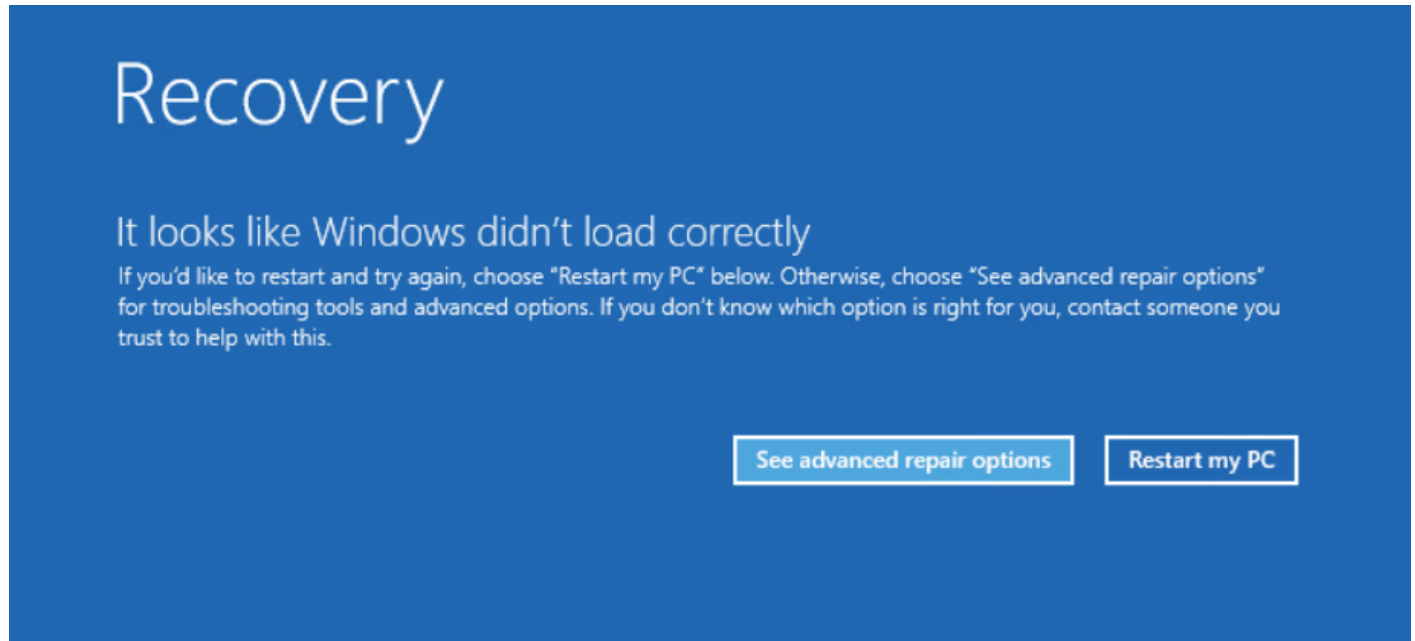


Channel File 291 Bootloop

To reboot a machine into safe mode (workstation or server) follow these steps..

At the recovery screen hit "see advanced.."



Troubleshoot

Choose an option



Continue

Exit and continue to Windows Server



Turn off your PC



Use a device

Use a USB drive, network connection, or Windows recovery DVD



Troubleshoot

Reset your PC or see advanced options

Advanced Options

Startup Settings



Advanced options



System Image Recovery

Recover Windows using a specific system image file



Startup Settings

Change Windows startup behavior



Command Prompt

Use the Command Prompt for advanced troubleshooting



UEFI Firmware Settings

Change settings in your PC's UEFI

Hit reboot

Startup Settings

Restart to change Windows options such as:

- Enable low-resolution video mode
- Enable debugging mode
- Enable boot logging
- Enable Safe Mode
- Disable driver signature enforcement
- Disable early-launch anti-malware protection
- Disable automatic restart on system failure

Restart

Once the server reboots you'll see this recovery option screen. I've been selecting "safe mode with networking" since there's a chance you'll still be able to auth using your normal elevated creds (if not cached).

Advanced Boot Options

Choose Advanced Options for: Windows Server
(Use the arrow keys to highlight your choice.)

Repair Your Computer

Safe Mode

Safe Mode with Networking

Safe Mode with Command Prompt

Enable Boot Logging

Enable low-resolution video

Last Known Good Configuration (advanced)

Debugging Mode

Disable automatic restart on system failure

Disable Driver Signature Enforcement

Disable Early Launch Anti-Malware Driver

Start Windows Normally

Description: Start Windows with core drivers, plus networking support.

ENTER=Choose

ESC=Cancel

Once you've logged into the server you need to open up cmd or powershell.

```
C:\Windows\System32\drivers\CrowdStrike
```

```
dir
```

(to list all files)

```
Select Administrator: Windows PowerShell

-a----      7/3/2024   12:46 AM             27396 C-00000263-00000000-00000030.sys
-a----     11/16/2023   11:17 PM             242516 C-00000264-00000000-00000015.sys
-a----      7/4/2024   12:17 AM          3494924 C-00000265-00000000-00000158.sys
-a----     11/6/2023   11:44 AM              96 C-00000266-00000000-00000002.sys
-a----     5/10/2024   12:07 AM             6068 C-00000268-00000000-00000008.sys
-a----     7/16/2024   12:56 AM           313452 C-00000269-00000000-00000062.sys
-a----     5/28/2024   12:10 AM            20404 C-00000270-00000000-00000012.sys
-a----     7/18/2024   12:56 AM          1734324 C-00000273-00000000-00000277.sys
-a----     7/18/2024   11:56 PM          1744756 C-00000273-00000000-00000278.sys
-a----     7/18/2024   12:56 AM          342460 C-00000274-00000000-00000168.sys
-a----     7/18/2024   12:56 AM           95836 C-00000276-00000000-00000099.sys
-a----     6/14/2024   12:16 AM            5364 C-00000279-00000000-00000009.sys
-a----     7/18/2024   12:56 AM           54164 C-00000281-00000000-00000053.sys
-a----     7/18/2024   12:21 AM          927084 C-00000283-00000000-00000140.sys
-a----      7/4/2024   12:17 AM           18308 C-00000284-00000000-00000028.sys
-a----     11/6/2023   12:28 PM            4628 C-00000285-00000000-00000002.sys
-a----     7/16/2024   12:56 AM          98092 C-00000286-00000000-00000053.sys
-a----      2/1/2024    11:12 PM           2020 C-00000288-00000000-00000002.sys
-a----     7/17/2024   11:51 PM          343284 C-00000289-00000000-00000107.sys
-a----     7/18/2024   11:56 PM           41004 C-00000291-00000000-00000034.sys
-a----     7/18/2024   12:56 AM          25884 C-00000293-00000000-00000029.sys
-a----     11/6/2023   11:46 AM             56 C-00000500-00000000-00000001.sys
-a----     11/6/2023   11:46 AM             56 C-00000502-00000000-00000001.sys
-a----     11/6/2023   11:46 AM             56 C-00000508-00000000-00000001.sys
```

Copy this filename (C-00000291-etc) and then run this:

```
del <filename you copied>
```

Reboot the machine.

Procedures for Machines Requiring Added Storage Drivers

Machines like the ProBook 650 G8 may not have the "Startup Settings" option above. Instead, follow these steps.

- 1. Load the correct driver for the machine to an external drive.
- 2. Use the Command Prompt option in the recovery mode which will open a command prompt into the Windows Recovery Environment, mapped as X:\
- 3. Type DISKPART to enter disk partition mode.

This screenshot is for illustrative purposes only. Your disk and partition numbers will vary.

```

C:\Windows\system32>diskpart 1
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-6PA00DNIJKD

DISKPART> list disk 2

   Disk ###  Status              Size       Free       Dyn  Gpt
   -----  -
   Disk 0    Online              465 GB     7168 KB
   Disk 1    Online              931 GB     6144 KB
   Disk 2    Online              128 GB     1024 KB

DISKPART> select disk 1 3
Disk 1 is now the selected disk.

DISKPART> list partition 4

   Partition ###  Type              Size       Offset
   -----  -
   Partition 1    Primary           337 GB     1024 KB
   Partition 2    Primary           593 GB       337 GB

DISKPART> select partition 1 5
Partition 1 is now the selected partition.

```

4. Type List Disk and identify the disk number, based on its size, that contains the driver
5. Type Select Disk # based on the size and hit enter - the selected disk is now active
6. Type List Partition and identify the primary partition
7. Type Select Partition # and hit enter - the selected partition is now active
8. Type assign letter=[drive letter] where drive letter is any available drive letter (at this point, any except x)
9. Type EXIT to leave disk partitioning mode
10. Change drive letter to the drive letter you just assigned.
11. Change directories to the directory containing the .inf file for the storage driver - in the example included and attached to this document, that is the *:\src\driver\ directory but this may be different for other drivers.
12. Type pnputil -i -a drivename.inf to load the driver into active memory.
13. Repeat steps 3 through 9 above, but this time select the new, larger drive that you should now be able to see. Select its primary partition and mount it to a different drive letter than the one you chose in step 8.
14. Once out of disk partitioning mode again, select your new drive letter.
15. Change directory to *:\Windows\System32\drivers\CrowdStrike
16. Rename any files beginning with "C-00000291" to end with ".old" instead of ".sys" and then restart the system.
17. You're done!

Revision #8

Created 19 July 2024 08:01:50 by Shawn Hoy

Updated 17 September 2024 13:26:07 by Alex Gallegos