

CompTIA A+ Core 2 Exam 220-1102

Lesson 11



Managing Windows

Objectives

- Use management consoles
- Use performance and troubleshooting tools
- Use command-line tools

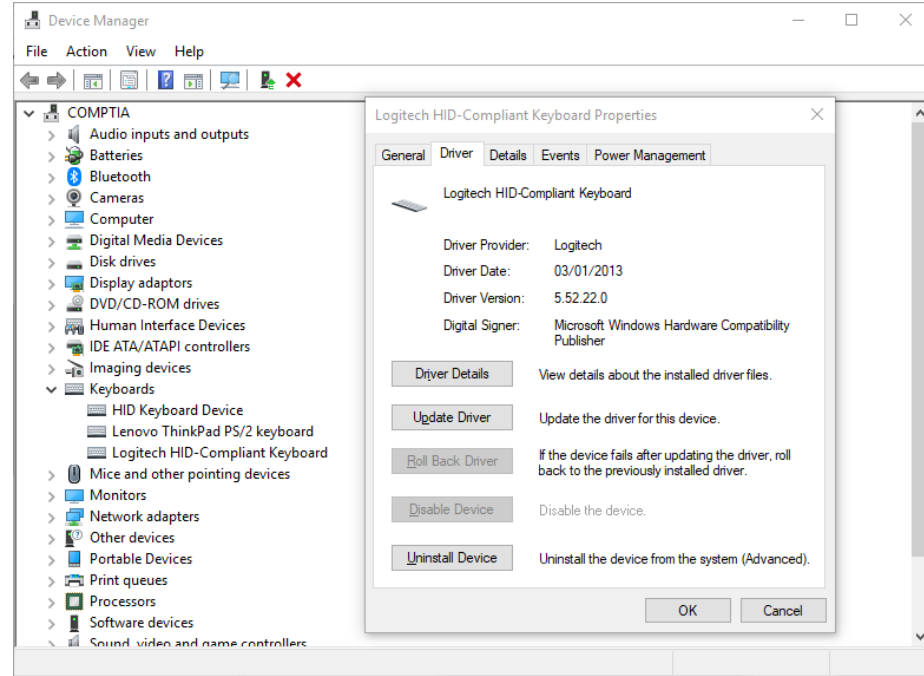
Lesson 11

Topic 11A

Use Management Consoles

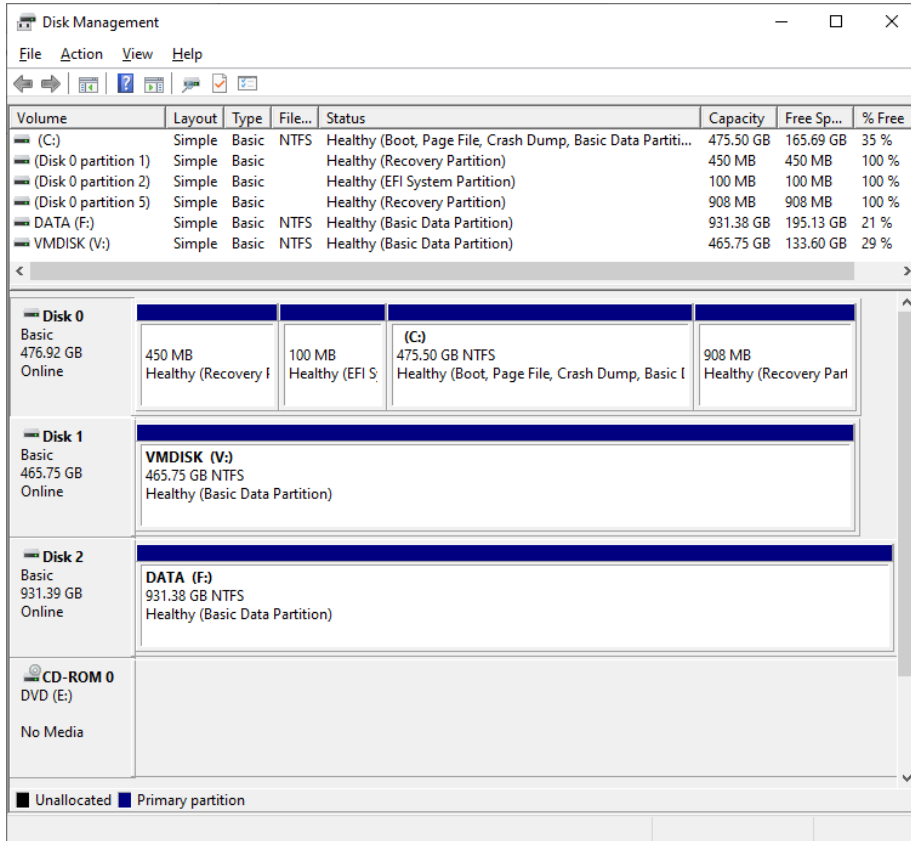
Device Manager

- Device Manager (devmgmt.msc)
- Updating and troubleshooting devices
- Removing, uninstalling, and disabling devices



Screenshot courtesy of Microsoft

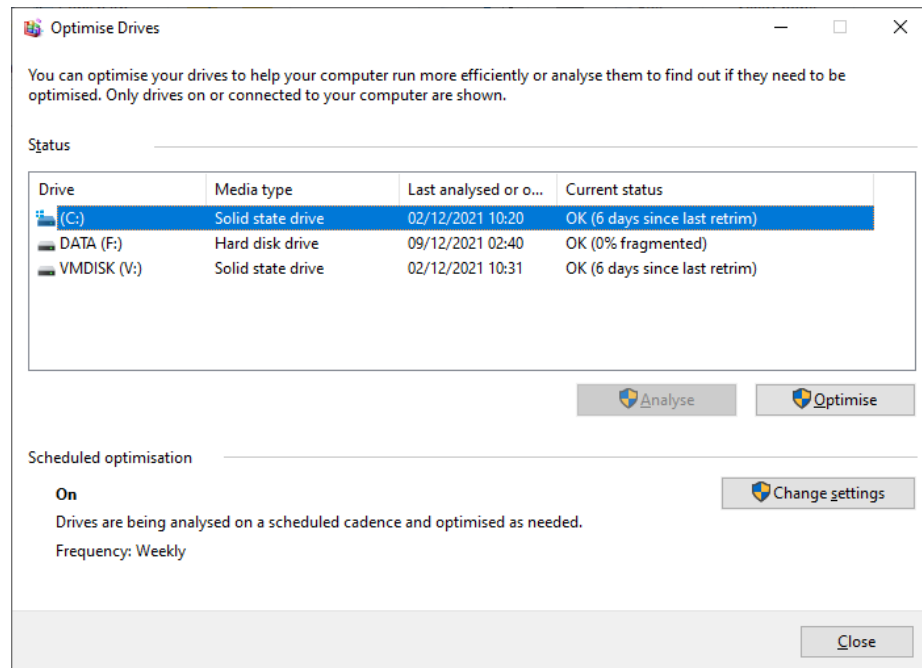
Disk Management Console



- Disk Management (diskmgmt.msc)
- Disks versus partitions/volumes/drives
- System, boot, and recovery volumes
- Initialize disks and create formatted partitions
- Repartitioning and dynamic disks

Disk Maintenance Tools

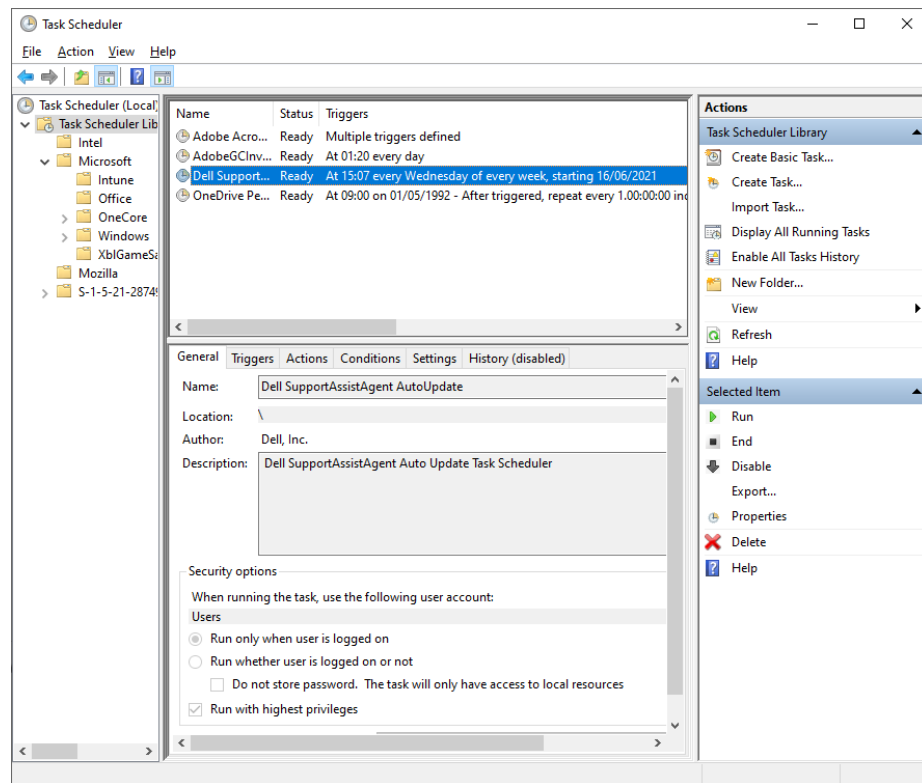
- Disk issues
 - Fragmentation, diminishing capacity, errors
- Defragment and Optimize Drives (dfrgui.exe)
 - Improve read times by reallocating file data locations
 - Hard disk drives (HDDs) versus solid state drives (SSDs)
 - Disk Cleanup (cleanmgr.exe)
 - Identify and remove unwanted file caches



Screenshot courtesy of Microsoft

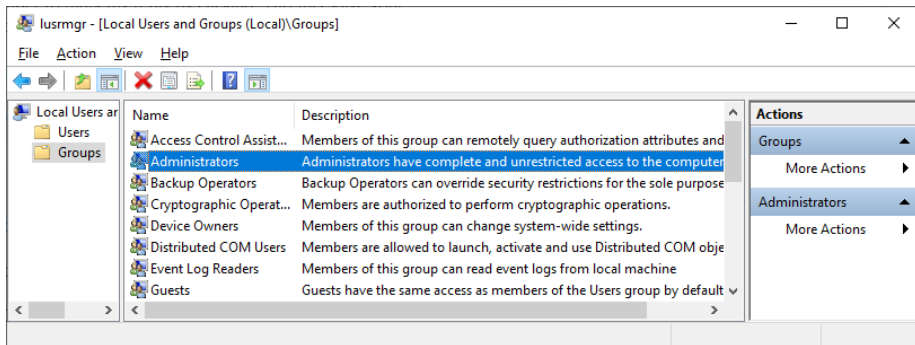
Task Scheduler

- Task Scheduler (tasksch.msc)
- Automate system activity/script
- Run tasks to date/time schedule
- Define custom task triggers
- Set credentials



Screenshot courtesy of Microsoft

Local Users and Groups Console

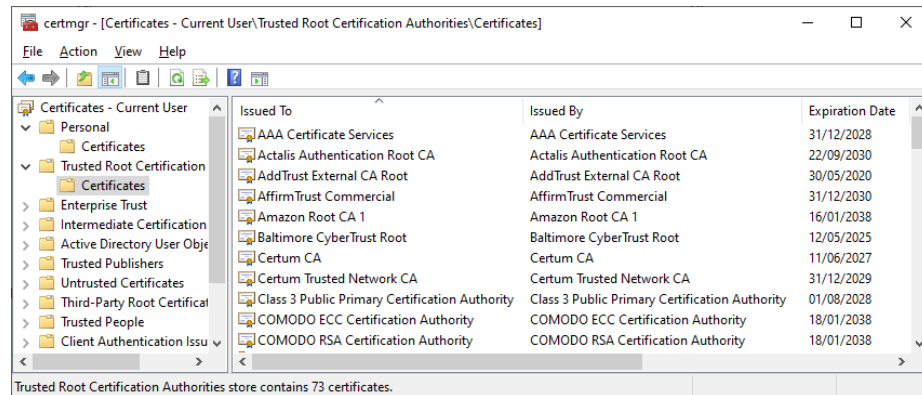


Screenshot courtesy of Microsoft

- Local Users and Groups (lusrmgr.msc)
- User accounts
 - Add, modify and remove
 - Reset password
- Security groups
 - Collection of user accounts
 - Allocate permissions to group
 - User accounts inherit permissions from groups

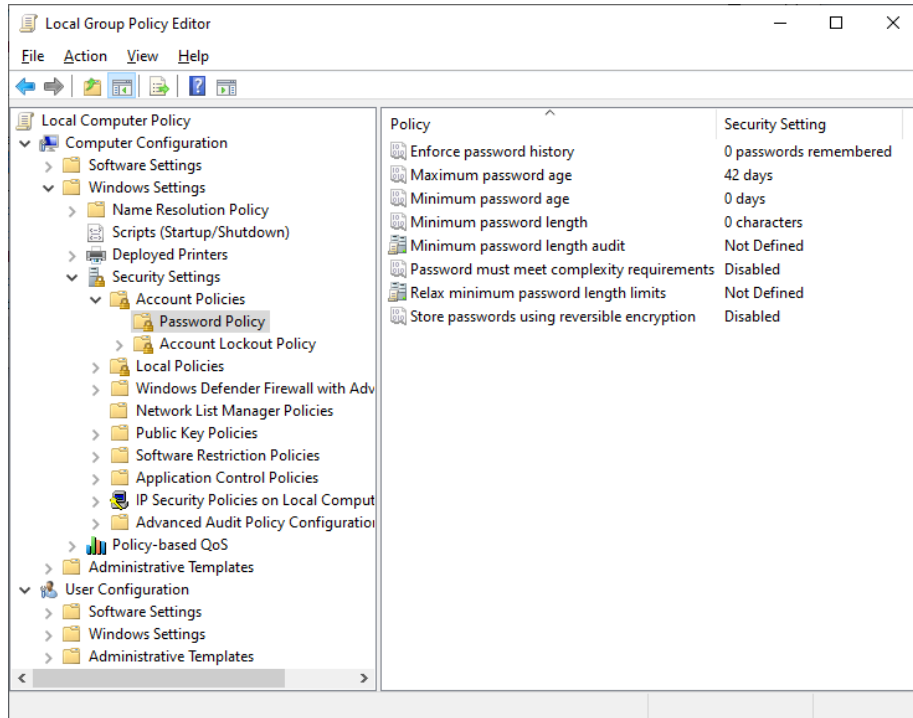
Certificate Manager

- Certificate Manager (certmgr.msc)
- User and computer certificates assert a digital identity
- Root certificates establish trust for certificate authorities (CA)
 - CAs issue user/computer certificates
 - Rogue root certificates are a security risk



Screenshot courtesy of Microsoft

Group Policy Editor

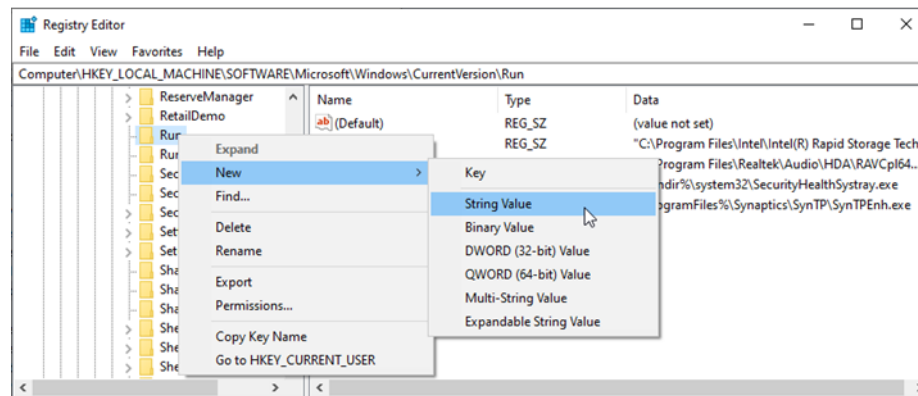
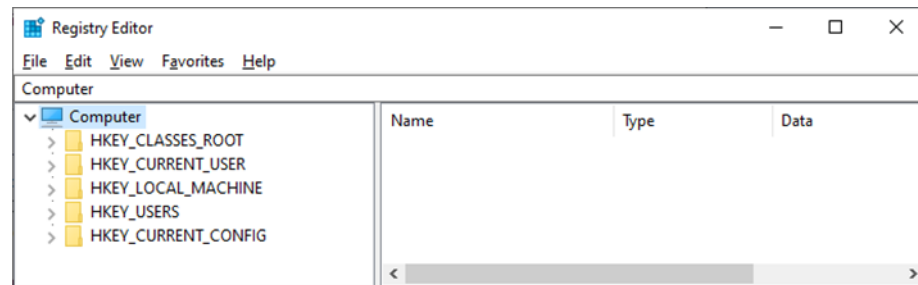


Screenshot courtesy of Microsoft

- Group Policy Editor (gpedit.msc)
- Detailed system and security configuration settings
- Administrative Templates

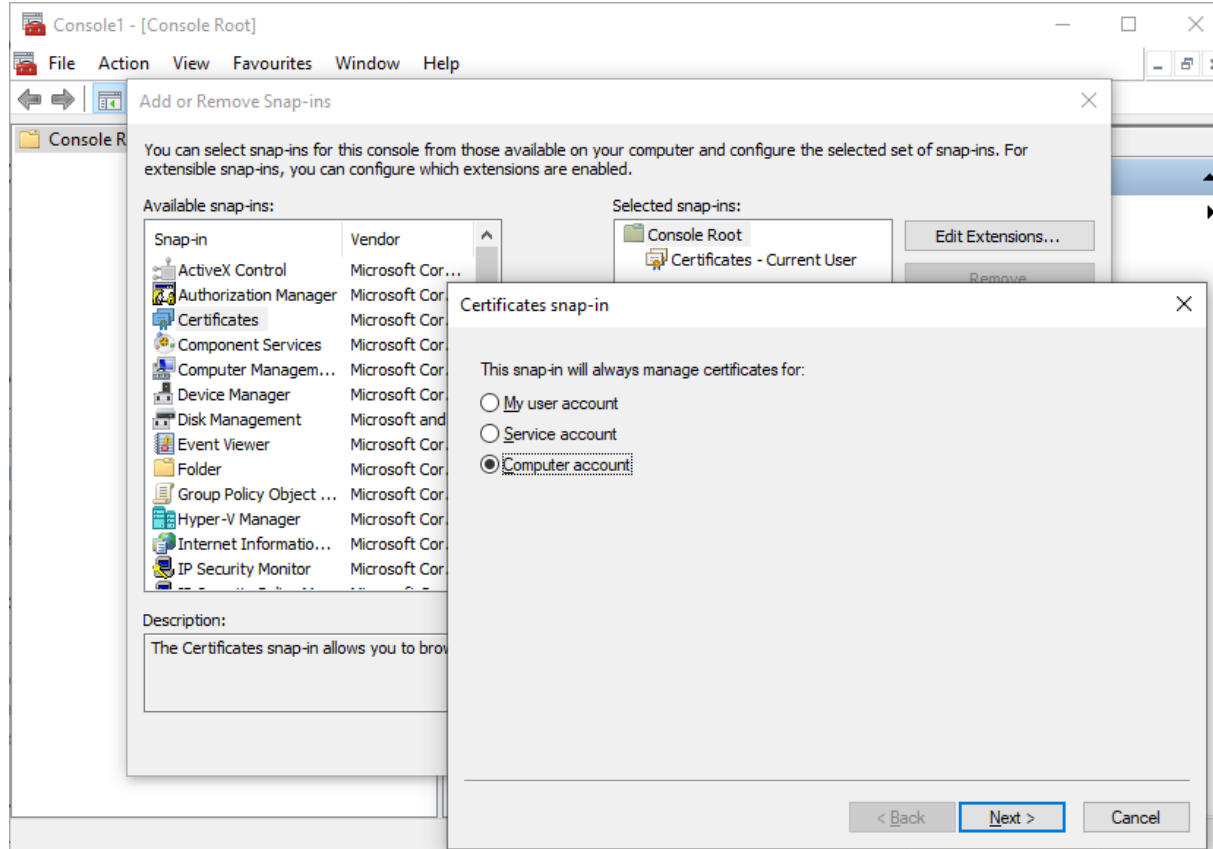
Registry Editor

- Registry Editor (regedit.exe)
 - Direct edits to system configuration database
- Root keys
 - HKEY_LOCAL_MACHINE
 - HKEY_USERS
- Editing the registry
 - Subkeys and value entries
 - Name, data type, value
 - Export and import file formats



Screenshots courtesy of Microsoft

Custom Microsoft Management Consoles



Screenshot courtesy of Microsoft

Review Activity: Management Consoles

- Device Manager
- Disk Management Console and Disk Maintenance Tools
- Task Scheduler
- Local Users and Groups Console
- Certificate Manager
- Group Policy Editor
- Registry Editor
- Custom Microsoft Management Consoles

Lab Activity

- Assisted Lab: Use Management Consoles
 - Create a management console to perform a series of disk, registry, and scheduling administrative tasks

Lesson 11

Topic 11B

Use Performance and Troubleshooting Tools

System Information

The screenshot shows the Windows System Information window. On the left is a tree view with categories like Hardware Resources, Components, and Software Environment. The main area on the right displays a table of system details. The 'OS Name' row is highlighted in blue. At the bottom, there is a search bar and two checkboxes for search options.

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19044 Build 19044
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	COMPTIA-LABS
System Manufacturer	HP
System Model	HP Z240 Tower Workstation
System Type	x64-based PC
System SKU	J9C26EA#ABU
Processor	Intel(R) Xeon(R) CPU E3-1245 v5 @ 3.50GHz, 3501 Mhz, 4 Core(s), 8 Logical Proces...
BIOS Version/Date	HP N51 Ver. 01.82, 28/04/2021
SMBIOS Version	2.7
Embedded Controller Version	5.56
BIOS Mode	UEFI
BaseBoard Manufacturer	HP
BaseBoard Product	802F
BaseBoard Version	
Platform Role	Workstation
Secure Boot State	Off
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume4

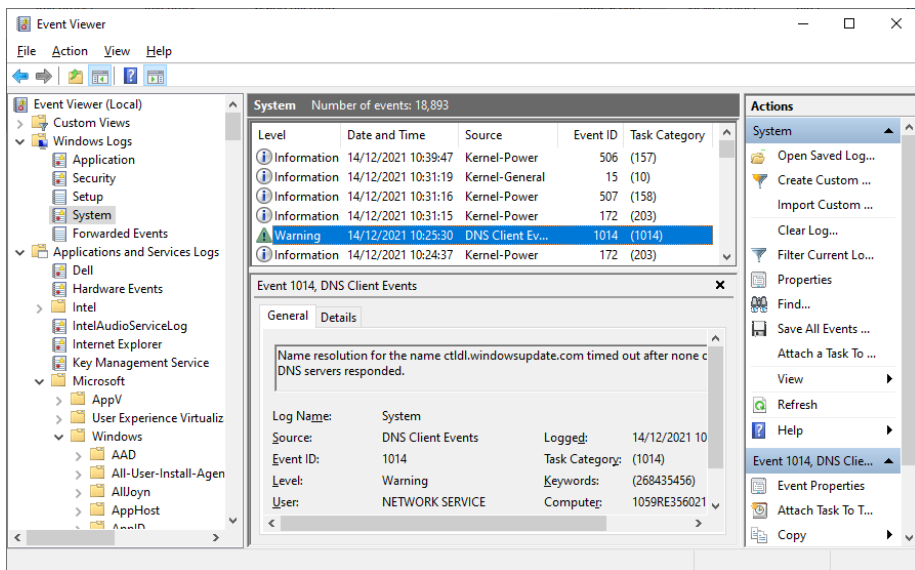
Find what:

☐ Search selected category only ☐ Search category names only

Find Close Find

Screenshot courtesy of Microsoft

Event Viewer

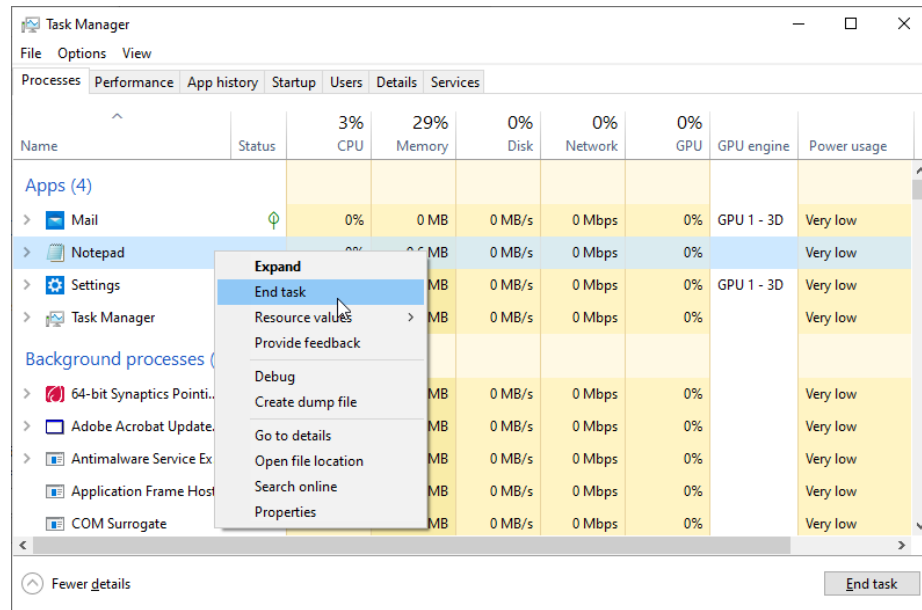


Screenshot courtesy of Microsoft

- Default log files
 - System, security, application, setup
 - Application/service log files
- Event sources and severity levels
 - Source application and ID
 - Critical, error, warning, and information levels
 - Audit success/failure

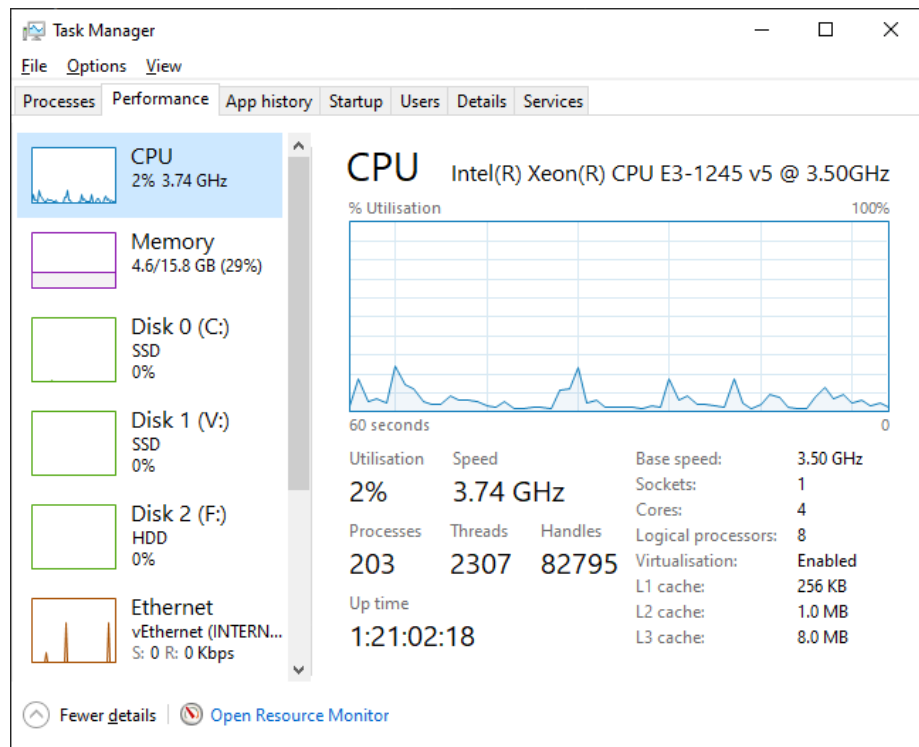
Task Manager Process Monitoring

- Task Manager utility (taskmgr.exe)
 - CTRL+SHIFT+ESC
 - Taskbar shortcut menu
- Processes and Details tabs
 - Manage software loaded into memory



Screenshot courtesy of Microsoft

Task Manager Performance Monitoring

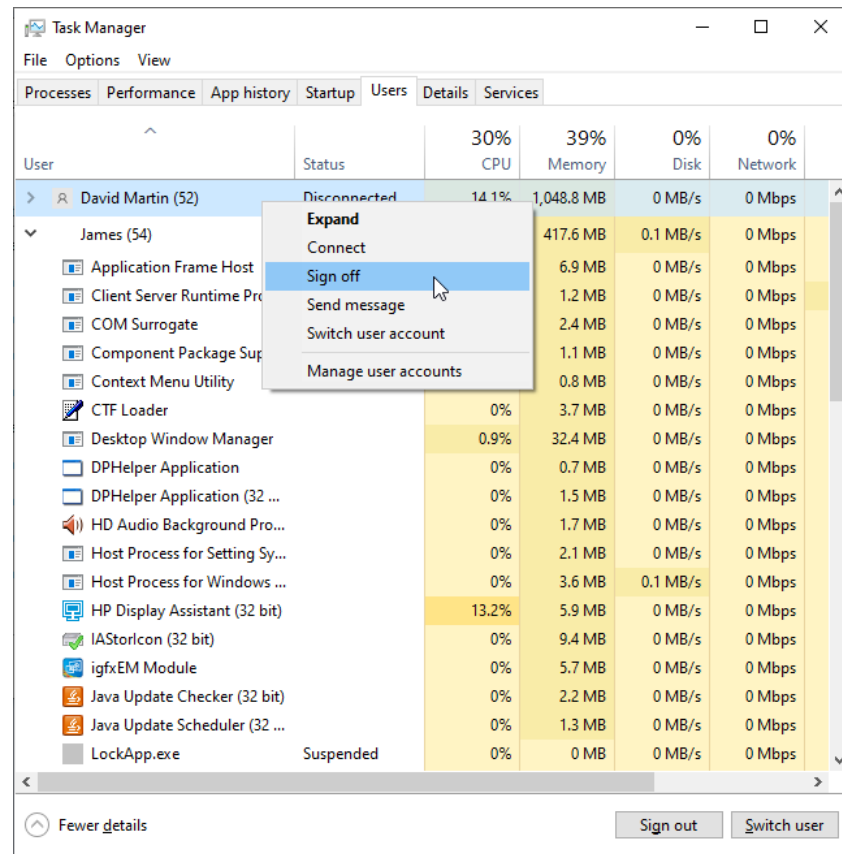


Screenshot courtesy of Microsoft

- Performance and App History tabs
- View current resource utilization
- CPU and graphics processing unit (GPU)
- Memory
- Disks
- Network

Task Manager User Monitoring

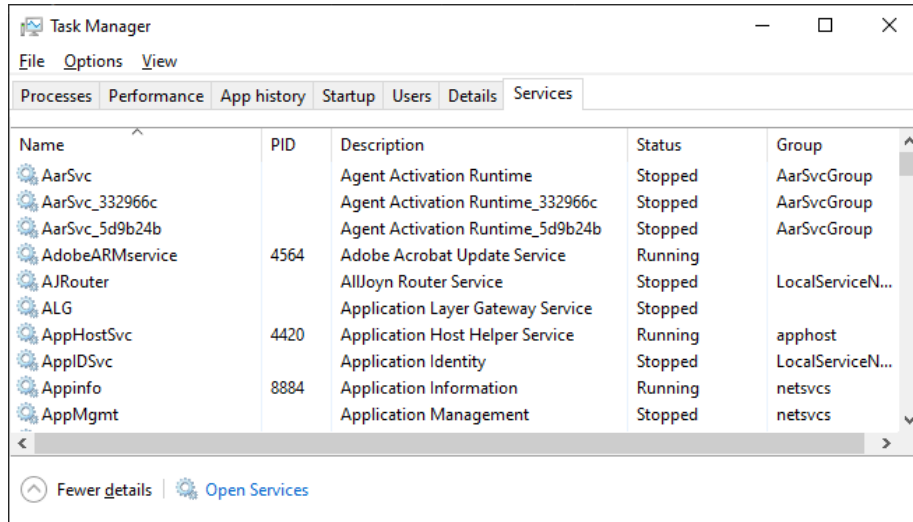
- Users tab
 - Manage logged on accounts



Screenshot courtesy of Microsoft

Startup Processes and Services Console

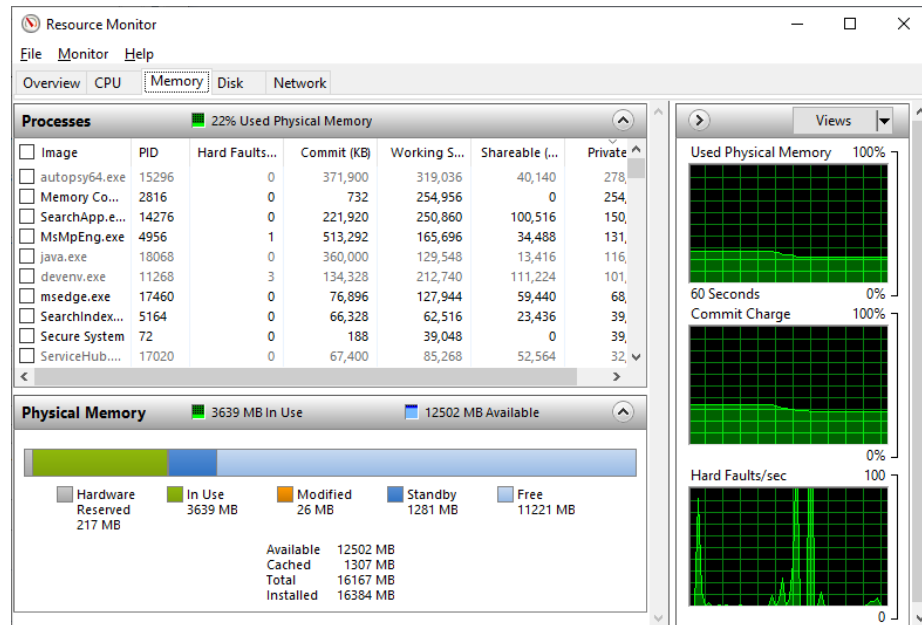
- Task Manager Startup tab
 - View processes that run at startup
- Task Manager Services tab
 - View status of background processes
- Services console (services.msc)



Screenshot courtesy of Microsoft

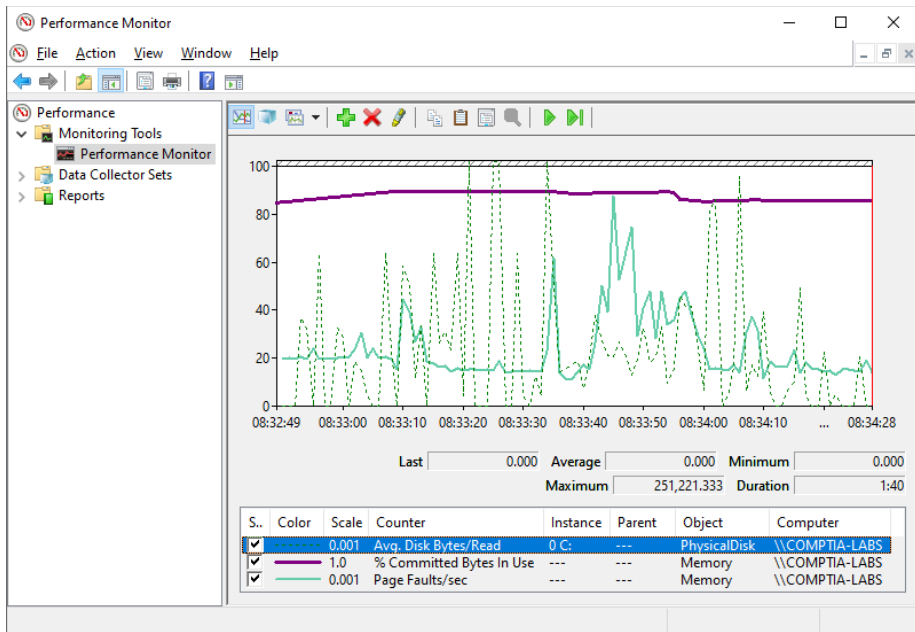
Resource Monitor and Performance Monitor

- Resource Monitor (resmon.msc)
 - More detailed real-time performance data
- Performance Monitor (perfmon.msc)
 - Record performance indicators (counters) over time
 - Run regular reports for comparison
 - Collect event traces



Screenshot courtesy of Microsoft

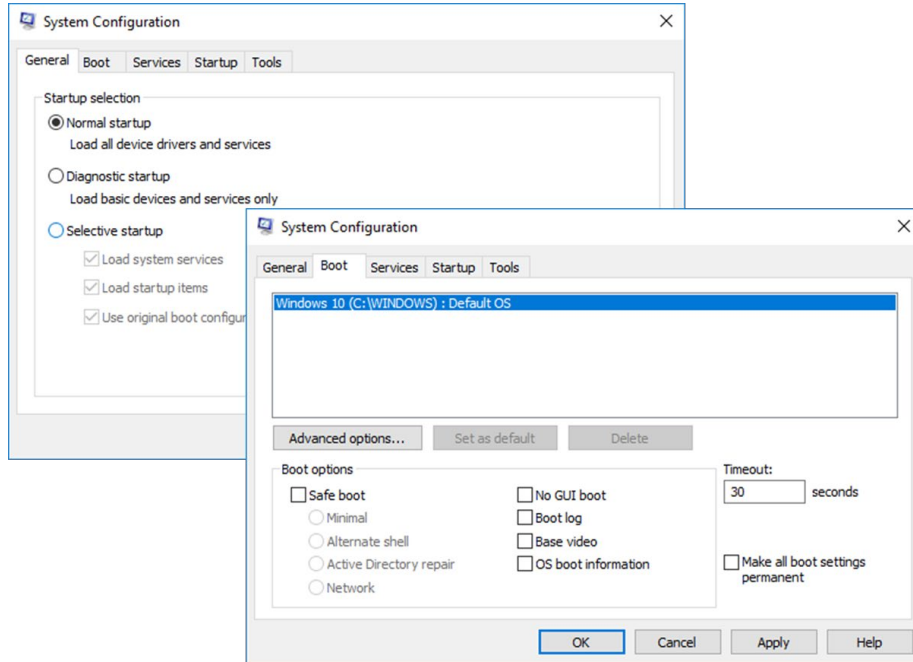
Performance Counters



Screenshot courtesy of Microsoft

- Processor
 - % Processor Time, % Privileged Time, % User Time
- Physical Disk
 - % Disk Time, Average Disk Queue Length
- Memory
 - Available Bytes, Pages/sec
- Paging File
 - % Usage

System Configuration Utility



Screenshot courtesy of Microsoft

- System Configuration Utility (msconfig.exe)
- General tab
 - Select boot mode
- Boot tab
 - Set custom boot parameters
- Services tab
 - View status of background processes
- Tools tab

Review Activity: Performance and Troubleshooting Tools

- System Information
- Event Viewer
- Task Manager Process Monitoring, Performance Monitoring, and User Monitoring
- Startup Processes and Services Console
- Resource Monitor and Performance Monitor
- Performance Counters
- System Configuration Utility

Lab Activity

- Assisted Lab: Use Task Manager
 - Use Task Manager to configure processes, startup items, and services
- Assisted Lab: Monitor Performance and Event Logs
 - Use management tools to investigate potential malware and system performance issues.

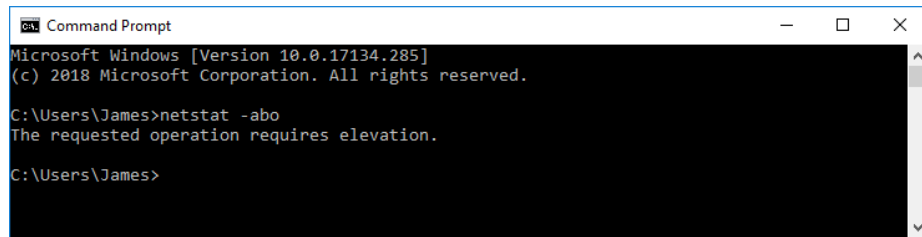
Lesson 11

Topic 11C

Use Command-line Tools

Command Prompt

- Cmd.exe shell
- Run as administrator
- Command syntax
 - Prompt
 - Command name
 - Arguments and switches
- Getting help
 - [command name] /?



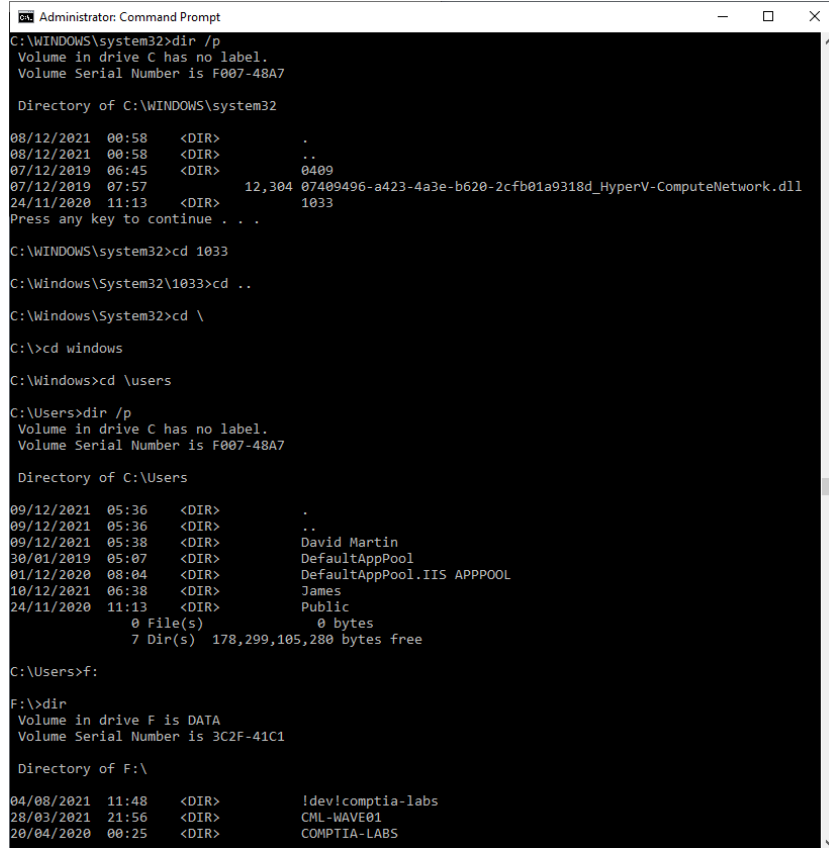
```
Command Prompt
Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\James>netstat -abo
The requested operation requires elevation.

C:\Users\James>
```

Screenshot courtesy of Microsoft

Navigation Commands



```
Administrator: Command Prompt
C:\WINDOWS\system32>dir /p
Volume in drive C has no label.
Volume Serial Number is F007-48A7

Directory of C:\WINDOWS\system32

08/12/2021  00:58  <DIR>          .
08/12/2021  00:58  <DIR>          ..
07/12/2019  06:45  <DIR>          0409
07/12/2019  07:57                12,304  07409496-a423-4a3e-b620-2cfb01a9318d_HyperV-ComputeNetwork.dll
24/11/2020  11:13  <DIR>          1033
Press any key to continue . . .

C:\WINDOWS\system32>cd 1033
C:\Windows\System32\1033>cd ..
C:\Windows\System32>cd \
C:\>cd windows
C:\Windows>cd \users
C:\Users>dir /p
Volume in drive C has no label.
Volume Serial Number is F007-48A7

Directory of C:\Users

09/12/2021  05:36  <DIR>          .
09/12/2021  05:36  <DIR>          ..
09/12/2021  05:38  <DIR>          David Martin
30/01/2019  05:07  <DIR>          DefaultAppPool
01/12/2020  08:04  <DIR>          DefaultAppPool.IIS APPPOOL
10/12/2021  06:38  <DIR>          James
24/11/2020  11:13  <DIR>          Public
               0 File(s)              0 bytes
               7 Dir(s)  178,299,105,280 bytes free

C:\Users>f:
F:\>dir
Volume in drive F is DATA
Volume Serial Number is 3C2F-41C1

Directory of F:\

04/08/2021  11:48  <DIR>          Idev\comptia-labs
28/03/2021  21:56  <DIR>          CML-WAVE01
20/04/2020  00:25  <DIR>          COMPTIA-LABS
```

Screenshot courtesy of Microsoft

- Prompt and working directory
- List directory contents
 - `dir`
- Change directory
 - `cd xxxx`
 - `cd ..`
 - `cd \`
- Drive navigation
 - `C:`
 - `D:`

File Management Commands

- Move and copy files
 - copy
 - xcopy
 - robocopy
- Creating a directory
 - md
- Removing a directory
 - rd
 - rd /s

Disk Management Commands

```
Administrator: Command Prompt - diskpart
DISKPART> select disk 0
Disk 0 is now the selected disk.
DISKPART> detail disk
NVMe SAMSUNG MZVPV512
Disk ID: {5956221B-3300-452F-B899-2B6CF427BD10}
Type : NVMe
Status : Online
Path : 0
Target : 0
LUN ID : 0
Location Path : PCIRoot(0)#PCI(1B00)#PCI(0000)#NVME(P00T00L00)
Current Read-only State : No
Read-only : No
Boot Disk : Yes
Pagefile Disk : Yes
Hibernation File Disk : No
Crashdump Disk : Yes
Clustered Disk : No

Volume ### Ltr Label Fs Type Size Status Info
-----
Volume 1 C NTFS Partition 475 GB Healthy Boot
Volume 2 Recovery NTFS Partition 450 MB Healthy Hidden
Volume 3 FAT32 Partition 100 MB Healthy System
Volume 4 NTFS Partition 908 MB Healthy Hidden

DISKPART> select volume 1
Volume 1 is the selected volume.
DISKPART> detail volume
Disk ### Status Size Free Dyn Gpt
-----
* Disk 0 Online 476 GB 1024 KB *

Read-only : No
Hidden : No
No Default Drive Letter: No
Shadow Copy : No
Offline : No
BitLocker Encrypted : No
Installable : Yes

Volume Capacity : 475 GB
Volume Free Space : 166 GB

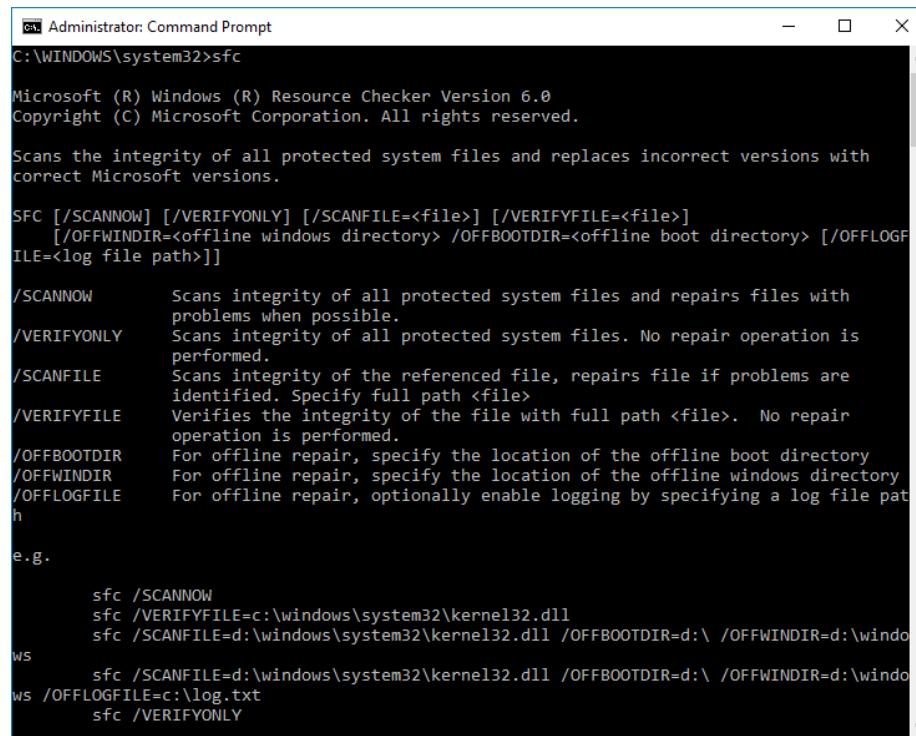
DISKPART>
```

Screenshot courtesy of Microsoft

- Manage partitions and file systems
 - diskpart
- Write a new file system to a drive
 - format
- Scan disk for unusable sectors
 - chkdsk

System Management Commands

- Shut down and restart the computer
 - shutdown
- Scan for damaged or missing system files
 - sfc
- Report Windows version and build
 - winver



```
Administrator: Command Prompt
C:\WINDOWS\system32>sfc

Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (C) Microsoft Corporation. All rights reserved.

Scans the integrity of all protected system files and replaces incorrect versions with
correct Microsoft versions.

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

/SCANNOW           Scans integrity of all protected system files and repairs files with
                   problems when possible.
/VERIFYONLY        Scans integrity of all protected system files. No repair operation is
                   performed.
/SCANFILE          Scans integrity of the referenced file, repairs file if problems are
                   identified. Specify full path <file>
/VERIFYFILE        Verifies the integrity of the file with full path <file>. No repair
                   operation is performed.
/OFFBOOTDIR        For offline repair, specify the location of the offline boot directory
/OFFWINDIR         For offline repair, specify the location of the offline windows directory
/OFFLOGFILE        For offline repair, optionally enable logging by specifying a log file path

e.g.

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
```

Screenshot courtesy of Microsoft

Review Activity: Command-line Tools

- Command Prompt
- Navigation Commands
- File Management Commands
- Disk Management Commands
- System Management Commands

Lab Activity

- Assisted Lab: Use Command-line Tools
 - Use the cd, dir, md, copy, del, robocopy and shutdown utilities.
- APPLIED Lab: Support Windows 10
 - Work independently to create a management console to perform a series of disk, registry, and scheduling administrative tasks

CompTIA A+ Core 2 Exam 220-1102

Lesson 11



Summary