Troubleshooting Windows® Boot and Startup

Exploring Windows XP Boot Options and Recovery Console

Saul Coval
Systems Analyst & Developer
Global Support Automation

COVAL Systems

Introduction

- Kinds of problems we're addressing:
  - Crashes and hangs during boot
  - Error messages during boot
  - Errors messages during the logon process
- Causes:
  - 3rd party drivers and applications
  - System file corruption due to hardware problems or blue screens (from 3rd party drivers)
- Common response: "Reinstall Windows"
- You can do better than that by understanding the boot and startup process and the tools available to track down and repair problems

COVAL Systems

Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

Boot Process Terminology

- Boot begins during installation when Setup writes various things to disk
- System volume:
  - Master Boot Record (MBR)
  - Boot sector
  - NTLDR – NT Boot Loader
  - NTDETECT.COM
  - BOOT.INI
  - SCSI driver – Ntbootdd.sys
- Boot volume:
  - System files – %SystemRoot%: Ntoskrnl.exe, Hal.dll, etc.

COVAL Systems

The Boot Process

1. MBR
   - Contains small amount of code that scans partition table
     - 4 entries
     - First partition marked active is selected as the system volume
   - Loads boot sector of system volume
2. Boot sector (NT-specific code)
   - Reads root directory of volume and loads NTLDR

COVAL Systems

x86 and x64 Boot Process

3. NTLDR (screen is black)
   - Moves system from 16-bit to 32-bit mode and enables paging
   - Reads and uses Ntbootdd.sys to perform disk I/O if the boot volume is on a SCSI disk
     - Uses BIOS to read from system volume's disk
     - This is a copy of the SCSI miniport driver used when the OS is booted
   - Reads Boot.ini
     - Boot.ini selections point to boot drive
     - Specifies OS boot selections and optional switches (most for debugging/troubleshooting) that passed to kernel during boot
   - If more than one selection, NTLDR displays boot menu (with timeout)
   - If you select a 64-bit installation, NTLDR moves the CPU into 64-bit mode

COVAL Systems

The Boot Process (cont)

3. NTLDR (cont)
   - Once boot selection made, user can type F8 to get to special boot menu
     - Last Known Good, Safe modes, hardware profile, Debugging mode
   - NTLDR executes Ntdetect.com to perform BIOS hardware detection (x86 and x64 only)
     - Later saved into HKLM\Hardware\Description
   - NTLDR loads the SYSTEM hive (HKLM\System), boot drivers, Ntoskrnl.exe, Hal.dll and transfers control to main entry point of Ntoskrnl.exe
     - Boot driver: critical to boot process (e.g. boot file system driver)

COVAL Systems

The Boot Process (cont)

4. Ntoskrnl (splash screen appears)
   - Initializes kernel subsystems in two phases:
     - First phase is object definition (process, thread, driver, etc)
     - Second builds on the base that the objects provide
     - This is done in the context of a kernel-mode system thread that becomes the idle thread
   - I/O Manager starts boot-start drivers and then loads and starts system-start drivers
   - Finally, Ntoskrnl creates the Session Manager process (\Windows\System32\Smss.exe), the first user-mode process

COVAL Systems

Driver Load Order

- Every driver has a key in HKLM\System\CurrentControlSet\Services
  - Type: 1 for driver, 2 for file system driver, others are Win32 services
  - Start: 0 = boot, 1 = system, 2 = auto, 3 = manual, 4 = disabled
- Special case: the file system driver for the system volume is always loaded and started, regardless of what its start type is
- Viewing driver start types:
  - Run LoadOrd from Sysinternals
  - Run Msinfo32 and goto Software Environment\System Drivers
  - Run Driverquery (/v for verbose)

COVAL Systems

The Boot Process (cont)

5. Smss.exe:
   - Runs programs specified in BootExecute e.g. autochk, the native API version of chkdsk
   - Processes “Delayed move/rename” commands
     - Used to replace in-use system files by hotfixes, service packs, etc.
   - Initializes the paging files and rest of Registry (hives or files)
   - Loads and initializes kernel-mode part of Win32 subsystem (Win32k.sys)
   - Starts Csrss.exe (user-mode part of Win32 subsystem)
   - Starts Winlogon.exe

COVAL Systems

The Boot Process (cont)

6. Winlogon.exe:
   - Starts LSASS (Local Security Authority)
   - Loads GINA (Graphical Identification and Authentication) to wait for logon
     - default is Msgina.dll
   - Starts Services.exe (the service controller)
7. Services.exe starts Win32 services marked as “automatic” start
   - Also includes any drivers marked Automatic start (Start value is 2)
   - Service startup continues asynchronous to logons

End of normal boot process

COVAL Systems

Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

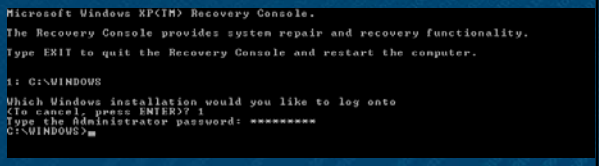
MBR Corruption

- Symptoms:
  - Hang at a black screen after BIOS executes
  - “Invalid Partition Table”, “Error loading operating system” or “Missing operating system” message on black screen
- Cause:
  - MBR is corrupt
- Resolution:
  - Boot into Recovery Console
  - Execute the RC’s “fixmbr” command
    - If the partition table is corrupt you have to rely on restoring a backup MBR or use 3rd-party disk repair tools

COVAL Systems

The Recovery Console

- Description:
  - Simple repair-oriented command-line environment
  - Built on a minimal NT kernel
  - Bootable from Win2K/XP/Server 2003 Setup CD
    - Type “r” to repair and then select the installation
  - Installable onto hard disk (winnt32.exe /cmdcons)



COVAL Systems

The Recovery Console

- Capabilities:
  - File commands: rename, move, delete, copy
  - Service/Driver commands: listsvc, enable, disable
  - MBR/Boot sector commands: fixmbr, fixboot
- Limitations:
  - Must “log into” the system with the Administrator password
  - Limits on what you can access:
    - Only access system directory and root of non-removable media
    - Can only copy files onto system, not off
    - You can override these in the Local Security Policy editor (secpol.msc) on the installation when its running
  - No networking, file editing, or registry editing

COVAL Systems

Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

Boot Sector Corruption

- Symptoms:
  - Black screen hang
  - “A disk read error occurred”, “NTLDR is missing” or “NTLDR is compressed” error message on black screen
- Cause:
  - Boot sector corruption
- Troubleshooting:
  - Boot into RC
  - Execute “fixboot” command

COVAL Systems

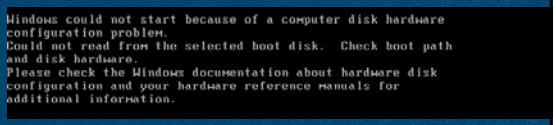
Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

Boot.ini Problems

- Symptom:
  - NTOSKRNL complains that boot device is inaccessible

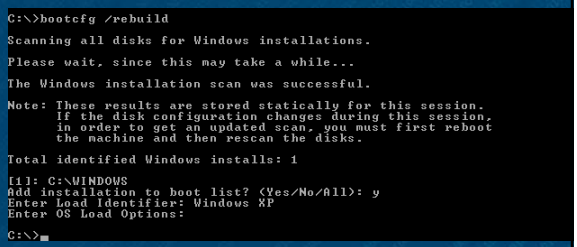


- Cause:
  - Boot.ini is missing or corrupt
  - Boot.ini is out-of-date because a partition has been added

COVAL Systems

Boot.ini Problems

- Troubleshooting:
  - Boot into RC
  - Run Bootcfg /rebuild



COVAL Systems

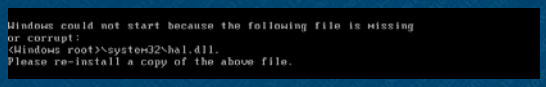
Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- System file corruption
- Boot.ini misconfiguration
- Crashes or hangs
- Driver or service startup failure
- Logon problems

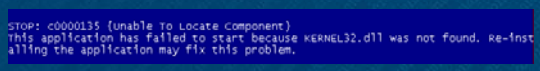
COVAL Systems

System File Corruption

- Symptom:
  - Error message indicating that NTLDR, NTOSKRNL.EXE, HAL.DLL or other system file is missing or corrupt



  - Blue screen with corruption message



COVAL Systems

System File Corruption

- Causes:
  - Disk is corrupt
  - File is missing or corrupt
- Troubleshooting:
  - Boot into RC
    - Run Chkdsk
    - If no chkdsk errors obtain clean copy of file and replace file
      - Check in \Windows\System32\DLLCache for backup
      - Replacement must be identical match i.e. from same hotfix or service pack
  - If can't find replacement use Automated System Recovery (ASR)

COVAL Systems

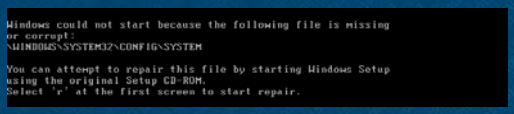
Automated System Recovery (ASR)

- Description:
  - Backup of all system state and user data on system volume
    - Includes registry, system files, boot sector, MBR
  - Made by Windows Backup
  - Boot into ASR from Windows setup (press F2 when prompted) and insert the ASR floppy
- Capabilities:
  - Will restore entire system state, including boot sector, MBR, system files, and registry
- Limitations:
  - You have to keep the backup up-to-date
  - No control over granularity of restore (all-or-nothing)

COVAL Systems

SYSTEM Hive Corruption

- Symptom:
  - NTLDR reports that System hive is corrupt



- Causes:
  - Disk is corrupt
  - System hive is corrupted or deleted

COVAL Systems

System Hive Corruption

- Troubleshooting:
  - Boot into RC
  - Run Chkdsk
  - Copy backup copy of System hive from \Windows\Repair to \Windows\System32\Config
    - Windows Setup makes backup after it completes
    - Backing up "System State" with Windows Backup update the Repair directory
    - Note: on XP you can get more recent hives from System Restore points (covered later)

COVAL Systems

Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

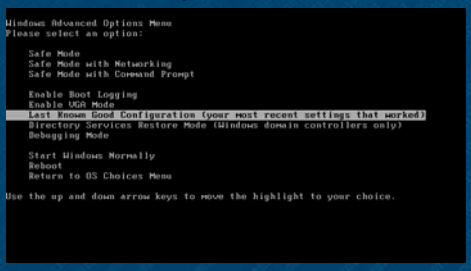
Post-Splash Screen Crash or Hang

- Symptoms:
  - System blue screens on boot
  - Hang before logon prompt appears
  - NOTE: If system auto-reboots on crash you won't see the blue screen!
- Causes:
  - Buggy driver
  - Registry corruption of non-System hive
- Troubleshooting:
  - Last Known Good
    or
  - Safe Mode
    or
  - RC

COVAL Systems

Accessing Last Known Good

- Enable it by pressing F8 and selecting it in the Advanced Options boot menu



COVAL Systems

LKG Description

- Last Known Good (LKG) Uses backup of registry control set last used to boot successfully
- A Control Set is core startup configuration
  - HKLM\System\Control00n
  - Control set only includes core OS and driver configuration
  - Control set does *not* include Software, SAM, Security, or Users
  - HKLM\System\Select\Current points at active Control Set

COVAL Systems

LKG Description

- Boot control makes a copy of the control set that booted the system
  - Copy is ControlSet00n, where 00n is the next available number
- After a successful boot:
  - 1. LastKnownGood is set to the copy
  - 2.The previous LastKnownGood is deleted
- By default, “Successful boot” is determined when
  - All the auto-start services have started successfully
  - A successful interactive log in
    - Can be overridden programmatically

COVAL Systems

LKG Capabilities

- Restores bootable configuration when:
  - A new driver was installed since the last successful boot
  - A driver’s settings were modified since the last successful boot
  - System settings were modified since the last successful boot

COVAL Systems

LKG Limitations

- Doesn’t work if:
  - An existing driver was updated
  - A latent driver bug for some reason becomes active
  - Files or registry hives are missing or corrupt

COVAL Systems

Leveraging the Failed Control Set

- When you use LKG the control set you avoid is saved as the Failed control set
  1. Look at the Failed value in the Select key – this is the control set that you aborted
  2. Export the current control set and failed control set to .reg files
  3. Massage the text so that there are no differences in the control set name
  4. Windiff or Fc to see what’s different

COVAL Systems

Safe Mode Description

- Try Safe Mode if LKG doesn’t work
  - Accessible from same boot menu as LKG
- Idea is to only include core set of drivers/services
  - Modeled after Safe Mode in Windows 95
  - Avoids third-party and unnecessary drivers, which hopefully are what’s causing the boot problem

COVAL Systems

Safe Mode Description

- HKLM\System\CurrentControlSet\Safeboot guides safe mode by specifying names and groups of drivers
  - Normal, Network, Command-Prompt
    - No networking in Normal
    - Networking includes networking services
    - Command-Prompt is same as Normal except launches Command Prompt instead of Explorer as shell for when Explorer shell extensions cause logon problems
  - Directory Services Restore Mode: not for boot troubleshooting (for repairing or restoring Active Directory database from backup)

COVAL Systems

Safe Mode Internals

- Registry keys guide what's in safe modes:
  - HKLM\System\CurrentControlSet\SafeBoot\Minimal is for Normal and Command-Prompt
    - HKLM\System\CurrentControlSet\SafeBoot\AlternateShell specifies shell for Command-Prompt boot
  - HKLM\System\CurrentControlSet\SafeBoot\Network is for Network
  - Drivers and services must be listed by name or by group to be loaded
- Exception: all boot-start drivers load regardless!
  - System assumes they are necessary to boot

COVAL Systems

Using Safe Mode

- If Safe Mode works determine what's wrong:
  - Compare boot logs
  - Analyze a crash dump
- Boot logging:
  - Select it from same menu as LKG and Safe Mode and boot to the failure
    - Saves log in \Windows\Ntbtlog.txt
  - Reboot in Safe Mode
    - Safe Mode appends to the boot log
  - Extract failed boot and Safe Mode entries to separate files, strip "Did not load driver" lines and compare e.g. Windiff, fc

COVAL Systems

Analyzing a Crash Dump

- Boot into Safe Mode
- Download and install the Microsoft Debugging Tools for Windows
- Run Windbg and select File|Open Crash Dump
  - Open \Windows\Memory.dmp if available, otherwise most recent file in \Windows\Minidump
- Type !analyze –v to see if debugger identifies faulty driver

COVAL Systems

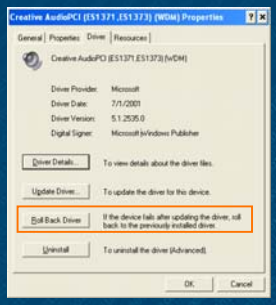
Resolving the Faulty Driver Issue

- If you can determine what driver is causing the problem:
  - Roll back to a previous version if one is available and known to be stable
    or
  - Disable it with Device Manager
    - Note: can't do this for non-PnP drivers: use the registry editor

COVAL Systems

Using Driver Rollback

- Access the rollback option on the Driver tab of a device's properties
- Backup drivers are stored in \Windows\System32 \Reinstallbackups



COVAL Systems

Disabling Drivers

- Open the Device Manager on the Hardware page of the System applet
  - Change usage to Disabled
- Or use the SC command to change the start type of a specific driver

COVAL Systems

Finding the Faulty Driver

- There are three approaches when you can't determine what driver is causing the boot to fail:
  - Use the Driver Verifier to catch the faulty driver
  - Disable drivers that don't load in Safe Mode one by one until the system boots normally
  - Use System Restore (Windows XP only) as a last resort

COVAL Systems

The Driver Verifier

- The Driver Verifier catches drivers performing illegal operations:
  - Buffer overflow
  - Invalid memory access
  - Invalid I/O commands
- Launch it with Start->Run->Verifier
- Enable the Driver Verifier on all drivers from within Safe Mode
  - Choose "custom settings" and then "select individual settings"
    - Check all settings except "low resource simulation"
- Boot normally and you'll hopefully get a crash that is easy to analyze
  - Note: the Driver Verifier is disabled in Safe Mode

COVAL Systems

System Restore Description

- Rollback system to previous state (registry, COM+ registration database, user profiles, other files not protected by WFP)
  - New to XP (not included with Server 2003)
  - Enabled by default
- Replacement of certain file types causes original version to be stored in a restore point folder
  - 569 file types monitored—see Platform SDK for list
  - Restore operation replaces these files
- Implemented as a service and a filter driver
- Access the System Restore Wizard from Start->Help and Support->System Restore
  - Safe Mode asks when you log in if you want to run the wizard

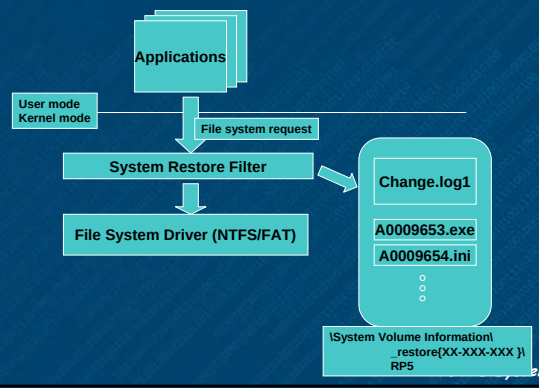
COVAL Systems

System Restore Creation

- Restore Points are created:
  - Every 24 hours no one is logged on
  - Every 12 hours when someone is logged on
  - When installing an unsigned driver
  - When explicitly requested by user or an install program (via an API or script)
    - Start->Help and Support -> System Restore

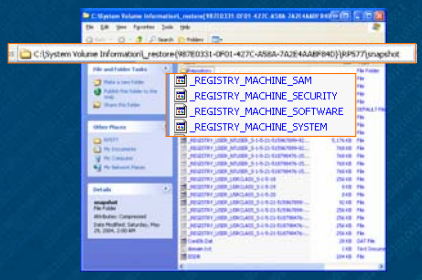
COVAL Systems

System Restore Internals



Using System Restore

- Note that you can also use restore points to obtain backup registry hives



COVAL Systems

When Safe Mode Fails

- Symptom:
  - Safe mode crashes the same as a normal boot
- Causes:
  - The driver causing the crash also loads in safe mode
- Troubleshooting:
  - Determine the problematic driver:
    - Boot into RC and look at the last line in the boot log
    - Boot into debugging mode
  - Disable it with the RC's "disable" command

COVAL Systems

Debugging Mode

1. Connect a second computer (the "host") via serial cable and configure kernel-debugging in Windbg
2. Select Debugging mode from the same Advanced Boot options menu (press F8) as LKG and Safe Mode on the crashing system (the "target")
3. When the target crashes you'll get a Windbg prompt on the host:
   - Perform a !analyze –v
   - Use .dump to save minidump on host for later analysis (.dump /f for full dump)

- For more information see the Debugging Tools Help file

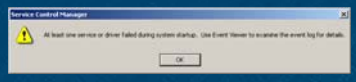
COVAL Systems

Agenda

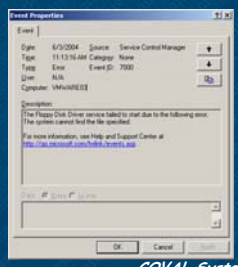
- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

One or More Drivers or Services Failed to Start



- The Service Control Manager reports failed drivers or services after a boot
  - Note: you won't see this on Professional!
- Determine the driver or service by looking at the event log



COVAL Systems

Agenda

- The boot process
- MBR corruption
- Boot sector corruption
- Boot.ini misconfiguration
- System file corruption
- Crashes or hangs
- Driver or service startup failure
- Logon problems

COVAL Systems

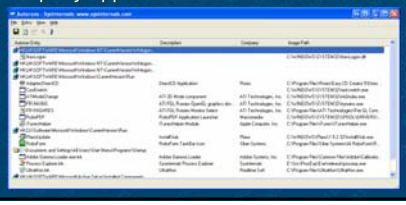
The Logon Process

- Winlogon sends username/password to Lsass
  - Either on local system for local logon, or to Netlogon service on a domain
- Creates processes for executables listed in HKLM\Software\Microsoft\Windows NT \CurrentVersion\WinLogon\Userinit
  - By default: Userinit.exe
  - Runs logon script, restores drive-letter mappings, starts shell
- Userinit creates a process to run HKLM\Software\Microsoft\Windows NT \CurrentVersion\WinLogon\Shell
  - By default: Explorer.exe
- There are other places in the Registry that control programs that start at logon

COVAL Systems

Logon Errors

- Run MsConfig (XP and higher)
  - Doesn't show you lots of things
- Run Sysinternals Autoruns to see what applications automatically start
  - Select "show only non-microsoft" to isolate third-party applications



COVAL Systems

Capturing a Logon Trace

- If an autostarting application you want is having errors, run Filemon and Regmon to capture a logon trace
  - Use PsExec from Sysinternals to start them in the system account:
    psexec –s –i –d c:\sysint\regmon.exe
  - After logging out and back in stop capture:
    - Look for access denied errors in Regmon and Filemon
    - In Filemon look for file and path not found errors

COVAL Systems

Errors After Logon

- For any errors after this point you're on your own!

COVAL Systems

For More Info...

- Take our advanced internals and troubleshooting classes or check out our videos (see www.solsem.com)
- Get the next edition of our book (to be called *Windows Internals 4th edition*)

COVAL Systems

Community Resources

- Microsoft Community Resources
  http://www.microsoft.com/communities/default.mspx
- Non-Microsoft Community Resources
  http://www.microsoft.com/communities/related/default.mspx
- Newsgroups
  Converse online with Microsoft Newsgroups, including Worldwide
  http://www.microsoft.com/communities/newsgroups/default.mspx
- User Groups
  Meet and learn with your peers
  http://www.microsoft.com/communities/usergroups/default.mspx
- Attend a free chat
  http://www.microsoft.com/communities/chats/default.mspx
- Attend a free web cast
  http://www.microsoft.com/usa/webcasts/default.asp
- Most Valuable Professional (MVP)
  http://mvp.support.microsoft.com/

COVAL Systems

Be an IT Hero with Microsoft Learning

To get the best from Microsoft products and technology visit Microsoft Learning situated in the main exhibition hall entrance today

- Talk to Microsoft Learning Experts on assessments, training and certification for Microsoft products and technology
- **PLUS** visit the Microsoft Learning Bookstore for 20% off all Microsoft Press titles as well as a FREE It Hero T-shirt with any two purchases
- **PLUS** buy a subscription to TechNet today and you can qualify now for a years FREE subscription until October 2005*

*Terms and Conditions apply – ask the Microsoft Learning Booth for details

COVAL Systems

Exploring Windows XP Boot Options and Recovery Console

Saul Coval
Systems Analyst & Developer
Global Support Automation

Introduction

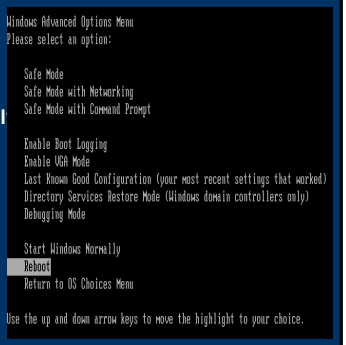
This presentation will discuss the Windows® XP Advanced Options menu available during startup, as well as the Recovery Console utility and its associated commands.

Available Boot Options

- Safe Mode
- Safe Mode with Networking
- Safe Mode with Command Prompt
- Enable Boot Logging
- Enable VGA Mode
- Last Known Good Configuration

Available Boot Options (2)

- Directory Services Restore Mode
- Debugging Mode
- Start Windows Normall
- Reboot
- Return to OS Choices Menu



Starting Boot Options

- Use Microsoft Configuration Utility (msconfig)
- Press F8 during the boot process
- System crash
- Edit Boot.ini

What Is Safe Mode?

- Minimal startup mode for troubleshooting
- Provides alternative when computer cannot start normally
- Three options
- Entering earlier versions

There is no support for serial (COM) ports and IEEE 1394 in safe mode

Safe Mode

- Minimal list of drivers
- Standard VGA
- Core operating system services
- No startup programs

Safe Mode with Networking

- Safe mode with networking
  - Provides stable environment to test networking issues
- Isolates test from:
  - Third-party programs
  - Third-party services
- Ping, IPConfig, Network Diagnostics

Safe Mode with Command Prompt

- Alternate shell
- Cmd.exe
- 32-bit environment

This is the same configuration as safe mode, with the explorer shell replaced by Cmd.exe

Enable Boot Logging

- Ntbtlog.txt
- This file is appended
- Normal boot

Safe Mode, Safe Mode with Networking, and Safe Mode with Command Prompt → Adds a list of all the drivers and services that are loaded to the boot log

The boot log can be useful to determine problems with drivers or services

Enable VGA Mode

- Video resolution is not optimized
- Video driver prevents normal boot
- Refresh rate
- Basic video driver for safe mode

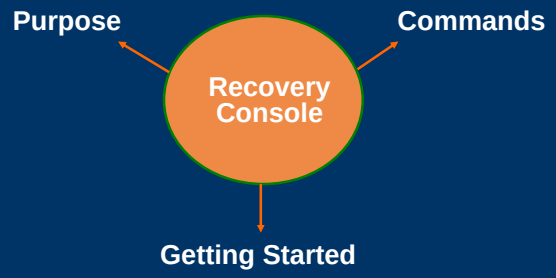
Last Known Good Configuration

- Registry and drivers
- Use only in cases of incorrect configuration
- Last successful log on

Registry key:

HKEY_LOCAL_MACHINE\System\Select

Recovery Console

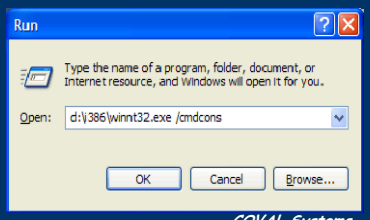


Why Use Recovery Console?

- Windows XP will not boot
- Cannot access safe mode
- Access NTFS, FAT, and FAT32 partitions

Starting Recovery Console

- Boot floppies
- CD-ROM
- Boot menu

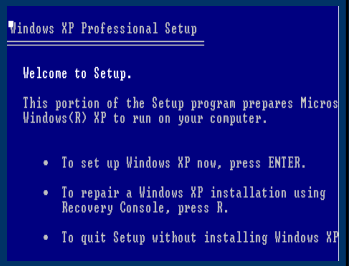


From Boot Floppies

- CD-ROM required
- Web only
- Six floppy disks
- Version specific
- Q310994, "Obtaining Windows XP Setup Boot Disks"

From CD-ROM

- Boot from the CD-ROM
- Begin setup process
- Press F10 or press R
- CD-ROM drive locks



From Boot Menu Selection

- Run Winnt32/cmdcons
- Approximately 7 MB
- Boot.ini
- Boot menu

An example of the Boot.ini entry:

C:\cmdcons\bootsect.dat= “Microsoft Windows Recovery Console” /cmdcons

Logon Process

- Steps to log on
  - Select the installation
  - Select the number
  - Enter administrator password
- Three tries to log on
- Windows XP Home Edition

Secure Limited Access

- Limited access to files
- Limited access to directories
- System and software hives

Recovery Console Commands

- Service commands
- Drive commands
- MAP command
- File controls
- Directory usage and commands
- BootCFG command
- Other commands

Service Commands

Enable Service	*Enable Spooler Service_Demand_Start*
Disable Service	*Disable Spooler*
Listsvc	*Browser Auto Computer Browser Cdrom Sys CD-ROM Driver*

Drive Commands – Format

- Format a partition
- Drive: the drive to format
- Uses switches

The syntax to use the Format command is:

Format [Drive:] [/Q] [/FS:file-system]

Drive Commands – Diskpart

- Delete partitions
- Create partitions
- Similar to setup screen

The syntax to use the Diskpart command is:

Diskpart [/add | /delete] [Device-name | drive-name | partition-name] [size]

Drive Commands – Chkdsk

- Detect bad sectors
- Common switches
  - /P
  - /R

The syntax to use the Chkdsk command is:

chkdsk [Drive: [/P] [/R]

MAP Command

- Map
  - Example of the MAP command:
    C: FAT32 2102MB\device\harddisk0\Partition1
    D: NTFS 2102MB\device\harddisk0\partition2
- Map ARC
  - Example of the MAP arc argument:
    C: FAT32 2102MB
    multi(0)disk(0)rdisk(0)partition(1)
    D: NTFS 2102MB
    multi(0)disk(0)rdisk(0)partition(2)

File Controls

Copy

Copy command syntax :
Copy Source [Destination]

Delete

Delete command syntax:
Delete [Drive:] [path] filename

Directory Commands

- Directory (DIR)
  - DIR [drive:] [path][filename]
- Make Directory (MD)
  - MD [drive:] path
- Remove Directory (RD)
  - RD [drive:] path
- Change Directory (CD)
  - CD [path] [..] [drive:]

Be sure to use a space with the commands

Bootcfg Commands

- Bootcfg
  - /default
  - /add
  - /rebuild
  - /scan
  - /list
  - /redirect /disable redirect

Other Commands

Command	Description
Batch	Permits the Recovery Console commands to run from a batch file
CLS	Clears the screen
UP Arrow	Retrieves previously typed commands
Attrib	Adds or removes attributes from files

Other Commands (2)

Command	Description
SystemRoot	Moves you back to %windir% from the current location
More or Type	Displays a text file
Ren	Permits you to rename an existing file
Exit	Exits from the Recovery Console

COVAL Systems 91

Repair Functionality

FixMBR — Rewrites the master boot record

Fixboot — Writes a new boot sector

Warning: Changing the master boot record can remove data

COVAL Systems 92

Expand Functionality

- Extracts from cabinet (.cab) files
- Expands
- Destination directory must have permitted access
- Switches
  - /Y /F /D

The syntax to use the Expand functionality is:

```
Expand source [/F:filespec] [destination] [/y] [/D]
```

COVAL Systems 93

Policy Changes

- Administrative password
- Environment variables
- Registry changes
- Set command

```
AllowAllPaths = True\False
AllWildCards = True\False
AllRemovableMedia = True\False
NoCopyPrompt = True\False
```

COVAL Systems 94

Additional Resources

Knowledge Base Articles

- Q315222, "A Description of the Safe Boot Mode Options in Windows XP"
- Q305595, "HOW TO: Create a Boot Disk for an NTFS or FAT Partition"
- Q240831, "How to Copy Files from Recovery Console to Removable Media"
- Q316434, "HOW TO: Do Advanced Clean-Boot Troubleshooting in Windows XP"
- Q310602, "How to Disable a Service or Device that Prevents Windows from Booting"

COVAL Systems 95

Additional Resources (2)

Knowledge Base Articles

- Q307654, "HOW TO: Install and Use the Recovery Console in Windows XP"
- Q291980, "A Discussion About the Bootcfg Command and Its Uses"
- Q314058, "Description of the Windows XP Recovery Console"
- Q307852, "HOW TO: Start Your Computer with Last Known Good Configuration"

COVAL Systems 96