Chapter 14

Maintaining and Optimizing Operating Systems

Episode 14.01

Episode title: **Maintaining Windows**

Objective: Software updates are crucial to maintaining a healthy system. An unpatched system can spell disaster to a network. Although Windows has made their update process relatively hands-free, there are still some things to take note of.

Lower 3rds

OBJ - Patch management

OBJ - OS updates

OBJ - Application updates

Software updates are crucial to maintaining a healthy system

An update is a patch, fix, or correction to an existing Windows edition

Patch management involves the identification and application of software updates

At End of Life (EOL) all support is ceased

Lower 3rds

Upgrade is moving from one version of Windows to another

Patch management

Security updates

Windows Update

Delivery optimization

OS update failure

Lower 3rds

0x80070002 ERROR_FILE_NOT_FOUND

0x8007000D ERROR_INVALID_DATA

0x80070057 ERROR_INVALID_PARAMETER

0x80092003 CRYPT_E_FILE_ERROR

DISM in PowerShell

End of life or EOL

Patch Management

Involves the identification and application of software updates on devices, which can include

- servers
- workstations
- standalone PCs
- mobile devices
- many peripheral devices

Patch Management

A patch is one or more changes to existing software

In most cases, patches correct:

- known errors
- vulnerabilities
- flaws in the software

Patches can also include new features

OS Update Failure

We can’t demonstrate an OS update failure, but each failure notice message has an error code associated with it

OS Update Failure

0x80070002 ERROR_FILE_NOT_FOUND	0x8007000D ERROR_INVALID_DATA	0x80070057 ERROR_INVALID_PARAMETER	0x80092003 CRYPT_E_FILE_ERROR An I/O
A specified file can't be found	A vital data field has an invalid value	A parameter in the update is incorrect	Error occurred when Windows Update reads or writes to a file

End of Life (EOL)

Not an update issue, but application could lead to a possible upgrade

Creator will notify its users that a product will be EOL at a future date.

After that date, the provider will cease all support:

- No new releases
- No updates
- No upgrades

Episode 14.02

Episode title: **Maintaining macOS**

Objective: In this episode, Steve enlists the help of Michael "Mac Maniac" Smyer, who walks us through how easy it is to maintain the macOS and its applications. Michael also discusses how to customize login items and the different types of application files.

Lower 3rds

Apple periodically makes updates to the macOS operating system that can include updates to system functions, system folders, apps, and security processes.

The Software Update app checks for updates or new software automatically.

Lower 3rds

DMG file or a disk image file

A PKG or package file could be inside a DMG file or downloaded directly

Apps download from the Apple Store have an APP extension

Apps downloaded and installed from the Internet or a disk can be removed

Lower 3rds

MacOS hides system folders to protect them from being accidently deleted or altered

DMG file or a disk image file

a PKG or package file, which could be what you find inside a DMG file or downloaded directly

Lower 3rds

Apps download from the Apple Store and those installed from a DMG or PKG file, will have an APP extension

Apps that have been downloaded and installed from the Internet or a disk can be removed

Lower 3rds

MacOS hides its system folders to protect them from being accidently deleted or altered.

/Applications

/Users

/Library

/System

Lower 3rds

/Users/Library

apply the XProtect app

Rapid Security Resources or RSRs

Episode 14.03

Episode title: **Maintaining Linux**

Objective: While Windows is a one-size-fits-all product, Linux is quite different. The whole concept behind Linux is an almost total control over the environment. However, this control brings with it a massive amount of responsibility for patch and application management of the OS.

Lower 3rds

OBJ - apt

OBJ - dnf

It's important to keep a Linux system updated

The common way to update a Linux system is from the command line interface

The commands to update a Linux system from the CLI are apt and dnf

The sources.list is used to indicate what is to be updated.

The command sudo apt-get upgrade gathers the updates available

On Linux distros based on Red Hat, the dnf command is the package manager

Lower 3rds

Process initiated by the update command /etc/apt/sources.list

Commands Used to Update a Linux system

```
kali@kali:~$ grep -v '#' /etc/apt/sources.list | sort -u
deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

Debian-based package management system (*deb*)

There are four:

- Main
- Contrib
- non-free
- non-free-firmware

Commands Used to Update a Linux System

Commands Used to Update a Linux system

sources.list file indicates what is to be updated

```
 /etc/apt $sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.5 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [120 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 74.1 MB in 7s (10.7 MB/s)
896 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Command sudo apt-get upgrade

```
  tumbler-common tzdata tzdata-legacy ucf udev udisks2 unzip upower us
  va-driver-all vim vim-common vim-runtime vim-tiny vpnc wamerican wge
  x11-xserver-utils xauth xcvt xdg-desktop-portal-gtk xdg-user-dirs xd
  xfce4-notifyd xfce4-panel-profiles xfce4-power-manager xfce4-power-m
  xfce4-taskmanager xfce4-timer-plugin xfce4-whiskermenu-plugin xfce4-
  xserver-common xserver-xorg xserver-xorg-core xserver-xorg-legacy xt
  zsh-syntax-highlighting zstd
764 upgraded, 0 newly installed, 0 to remove and 132 not upgraded.
Need to get 505 MB of archives.
After this operation, 23.9 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Episode 14.04

Episode title: **Working with Applications**

Objective: It's important to consider hardware requirements and impact to your device, network, and operation before installing any applications. This episode covers these requirements, as well as some tips for using and troubleshooting applications.

Lower 3rds

OBJ - 32-bit vs. 64-bit dependent application requirements

OBJ - Dedicated vs. integrated graphics card

OBJ - Video Random-access Memory (VRAM) requirements

OBJ - RAM requirements

OBJ - Central processing unit (CPU) requirements

OBJ - External hardware tokens

Time-based One-time Passwords (TOTP)

USB security tokens

Challenge-response tokens

Smart cards

Biometric hardware tokens

Bluetooth tokens

Lower 3rds

OBJ - Storage requirements

Virtually all application software lists the minimum amount of data storage it requires

OBJ - Application to OS compatibility

Application executables

Libraries

Configurations

Documentation

system image

OBJ - Physical media vs. mountable ISO file

OBJ - Downloadable package

OBJ - Image deployment

Lower 3rds

OBJ - Device

OBJ - Network

OBJ - Operation

OBJ – Business

VRAM is memory specifically for dedicated GPUs

Application software packaging, information sheets, or websites lists the hardware and system requirements it needs to perform correctly and effectively

Application software is retrieved or acquired in some form of a distribution

There are potential impacts to consider before installing an application

Lower 3rds

OBJ - Device

OBJ - Network

OBJ - Operation

OBJ – Business

VRAM is memory specifically for dedicated GPUs

Application software packaging, information sheets, or websites lists the hardware and system requirements it needs to perform correctly and effectively

Application software is retrieved or acquired in some form of a distribution

There are potential impacts to consider before installing an application

32-bit vs. 64-bit application requirements

32-bit application will run on a 64-bit system, but a 64-bit system cannot run on a 32-bit system

Dedicated vs. integrated graphics card

Some apps need high graphics and require a dedicated GPU

- games
- video editing

Others, work fine with integrated graphics

- browsers
- word processors

Video random-access memory (VRAM) requirements

VRAM stores the data that forms a graphic, including

- textures, frame buffers, and other visual data

which supports the GPU accessing and processing the data efficiently

Typically applications requiring VRAM will require from 4GB to 16GB

RAM requirements

The RAM requirements of an application are specifically referring to main memory

Central processing unit (CPU) requirements

Requirements typically include:

- Manufacturer (AMD or Intel)
- Architecture (x86 or x64)
- processor cores
- perhaps even a clock speed

External hardware tokens

Hardware tokens improve the security of an application by adding an external or physical layer to the authentication of users

Application and operating system compatibility

MacOS applications won't install and run on a Windows system, and *vice versa*

Episode 14.05

Episode title: **Backing Up Your Data in Windows**

Objective: Windows has provided many different tools over the years to enable techs (and users) to back up important files. A good tech knows these Windows tools to help their users recover data when things go wrong.

Lower 3rds

- OBJ - Backup
  - OBJ – Full - backup of everything
  - OBJ – Incremental - only backups changes from the last backup of any type
  - OBJ – Differential - backup all changes from the last full backup
  - OBJ - Synthetic full - Combines last full back up with incremental backups
- OBJ - Recovery
  - OBJ - In-place/overwrite
  - OBJ - Alternative location
- OBJ - Backup testing
  - OBJ - Frequency
- OBJ - Backup rotation schemes
  - OBJ - Onsite vs. offsite
  - OBJ - Grandfather-father-son (GFS)
- OBJ - 3-2-1 backup rule

Lower 3rds

Regularly scheduled backups and setting system restore points are absolutely critical

First-In-First-Out (FIFO)

Grandfather, father and son

3-2-1 backup rule - 3 backup copies on 2 media forms and at least one off-site

Synthetic full backups combine the last full back up with incremental backups to create a full backup that is up to date

In-place recovery restores data from storage device on the same system or network

Overwrite recovery can restore an overwritten folder or file(s)

Backup

Types of backups:

- Full
- Incremental
- Differential
- Synthetic backup

Synthetic backup creates full backup that is always up to date

Recovery

In-place recovery:

- Restore data from an attached storage device on the same system or network

Overwrite recovery:

- restore an overwritten volume, folder, or file(s) from a backup

Backup Testing

- Is the data really on the backup media?
- Can the backup media be restored?
- Will the restoration process meet the time to recover requirements of the disaster recovery plan?

Regular testing procedure should be conducted to answer these questions

3-2-1 Backup Rule

What that means:

- 3 backup copies
- 2 media forms
- One off-site in the cloud

Episode 14.06

Episode title: **Backing Up Your Data in Linux and macOS**

Objective: Backing up data in Linux and macOS follows the same best practices as Windows, with a few different tools.

Lower 3rds

OBJ – Backups

The tool usually used to make a backup from the command line is the tar command

Time Machine is a built-in backup app on a Mac

To back up a MAC system, Time Machine is the most common method

grandfather/father/son or a 3-2-1 backup plan

Two tar Commands

$tar cvf /dev/rmt/0 * :

- Create
- Verbose
- Directory
- File
- Archive device

$tar cvf /home/backup * :

- Create
- Verbose
- Location in home directory

Time Machine

Built-in backup app on a Mac:

- Creates backups on external USB or other storage devices
  - SSD drive