No Boot fix

check disk info with diskpart

use `diskpart` command to enter enter diskpart utility

> Microsoft DiskPart version 10.0.22621.1

```
Copyright (C) Microsoft Corporation.
On computer: CHAO-LAPTOP
```

```
list disk
```

```
DISKPART>
Disk ###  Status      Size     Free     Dyn  Gpt
--------  ----------  -------  -------  ---  ---
Disk 0    Online       476 GB  1024 KB      *
```

```
select disk 0
```

```
DISKPART>
Disk 0 is now the selected disk.
```

```
list partition
```

```
DISKPART>
Partition ###  Type          Size     Offset
-------------  ------------  -------  -------
Partition 1    System         100 MB  1024 KB
Partition 2    Reserved        16 MB   101 MB
Partition 3    Primary         99 GB   117 MB
Partition 4    Recovery       674 MB    99 GB
Partition 5    Primary        376 GB   100 GB
```

Note! ***System partition*** is where bootmgr, BCD stored, while ***Boot partition*** is where Windows OS actually installed.

```
list vol
```

```
DISKPART>
Volume ###  Ltr  Label      Fs     Type       Size     Status     Info
----------  ---  ---------  -----  ---------  -------  ---------  --------
Volume 0     C               NTFS   Partition    99 GB  Healthy    Boot
Volume 1     D               NTFS   Partition   376 GB  Healthy
Volume 2                     FAT32  Partition   100 MB  Healthy    System
Volume 3                     NTFS   Partition   674 MB  Healthy    Hidden
```

you can use `assign` command to assign a drive letter to a volume which doesn't contain a letter

```
select vol 2
assign
```

```
DISKPART>
Volume 2 is the selected volume.
```

> DISKPART>
> DiskPart successfully assigned the drive letter or mount point.

you can check again with `list vol`

```
list vol
```

> DISKPART>
> Volume ### Ltr Label Fs Type Size Status Info
>
> ---
>
> Volume 0 C NTFS Partition 99 GB Healthy Boot
> Volume 1 D NTFS Partition 376 GB Healthy
>
> - Volume 2 E FAT32 Partition 100 MB Healthy System
>   Volume 3 NTFS Partition 674 MB Healthy Hidden

if you want to remove a drive letter, use `remove letter=?`

```
remove letter=e
```

bcdedit

we use `bcdedit` to verify location of ***bootmgr*** and ***winload*** , run `bcdedit` without options, will bring us

> ## Windows Boot Manager
>
> identifier {bootmgr}
> device partition=\Device\HarddiskVolume1
> path \EFI\Microsoft\Boot\bootmgfw.efi
> description Windows Boot Manager
> locale en-US
> inherit {globalsettings}
> default {current}
> resumeobject {2e42493b-3d89-11ee-bea9-89d616f9a0ab}
> displayorder {current}
> toolsdisplayorder {memdiag}
> timeout 30
>
> ## Windows Boot Loader
>
> identifier {current}
> device partition=C:
> path \Windows\system32\winload.efi
> description Windows 11
> locale en-US
> inherit {bootloadersettings}
> recoverysequence {2e42493d-3d89-11ee-bea9-89d616f9a0ab}
> displaymessageoverride Recovery
> recoveryenabled Yes
> isolatedcontext Yes

```
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {2e42493b-3d89-11ee-bea9-89d616f9a0ab}
nx                      OptIn
bootmenupolicy          Standard
hypervisorlaunchtype    Auto
quietboot               No
sos                     No
```

as ***bootmgr*** and ***winload*** files all use ***.efi*** extension, we know that this machine is ***UEFI*** based.

to avoid boot loop, and use advanced options, we run the 2 commands below

```
bcdedit /set {default} recoveryenabled off
bcdedit /set {default} advancedoptions on
```

you may also toggle the ***bootmenupolicy*** with

```
bcdedit /set {default} bootmenupolicy legacy
bcdedit /set {default} bootmenupolicy standard
```

***Note! after fixing problems for our customers, we must set `recoveryenabled on` and `advancedoptions off` ***

if you encounter a situation that ***BCD*** is good, but `bcdedit` returns error, try use `/store` option

```
bcdedit /store e:\efi\microsoft\boot\BCD /set {default} recoveryenabled off
```

to back up, and restore BCD, use `/export` and `/import`

```
bcdedit /export c:\temp\BCD_BACKUP
bcdedit /import c:\temp\BCD_BACKUP
```

MBR or *Boot Code* damaged?

```
bootrec /fixmbr
bootrec /fixboot
```

BCD damaged?

```
bootrec /scanos
bootrec /rebuildbcd
```

failed to rebuild BCD

```
rem for bios based

bcdedit /export C:\BCD_Backup
c:
```

```
cd boot
attrib bcd -s -h -r
ren c:\boot\bcd bcd.old
bootrec /RebuildBcd

rem for UEFI based

bcdedit /export C:\BCD_Backup
c:
cd EFI\Micorsoft\boot
attrib bcd -s -h -r
ren bcd bcd.old
bootrec /RebuildBcd
```

boot manager missing?

BIOS	UEFI
copy ***bootmgr*** to ***Sys_part***	copy ***bootmgfw.efi*** to ***Sys_part\EFI\Microsoft\Boot***

if in BIOS machine, system partition is not active

in `diskpart`, `select vol x` use command `active`, if you wanna do reverse, just use `inactive`

create a new system partition

```
rem select a vol with enough free space
diskpart
select vol 2
shrink desired=500 minimum=250
create partition efi size=500
select vol <new>
format fs=fat32 label="new_sys"
assign
rem optionally active the partition if in BIOS
bcdboot C:\Windows /s E:
optionally go to old EFI partition, rename EFI folder as EFI_OLD
```

Windows Recovery Environment (RE) and Preinstallation Environment (PE)

a mini OS to fix or install Windows OS

how to enter RE

1. on login screen, hold ***shift***, click restart
2. Windows 10, select Start > Settings > Update & security > Recovery > under Advanced Startup, click Restart now.
3. in command prompt, `shutdown /r /o /t 0`,

4. Boot from RE.iso
5. after 2 consecutive boot failures, computer will enter RE spontaneously

Advanced Boot Options

allows users to boot into safe mode, last know good configuration, disable driver signature enforcement, etc.

if you don't see LKGC, you may enable it with registry.

> Under key
>
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Configuration Manager\LastKnownGood\
>
> Create REG_DWORD value
>
> Enabled 1 for enable, 0 for disable

clean boot

> 1. Use msconfig ==> service ==> hide all ms svc ==> disable all
> 2. Tskmgr ==> Startup===> disable all manually
> 3. Restart computer

Boot loop, Start == 2 && (errorcontrol == 2||3)

sometimes, boot loop could still happen even `bcdedit /set recoveryenabled off`, `disable auto restart after boot failure` is configured. This is caused by ***errorcontrol*** in service registry

> find all services with Start value 2, and change their errorcontrol value from 2||3 to 0||1
>
> you may also use a PowerShell to do it automatically

Disable Driver Signature Enforcement

1. how to find unsigned drivers?

1. use sigverif
2. Event viewer Applications and Services Logs -> Microsoft -> Windows -> CodeIntegrity -> Operational
3. Sigcheck sigcheck -u -e -s c:\windows\system32 > 1.txt

2. after finding problem drivers, what do you do?

1. MS driver: update them
2. third parties, contact vendors

3. no driver updates available?

1. Copy Catroot folder from working machine C:\Windows\System32\CatRoot{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
2. Use sigcheck to verify if a server is reallt unsiged
3. Copy signed driver from a working server

Last Known Good Configuration LKGC

if you cannot find LKGC in advanced boot options, enable it via registry

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Configuration Manager\LastKnownGood\
>
> Create REG_DWORD value
>
> Enabled 1 for enable, 0 for disable

Restore registry backups

before Windows 10 1803, ***%windir%\system32\config\regbak*** is used to backup the registry, you may copy ***SYSTEM***, ***SOFTWARE*** back to the parent folder to restore registry

you may also reenable registry periodic back in registry

> Control\Session mnager\Configuration manager\
>
> EnablePeriodicBackup REG_DWORD 1

CHKDSK and SFC

```
chkdsk c: /f /r
sfc /scannow /offbootdir=c:\  /offwindir = c:\Windows
```

BIG FILE , copying system files

copy files from a normal machine to problematic machines, note those machine should have same hardware, system, patch level, etc.

> files under ***system32*** and ***system32\drivers***
>
> ***Note! files ONLY, not sub-folders.***

or you can try copy files from ***C:\Windows\WinSxS*** on the problematic machine

Clean boot

1. Use msconfig ==> service ==> hide all ms svc ==> disable all
2. Tskmgr ==> Startup===> disable all manually
3. Restart computer

Load and unload hives

Regedit

1. File ==> load hive
2. File ==> unload hive

reg.exe

```
Reg load hklm\offline_system <path to system hive>
Reg unload hklm\offline_system
```

Manually disable a driver

> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SERVICENAME\
>
> change ***Start*** value to 4

Stop Error 7B

1. Review `diskpart`, `bcdedit`, `bootrec`, and `bcdboot`

2. Windows Update and DISM

```
Dism /Image:C: /get-packages
rem You will see update installing status
Dism /image:c:\ /cleanup-image /revertpendingactions
rem And you will remove images, and pending actions
```

after using `DISM`, you need to rename ***pending.xml*** to ***pending.xml.old*** under ***WinSxS*** folder

You also need to load offline `COMPONENT`, and delete ***PendingXmlIdentifier*** key if exists, load offline `SYSTEM`, and delete ***pendingfilerenameoperations*** key if exits under `Control\session manager\`

Note! Always back up keys before delete them !

3. Check important sys drivers, services

make sure services below exists under ***Controlset00x\Services***, and their Start values are ***0***.

> - ACPI
> - DISK
> - VOLMGR
> - VOLSNAP
> - VOLUME
> - PARTMGR

If any of those drivers doesn't exits, copy hive backups from regbak folder

Check upperfilters, lowerfilters, under

> \Control\Class{4D36E96A-E325-11CE-BFC1-08002BE10318}

> \Control\Class{4D36E967-E325-11CE-BFC1-08002BE10318}
>
> \Control\Class{4D36E97B-E325-11CE-BFC1-08002BE10318}
>
> \Control\Class{71A27CDD-812A-11D0-BEC7-08002BE2092F}

If you find non-Microsoft deriver values, delete them

Some more on DISM

To get information about a package

```
DISM /image:c:\ /get-packageinfo /packagename :>package-identity>
```

To uninstall an installed package

```
Dism /image:c:\ /remove-package /packagename:<package_identity>
```

Disable Trustedinstaller

Locate ***\CurrentControlSet\Services\TrustedInstaller*** and change registry value Start to 4.

Review of *Start* Value in Services

0	Boot
1	System
2	Auto
3	Manual
4	Disabled

Collect some logs

manually check logs under

> C:\Windows\Logs\CBS
>
> C:\Windows\INF\setupapi.dev.log
>
> C:\Windows\System32\Winevt\Logs
>
> Or use a script

Bonus

Boot logging & Procmon

1. Enable in procmon options --> enable boot logging
2. Export key Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PROCMON23

3. Import key in the problematic machine
4. Modify hive name and controlset
5. Copy driver Copy the driver C:\windows\system32\drivers\procmon23.sys from normal machine to problematic one
6. Disable driver signature enforcement
7. Hard reboot machine
8. Enter recovery mode, copy out \windows\procmon.pmb to normal machine
9. Open procmon and save boot log

p2v, disk2vhd

1. Use disk2vhd tool to convert hard disk to a virtual hard disk
2. Choose systempartition,and boot partition while create vhdx

7b after p2v, attach vhdx, and use bcdboot

1. Load problematic vhdx to another hyper-v machine
2. Boot to normal virtual machine and run diskpart
3. Find boot partition letter from problematic vhdx
4. If letter is E for example, run bcdboot e:\windows
5. Load problematic systemhive and change HKLM\LoadHive\CurrentControlSet\Services\intelide start value to 0.
6. Resart normal virtual machine, and you will get dual-boot

Net use for file transfer

1. Create a sharable folder on a normal machine
2. Try use the problematic machine to ping the normal one
3. In command prompt use net use * "\\normal_host\sharefolder" /user:username password /persistent:no
4. Use xcopy [files or directories] [net_drive\path] /e /c /h /I

> **Caution:**
>
> When create shareable folders, try give permission to an existing user on the normal host, instead of "everyone"
>
> Net use * will set the shareable folder as a net drive and assign an available drive letter for it.

Stop 6B BootCat.cache, and RootCat\

- System check signature of drivers from BootCat.cache
- BootCat.cache is built based on files under catroot{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
- You can try rename bootcat.cache to bootcat.cache.old, and let system recreate it
- Or you can copy catroot{F750E6C3-38EE-11D1-85E5-00C04FC295EE} from a normal machine(always remember back up)

Attrib, dir, xcopy

While manupilating while files in command prompt, attrib, dir, xcopy are often used

```
Attrib /d /s -h -s -r
Rem remove hide, system, read-only attributes for all files subfolders
Dir /s /a
Rem show all files in current and subfolders
Xcopy source dest /c /h /i /e
Rem copy files including system, hidden, empty folders, etc.
```

Note: xcopy might throw sharing violation errorwhile trying to copy some crucial files such as BCD, you may try boot from mounted iso, and copy from command prompt.

No Boot Mind Mapping Diagram