System Administration

Platform Technologies

Based on

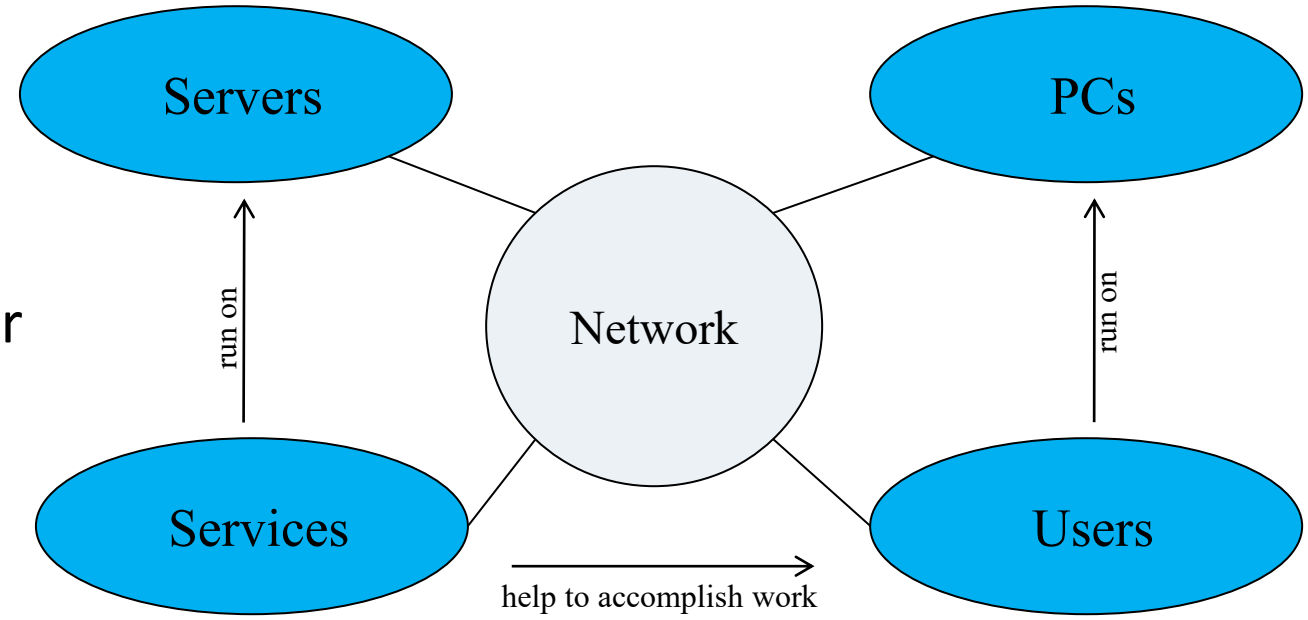
Principles of System Administration by Mark Burgess

Advanced Network and System Administration by James Walden

System Administration by James Childress

What is system administration?

- System:
  - An organized collection of computers interacting with a group of users
- System Administration
  - Activities that make the computer system functional
- System Administrator
  - Personal responsible for making computer systems functional (Sysadmin)



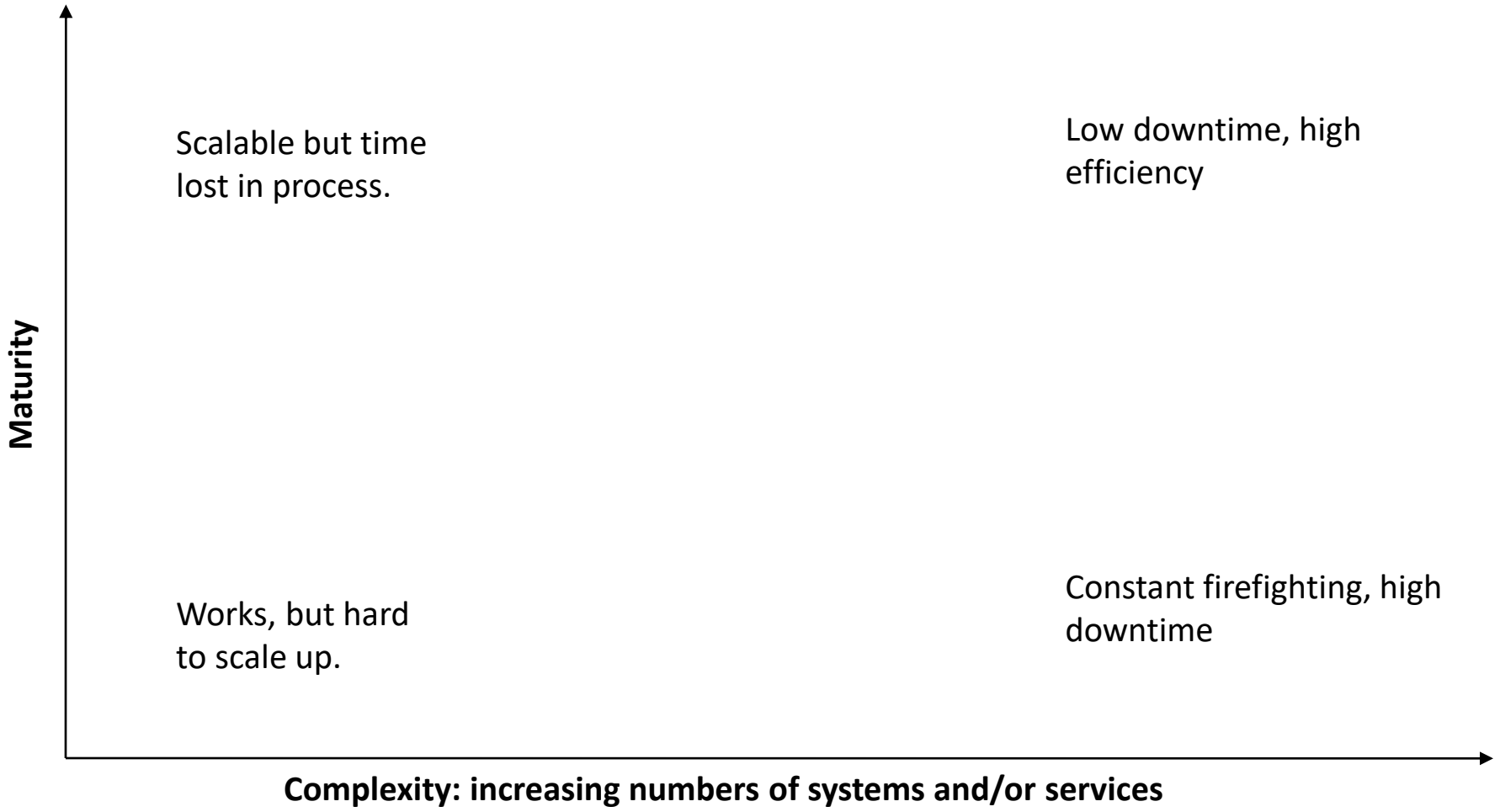
Who is a Sysadmin?

- In a “small company” the Sysadmin may be the entire information technology staff.
  - The Sysadmin may do everything from telephone, to fax, to computer management.
  - Sysadmin may have to order supplies, deal with users, develop software, repair hardware, etc.
- In a large company the Sysadmin may be one member of a large group.
  - May be responsible for one aspect of the data center operation.
    - Programmers
    - Database Administrators
    - Network Administrators
    - Operators

Types of Sites

- Small
  - 2-10 computers, 1 OS, 2-20 users.
  - Small staff size requires outsourcing to obtain most specialized skills.
- Midsized
  - 11-100 computers, 1-3 OSes, 21-100 users.
- Large
  - 100+ computers, multiples OSes, 100+ users
  - Outsources to reduce costs, some specializations.

Maturity and Complexity



Common Activities

1. Add and remove users.
2. Add and remove hardware.
3. Perform backups.
4. Install new software systems.
5. Troubleshooting.
6. System monitoring.
7. Auditing security.
8. Help users.
9. Communicate.

- The basic of system administration responsibilities can be summarized as – SUM CRUD
  - Software
  - Users
  - Machines

  - Create
  - Read
  - Update
  - Delete

User Management

- Creating user accounts
  - Consistency requires automation
  - Startup (dot) files
- Namespace management
  - Usernames and UIDs
  - Multiple namespaces or SSI?
- Removing user accounts
  - Consistency requires automation
  - Many accounts across different systems

Hardware Management

- Adding and removing hardware
  - Configuration, cabling, etc.
- Purchase
  - Evaluate and purchase servers + other hardware
- Capacity planning
  - How many servers? How much bandwidth, storage?
- Data Center management
  - Power, racks, environment (cooling, fire alarm)
- Virtualization
  - When can virtual servers be used vs. physical?

Backups

- Backup strategy and policies
  - Scheduling: when and how often?
  - Capacity planning
  - Location: on-site vs. off-site.
- Monitoring backups
  - Checking logs
  - Verifying media
- Performing restores when requested

Software Installation

- Automated consistent OS installs
  - Desktop vs. server OS image needs.
- Installation of software
  - Purchase, find, or build custom software.
- Managing software installations
  - Distributing software to multiple hosts.
  - Managing multiple versions of a software pkg.
- Patching and updating software

Troubleshooting

- Problem identification
  - By user notification
  - By log files or monitoring programs
- Tracking and visibility
  - Ensure users know you’re working on problem
  - Provide an ETA if possible
- Finding the root cause of problems
  - Provide temporary solution if necessary
  - Solve the root problem to permanently eliminate

System Monitoring

- Automatically monitor systems for
  - Problems (disk full, error logs, security)
  - Performance (CPU, mem, disk, network)
- Provides data for capacity planning
  - Determine need for resources
  - Establish case to bring to management

Helping Users

- Request tracking system
  - Ensures that you don’t forget problems.
  - Ensures users know you’re working on their problem; reduces interruptions, status queries.
  - Lets management know what you’ve done.
- User documentation and training
  - Policies and procedures
- Schedule and communicate downtimes

Communicate

- Customers
  - Keep customer appraised of process.
    - When you've started working on a request with ETA.
    - When you make progress, need feedback.
    - When you're finished.
  - Communicate system status.
    - Uptime, scheduled downtimes, failures.
  - Meet regularly with customer managers.
- Managers
  - Meet regularly with your manager.
  - Write weekly status reports.

Ethics in System Administration

Ethics

- Work place ethics are the rules of personal conduct established by social traditions and the employer for the workplace environment.
- Computers are a part of our work place.
- Employers are concerned about how their employees use the computing resources.
- Any information not belonging to an individual should be considered sensitive information by them.
- Accessing sensitive information requires coordinating such access with management and security personnel in accordance with documented “policy”.

Ethics in System Administration

- The SA may have the ability to access any
  - Files
  - Backups
  - E-mail
  - Internet usage
  - Corporate secrets
- The SA may be subject to special security clearance, a position of trust
  - Polygraph tests
  - Personal back ground checks
  - Credit reports
  - Drug testing

Ethics in System Administration

- The SA is providing a service to users.
- The computing system does not exist solely for the SA's personal amusement.
- The system-users will ultimately determine an SAs future based upon satisfaction.
- An SA must be objective in dealing with colleagues and customers.
- Separate personal and professional views.

Informed Consent

- Informing your customers of events that will impact their system usage and the availability of services.
- Customers should give consent without coercion.
- SLA – service level agreement between the SA staff and the system users.
  - Establishes expectations for users
  - Establishes responsibilities for the SA staff.

Usage Policy

- If there is no usage policy, create one.
- Employees should read and sign the policy documenting they understand the usage policy
- The employer has an ethical responsibility to disclose the policy.
- Do not use agency resources for personal use:
  - Starting a new business
  - Hosting a web site
  - Downloading copyrighted materials
  - Downloading illegal materials.
  - Pirating software

Privileged Access Conduct

- Privileged usage requires responsibility
- Privileged usage is solely for necessary work-related uses.
- Privileged users should sign the document to acknowledge they understand their responsibilities.
- Privileged users may have their access restricted on a regular basis for auditing purposes.
- Passwords to privileged accounts should be changed regularly, at least twice a year.
- A list of privileged users should be kept up to date.

Privileged Access Conduct

- All policies should be in writing and made available to privileged users.
- Warnings explaining what to expect when policies are violated.
- Procedures should be developed to minimize errors.
  - example: Backups of critical data should be made before system changes are implemented
- When someone is terminated or leaves voluntarily, appropriate measures must be taken:
  - Change passwords
  - Close accounts
  - Notify vendors, clients, etc.

Copyright Adherence

- Organizations should have policies stating that their members abide by copyright laws.
- Software piracy is pervasive and is considered stealing.
- Companies are concerned about the liability of using pirated software.

Privacy Expectations

- Many organizations consider the computer and all related data and resources to be the property of the organization.
- Your files and e-mail may be owned by your employer.
- In the financial community, e-mail, phone usage, & internet usage is monitored. (Informed Consent)
- A policy on privacy and monitoring should be in writing and provided to all employees (disclosure).
- Privacy laws may be different in another country where you are doing business.

Unethical/Illegal Requests

- Resist.
- Document any and all requests made by colleagues to do any illegal or unethical activity.
- Coercion may be used. Check the employee's guidelines for what to do.
- If the request seems dubious, check company policies and laws.
- If given a dubious request, ask for the request in writing.
- Be careful about making accusations without evidence.

Working with Law Enforcement

- Organizations should have a policy outlining how to work with law enforcement agencies.
- Verify the identities of LEA people requesting information.
- Beware of Social Engineering!

Skills Required

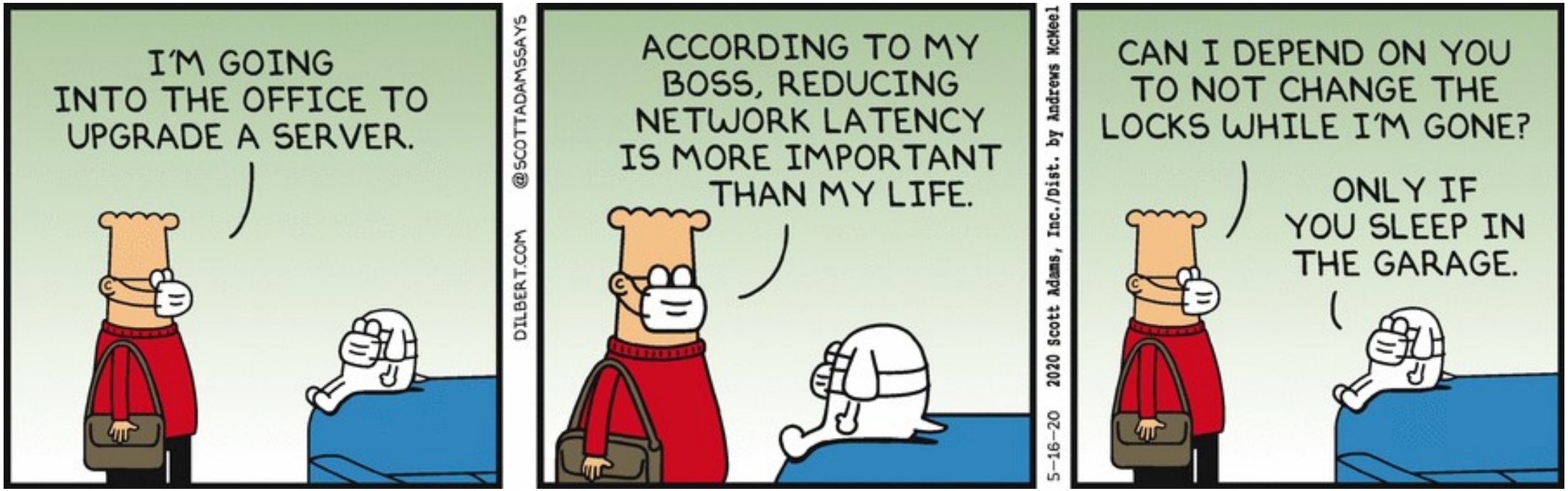
- Ability to create/follow Policies and Procedures
- Delegation and Time Management
- Customer Service Attitude
- Desire to learn
- Ethics
- Knowledge of technical aspects
  - Hardware
  - Software
  - Problem Solving

Specialized Skills

- Heterogeneous Environments
  - Integrating multiple-OSes, hardware types, network protocols, or sites.
- Databases
  - SQL RDMS
- Networking
  - Complex routing, high speed networks, voice.
- Security
  - Firewalls, authentication, NIDS, cryptography.
- Storage
  - NAS, SANs, cloud storage.
- Virtualization and Cloud Computing
  - VMware, cloud architectures.

Suggested courses

- System Administration and IT Infrastructure Services (Google)
  - https://www.coursera.org/learn/system-administration-it-infrastructure-services
- Fundamentals of Red Hat Enterprise Linux (RedHat)
  - https://www.edx.org/course/fundamentals-of-red-hat-enterprise-linux
- Introduction to Linux (The Linux Foundation)
  - https://www.edx.org/course/introduction-to-linux
- Windows Server Management and Security (University of Colorado)
  - https://www.coursera.org/learn/windows-server-management-security
- Google IT Support Professional Certificate (Google)
  - https://www.coursera.org/professional-certificates/google-it-support


I'M GOING INTO THE OFFICE TO UPGRADE A SERVER.
DILBERT.COM @SCOTTADAMSSAYS
ACCORDING TO MY BOSS, REDUCING NETWORK LATENCY IS MORE IMPORTANT THAN MY LIFE.
5-16-20 2020 Scott Adams, Inc./Dist. by Andrews McMeel
CAN I DEPEND ON YOU TO NOT CHANGE THE LOCKS WHILE I'M GONE?
ONLY IF YOU SLEEP IN THE GARAGE.