

# UNIX System Administration

---

---

CIS 68C1

UNIX System Administration

# Introduction

---

- UNIX History and Background
  - ✗ Major UNIX Directions
    - ✗ System V
    - ✗ Berkeley 4.x
    - ✗ Open source based
      - ✗ Linux
      - ✗ FreeBSD
    - ✗ Standards
      - ✗ POSIX
      - ✗ XOpen Spec 1170

# Administration – Essential Tasks

---

- Responsibilities of a UNIX Administrator
  - ✗ User account management
  - ✗ System hardware management
  - ✗ Backups
  - ✗ Software installation and maintenance
  - ✗ System monitoring
  - ✗ Troubleshooting
  - ✗ Maintenance of local documentation
  - ✗ Security audits
  - ✗ User assistance

# Administration – Essential Tasks

---

- User Account Management
  - ✗ Home directories
  - ✗ Group membership
  - ✗ Mail
  - ✗ Default startup files
  - ✗ Permissions
  - ✗ Accounting and restrictions
  - ✗ Communicating policies and procedures
  - ✗ Disabling / removing user accounts

# Administration – Essential Tasks

- System Hardware Management
  - ✗ Capacity planning
  - ✗ Hardware evaluation and purchase
  - ✗ Adding and removing hardware
    - ✗ Hardware configuration
    - ✗ Cabling, wiring, dip switches, etc.
  - ✗ Device driver installation
    - ✗ Kernel configuration
  - ✗ Creating device entries
  - ✗ System configuration and settings
  - ✗ User notification and documentation

# Administration – Essential Tasks

- Backups
  - ✗ Disk and backup media capacity planning
  - ✗ Performance considerations
  - ✗ Network and system impact
  - ✗ Disaster recovery
    - ✗ Onsite vs. offsite
    - ✗ Periodic testing
    - ✗ Multiple copies
  - ✗ User communication
    - ✗ Schedules
    - ✗ Downtime schedules and policies
    - ✗ Restore guarantees and procedures
    - ✗ Loss tolerance

# Administration – Essential Tasks

---

- Software Installation and Maintenance
  - ✗ Evaluation of software
  - ✗ Installation
  - ✗ Downloading and building
  - ✗ Installation directories and availability
  - ✗ Security
  - ✗ Patches and updates
  - ✗ User notification
  - ✗ Local documentation

# Administration – Essential Tasks

- System Monitoring
  - ✗ Security
    - ✗ File and directory permissions
    - ✗ Passwords
    - ✗ Break-ins
  - ✗ Hardware functioning and operational
  - ✗ Capacity
    - ✗ Disk
    - ✗ Network
  - ✗ System performance
  - ✗ Activity logs
    - ✗ Examination
    - ✗ Periodic rotation and truncation

# Administration – Essential Tasks

---

- Troubleshooting
  - × Problem discovery and diagnosis
    - × Often very difficult
  - × Root cause analysis
  - × Resolution
  - × Implementation
  - × Often requires
    - × Broad and thorough system knowledge
    - × Outside experts
    - × Luck!
  - × Expediency

# Administration – Essential Tasks

- Maintenance of Local Documentation
  - ✗ Administrative procedures and policies
    - ✗ Backup media locations
    - ✗ Hardware
      - ✗ Location
      - ✗ Description, connection, and configuration details
    - ✗ Software
      - ✗ Install media and/or download location
      - ✗ Installation, build, and configuration details
      - ✗ Patches installed
  - ✗ Acceptable use policies for users

# Administration – Essential Tasks

---

## □ Security Audits

- ✗ System logging and audit facilities
  - ✗ Evaluation and implementation
  - ✗ Monitoring and analysis
  - ✗ Traps, auditing, and monitoring programs
- ✗ Unexpected or unauthorized use detection
- ✗ System vulnerabilities analysis
- ✗ Monitoring of security advisories and newsgroups
  - ✗ Security holes and weaknesses

# Administration – Essential Tasks

---

- User Assistance
  - × Time intensive
  - × Software availability and usage
  - × Software configuration settings and variables
  - × Hardware usage, maintenance and troubleshooting
  - × Writing FAQs

# Administrative Utilities

- Administration via Command Line vs. GUI
  - ✗ Command line utilities
    - ✗ Require more knowledge to use
    - ✗ Typically similar on many UNIX systems
    - ✗ More advanced troubleshooting, problem resolution and capabilities
  - ✗ GUI-based utilities
    - ✗ Easier to use for basic or simple configuration
    - ✗ Specific to each UNIX system
    - ✗ Not widely available
    - ✗ Not standardized

# Administration Challenges

- Administration is Challenging
  - × Broad knowledge of hardware and software
  - × Balancing conflicting requirements
    - × Short-term needs vs. long term planning
    - × Requirements : end user vs. company
    - × Service provider vs. police model
  - × Work well and efficiently under pressure
  - × 24x7 availability
  - × Flexibility, tolerance, and patience
  - × Communication