UEAMPUS
STUDY GUIDE

Level 5 System Administration

uecampus.com/

First published in 2026 by UE Campus

Unit specifications can be found on the UE Campus Portal: https://uecampus.com/

Contents

Using your Study Guide

Welcome to the study guide, designed to support you in completing your Level 5 Diploma in Information Technology.

This study guide follows the order of the syllabus, which is the basis for your studies. Each chapter starts by listing the syllabus learning outcomes covered and the assessment criteria.

Level 5 Units

Unit Reference	Mandatory Units	Level	TQT	Credit	GLH
F/617/6740	Technopreneurship	5	200	20	100
J/617/6741	Network Security	5	200	20	100
L/617/6742	C#.NET Programming	5	200	20	100
R/617/6743	System Administration	5	200	20	100
Unit Reference	**Optional Units**	**Level**	**TQT**	**Credit**	**GLH**
Y/617/6744	Network Routing and Switching	5	200	20	100
D/617/6745	Network Design and Administration	5	200	20	100
H/617/6746	Content Management Systems	5	200	20	100
M/617/6748	Web Design 2	5	200	20	100
T/617/6749	Business to Business (B2B) E-commerce	5	200	20	100
K/617/6750	Business to Consumer (B2C) E-commerce	5	200	20	100

The study guide includes a number of features to enhance your studies:

📝	**'Over to you:'** activities for you to apply what you have learned.
🌍	**'Industry Insights:'** discover up-to-date trends, expert opinions, and real-world examples from system administration practice.
🧭	**'Did you know?'** highlights interesting facts or surprising information to deepen your understanding.
💼	**'Case studies:'** realistic scenarios to reinforce and test your understanding.
📱	**'Revision on the go:'** use your phone camera to capture key pieces of learning and save them as revision notes.
❗	**'Need to know:'** key pieces of information highlighted in the text.
💡	**'Examples:'** illustrating points made in the text to show how it works in practice.

Note: Website addresses current as of March 2026.

Level 5 System Administration

About this unit

This unit aims to provide you with the knowledge and skills needed to administer systems in both Linux and Windows environments. System administration is one of the most fundamental and essential roles in information technology – every organisation that uses computers depends on system administrators to keep their infrastructure running securely, efficiently, and reliably.

You will study the role of the system administrator, explore the key elements of system administration including user management, file systems, directory services, and policies, and understand the critical importance of backup, restore, and performance tuning. You will then develop practical skills in shell scripting (Bash and PowerShell), user and group management, file and printer sharing, snapshot creation, and performance optimisation across both Linux and Windows platforms.

By the end of this unit, you will have the knowledge and practical skills to administer multi-platform IT environments – a capability that is in constant demand across every sector of the economy.

Chapter One – Understanding System Administration

Introduction

This chapter provides the theoretical foundation for system administration. You will analyse the role and responsibilities of a system administrator, examine the key elements that comprise system administration, study the history and function of directory services (Active Directory and LDAP), understand the difference between snapshots and backups, analyse local and group policies, evaluate backup and restore strategies, and consider the requirements for managing applications across an enterprise.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Understand system administration.**

Assessment Criteria

1.1 Analyse the role of the system administrator.

1.2 Analyse the elements within system administration.

1.3 Analyse the history of the active directory and Lightweight Directory Access Protocol (LDAP).

1.4 Analyse the difference between snapshots and backups.

1.5 Analyse the differences between local and group policies on Windows and Linux.

1.6 Analyse the role and requirements of backup and restore policies.

1.7 Analyse the requirements of managing applications.

1.1 The role of the system administrator

Over to you – Video Watch: What Does a System Administrator Do?

Watch this YouTube video:

Title: System Administrator – What Is It? And How to Become One – PowerCert Animated Videos

Duration: 10:15

Link: https://www.youtube.com/watch?v=d2a6pP9x_LM

After watching, list the top five responsibilities of a system administrator and explain why each is critical to an organisation's operations.

Defining the System Administrator Role

A system administrator (sysadmin) is responsible for the installation, configuration, maintenance, and reliable operation of an organisation's computer systems and network infrastructure. The role spans both hardware and software, covering servers, workstations, network equipment, storage systems, and the services that run on them.

Core Duties

- Server administration – installing, configuring, and maintaining physical and virtual servers running Windows Server, Linux (Ubuntu Server, CentOS/RHEL, Debian), or both. This includes operating system updates, security patches, and performance monitoring.
- User and access management – creating, modifying, and disabling user accounts; managing group memberships; enforcing password policies; implementing role-based access control (RBAC).
- Network services – configuring and maintaining essential network services including DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Active Directory, LDAP, NTP (Network Time Protocol), and VPN services.
- Storage management – managing disk storage, file systems, RAID configurations, network-attached storage (NAS), storage area networks (SAN), and cloud storage.
- Backup and disaster recovery – designing and implementing backup strategies, testing restores, maintaining disaster recovery plans, and ensuring business continuity.
- Security – implementing and maintaining firewalls, antivirus, intrusion detection systems, encryption, audit logging, and security policies. System administrators are often the first line of defence against security threats.
- Monitoring and performance – continuously monitoring system health, resource utilisation (CPU, memory, disk, network), and service availability using tools like Nagios, Zabbix, Prometheus, or Windows Performance Monitor.
- Automation – writing scripts (Bash, PowerShell, Python) to automate repetitive tasks, reduce human error, and improve efficiency.

- Documentation – maintaining accurate documentation of configurations, procedures, network diagrams, and runbooks.
- Helpdesk and escalation – providing technical support, troubleshooting issues, and escalating complex problems to specialist teams.

Related Fields and Career Paths

- DevOps Engineer – combines system administration with software development practices, focusing on CI/CD pipelines, infrastructure as code (Terraform, Ansible), and cloud deployment.
- Cloud Administrator/Engineer – specialises in managing cloud infrastructure (AWS, Azure, GCP) including virtual machines, containers, serverless functions, and managed services.
- Site Reliability Engineer (SRE) – a discipline originated at Google that applies software engineering practices to operations, focusing on system reliability, scalability, and automation.
- Security Administrator – specialises in the security aspects of system administration, including firewall management, vulnerability scanning, and incident response.
- Database Administrator (DBA) – specialises in database installation, configuration, tuning, backup, and security.

Professional Certifications

Professional certifications validate sysadmin skills and are highly valued by employers:

- CompTIA Linux+ and CompTIA Server+ – vendor-neutral certifications covering Linux and server administration fundamentals.
- Red Hat Certified System Administrator (RHCSA) and RHCE – widely respected Linux certifications focused on Red Hat Enterprise Linux.
- Microsoft Certified: Windows Server Hybrid Administrator Associate – validates skills in Windows Server administration, Active Directory, and hybrid cloud.
- AWS Certified SysOps Administrator – cloud-focused certification for managing AWS infrastructure.
- LPIC-1 and LPIC-2 – Linux Professional Institute certifications covering system administration at intermediate and advanced levels.

Did you know?

According to the 2024 Stack Overflow Developer Survey, Linux is the most commonly used operating system for professional server infrastructure, with over 55% of developers deploying to Linux servers. However, Windows Server remains dominant in enterprise environments, particularly for organisations using Microsoft 365, Exchange, SharePoint, and SQL Server. The most effective system administrators are proficient in both platforms, as most organisations operate mixed (heterogeneous) environments.

Over to you – Role Analysis

Research job advertisements for system administrator positions on LinkedIn, Indeed, or Glassdoor. Analyse at least five job listings and identify: (1) the most commonly required technical skills, (2) the most commonly required certifications, (3) the typical salary range in the UK, (4) whether Linux, Windows, or both are required, and (5) any soft skills mentioned. Summarise your findings in a 400-word report.

1.2 Elements within system administration

System administration encompasses multiple interrelated elements that must work together to provide a secure, reliable, and efficient IT environment.

Managing Users and Groups

User and group management is foundational to system administration. Every individual who accesses the system must have an account, and those accounts must be organised into groups for efficient permission management. In Linux, users are managed through commands like useradd, usermod, userdel, and passwd, with user information stored in /etc/passwd, /etc/shadow, and /etc/group. In Windows, users are managed through Active Directory Users and Computers (ADUC), PowerShell cmdlets (New-ADUser, Set-ADUser, Get-ADUser), or local user management (lusrmgr.msc). Groups enable administrators to assign permissions collectively rather than individually, dramatically simplifying access control at scale.

Managing File Systems

File system management involves creating, mounting, monitoring, and maintaining the storage volumes where data resides. Linux supports multiple file systems including ext4 (the default for most distributions), XFS (high-performance, used by Red Hat), Btrfs (modern features like snapshots and checksums), and ZFS (advanced features, popular on servers). Windows uses NTFS (the standard since Windows NT), ReFS (Resilient File System for Windows Server), and FAT32/exFAT for removable media. Key tasks include partitioning disks (fdisk, diskpart), creating file systems (mkfs, Format-Volume), mounting volumes, managing quotas, monitoring disk space (df, du, Get-PSDrive), and implementing RAID for redundancy.

Automating Tasks, Processes and Daemons

Automation is what separates a good system administrator from a great one. Repetitive tasks – backups, log rotation, user provisioning, system updates, health checks – should be automated to save time, reduce errors, and ensure consistency:

- Linux: cron (scheduled tasks using crontab), systemd timers (modern alternative to cron), at (one-time scheduled tasks), and shell scripts (Bash).
- Windows: Task Scheduler (GUI-based scheduling), PowerShell scripts, Group Policy for deployment, and Windows Services.
- Daemons (Linux) / Services (Windows) – long-running background processes that provide essential functionality. Examples: sshd (SSH server), httpd/nginx (web server), mysqld (database), cron (task scheduler). Managed with systemctl on modern Linux systems (systemctl start/stop/enable/status servicename) and services.msc or sc.exe on Windows.

Network Services

System administrators configure and maintain critical network services:

- DHCP – automatically assigns IP addresses, subnet masks, gateways, and DNS server addresses to client devices. Configured in dhcpd.conf on Linux or through the DHCP Server role on Windows Server.
- DNS – translates domain names to IP addresses. BIND is the most common Linux DNS server; Windows Server includes an integrated DNS role tightly coupled with Active Directory.
- Mail servers – Postfix, Sendmail (Linux), or Microsoft Exchange (Windows) for organisational email.
- NFS (Network File System) – a Linux/Unix protocol for sharing files across a network, allowing remote directories to be mounted as if they were local.
- NIS (Network Information Service) – a directory service for distributing system configuration data (users, groups, hosts) across a network of Unix/Linux systems.
- WINS (Windows Internet Name Service) – a legacy Microsoft service for resolving NetBIOS names to IP addresses, largely replaced by DNS in modern environments.

Industry Insight – Infrastructure as Code

Modern system administration is increasingly moving towards Infrastructure as Code (IaC) – managing servers and infrastructure through machine-readable definition files rather than manual configuration. Tools like Ansible (agentless, YAML-based), Puppet, Chef, and Terraform allow administrators to define the desired state of their infrastructure in code, version-control it with Git, and deploy it consistently across hundreds or thousands of servers. IaC is a core practice in DevOps and is essential for managing cloud infrastructure at scale.

Explore: https://docs.ansible.com/ansible/latest/getting_started/

Over to you – Service Configuration

Using a Linux virtual machine (Ubuntu Server recommended, available free at https://ubuntu.com/server), configure: (1) a DHCP server that assigns IP addresses in the range 192.168.1.100–192.168.1.200, (2) a DNS server that resolves a custom domain (e.g. lab.local) to a local IP address, and (3) an NFS share that exports a directory to clients on the network. Document each step with commands and screenshots. If you do not have access to a Linux VM, document the theoretical steps with the commands you would use.

1.3 Active Directory and LDAP

Directory services are centralised databases that store and manage information about network resources – users, computers, printers, groups, and organisational units. They provide a single point of authentication and authorisation for the entire network.

Lightweight Directory Access Protocol (LDAP)

LDAP is an open, vendor-neutral, industry-standard protocol for accessing and maintaining distributed directory information services over a network. Developed in the early 1990s at the University of Michigan as a lightweight alternative to the X.500 directory access protocol (DAP), LDAP has become the foundation for virtually all modern directory services.

LDAP organises data in a hierarchical tree structure (the Directory Information Tree or DIT). Each entry in the tree has a Distinguished Name (DN) that uniquely identifies it – for example: CN=John Smith,OU=IT Department,DC=company,DC=com. LDAP supports operations including bind (authenticate), search (query the directory), add, delete, modify, and compare. The protocol typically runs on port 389 (unencrypted) or port 636 (LDAPS, encrypted with TLS). Open-source LDAP implementations include OpenLDAP and 389 Directory Server.

Microsoft Active Directory (AD)

Active Directory Domain Services (AD DS), introduced with Windows 2000 Server, is Microsoft's implementation of a directory service. AD uses LDAP as its access protocol and Kerberos as its authentication protocol. It has become the de facto standard for identity management in enterprise Windows environments.

Key Active Directory concepts:

- Domain – the basic organisational unit. All objects (users, computers, groups) belong to a domain. A domain defines a security boundary and an administrative scope.
- Domain Controller (DC) – a server running AD DS that authenticates users and stores the directory database. Multiple DCs provide redundancy through multi-master replication.
- Organisational Unit (OU) – a container within a domain for organising objects and applying Group Policies. OUs typically mirror the organisation's structure (departments, offices, teams).
- Forest and Tree – a forest is the top-level container consisting of one or more domain trees. A tree is a collection of domains sharing a contiguous DNS namespace.
- Group Policy Objects (GPOs) – configurations applied to users and computers within OUs to enforce security settings, deploy software, configure desktop environments, and more. GPOs are one of AD's most powerful features.
- DNS integration – AD relies heavily on DNS for locating domain controllers and services. AD-integrated DNS zones are stored in the AD database and replicated automatically.

Over to you – Video Watch: Active Directory Explained

Watch this YouTube video:

Title: Active Directory Tutorial for Beginners – IT Career Questions

Duration: 15:22

Link: https://www.youtube.com/watch?v=85-bp7XxWDQ

After watching, draw a diagram showing the relationship between a Forest, Trees, Domains, OUs, and objects (users, computers). Explain the role of a Domain Controller.

History and Evolution

- 1988: X.500 standard published – the original directory service standard, complex and heavyweight.
- 1993: LDAP v2 developed at University of Michigan as a lightweight X.500 frontend.
- 1997: LDAP v3 (RFC 2251) – the current standard, adding support for extensibility, referrals, and stronger security.
- 1999: OpenLDAP project founded – the most widely used open-source LDAP implementation.
- 2000: Windows 2000 Server introduces Active Directory – Microsoft's LDAP-based directory service.
- 2003–2022: AD evolves through Windows Server 2003, 2008, 2012, 2016, 2019, and 2022 with features like AD Federation Services (ADFS), Azure AD (now Microsoft Entra ID), and hybrid identity management.
- 2020s: Azure Active Directory (renamed Microsoft Entra ID in 2023) extends on-premises AD to the cloud, providing identity management for cloud and SaaS applications.

Did you know?

Microsoft Entra ID (formerly Azure AD) now manages over 1.4 billion identities and processes over 150 billion authentication requests daily. While traditional on-premises Active Directory remains critical for managing Windows Server environments, hybrid identity – where users have a single identity that works across both on-premises and cloud resources – has become the standard for modern enterprise IT. Tools like Azure AD Connect synchronise on-premises AD with Entra ID, enabling single sign-on (SSO) to both local resources and cloud services like Microsoft 365, Salesforce, and thousands of other SaaS applications.

1.4 Snapshots vs backups

Both snapshots and backups are mechanisms for protecting data and enabling recovery, but they serve different purposes and have different characteristics. Understanding the distinction is essential for designing an effective data protection strategy.

Snapshots

A snapshot is a point-in-time copy of the state of a system, disk, or file system. It captures the exact state of the data at the moment the snapshot is taken, without copying the entire data set. Instead, snapshots typically use a copy-on-write (CoW) mechanism: when data is changed after the snapshot, the original data blocks are preserved and only the changes are tracked.

- Speed – snapshots are created almost instantly because they don't copy data; they only record a pointer to the current state.
- Storage efficiency – snapshots initially consume very little additional storage; space usage grows as data changes.
- Use cases – rapid rollback before system changes (patches, upgrades), development and testing (create a snapshot, test, roll back), and short-term recovery points.
- Limitations – snapshots are stored on the same storage system as the original data. If the storage system fails, both the data and the snapshots are lost. Snapshots are not a substitute for backups. Performance can degrade if too many snapshots accumulate.

Backups

A backup is an independent copy of data stored on a separate storage medium or location. Backups are designed for long-term data protection and disaster recovery.

- Independence – backups are stored separately from the original data (different disk, tape, cloud storage, offsite location), protecting against hardware failure, ransomware, and physical disasters.
- Types – full backup (copies all data), incremental backup (copies only changes since the last backup), differential backup (copies changes since the last full backup).
- Use cases – disaster recovery, long-term data retention, compliance requirements, protection against ransomware (offline/air-gapped backups).
- Limitations – backups take longer to create than snapshots; restoration can be time-consuming; require separate storage infrastructure and management.

Feature	Snapshot	Backup
Speed	Near-instant	Minutes to hours
Storage location	Same system	Separate location
Protection against storage failure	No	Yes

Long-term retention	No (performance impact)	Yes
Ransomware protection	Limited	Yes (if offline/air-gapped)
Purpose	Short-term rollback	Disaster recovery, compliance
Granularity	Entire volume/VM	Files, folders, or volumes

Best practice: use snapshots for short-term, rapid recovery (before making changes) and backups for long-term data protection and disaster recovery. The two are complementary, not interchangeable.

Over to you – Data Protection Plan

A small company has two physical servers (one Windows, one Linux), a NAS for shared files, and a cloud-hosted web application. Design a data protection plan that combines snapshots and backups. Specify: (1) what would be protected by snapshots and how often, (2) what would be backed up, the backup type (full/incremental/differential), and the schedule, (3) where backups would be stored, (4) how often you would test restores, and (5) estimated RPO and RTO for each system. Present as a structured table.

1.5 Local and group policies on Windows and Linux

Policies are sets of rules and configurations that control the behaviour and security of users and computers. They are one of the most powerful tools available to system administrators for enforcing standards and security across an organisation.

Windows: Local Policy vs Group Policy

Local Policy

Local policies (configured via gpedit.msc on individual machines) apply only to the specific computer on which they are set. They are suitable for standalone machines not joined to a domain. Local policies cover: password policies (length, complexity, expiry), account lockout policies, audit policies (login events, object access), user rights assignments (who can log on locally, shut down the system), and security options (interactive logon messages, LAN Manager authentication level).

Group Policy (Active Directory)

Group Policy Objects (GPOs) are centrally managed policies applied through Active Directory to users and computers within OUs. GPOs are far more powerful than local policies because they can be applied to hundreds or thousands of machines simultaneously from a single location. GPO capabilities include everything local policies offer plus: software deployment (install, update, remove applications remotely), folder redirection (redirect Desktop, Documents to network shares), drive mapping, printer deployment, desktop restrictions (lock wallpaper, restrict Control Panel access), Windows Firewall configuration, BitLocker encryption enforcement, and PowerShell script execution at startup/shutdown/logon/logoff.

When a conflict exists between local policy and GPO, the GPO always wins (following the LSDOU order: Local, Site, Domain, OU – with OU being the highest priority).

Linux: Policy Management

Linux does not have a direct equivalent of Windows Group Policy, but achieves similar results through different mechanisms:

- PAM (Pluggable Authentication Modules) – controls authentication policies: password complexity (/etc/security/pwquality.conf), account lockout (pam_faillock), session limits, and login restrictions.
- sudoers (/etc/sudoers) – defines which users can execute commands with elevated privileges (sudo), and which commands they are allowed to run.
- SELinux / AppArmor – mandatory access control (MAC) frameworks that enforce security policies beyond standard file permissions. SELinux (used by Red Hat/CentOS) and AppArmor (used by Ubuntu) restrict what processes can access.

- Configuration management tools – Ansible, Puppet, and Chef serve a similar role to GPOs in Linux environments, allowing administrators to define and enforce configurations centrally across many servers.
- SSH configuration (/etc/ssh/sshd_config) – controls remote access policies: allowed authentication methods, root login restrictions, port settings, and connection limits.

Case Study – Policy Implementation

A university IT department needs to enforce the following policies across 200 Windows computers in student labs and 50 Linux servers in the data centre: (1) password minimum length of 12 characters with complexity, (2) account lockout after 5 failed attempts, (3) automatic screen lock after 10 minutes of inactivity, (4) restrict student lab PCs from accessing Control Panel and installing software, (5) enforce full disk encryption on all servers.

Task: For each policy requirement, specify: (a) how you would implement it on Windows (Local or Group Policy, and the specific policy path), (b) how you would implement it on Linux (the configuration file or tool), and (c) how you would verify that the policy is applied correctly. Present as a structured report.

1.6 Backup and restore policies

A backup and restore policy is a formal document that defines an organisation's approach to protecting data through regular backups and ensuring the ability to restore data when needed. Without a clear policy, backup practices tend to be inconsistent, untested, and unreliable – often discovered to be inadequate only when a real disaster strikes.

Key Components of a Backup Policy

- Scope – what systems and data are covered. Classify data by criticality: mission-critical (cannot operate without it), important (significant impact if lost), and standard (minimal impact).
- Backup schedule – how often each category of data is backed up. A common approach: full backup weekly, incremental backups daily. Mission-critical systems may require more frequent backups or continuous data protection (CDP).
- Retention periods – how long backups are retained. This is driven by business requirements and regulatory compliance (e.g. financial records may need to be retained for 7 years under UK regulations).
- Storage locations – where backups are stored. The 3-2-1 rule: 3 copies, 2 different media types, 1 offsite/cloud. Air-gapped or immutable backups provide protection against ransomware.
- Recovery Time Objective (RTO) – the maximum acceptable time to restore a system after a failure. Determines the technology and processes needed (a 1-hour RTO requires very different infrastructure than a 24-hour RTO).
- Recovery Point Objective (RPO) – the maximum acceptable amount of data loss, measured in time. An RPO of 4 hours means you can afford to lose up to 4 hours of data, so backups must occur at least every 4 hours.
- Testing and verification – regular testing of backup restores is essential. A backup that cannot be restored is worthless. Schedule quarterly or monthly restore tests.
- Responsibilities and procedures – who is responsible for backups, who monitors them, who performs restores, and the escalation process when backups fail.
- Encryption – backups should be encrypted, especially those stored offsite or in the cloud, to protect sensitive data.

Backup Tools

- Linux: rsync (file-level backup and synchronisation), tar (archive creation), Bacula (enterprise backup), BorgBackup (deduplicated, encrypted), Veeam Agent for Linux.
- Windows: Windows Server Backup (built-in), Veeam Backup & Replication (enterprise), System Center Data Protection Manager (DPM), robocopy (file-level), wbadmin (command-line).
- Cloud: AWS Backup, Azure Backup, Google Cloud Backup – managed backup services for cloud workloads.

Over to you – Backup Policy

Write a backup and restore policy for a small business with: 2 Windows servers (file server and application server), 1 Linux server (web server and database), 10 workstations, and a budget of £500/month for backup infrastructure. Your policy should cover: scope, backup schedule (with type), retention periods, storage locations, RTO and RPO targets, testing schedule, and responsibilities. Present as a formal policy document of approximately 600 words.

1.7 Managing applications

Application management involves installing, configuring, updating, and removing software across an organisation's systems. In an enterprise environment with hundreds or thousands of computers, manual application management is impractical – centralised, automated approaches are essential.

Linux Application Management

- Package managers – APT (Advanced Package Tool) on Debian/Ubuntu (apt install, apt update, apt upgrade), YUM/DNF on Red Hat/CentOS/Fedora (dnf install, dnf update), and Zypper on SUSE. Package managers handle dependency resolution, installation, updates, and removal.
- Repositories – centralised collections of software packages. Official repositories are maintained by the distribution maintainers. Third-party repositories (PPAs on Ubuntu, EPEL on Red Hat) provide additional software.
- Snap and Flatpak – modern universal package formats that bundle applications with their dependencies, enabling distribution-independent installation.
- Configuration management – Ansible playbooks can deploy and configure applications across hundreds of servers simultaneously.

Windows Application Management

- Group Policy Software Deployment – deploy MSI packages to users or computers through Active Directory GPOs. Applications can be assigned (installed automatically) or published (available in Add/Remove Programs).
- Microsoft Endpoint Configuration Manager (MECM/SCCM) – enterprise-grade application deployment, patching, and compliance management for Windows environments.
- Windows Package Manager (winget) – a command-line tool (introduced in Windows 10) for installing and managing applications: winget install Mozilla.Firefox.
- Microsoft Intune – cloud-based endpoint management for deploying applications to both managed and BYOD devices.
- Registry – the Windows Registry (regedit.exe) is a hierarchical database storing configuration settings for the OS, applications, and hardware. System administrators use the Registry to customise application behaviour, enforce settings, and troubleshoot issues. Key hives include HKEY_LOCAL_MACHINE (system-wide settings) and HKEY_CURRENT_USER (per-user settings). Caution: incorrect Registry modifications can render a system unbootable.

Industry Insight – Containers and Application Management

Modern application management increasingly uses containerisation. Docker containers package applications with all their dependencies into lightweight, portable units that run

consistently across any environment. Kubernetes orchestrates containers at scale, automating deployment, scaling, and management across clusters of servers. For system administrators, this means managing container runtimes (Docker, containerd), orchestration platforms (Kubernetes, Docker Swarm), container registries (Docker Hub, AWS ECR), and the underlying infrastructure. Containerisation is a fundamental shift in how applications are deployed and managed, and understanding it is increasingly essential for system administrators.

Explore: https://docs.docker.com/get-started/

Reading List

- Barrett, D.J. (2024). *Efficient Linux at the Command Line*. 2nd edn. Sebastopol, CA: O'Reilly Media.
- Limoncelli, T.A., Hogan, C.J. & Chalup, S.R. (2023). *The Practice of System and Network Administration*. 3rd edn. Boston: Addison-Wesley.
- Nemeth, E., Snyder, G., Hein, T.R. & Whaley, B. (2023). *UNIX and Linux System Administration Handbook*. 6th edn. Boston: Addison-Wesley.
- Petersen, R. (2024). *The Complete Reference: Linux*. 8th edn. New York: McGraw-Hill.
- Stanek, W.R. (2024). *Windows Server Administration Fundamentals*. Updated edn. Redmond, WA: Microsoft Press.
- Warner, T.L. (2024). *PowerShell in a Month of Lunches*. 5th edn. Shelter Island, NY: Manning.

Summary

In this chapter, you have developed a comprehensive understanding of system administration. You have analysed the role, responsibilities, and career paths of system administrators. You have examined the key elements of system administration including user and group management, file system management, task automation, and network services. You have studied the history and architecture of Active Directory and LDAP. You have analysed the critical differences between snapshots and backups. You have evaluated local and group policies on both Windows and Linux, understanding how they enforce security and standards. You have analysed the components of effective backup and restore policies. Finally, you have examined application management approaches across both platforms, including modern trends like containerisation.

Chapter Two – User Management and File System Management

Introduction

This chapter is the practical heart of the unit. You will write shell scripts to automate administration tasks, set up users and groups, configure file and printer sharing, create snapshots, and tune system performance – all on both Linux and Windows platforms.

Learning Outcomes

On completing the chapter, you will be able to:

1. **Perform user management and file system management.**

Assessment Criteria

2.1 Write shell scripts that enable administration tasks to be performed on Linux and Windows systems: Get Help; Check Services; List Users and ping a list of servers.

2.2 Set up and configure users and groups to the agreed standard.

2.3 Install and configure file and printer sharing to agreed standards.

2.4 Write shell scripts to perform snapshots on Linux and Windows servers to agreed standards.

2.5 Tune performance through the application of a range of utilities and tools to agreed standards.

2.1 Shell scripting for administration tasks

Shell scripting is one of the most valuable skills for a system administrator. Scripts automate repetitive tasks, ensure consistency, reduce human error, and save enormous amounts of time.

Over to you – Video Watch: Bash Scripting

Watch this YouTube video:

Title: Bash Scripting Tutorial for Beginners – Learn Linux

Duration: 32:42

Link: https://www.youtube.com/watch?v=tK9Oc6AEnR4

Watch the first 15 minutes covering variables, conditions, and loops in Bash. Write a simple script that greets the user and displays the current date and system uptime.

Bash Scripting (Linux)

Bash (Bourne Again Shell) is the default shell on most Linux distributions. A Bash script is a text file containing a sequence of commands, beginning with the shebang line #!/bin/bash:

Script 1: Get Help (Display System Information)

```
#!/bin/bash
echo "=== System Information ==="
echo "Hostname: $(hostname)"
echo "OS: $(cat /etc/os-release | grep PRETTY_NAME | cut -d= -f2)"
echo "Kernel: $(uname -r)"
echo "Uptime: $(uptime -p)"
echo "Disk Usage:"
df -h / | tail -1
echo "Memory Usage:"
free -h | grep Mem
```

Script 2: Check Services

```
#!/bin/bash
SERVICES=("sshd" "nginx" "mysql" "cron")
for svc in "${SERVICES[@]}"; do
  if systemctl is-active --quiet $svc; then
    echo "[RUNNING] $svc"
  else
```

```
    echo "[STOPPED] $svc"
  fi
done
```

Script 3: List Users

```
#!/bin/bash
echo "=== System Users (UID >= 1000) ==="
awk -F: '$3 >= 1000 && $3 < 65534 {print $1, $3, $6}' /etc/passwd
```

Script 4: Ping a List of Servers

```
#!/bin/bash
SERVERS=("192.168.1.1" "192.168.1.2" "google.com")
for server in "${SERVERS[@]}"; do
  if ping -c 1 -W 2 $server > /dev/null 2>&1; then
    echo "[UP] $server"
  else
    echo "[DOWN] $server"
  fi
done
```

PowerShell Scripting (Windows)

PowerShell is Microsoft's task automation and configuration management framework. Unlike Bash (which works primarily with text), PowerShell works with .NET objects, making it extremely powerful for Windows administration:

Over to you – Video Watch: PowerShell Basics

Watch this YouTube video:

Title: PowerShell For Beginners Full Course – Nerd's Lesson

Duration: 3:37:17

Link: https://www.youtube.com/watch?v=UVUd9_k9C6A

Watch the first 20 minutes covering cmdlets, variables, and the pipeline. Write a PowerShell script that displays the computer name, OS version, and available disk space.

Script 1: Get Help (System Information)

```
# Get-SystemInfo.ps1
```

```
Write-Host "=== System Information ==="
Write-Host "Computer: $env:COMPUTERNAME"
Write-Host "OS: $((Get-CimInstance Win32_OperatingSystem).Caption)"
Write-Host "Uptime: $((Get-CimInstance Win32_OperatingSystem).LastBootUpTime)"
Get-CimInstance Win32_LogicalDisk | Format-Table DeviceID, Size, FreeSpace
```

Script 2: Check Services

```
$services = @("W32Time", "Spooler", "WinRM", "MSSQLSERVER")
foreach ($svc in $services) {
  $status = (Get-Service -Name $svc -ErrorAction SilentlyContinue).Status
  if ($status -eq "Running") { Write-Host "[RUNNING] $svc" -ForegroundColor Green }
  else { Write-Host "[STOPPED] $svc" -ForegroundColor Red }
}
```

Script 3: List Users

```
Get-LocalUser | Select-Object Name, Enabled, LastLogon | Format-Table -AutoSize
# For Active Directory users:
# Get-ADUser -Filter * | Select-Object Name, SamAccountName, Enabled
```

Script 4: Ping Servers

```
$servers = @("192.168.1.1", "192.168.1.2", "google.com")
foreach ($server in $servers) {
  if (Test-Connection -ComputerName $server -Count 1 -Quiet) {
    Write-Host "[UP] $server" -ForegroundColor Green
  } else { Write-Host "[DOWN] $server" -ForegroundColor Red }
}
```

Over to you – Scripting Project

Write both a Bash script and a PowerShell script for each of the four tasks above. Test them on a Linux VM and a Windows machine. Then extend one script of your choice with additional features (e.g. add logging to a file, email alerts for failed pings, or coloured output). Submit all scripts with comments explaining each section, plus screenshots of the output.

2.2 Setting up and configuring users and groups

Linux User and Group Management

Essential commands for managing users and groups on Linux:

- useradd username – creates a new user. Options: -m (create home directory), -s /bin/bash (set shell), -G groupname (add to supplementary group), -e YYYY-MM-DD (account expiry date).
- usermod -aG groupname username – adds a user to a supplementary group (-a = append, -G = supplementary group).
- userdel -r username – deletes a user and their home directory.
- passwd username – sets or changes a user's password.
- groupadd groupname – creates a new group.
- groupdel groupname – deletes a group.
- id username – displays a user's UID, GID, and group memberships.
- chown user:group file – changes file ownership.
- chmod 755 file – sets file permissions (rwxr-xr-x).

Windows User and Group Management

- Local users: lusrmgr.msc (GUI), net user username password /add (command line), New-LocalUser (PowerShell).
- Active Directory: Active Directory Users and Computers (ADUC), or PowerShell: New-ADUser -Name "John Smith" -SamAccountName jsmith -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force) -Enabled $true.
- Groups: New-ADGroup -Name "IT Staff" -GroupScope Global -GroupCategory Security, Add-ADGroupMember -Identity "IT Staff" -Members jsmith.
- Windows Server access control uses NTFS permissions (Read, Write, Modify, Full Control) and Share permissions. The effective permission is the most restrictive combination of NTFS and Share permissions.

Case Study – User Provisioning

A company with 50 employees needs to set up accounts for 10 new IT department staff. Each user needs: a domain account with a standard naming convention (first initial + surname), membership in the 'IT-Staff' and 'VPN-Users' groups, a home folder on the file server mapped as drive H:, and a mailbox.

Task: Write: (1) a PowerShell script that creates all 10 AD users from a CSV file (columns: FirstName, LastName, Department), adds them to the required groups, and creates home folders, (2) a Bash script that creates 10 equivalent users on a Linux server with home

directories and group memberships. Test your scripts and document the process with screenshots.

2.3 File and printer sharing

Linux File Sharing with NFS and Samba

NFS (Network File System) is the native Linux/Unix file sharing protocol. To share a directory: (1) install the NFS server (apt install nfs-kernel-server), (2) add an entry to /etc/exports (e.g. /shared 192.168.1.0/24(rw,sync,no_subtree_check)), (3) export the share (exportfs -a), (4) on the client, mount it (mount server:/shared /mnt/shared or add to /etc/fstab for persistence).

Samba provides SMB/CIFS file sharing, enabling Linux systems to share files with Windows clients (and vice versa). Configuration is managed through /etc/samba/smb.conf, where you define shares with settings for path, valid users, read/write permissions, and browsability.

Windows File and Printer Sharing

Windows uses the SMB (Server Message Block) protocol for file and printer sharing. Shares can be created through: File Explorer (right-click > Properties > Sharing), Server Manager (File and Storage Services), PowerShell (New-SmbShare), or the command line (net share). NTFS permissions control who can access files; Share permissions control network access. Best practice: set Share permissions to 'Everyone: Full Control' and use NTFS permissions for granular access control.

Printer sharing on Windows is configured through Print Management (printmanagement.msc) or Settings > Printers. Printers can be deployed to users via Group Policy (Computer Configuration > Policies > Windows Settings > Deployed Printers) for automatic installation.

Over to you – File Sharing Setup

Set up file sharing in a lab environment: (1) On a Linux VM, create an NFS share and a Samba share. Mount the NFS share from a Linux client and the Samba share from a Windows client. (2) On Windows Server, create a shared folder with specific NTFS permissions for different groups (IT-Staff: Modify, Managers: Read, Everyone: Deny). Deploy a shared printer via Group Policy. Document all steps with commands and screenshots.

2.4 Snapshots on Linux and Windows servers

Linux Snapshots with LVM

Logical Volume Manager (LVM) is the standard tool for creating snapshots on Linux. LVM snapshots capture the state of a logical volume at a point in time:

```
# Create a snapshot of /dev/vg01/lv_data
lvcreate --size 5G --snapshot --name snap_data /dev/vg01/lv_data

# Mount the snapshot (read-only) to access the point-in-time data
mount -o ro /dev/vg01/snap_data /mnt/snapshot

# Restore from snapshot (merging)
lvconvert --merge /dev/vg01/snap_data

# Remove a snapshot
lvremove /dev/vg01/snap_data
```

Bash script to automate snapshots:

```
#!/bin/bash
DATE=$(date +%Y%m%d_%H%M%S)
SNAP_NAME="snap_data_$DATE"
lvcreate --size 5G --snapshot --name $SNAP_NAME /dev/vg01/lv_data
echo "Snapshot $SNAP_NAME created at $(date)" >> /var/log/snapshots.log
```

Windows Snapshots with Volume Shadow Copy

Windows uses Volume Shadow Copy Service (VSS) for creating point-in-time snapshots (shadow copies):

```
# PowerShell: Create a VSS snapshot
$shadow = (Get-WmiObject -List Win32_ShadowCopy).Create("C:\", "ClientAccessible")

# Enable shadow copies for a volume via GUI:
# Right-click drive > Properties > Shadow Copies > Enable

# PowerShell script to automate:
$volume = "C:\"
```

```
$shadowClass = [WMICLASS]"root\cimv2:Win32_ShadowCopy"
$result = $shadowClass.Create($volume, "ClientAccessible")
"Shadow copy created at $(Get-Date)" | Out-File -Append C:\Logs\snapshots.log
```

For virtual machines, Hyper-V checkpoints and VMware snapshots provide VM-level snapshots that capture the entire VM state including memory. These are managed through the hypervisor's management tools.

Over to you – Snapshot Scripting

Write: (1) a Bash script that creates an LVM snapshot, logs the action, and emails a notification (using the mail command or a placeholder), and (2) a PowerShell script that creates a VSS shadow copy and logs the action. Both scripts should include error handling (check if the snapshot was created successfully). Test on a Linux VM with LVM and a Windows Server. Submit your scripts with comments and output screenshots.

2.5 Performance tuning

Performance tuning is the process of optimising system resources to ensure that servers and workstations run efficiently and meet the demands of their workloads.

Linux Performance Monitoring and Tuning

- top / htop – real-time display of CPU, memory, and process usage. htop provides a more user-friendly, colour-coded interface.
- vmstat – reports virtual memory statistics including processes, memory, swap, I/O, and CPU activity.
- iostat – reports CPU utilisation and disk I/O statistics. Essential for identifying storage bottlenecks.
- sar (System Activity Reporter) – collects, reports, and saves system activity information over time. Part of the sysstat package.
- free -h – displays memory and swap usage in human-readable format.
- df -h / du -sh – disk space usage (filesystem level and directory level respectively).
- nice / renice – adjust process priority (nice values from -20 highest priority to 19 lowest).
- Tuning parameters – kernel parameters can be tuned via /etc/sysctl.conf (e.g. vm.swappiness to control swap behaviour, net.core.somaxconn for network connection limits).

Windows Performance Monitoring and Tuning

- Task Manager (Ctrl+Shift+Esc) – real-time view of CPU, memory, disk, and network usage by process.
- Resource Monitor (resmon.exe) – more detailed view of resource usage including individual disk activity, network connections, and memory by process.
- Performance Monitor (perfmon.exe) – the most powerful built-in tool. Creates custom counters tracking any aspect of system performance over time. Data Collector Sets capture performance data for analysis.
- Windows Performance Toolkit (WPT) – advanced analysis tools including Windows Performance Recorder and Windows Performance Analyser for deep-dive performance investigation.
- PowerShell: Get-Process, Get-Counter, Measure-Object – cmdlets for scripted performance monitoring.
- Disk Defragmentation (Optimize-Volume) – optimises disk performance on HDDs (not needed for SSDs).
- Services optimisation – disabling unnecessary services reduces resource consumption and attack surface.

Common Performance Issues and Solutions

- High CPU usage – identify the offending process (top/Task Manager), check for runaway processes, malware, or insufficient hardware. Solutions: kill/restart the process, optimise application configuration, upgrade CPU.
- Memory exhaustion – insufficient RAM causes excessive swapping, severely degrading performance. Solutions: identify memory-hungry processes, increase RAM, optimise application memory settings, add swap space (Linux).
- Disk I/O bottleneck – slow disk performance due to heavy read/write activity. Solutions: upgrade to SSD, implement RAID, optimise database queries, add caching, move logs to separate disks.
- Network saturation – network bandwidth exceeded. Solutions: identify bandwidth-hungry applications (iftop, NetFlow), implement QoS (Quality of Service), upgrade network infrastructure.

Over to you – Video Watch: Linux Performance Monitoring

Watch this YouTube video:

Title: Linux Performance Monitoring and Tuning – Learn Linux TV

Duration: 22:15

Link: https://www.youtube.com/watch?v=PhE1B4YFhxE

After watching, run top, vmstat, and iostat on a Linux VM. Create a 10-minute performance baseline using sar. Identify the CPU, memory, and disk metrics you would monitor for a production server.

Case Study – Performance Troubleshooting

A company's file server (Windows Server 2022) is experiencing slow performance. Users report that accessing shared files takes 30+ seconds. The server has 16 GB RAM, a single 1 TB HDD, and a 1 Gbps network connection. The server also runs a SQL Server database for an internal application.

Task: Describe your troubleshooting methodology: (1) which monitoring tools you would use and what metrics you would check first, (2) three likely causes of the performance issue (explain your reasoning), (3) for each cause, describe the specific evidence you would look for in the monitoring data, and (4) recommend solutions for each cause, prioritised by likely impact and implementation effort. Write approximately 500 words.

Reading List

- Barrett, D.J. (2024). *Efficient Linux at the Command Line*. 2nd edn. Sebastopol, CA: O'Reilly Media.
- Jones, D. & Hicks, J. (2023). *Learn PowerShell in a Month of Lunches*. 4th edn. Shelter Island, NY: Manning.
- Nemeth, E., Snyder, G., Hein, T.R. & Whaley, B. (2023). *UNIX and Linux System Administration Handbook*. 6th edn. Boston: Addison-Wesley.
- Negus, C. (2024). *Linux Bible*. 11th edn. Indianapolis, IN: Wiley.
- Stanek, W.R. (2024). *Windows Server Administration Fundamentals*. Updated edn. Redmond, WA: Microsoft Press.
- Ward, B. (2024). *How Linux Works: What Every Superuser Should Know*. 3rd edn. San Francisco, CA: No Starch Press.

Summary

In this chapter, you have developed practical system administration skills for both Linux and Windows. You have written shell scripts in Bash and PowerShell to automate four essential tasks: gathering system information, checking services, listing users, and pinging servers. You have set up and configured users and groups on both platforms, understanding the commands, permissions, and best practices. You have installed and configured file and printer sharing using NFS, Samba, and Windows SMB. You have written scripts to create snapshots using LVM (Linux) and VSS (Windows). Finally, you have studied performance tuning using a range of monitoring utilities and tools, learning to identify and resolve common performance bottlenecks.

Glossary

Word / Term	Explanation
Active Directory	Microsoft's directory service for managing users, computers, and policies in Windows domains.
Ansible	An open-source automation tool for configuration management, application deployment, and orchestration.
APT	Advanced Package Tool; the package management system for Debian/Ubuntu Linux distributions.
Backup	An independent copy of data stored on separate media for long-term protection and disaster recovery.
Bash	Bourne Again Shell; the default command-line shell on most Linux distributions.
Cron	A Linux daemon for scheduling recurring tasks using crontab configuration files.
DHCP	Dynamic Host Configuration Protocol; automatically assigns IP addresses to network devices.
DNS	Domain Name System; translates domain names (e.g. google.com) to IP addresses.
Domain Controller	A Windows server running Active Directory that authenticates users and enforces policies.
GPO	Group Policy Object; a centrally managed set of policies applied through Active Directory.
LDAP	Lightweight Directory Access Protocol; an open standard for accessing directory services.
LVM	Logical Volume Manager; a Linux storage management layer supporting snapshots and dynamic volumes.
NFS	Network File System; a Linux/Unix protocol for sharing files across a network.
NTFS	New Technology File System; the standard file system for Windows with support for permissions and encryption.
OU	Organisational Unit; a container in Active Directory for organising objects and applying policies.
PAM	Pluggable Authentication Modules; a Linux framework for configuring authentication policies.
PowerShell	Microsoft's task automation and configuration management framework using object-based cmdlets.
RAID	Redundant Array of Independent Disks; combining multiple disks for performance or redundancy.
RPO	Recovery Point Objective; the maximum acceptable data loss measured in time.
RTO	Recovery Time Objective; the maximum acceptable downtime after a failure.
Samba	Software enabling Linux systems to share files with Windows clients using SMB protocol.

SELinux	Security-Enhanced Linux; a mandatory access control framework for Linux security.
SMB	Server Message Block; the protocol used for Windows file and printer sharing.
Snapshot	A point-in-time copy of system state, stored on the same system, for rapid rollback.
Sysadmin	System administrator; responsible for maintaining IT infrastructure.
systemctl	The command for managing systemd services on modern Linux distributions.
Task Scheduler	Windows tool for scheduling automated tasks and scripts.
VSS	Volume Shadow Copy Service; Windows service for creating point-in-time snapshots.

MCQs and True & False Questions (self-assessment)

True or False Questions

1. A system administrator is responsible for maintaining IT infrastructure.
2. Linux uses the Registry for system configuration.
3. Cron is used to schedule recurring tasks on Linux.
4. Active Directory uses the LDAP protocol.
5. A snapshot is stored on separate media from the original data.
6. Group Policy Objects apply only to local computers.
7. PowerShell works with .NET objects rather than plain text.
8. NTFS permissions and Share permissions are the same thing.
9. The 3-2-1 backup rule recommends 3 copies on 2 media types with 1 offsite.
10. NFS is a Windows-native file sharing protocol.
11. LVM allows creation of snapshots on Linux.
12. LDAP Distinguished Names use the format CN=Name,OU=Unit,DC=Domain.
13. The useradd command creates a new user on Windows.
14. Performance Monitor (perfmon) is a built-in Windows monitoring tool.
15. SELinux is a mandatory access control framework for Linux.
16. RPO measures the maximum acceptable downtime.
17. Samba allows Linux to share files with Windows clients.
18. The /etc/passwd file stores encrypted passwords on Linux.
19. systemctl is used to manage services on modern Linux systems.
20. VSS stands for Virtual Server Service.

Multiple Choice Questions

1. Which command creates a new user on Linux?

A. adduser

B. useradd

C. newuser

D. Both A and B

2. Which Windows tool manages Active Directory users?

A. regedit

B. lusrmgr.msc

C. ADUC

D. Task Manager

3. The default port for LDAP is:

A. 80

B. 443

C. 389

D. 3389

4. Which Linux file system supports snapshots natively?

A. ext4

B. FAT32

C. NTFS

D. Btrfs

5. Group Policy in Windows follows which priority order?

A. LSDOU

B. OUDSL

C. DLSOU

D. SLOUD

6. Which PowerShell cmdlet creates a new AD user?

A. Add-ADUser

B. New-ADUser

C. Create-ADUser

D. Set-ADUser

7. What does RPO measure?

A. Maximum downtime

B. Maximum data loss

C. Recovery speed

D. Backup frequency

8. Which Linux command displays real-time process information?

A. ls

B. top

C. cat

D. grep

9. Samba uses which protocol for file sharing?

A. NFS

B. FTP

C. SMB

D. HTTP

10. An LVM snapshot uses which mechanism?

A. Full copy

B. Copy-on-write

C. Mirror

D. Compression

11. Which tool is used for infrastructure as code?

A. Word

B. Excel

C. Ansible

D. Paint

12. Windows Server backup is managed by which command?

A. wbadmin

B. backup.exe

C. restore.cmd

D. xcopy

13. Which Linux file contains user account information?

A. /etc/users

B. /etc/passwd

C. /etc/accounts

D. /etc/login

14. Microsoft Entra ID was previously known as:

A. Active Directory

B. Azure AD

C. Windows NT Domain

D. LDAP

15. The vmstat command on Linux reports:

A. Virtual machine status

B. Video memory statistics

C. Virtual memory statistics

D. Volume mount status

16. Which backup type copies only changes since the last backup?

A. Full

B. Incremental

C. Differential

D. Mirror

17. In Windows, NTFS permissions are configured through:

A. Registry

B. Security tab in Properties

C. Task Manager

D. Device Manager

18. The shebang line in a Bash script is:

A. #!bash

B. #!/bin/bash

C. //bash

D. @bash

19. Which Windows service creates shadow copies?

A. DNS

B. DHCP

C. VSS

D. IIS

20. NIS stands for:

A. Network Information Service

B. Network Internet System

C. Node Identification Server

D. Network Install System

Answers to True/False Questions

1. *True.* Sysadmins maintain servers, networks, storage, and services.

2. *False.* Linux uses configuration files (e.g. /etc/ directory); the Registry is a Windows concept.

3. *True.* Cron uses crontab files to schedule recurring tasks on Linux.

4. *True.* Active Directory uses LDAP for directory queries and Kerberos for authentication.

5. *False.* Snapshots are stored on the same system; backups are stored on separate media.

6. *False.* GPOs apply centrally through Active Directory to users and computers in OUs.

7. *True.* PowerShell cmdlets output .NET objects, enabling powerful pipeline operations.

8. *False.* NTFS permissions control file access; Share permissions control network access. They are separate.

9. *True.* 3 copies, 2 media types, 1 offsite ensures robust data protection.

10. *False.* NFS is a Linux/Unix protocol; SMB is the Windows-native file sharing protocol.

11. *True.* LVM supports copy-on-write snapshots of logical volumes.

12. *True.* LDAP DNs follow a hierarchical format: CN=Name,OU=Unit,DC=Domain.

13. *False.* useradd is a Linux command; on Windows, use net user or New-LocalUser.

14. *True.* Performance Monitor provides detailed, customisable performance tracking.

15. *True.* SELinux enforces mandatory access control policies beyond standard permissions.

16. *False.* RPO measures maximum acceptable data loss; RTO measures maximum downtime.

17. *True.* Samba implements the SMB protocol on Linux for Windows-compatible sharing.

18. *False.* Modern Linux stores encrypted passwords in /etc/shadow, not /etc/passwd.

19. *True.* systemctl start/stop/enable/status commands manage systemd services.

20. *False.* VSS = Volume Shadow Copy Service, not Virtual Server Service.

Answers to Multiple Choice Questions

1. (D) Both A and B

2. (C) ADUC

3. (C) 389

4. (D) Btrfs

5. (A) LSDOU

6. (B) New-ADUser

7. (B) Maximum data loss

8. (B) top

9. (C) SMB

10. (B) Copy-on-write

11. (C) Ansible

12. (A) wbadmin

13. (B) /etc/passwd

14. (B) Azure AD

15. (C) Virtual memory statistics

16. (B) Incremental

17. (B) Security tab in Properties

18. (B) #!/bin/bash

19. (C) VSS

20. (A) Network Information Service