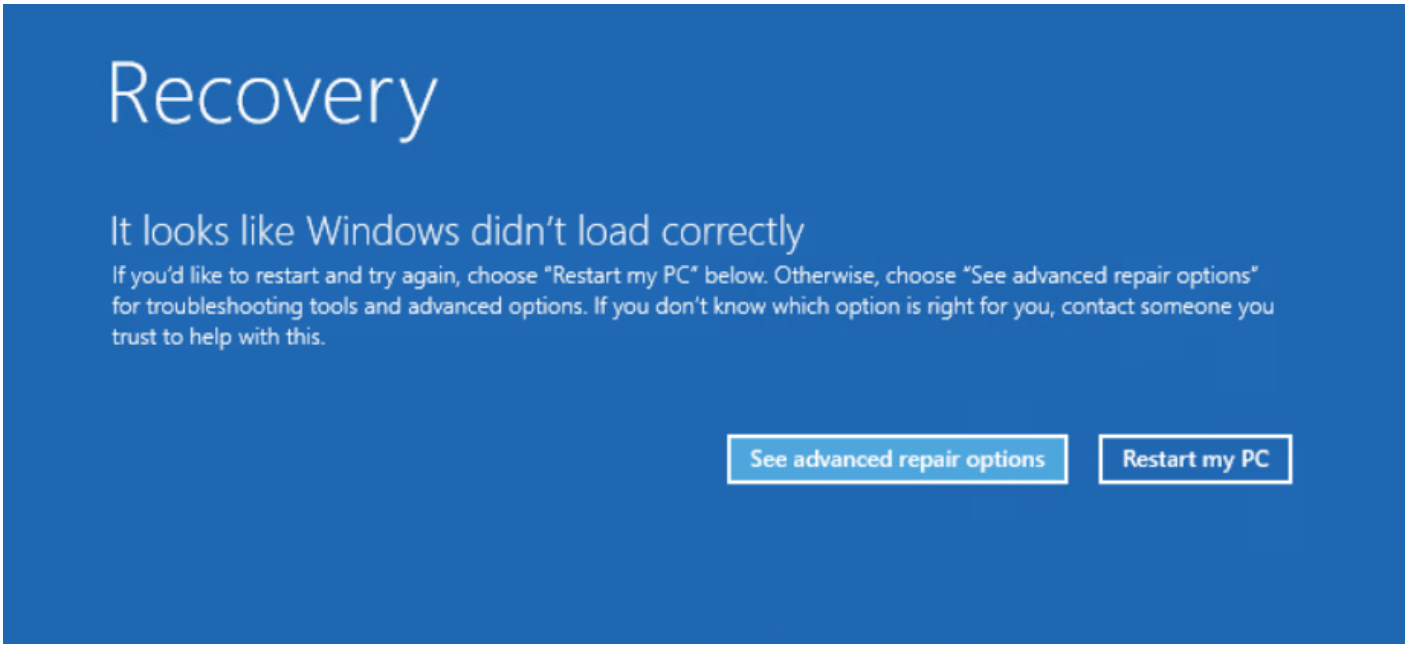
Crowdstrike

- Channel File 291 Bootloop

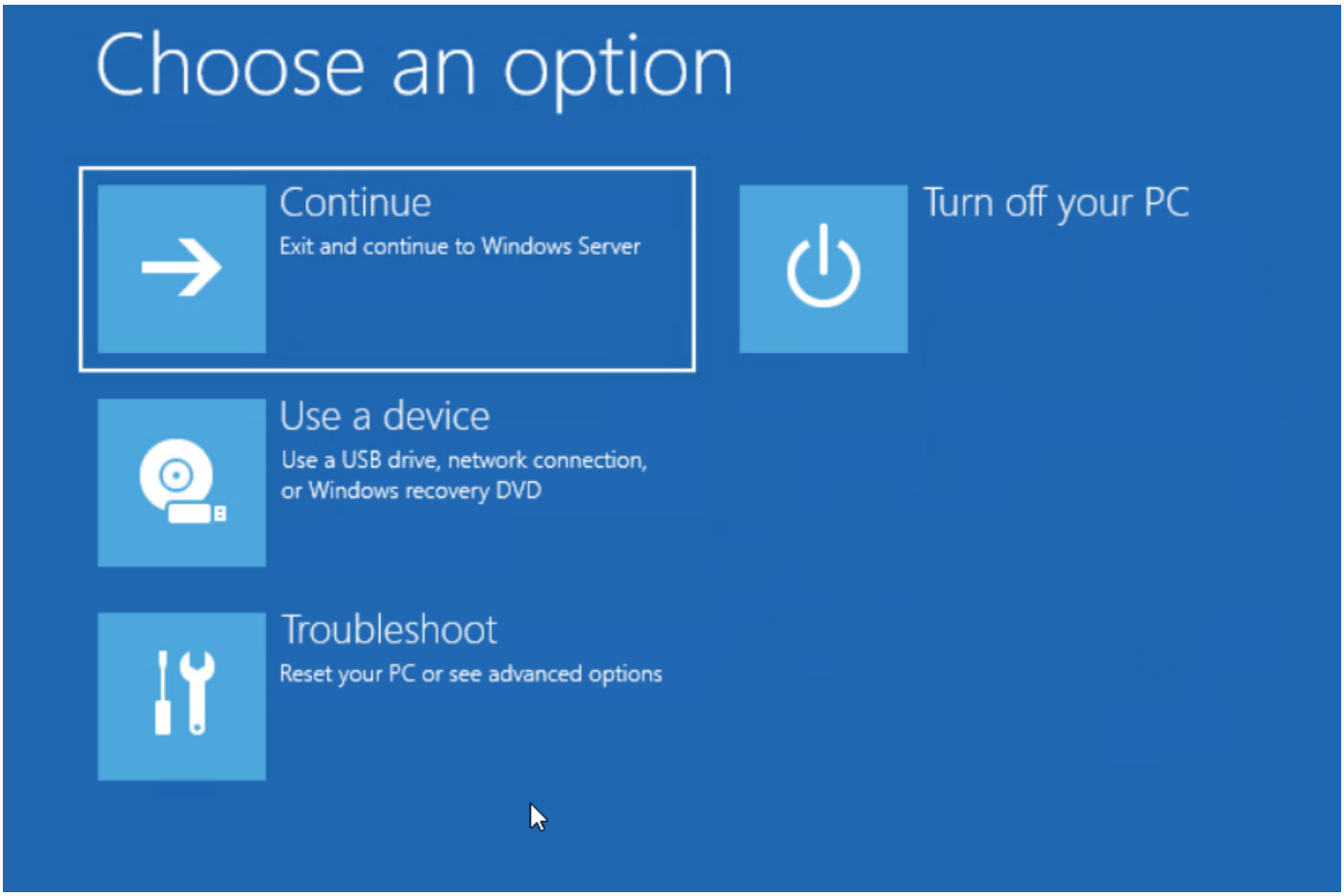
Channel File 291 Bootloop

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

At the recovery screen hit "see advanced.."

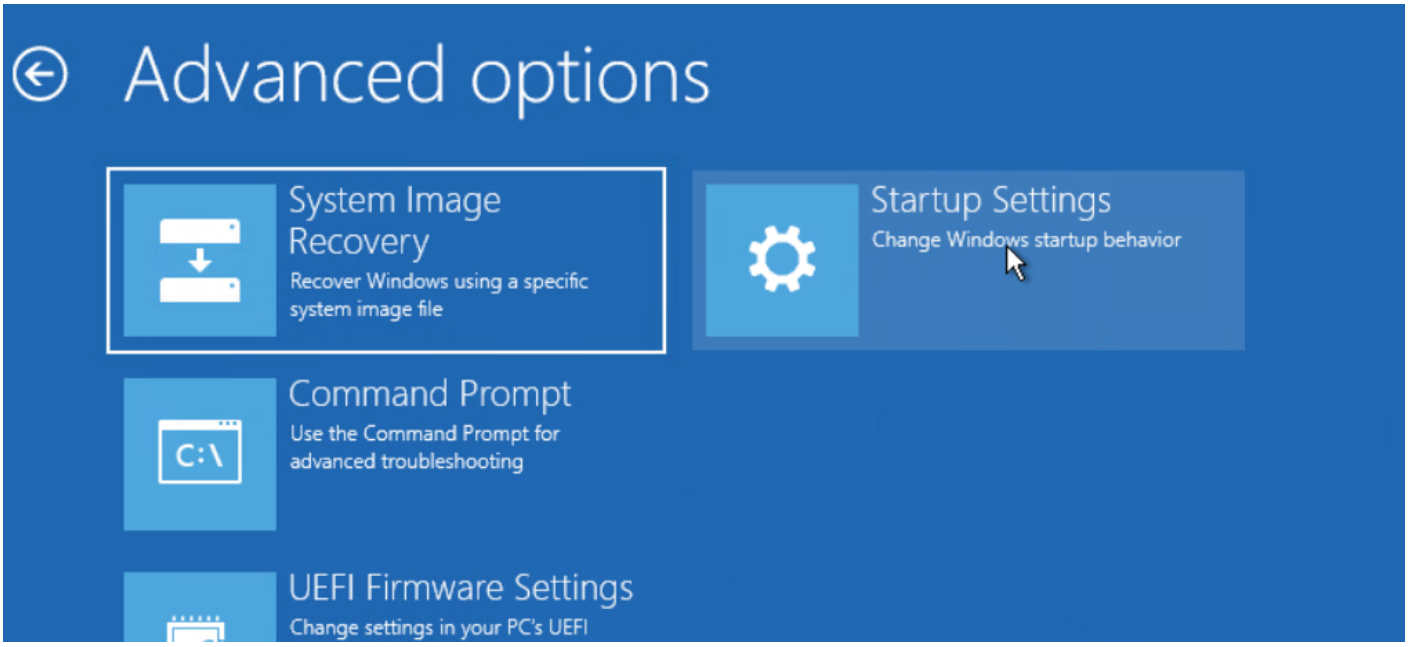


Troubleshoot

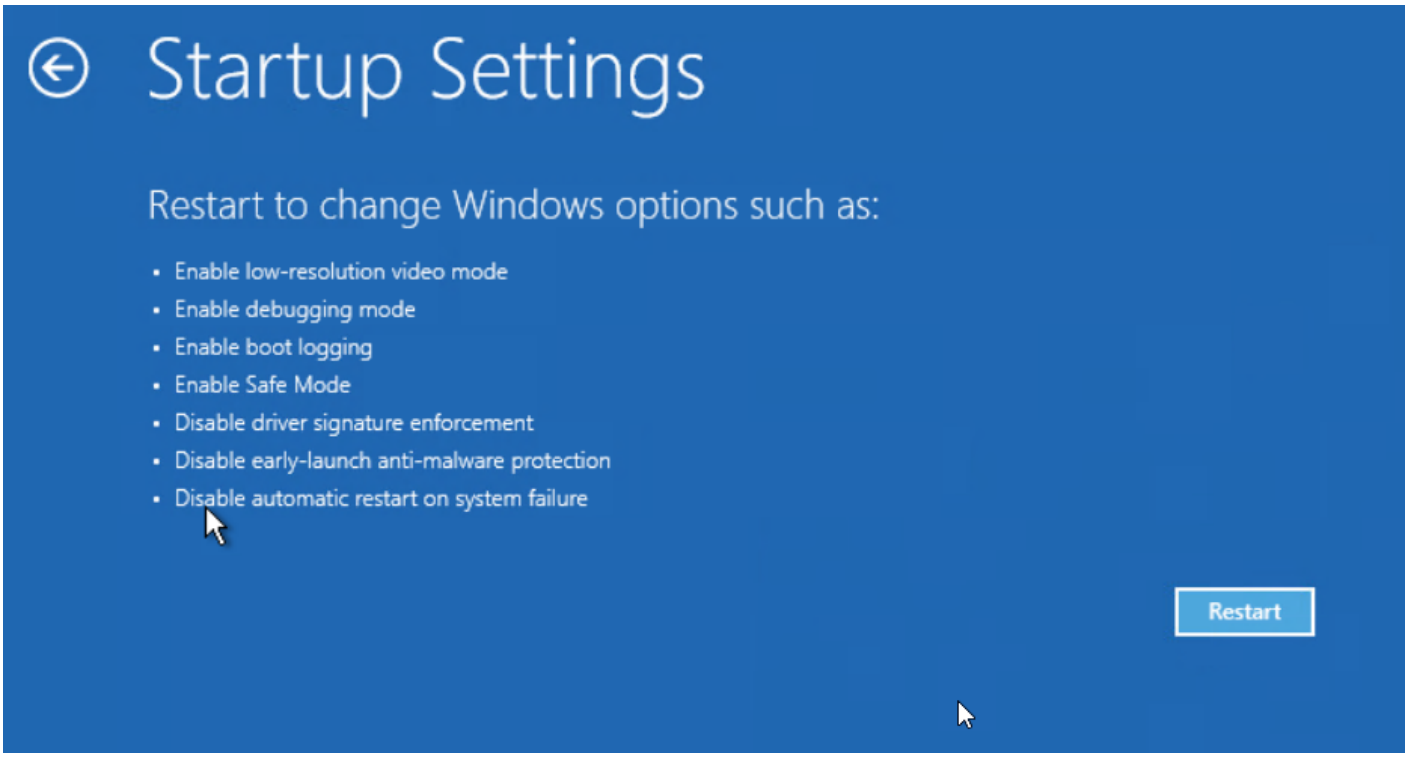


Advanced Options

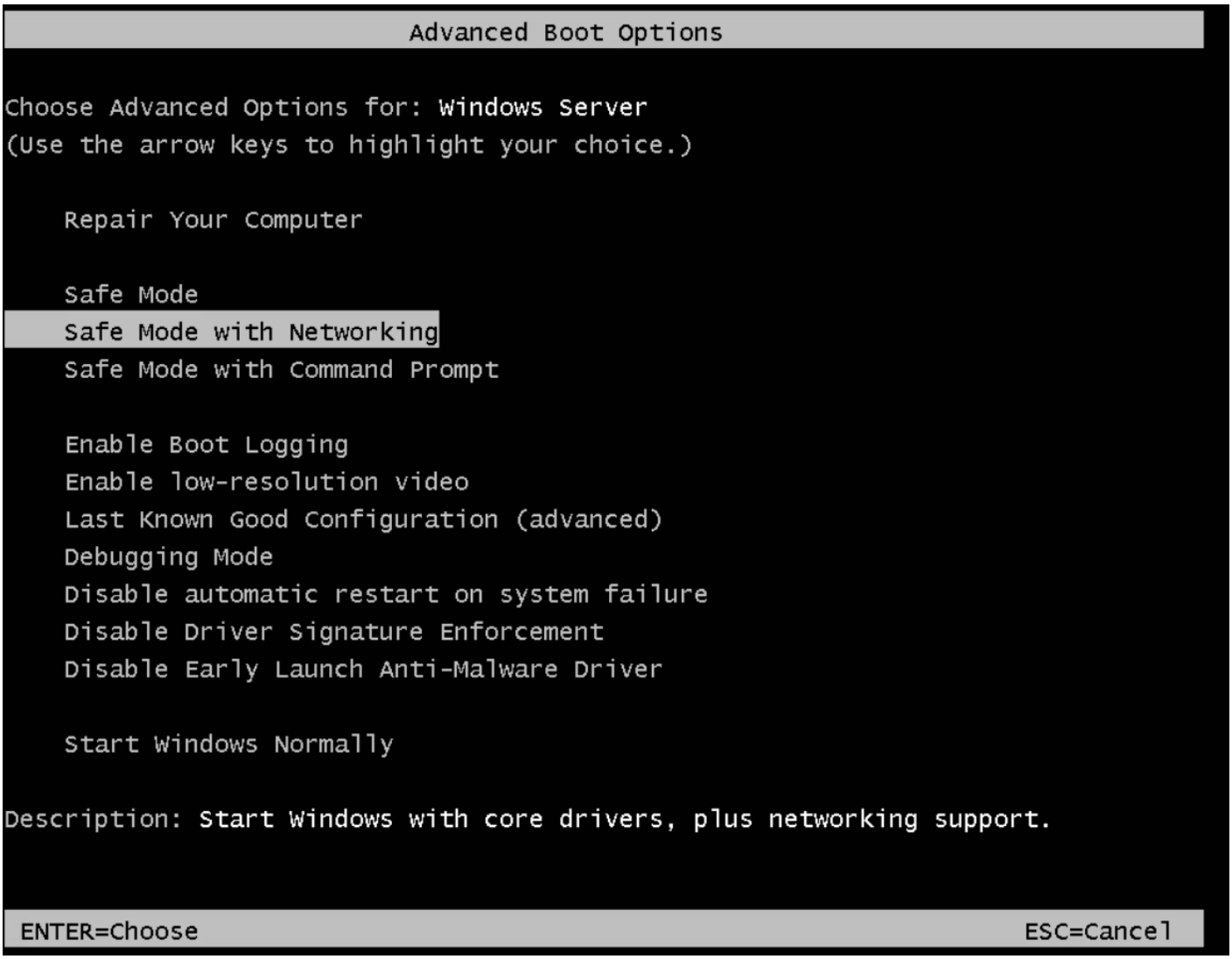
Startup Settings



Hit reboot



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).

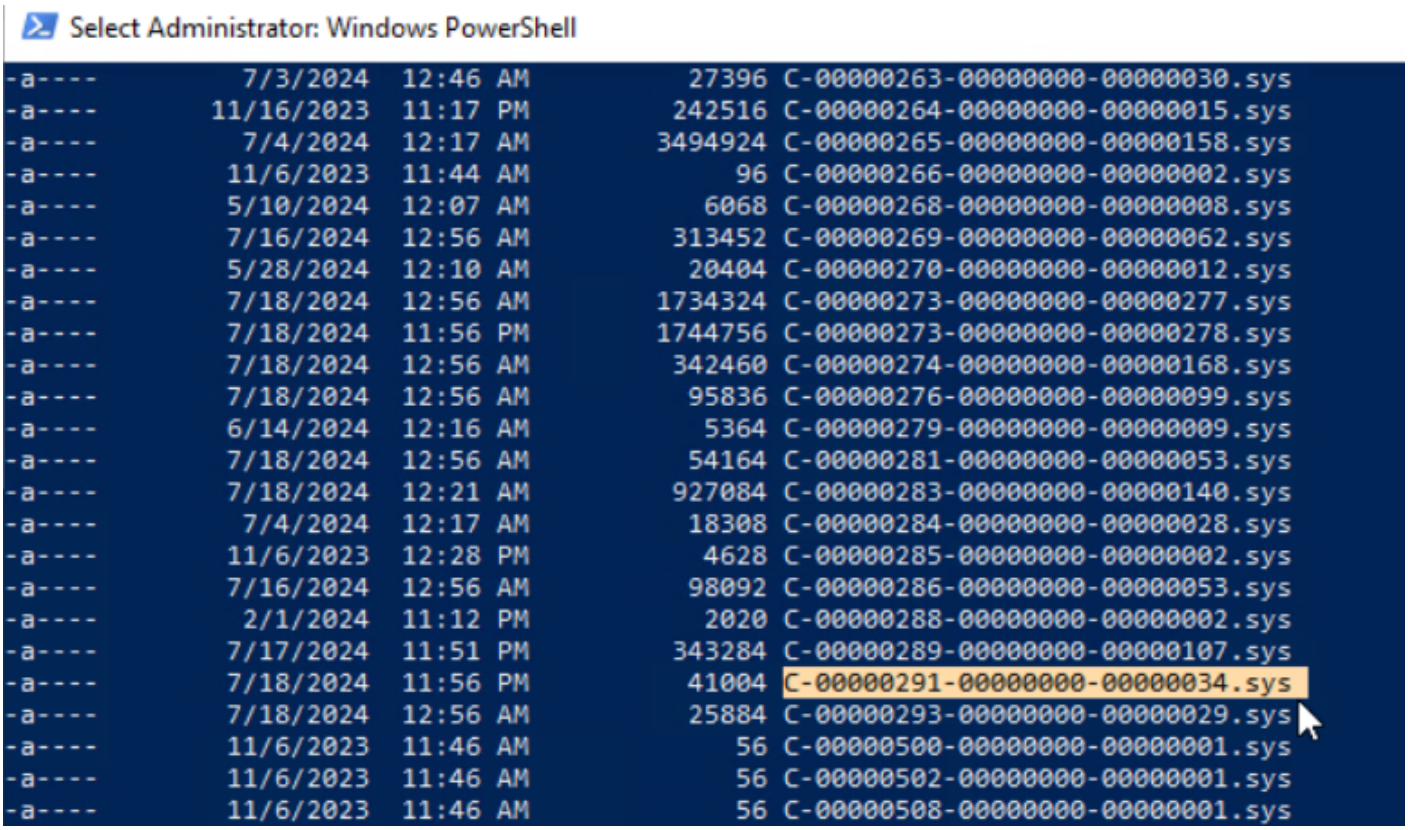


Once you've logged into the server you need to open up cmd or powershell.

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

```
dir
```

(to list all files)



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

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

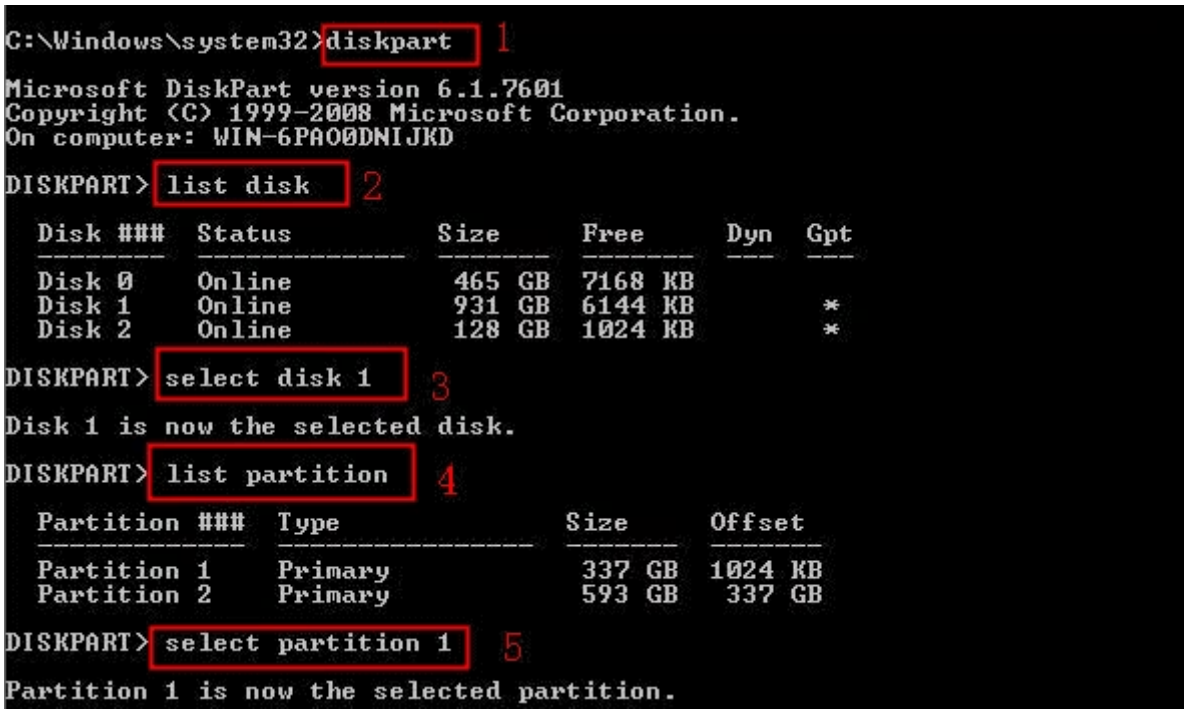
Reboot the machine.

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.



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 drivername.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!