Ocean Graham

Abstract

[Draw your reader in with an engaging abstract. It is typically a short summary of the document.   
When you’re ready to add your content, just click here and start typing.]

401IT – Operating Systems

[Assignment Title]



Table of Contents

[Table of Figures 1](#_Toc202859948)

[Introduction 2](#_Toc202859949)

[Operational Management of Operating Systems 2](#_Toc202859950)

[Process and service management 2](#_Toc202859951)

[file systems 7](#_Toc202859952)

[user accounts and access control 7](#_Toc202859953)

[memory management 7](#_Toc202859954)

[Security risks and management strategies 8](#_Toc202859955)

[OS vulnerabilities 8](#_Toc202859956)

[management strategies 8](#_Toc202859957)

[References 8](#_Toc202859958)

# Table of Figures

401IT – Operating Systems

# Introduction

In this coursework the author will demonstrate a high degree of understanding of operating systems and a critical analysis of the various operational aspects. This report will evaluate different aspects in relation to different operating systems, these being Linux, Windows and Windows Server.

# Operational Management of Operating Systems

## Process and service management

There are two types of functions that run on a computer, these being ‘Processes’ and ‘Services’. We first must identify the definition and differences between these two to understand how they are managed.

A Process is a program that requires initiation manually and is unnecessary to the function of the system. See Appendix 1 for more details about how processes work.

Processes may vary on the different operating systems but some examples for the different systems may be:

Linux –

* bash (command line)
* python (python script runner)
* vim (text editor)
* Search Engines

A screenshot of a computer program

AI-generated content may be incorrect.

Figure – Linux Task Manager – Processes

On Linux, commands are used such as ‘kill’ to terminate a process using its PID, and others such as ‘ps’, ‘top’ ‘htop’ and ‘systemctl’ to manage processes and services.

Windows –

* Windows Explorer (file explorer)
* Command Prompt (command line)
* Virtual Studio Code (script editor and runner)
* Word (text editor)
* Search Engines

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Windows Task Manager – Processes

On Windows, the language differs to Linux however the same actions can be performed. ‘taskkill’ is used to terminate a process with its PID, other commands which help manage the process and services include ‘tasklist’, ‘net start’ and ‘sc query’.

A service is a background process that performs necessary functions, managing hardware, all without user interaction. Services initiate automatically with the startup of the operating system. These manage many things such as:

* Program Execution
* Input/Output Operations
* Memory Management
* Process Management
* File System Manipulation

(*Operating System - Services - Tutorialspoint*, 2019)

Examples of Services include:

* Print Spooler
* Radio Management Services
* Windows Update Services (Windows)
* Apache2 (Linux)

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Windows Services Page and Print Spooler Service

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Windows Server Service Page

Processes and Services can be handled and managed using both Graphical User Interfaces (GUI) and Command-Line Interfaces (CLI). The 3 prior figures provide examples of GUI management of the functions. These two interfaces provide different strengths and weaknesses in use, the GUI providing easier user experience and effects to make it easier to navigate, whilst CLI is rawer and more direct. It is much more efficient and faster than the GUI and requires less resources (Marijan, 2023). The speed of the CLI gives value to admin users for troubleshooting.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure – Windows CLI showing running processes

A computer screen shot of white text

AI-generated content may be incorrect.

Figure – Windows CLI showing service information

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Linux CLI showing service information

Figure x, x and x show the CLI and how they may be used to find and look at process and service information in an alternative way to the GUI.

## file systems

A file system is a logical and physical system for organising, managing and accessing the files and directories on a devices storage media (Sullivan, 2018). Without a file system the system would have large amounts of data without any organisation or distinguishment. File systems between different OS have different approaches to file storage and therefore different architectures.

### Linux

Linux uses a file system designed specifically for Linux in 1992. The Extended File System has multiple iterations, but currently is on its 4th iteration EXT4. See Appendix 2 for more information on the EXT system.

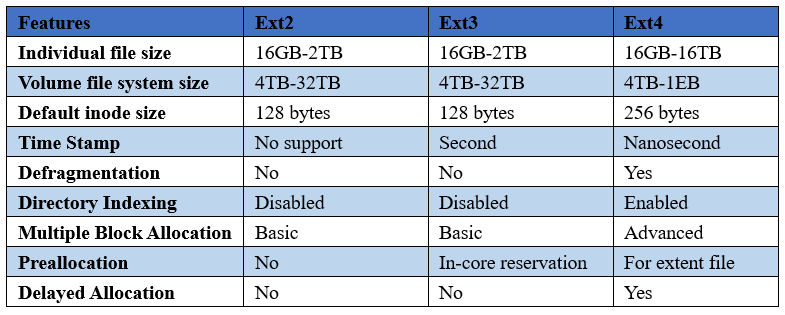


Figure – Comparison of iterations of EXT (*Partition Wizard,* 2021)

In Linux files and folders can be created simply with GUI with a click of the specific icon.

A black background with white text

AI-generated content may be incorrect.

Figure – Linux GUI File/Folder creation

Files and Folders can be created in the CLI with the ‘mkdir’ and ‘touch’ commands. And removed with the ‘rm’ and ‘rmdir’ commands, to enter or exit into a directory ‘cd’ command is used. To rename a file the ‘mv (file name) (new name)’ is used.

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Linux CLI File/Folder creation

### Windows and Windows Server

Windows uses multiple different systems, the File Allocation Table (FAT) and New Technology File System (NTFS).

FAT is an essential part of the file system which tracks where files are stored on a disk and works best for external media such as USB (Chakraborty, 2023). See Appendix 2.1 for details on FAT

NTFS is the default file system for Windows drives. NTFS provides reliability and security. See Appendix 2.2 for details on how NTFS improves reliability and security

Windows Server uses Resilient File System (ReFS). The ReFS system is designed to maximise data availability, handle large loads of data, and hold resilience against corruption. See Appendix 2.3 to see how ReFS is tailored to these features.

A screenshot of a computer

AI-generated content may be incorrect.

Figure Windows GUI File/Folder creation

Windows and Windows Server follow the same systems for creation, these two systems differ from Linux both in GUI and CLI. To make a directory it is the same as Linux ‘mkdir’, to make a file ‘echo’ is used, to delete a directory ‘rmdir’ is used, ‘del’ is used to delete a file. ‘cd’ is still used to move between directories.

A computer screen shot of a computer program

AI-generated content may be incorrect.

Figure – Windows CLI Folder/File creation

Microsoft and Linux hold many differences between the two file systems. Windows hold files on different drives/partitions such as C: and D: drives which acts to separate and segment groups of files. On the other hand, Linux works on a root directory, having all files branching out in a hierarchical tree structure. Windows views different items as devices or files whereas Linux view everything as a file (Whittaker, 2025). The systems used NTFS and EXT4 have major differences in compatibility, NTFS primarily being connected to Windows systems, contrast this to EXT4 which is open source meaning it can change source codes whilst the Windows systems lack this feature. NTFS is not case sensitive and cannot have duplicate folders, EXT4 being the opposite, this could be seen both positively or negatively depending on perspective, potentially affecting cohesion, but some may appreciate the specificity of case sensitivity. Conclusively, Linux and Windows are both high-performing with the different systems and it depends on the requirements of a person or organisation which OS better fits.

## user accounts and access control

A user account is a digital object created for a group or singular entity to access resources based on the account permissions assigned to that/those entities and restrict/deny access to settings or functions that may affect an organisations or systems integrity. See appendix 3 to see how user accounts improve security and resource management.

Access Control is used as the means in which user access is controlled for the 3 systems discussed. Two types of Access Control will be discussed that can be utilised in systems: Access Control Lists (ACL) and Role-Based Access Control (RBAC).  ACL is a table that lists permissions connected to a resource, telling the OS what a user may do and access, each user has an entry. RBAC, restricts access to a role which multiple users may be assigned to. The difference between ACL and RBAC is the prior is better fit for implementing security and restriction at a individual level with more granularity than RBAC, whilst RBAC is better for more wide-spread use and scalability.

Linux has 3 permission categories: Owner, Group, Others, for each directory/file. These each having 3 permission levels being read, write and execute and is calculated via the use of symbols which correlate to a numerical value, for example –‘rwxr-xr-x’ means 755, each of the 3 numbers meaning a user type, 7 meaning owner who has read write and execute privileges, and 5 for the group and others, who can only read and write, the first – indicates the file type ( - for file)

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Linux permissions

Windows has 3 types of users as well, being Admins (full control) Standard User (limited) and Guest (temporary access). However unlike Linux, Windows has 5 permission levels being Full Control (Perform any action to a file or folder, including modifying permissions), Modify (create new files and folders and modify and delete existing files and folders), Read and Execute (allows user to view contents of a file or folder and execute files), List Folder Contents  (allows user to view contents of a folder) and finally ‘Read’  (view contents of a file or folder)

A screenshot of a computer

AI-generated content may be incorrect.

Figure – Windows permissions

Windows server works in nearly the exact same way given both windows and windows server work on Microsoft’s framework, however it holds the addition of Special Permissions (offers a more granular “advanced’ permissions that allow more in depth access rights beyond the basic level) (*Understanding File and Folder Permissions in Windows | Dell UK*, n.d.)

## memory management

“In the realm of computing, memory management is essential for enhancing OS performance and ensuring efficient resource utilization.” (Jalaman & Teleron, 2024). Memory Management is the process of controlling how a computers memory is used and allocated. This topic consists of a group of key concepts and principles, all which have significance to memory management. First, the principles of memory management include protection against memory loss/high memory usage, logical and physical organisation, allocation and deallocation and to proper utilisation and tracking of memory. Next, we must understand there are three types of memory (hiruthicSha, 2025):

1. Resident Memory - which is physical memory in physical RAM.
2. Virtual Memory - which is address space allocated to a process. It temporarily uses the hard drive to store data (Huculak, 2022)
3. Shared Memory – Memory shared between processes. Multiple processes access the same memory block (Bansal, 2023).

there are two types of memory allocations being static and dynamic, examples of such are ‘stack’ and ‘heap’ respectively. There are major differences in purpose to these two aspects which can be seen in Appendix 4

There are multiple processes which are essential to memory management such as Addressing, Swapping and Buffers. Information on the different processes can be found in Appendix 4.1

Linux and Windows both have many similarities handling Memory Management but have different tweaks and ways of going about certain subjects. Windows sharing memory between kernel and user more evenly compared to Linux which gives more memory to the user. Windows virtual memory existing as a single physical hidden file on the hard disk ‘pagefile.sys’. Linux extracts the details of physical memory from the application software, meaning it uses multiple distinct address ranges, the physical system memory being divided into pages. (*Concepts Overview — the Linux Kernel Documentation*, n.d.). The two OS also map memory in different ways, windows using ‘VirtualAlloc’ whilst Linux uses ‘nmap’. Linux overall focuses on efficiency and page replacement being flexible and dynamic. whilst Windows has a more user friendly approach, resulting in a more rigid management system. This difference can be expected due to Linux’s open source nature whilst Windows acts more as a commercial product.

# Security risks and management strategies

## OS vulnerabilities

As with all systems, Linux, Windows and Windows Server hold vulnerabilities which leave them susceptible to damage from internal sources or external attacks.

## management strategies

[Linux vs. Windows: Cybersecurity Comparison - Blue Goat Cyber](https://bluegoatcyber.com/blog/linux-vs-windows-a-security-comparison/)

# References

# Appendix 1

Processes are made of attributes to help the OS manage and control it. These being stored in the Process Control Block (PCB). The PCB stores these attributes:

1. Process States
2. Process ID
3. Priority levels
4. Input Output Information
5. File Descriptors
6. Account Information
7. Memory Management Information

(GeeksforGeeks, 2024)

The PCB help the system share resources more effectively, it also allows the system to isolate processes, meaning ‘one process doesn’t inadvertently interfere with another’. (Vaishnav, 2022)

# Appendix 2

The EXT4 iteration improves file and volume storage and contain other features such as Defragmentation and Journaling. On the other hand, EXT4 requires more disk usage compared to the older versions however this is to be expected with its higher complexity.

# Appendix 2.1

There are two versions used primarily now, being FAT32 and extended FAT (exFAT), FAT32 works on a 32-bit system and is still in primary use having the benefit of compatibility with most current OS, however lacks the scalability today, not being able to store files over 4GB, exFAT resolves this problem, working on a 64-bit system and having a file limit of 16EB.

# Appendix 2.2

NTFS a recoverable file system that logs transactions against the file system, allowing the system to recall to the last commit point to “recover consistency within the system” (Deland-Han, 2021), this vastly reducing the threat of disk/file corruption. NTFS supports the Windows security model and multiple data streams, this allows concurrent processing. The Windows security model provides protection with concepts such as privilege roles, ACL and SIDs, this meaning unauthorised access cannot affect system-related operations. Finally, NTFS removes the limitations of file size, being able to store files up to 16EB. (*Windows Security Model*, 2024)

# Appendix 2.3

ReFS holds salvaging capabilities in threat of corruptions with an alternate copy of the corrupted data, as well as this it uses Proactive error corruption which uses a ‘scrubber’ which scans for latent corruption and triggers repair before it becomes a larger issue. NTFS uses Mirror-accelerated parity which helps deliver high performance and storage.

# Appendix 3

User accounts hold significance in system security according to (National Cyber Security Centre, *Principle 9*, n.d.): user accounts should help authorise access to data and services, as well as make sure customers (however this can be anyone that doesn’t have the correct authority) cannot modify or affect service configuration. Without User management systems, managing user access rights would be highly demanding in time and resources. (Gilad Maayan, 2024).

User access helps in resource management, administrators able to provide different users more/less resources respectively depending on the privilege roles. Higher roles requiring more resources such as files, applications and specific functions. (*Frontegg*, 2025)

# Appendix 4

Static memory works to allocate memory during the compilation process before a program starts running, whilst dynamic begins allocation during the execution of a program functions. (*Florida State University, n.d.*). Stack memory stores temporary variables created by a function, these variables being declared stored and initialised in run time (GeeksforGeeks, 2022). Advantages of this are that it is not easily corrupted and allows you to control the memory allocated and deallocated, this deallocation is also automatically done adding efficiency and reduction in time demands. However, with these benefits stack is very limited and too many objects may lead to a stack overflow (a type of buffer error).

Heap memory is blocks of memory allocated to each program that may be running. This process is dynamic and as a result segments may be requested when a program needs it. This memory can be accessed and altered wherever in the program it is assigned; it is not localised. (GeeksforGeeks, 2022) The benefits of this is that it doesn’t have any limitations to size, as well as this it allows access globally. On the other hand, it takes more time than the stack to execute, and due to its limitless memory, it may take all the memory an OS can offer which may affect other processes running.

# Appendix 4.1

**Addressing.** Addressing/Address binding is the mapping of data to memory locations, it also maps physical addresses to logical addresses.

**Swapping.** Swapping is the process that moves data between the main storage (RAM) to secondary storage (Disks), this is similar to moving information from short term memory to the long term memory. However swapping is only used when RAM space isn’t as this process degrades system performance. (GeeksforGeeks, 2023)

**Buffers and Ring buffers**. Buffers act as temporary storage in the memory, these play a major role in managing data flow between components that may operate and different speeds and processing rates (*LaptopJudge*, 2025). A Ring Buffer is a circular buffer that uses First in, First out (FIFO) logic system, this system reduces data loss as it overwrites older data as new data is added as apposed to a normal buffer which works on the Last in, First out (LIFO) logic which gets overwrites the newest data each time, which can result in data loss.