数用于指定系统保存分区，/offwindir 参数用于指定 Windows 系统所在分区。修复完成后进行系统重启即可，大家注意根据自己的实际情况来执行命令，不要直接照搬。

**使用SFC手动修复Windows 10指定文件**

默认情况下执行 SFC 命令会自动尝试对所有有问题的文件进行修复，当一个或多个文件无法自动修复时，通常都需要用户对其进行手动修复操作。与其说手动修复，其实就是在一台正常的 Windows 10 中把完好无损的文件拿过来替换掉已损坏的文件就 OK 了。

具体有哪些文件修复失败，可以在前面介绍过的 sfclogs.txt 日志文件中找到，下面我们只讲具体的操作方法。

1 点击 Windows + X 快捷键 – 选择「命令提示符（管理员）

2 在 CDM 窗口中执行如下命令：

takeown /f C:\要修复的文件路径

* 1

takeown/?(2019.05.05)

TAKEOWN [/S system [/U username [/P [password]]]]  
/F filename [/A] [/R [/D prompt]]

描述:  
该工具以重新分配文件所有权的方式允许管理员重新获取先前被拒绝访问  
的文件访问权。

参数列表:  
/S system 指定要连接到的远程系统。

/U [domain\]user 指定用户上下文，命令在此上下文中执行。

/P [password] 指定给定用户上下文的密码。如果省略，

提示输入。

/F filename 指定文件名或目录名模式。可以用通配符 "\*"

指定模式。允许共享名\文件名。

/A 将所有权给于管理员组，而不是当前用户。

/R 递归: 指示工具运行于指定的目录和子目录

里的文件上。

/D prompt 当前用户在一个目录里没有“列出文件夹”

权限时，使用默认答案。当在子目录里进行

递归 (/R) 操作时会发生这种情况。用有效

值 "Y" 获取所有权或用 "N" 跳过。

/SKIPSL 不遵循符号链接。

仅适用于 /R。

/? 显示此帮助消息。

注意: 1) 如果未指定 /A，文件所有权会将被授予

当前登录的用户。

2) 不支持用 "?" 和 "\*" 的混合模式。

3) /D 用于抑制确认提示。

示例:

TAKEOWN /?

TAKEOWN /F lostfile

TAKEOWN /F \\system\share\lostfile /A

TAKEOWN /F directory /R /D N

TAKEOWN /F directory /R /A

TAKEOWN /F \*

TAKEOWN /F C:\Windows\System32\acme.exe

TAKEOWN /F %windir%\\*.txt

TAKEOWN /S system /F MyShare\Acme\*.doc

TAKEOWN /S system /U user /F MyShare\MyBinary.dll

TAKEOWN /S system /U domain\user /P password /F share\filename

TAKEOWN /S system /U user /P password /F Doc\Report.doc /A

TAKEOWN /S system /U user /P password /F Myshare\\*

TAKEOWN /S system /U user /P password /F Home\Logon /R

TAKEOWN /S system /U user /P password /F Myshare\directory /R /A

takeown 这个命令就是更改文件「所有者」的命令，这让我想起了 N 多年前讲师不断重复的 take ownership。

3 在拿到文件所有权后，还需要使用如下命令获取文件的完全控制权限：

icacls C:\要修复的文件路径 /Grant Administrators:F

* 1

icacls(2019.05.05)

ICACLS name /save aclfile [/T] [/C] [/L] [/Q]  
将匹配名称的文件和文件夹的 DACL 存储到 aclfile 中  
以便将来与 /restore 一起使用。请注意，未保存 SACL、  
所有者或完整性标签。

ICACLS directory [/substitute SidOld SidNew […]] /restore aclfile  
[/C] [/L] [/Q]  
将存储的 DACL 应用于目录中的文件。

ICACLS name /setowner user [/T] [/C] [/L] [/Q]  
更改所有匹配名称的所有者。该选项不会强制更改所有  
身份；使用 takeown.exe 实用程序可实现  
该目的。

ICACLS name /findsid Sid [/T] [/C] [/L] [/Q]  
查找包含显式提及 SID 的 ACL 的  
所有匹配名称。

ICACLS name /verify [/T] [/C] [/L] [/Q]  
查找其 ACL 不规范或长度与 ACE  
计数不一致的所有文件。

ICACLS name /reset [/T] [/C] [/L] [/Q]  
为所有匹配文件使用默认继承的 ACL 替换 ACL。

ICACLS name [/grant[:r] Sid:perm[…]]  
[/deny Sid:perm […]]  
[/remove[:g|:d]] Sid[…]] [/T] [/C] [/L] [/Q]  
[/setintegritylevel Level:policy[…]]

/grant[:r] Sid:perm 授予指定的用户访问权限。如果使用 :r，

这些权限将替换以前授予的所有显式权限。

如果不使用 :r，这些权限将添加到以前授予的

所有显式权限。

/deny Sid:perm 显式拒绝指定的用户访问权限。

将为列出的权限添加显式拒绝 ACE，

并删除所有显式授予的权限中的相同权限。

/remove[:[g|d]] Sid 删除 ACL 中所有出现的 SID。使用

:g，将删除授予该 SID 的所有权限。使用

:d，将删除拒绝该 SID 的所有权限。

/setintegritylevel [(CI)(OI)]级别将完整性 ACE 显式

添加到所有匹配文件。要指定的级别为以下级别

之一:

L[ow]

M[edium]

H[igh]

完整性 ACE 的继承选项可以优先于级别，但只应用于

目录。

/inheritance:e|d|r

e - 启用继承

d - 禁用继承并复制 ACE

r - 删除所有继承的 ACE

https://csdnimg.cn/release/blogv2/dist/pc/img/newCodeMoreWhite.png

注意:  
Sid 可以采用数字格式或友好的名称格式。如果给定数字格式，  
那么请在 SID 的开头添加一个 \*。

/T 指示在以该名称指定的目录下的所有匹配文件/目录上

执行此操作。

/C 指示此操作将在所有文件错误上继续进行。

仍将显示错误消息。

/L 指示此操作在符号

链接本身而不是其目标上执行。

/Q 指示 icacls 应该禁止显示成功消息。

ICACLS 保留 ACE 项的规范顺序:

显式拒绝

显式授予

继承的拒绝

继承的授予

perm 是权限掩码，可以指定两种格式之一:

简单权限序列:

N - 无访问权限

F - 完全访问权限

M - 修改权限

RX - 读取和执行权限

R - 只读权限

W - 只写权限

D - 删除权限

在括号中以逗号分隔的特定权限列表:

DE - 删除

RC - 读取控制

WDAC - 写入 DAC

WO - 写入所有者

S - 同步

AS - 访问系统安全性

MA - 允许的最大值

GR - 一般性读取

GW - 一般性写入

GE - 一般性执行

GA - 全为一般性

RD - 读取数据/列出目录

WD - 写入数据/添加文件

AD - 附加数据/添加子目录

REA - 读取扩展属性

WEA - 写入扩展属性

X - 执行/遍历

DC - 删除子项

RA - 读取属性

WA - 写入属性

继承权限可以优先于每种格式，但只应用于

目录:

(OI) - 对象继承

(CI) - 容器继承

(IO) - 仅继承

(NP) - 不传播继承

(I) - 从父容器继承的权限

示例:

icacls c:\windows\\* /save AclFile /T

- 将 c:\windows 及其子目录下所有文件的

ACL 保存到 AclFile。

icacls c:\windows\ /restore AclFile

- 将还原 c:\windows 及其子目录下存在的 AclFile 内

所有文件的 ACL。

icacls file /grant Administrator:(D,WDAC)

- 将授予用户对文件删除和写入 DAC 的管理员

权限。

icacls file /grant \*S-1-1-0:(D,WDAC)

- 将授予由 sid S-1-1-0 定义的用户对文件删除和

写入 DAC 的权限。

4 然后再用一个完好无损的文件去替换掉损坏的文件即可，大家可以手动替换或用命令行：

copy C:\完好无损的文件 C:\要修复的文件路径

* 1

在文件替换完成后，你可以执行 SFC /verifyonly 来验证文件系统的完整性，查看问题是否已经得到修复。如果你只修复了个别文件，可以使用 sfc /VERIFYFILE=C:\文件路径 来进行查看，以避免长时间的完整扫描。

部分内容转自：<https://www.sysgeek.cn/sfc-fix-system-files-windows-10/>

[winsxs清理小工具BAT文件](https://download.csdn.net/download/luoxin859/5404889" \t "_blank)

05-18

[winsxs目录下的文件都是系统要用的各种库文件，system32下存放了这些dll的最新的版本，所有老版本的dll都放在winsxs下。所以只要你安装程序或者更新补丁，system32下的文件就会被更新，而同时winsxs就会增加一些旧文件，所以我们的C盘空间就在持续不断地减少，直到磁盘容量不够，被迫重装系统为止，如果你足够幸运，可以直接安装最新的SP的话，或许可以为winsxs节约一点微薄的空间。 winsxs目录下的不同版本文件都存放在特定命名规则的目录下，比如 C:\Windows\winsxs>dir msil\_microsoft.transactions.bridge.resources\* 驱动器 C 中的卷是 vista 卷的序列号是 989F-EFF3 C:\Windows\winsxs 的目录 msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6000.16386\_zh-cn\_1cde5a17d78fb5ec msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6000.16716\_zh-cn\_1cd75781d79605cf msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6000.20876\_zh-cn\_060fb27df137fddf msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6001.18000\_zh-cn\_1cb2dbd3d7e75eb8 msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6001.18106\_zh-cn\_1cb252ffd7e7f8cf msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6001.22221\_zh-cn\_05e71ebbf18d0b5e msil\_microsoft.transactions.bridge.resources\_b03f5f7f11d50a3a\_6.0.6002.18005\_zh-cn\_1c8e610fd838f2cc 0 个文件 0 字节 7 个目录 5,382,139,904 可用字节 这里的各个部分用下划线分割，其中我们关注的是“6.0.6000.16386”部分，它表示旧文件的版本号，之前则是唯一文件标识，之后是语言，最后部分是散列值（防止名字冲突）。 本工具的设计思想就是删除所有的旧文件。所有满足如下全部条件的目录都会被移动到C:\Windows\winsxs\_del目录中。 1.存在比自身更新的版本 2.本身不是最新版本 运行工具前的C盘剩余空间： 所列文件总数: 4473 个文件 3,336,376,627 字节 7655 个目录 326,840,320 可用字节 C:\Windows\winsxs\_del> 运行工具并且执行命令 for /d %v in (%SystemRoot%\winsxs\_del\\*.\*) do rd /s /q %v 删除所有可以删除的无用文件之后的剩余空间： 所列文件总数: 52 个文件 7,555,048 字节 131 个目录 5,383,979,008 可用字节 C:\Windows\winsxs\_del> 工具源代码如下：请保存为winsxs\_clear.bat即可。所有不再需要的文件会移动到c:\windows\winsxs\_del目录中，可以直接进行删除。 执行时候，务必请使用“管理员”权限。 1@echo off 2rem 获取windows版本 3set move\_dir=%SystemRoot%\winsxs\_del 4if not exist %move\_dir%\nul md %move\_dir% 5set winver=none 6FOR /F "eol=; tokens=4\* delims=] " %%i in ('ver') do set winver=%%i 7if "%winver%" == "none" got](https://download.csdn.net/download/luoxin859/5404889" \t "_blank)

[管理员取得所有权注册表文件](https://download.csdn.net/download/qq_25694027/8407791" \t "_blank)

01-29

[Windows Registry Editor Version 5.00 　　[HKEY\_CLASSES\_ROOT\\*\shell\runas] 　　@="管理员取得所有权" 　　"NoWorkingDirectory"="" 　　[HKEY\_CLASSES\_ROOT\\*\shell\runas\command] 　　@="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant administrators:F" 　　"IsolatedCommand"="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant administrators:F" 　　[HKEY\_CLASSES\_ROOT\exefile\shell\runas2] 　　@="管理员取得所有权" 　　"NoWorkingDirectory"="" 　　[HKEY\_CLASSES\_ROOT\exefile\shell\runas2\command] 　　@="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant administrators:F" 　　"IsolatedCommand"="cmd.exe /c takeown /f \"%1\" && icacls \"%1\" /grant administrators:F" 　　[HKEY\_CLASSES\_ROOT\Directory\shell\runas] 　　@="管理员取得所有权" 　　"NoWorkingDirectory"="" 　　[HKEY\_CLASSES\_ROOT\Directory\shell\runas\command] 　　@="cmd.exe /c takeown /f \"%1\" /r /d y && icacls \"%1\" /grant administrators:F /t" 　　"IsolatedCommand"="cmd.exe /c takeown /f \"%1\" /r /d y && icacls \"%1\" /grant administrators:F /t"](https://download.csdn.net/download/qq_25694027/8407791" \t "_blank)

[Takeown、Cacls、Icacls-文件、文件夹夺权用法\_takeown /f\_jie-l...](https://blog.csdn.net/coffee66666/article/details/107515300" \t "_blank)

[Takeown 获取文件or文件夹所有权](https://download.csdn.net/download/weixin_38551837/12876075" \t "_blank)

09-21

[Takeown工具以重新分配文件所有权的方式允许管理员重新获取先前被拒绝访问的文件访问权,需要的朋友可以参考下](https://download.csdn.net/download/weixin_38551837/12876075" \t "_blank)

[Takeown-夺取文件or文件夹所有权.docx](https://download.csdn.net/download/Lidx0710/25062378" \t "_blank)

[Windows下使用命令修改文件权限和所有者\_windows修改文件权限命令\_skyyx...](https://blog.csdn.net/s806903/article/details/125880272" \t "_blank)

6-20

[修改所有者,包括子目录中的文件: takeown /f 目录名 /r 修改文件权限 给目标文件或目录增加everyone用户的完全权限: cacls 文件或目录名 /p everyone:f /e 给目标文件和目录增加everyone权限,并清除其它用户的权限设置: ...](https://blog.csdn.net/s806903/article/details/125880272" \t "_blank)

[windows7批量设置文件权限命令参数详解\_man\_ted的博客](https://blog.csdn.net/u011849402/article/details/49445679" \t "_blank)