System Administration
and other stuff

Andy Steingruebl
steingra@earthlink.net
Goals

The goals of this lecture are to

_ Give you a basic understanding of the purpose and scope of system administration.

_ Teach you the basic duties of the system administrator.

_ Relate system administration to other IT work. How the system administrator relates to
  - Management
  - Users
System Administration Definition

System administration is the practice of installing, configuring, and managing computer systems and their associated peripherals.

The goal of system administration is to configure a system that is reliable, easy to use, and serves the need of the intended users.

Except for their own desktop, system administrators are not setting up machines for themselves.

System administration as a discipline is somewhere between engineering and art.
Definition

System administration is about putting together a network of computers ... getting them running and then *keeping* them running in spite of the activities of *users* who tend to cause the systems to fail. - Mark Burgess
System Administrator Duties

The basic duties of the system administrator are:

- System installation
- Administering user accounts
- Performing Backups
- Installing software and patches
- Monitoring, capacity planning, performance tuning
- Security Administration and Audit
- Documentation
- Helping users
- Storage Administration

Principles

Automate whenever possible

  _ Who likes doing the same manual labor over and over again?

Keep good records/documentation

  _ Or, don't get hit by a bus and be an indentured servant.

Simplify

  _ Complex systems are less reliable, harder to manage, and wake you up with a failure at 2am.

Systems and IT are not an end in themselves.
System Installation

What operating system do I want to install?
What components do I want to install?
  Why?
  Do I need all of them? Installed but unused software can become a maintenance burden and security liability.

How do I want to configure the disk?
Account Administration

Who should have an account on the machine?
  _ Policy?

What permissions should they have?
  _ Administrator, regular user, read-only?

System Policies
  _ Password composition, expiration?
  _ Accounts on all machines, or limited to only certain systems?
Backups

Policy

- What to back up, and for how long?
- Legal requirements?
  - Retention of certain types of information?
- Specific business requirements
  - Document retention policy
  - Electronic "shredding"
Backups – continued

A lot more complicated than it seems at first.

_ How do we get a stable copy of files that change all the time?

_ How do we back up large amounts of data?
  - Lots of tapes and lots of drives
  - Lots of network traffic?
  - Local tapes on each machine = operators on roller skates
Storage

SCSI vs. IDE

SANS

NAS

How do I pick?

How do I allocate, manage, report on, capacity plan?
Storage Interfaces/Buses

IDE

- Integrated Drive Electronics
- 1 bus can have 2 devices. Master and Slave.
- Only 1 device can talk at once.
- Commodity storage bus.
- Not good for high I/O rates. Does not scale well
- Fastest drives available are 7200RPM.
SCSI

SCSI

- Small Computer Systems Interface
- A communications bus for disks.
- SCSI supports multiple simultaneous transfers.
- Fastest drives are 15,000RPM.
- Drives are intelligent. They can often re-order transactions to get best performance based on location of drive head and platter.
Storage – New Directions

SCSI and IDE are both parallel technologies.

Parallel interfaces suffer from problems of "skew"

http://www.yale.edu/pclt/PCHW/IDESCSI.HTM has a good picture of this.

Higher speed electronics allow us to implement Serial technologies. Serial technologies do not suffer from skew problems.

- Fibre-Channel
- FireWire (IEEE 1394)
- USB-2.0
- SerialATA
Storage Area Networks (SANS)

Storage Area Networks are networks that move disk blocks as their main data elements.

_ Fibre-channel
  - 1 or 2 Gigabit/sec transport
    _ 100/200 Megabyte/sec
  - Can run over copper or fiber-optic cabling.
  - Fibre-channel is a data-link layer. Multiple network-layer protocols are defined.
    _ SCSI
    _ IP
  - Tanenbaum pages 326-327.

_ ISCSI
  - SCSI transported over IP.
SANS – continued

Why SANS?

- Allow us to share disks between many machines.
- Virtualized storage. Allows us to dynamically grow/shrink/partition storage resources between systems.
  - Treat Storage as a network-wide resource/utility.
  - Storage modeled as electricity or bandwidth.
- Higher performance
- Improved topology
  - Improved Fault Tolerance/Disaster Recovery
Network Attached Storage

Network Attached Storage is a paradigm for accessing file data over a network.

- NFS
- CIFS
- AFS

Used extensively in client-server computing. Usually a many -> one relationship between client and server.
NAS Continued

Semantics of NAS are File/Offset.

- NAS protocols are filesystems
- Filesystem to client is virtually indistinguishable from local filesystem.
- Server handles concurrent access, locking, permissions.
- Server "owns" the filesystem
SAN vs. NAS

Semantics
- Semantics of SAN are disk block
- Semantics of NAS are File/Offset

Filesystem
- SAN – each machine owns their filesystem on disk.
  - No standards for sharing filesystems.
- NAS – server owns the filesystem.
  - Arbitrates locks/concurrent access, permissions.
SAN vs. NAS
Which to Pick?

SAN

_ Choose when you need block-level semantics.
  - Database

_ When each filesystem will be used by only one server.

NAS

_ Choose when you need file/offset semantics.
  - Fileserver
  - Shared web storage repository

_ When you need concurrent access by multiple systems to the same data.
Security

System administrators touch on security all of the time.

- Authentication
- Authorization
- Audit
- Confidentiality
- Integrity
- Availability
Security

Audit is the most often overlooked component of security.

- System logs are critical
- Almost all server operating systems can generate audit logs.
  - You just have to be a wizard to understand most of them.
Audit Techniques

Sherlock Holmes approach

- Rule out everything that isn't a possibility. Anything left is suspicious.

Log files tend to have patterns.

- Remove known-good patterns
- Look through remaining logs for things that are suspicious.
- Add known-good patterns to known-good list
- Repeat

This process can take up to two weeks on a busy network.
Installing Software and Patches

A main activity of the system administrator is configuring additional software for use by users.

- Databases
- Programming tools
- Servers
  - Webserver
  - Application Server
  - Email
Patching

All systems have bugs
  _ Some more than others
Patching systems can be a full time job
  _ Unless you automate
  _ But, patches can themselves break things. Don't want to automate
  _ Catch-22
User Support

Depending on the organization, the system administrator must interact extensively with the user community. This is often the greatest challenge for the system administrator.

- System administrators often have a hard time understanding user problems.
- Users aren't very good at explaining problems.
  - The network is down
    - = I can't read my email
    = I can't get to cnn.com
A Model for User Support

Greg Jackson wrote an interesting article in this
Its all about speaking the same language, and understanding the problem from the non-IT perspective.
User Support
Teach Them to Fish

Give users the tools to help themselves.

- Good log messages
- A website or telephone status line that tells people what systems are up and which are down.
Certification

A very contentious subject

- Many believe that certifications don't demonstrate real knowledge, skills, ability.
- Certifications often very vendor dependent, cost a lot of money.
- MCSE's (Microsoft Certified System Engineer) are not guaranteed to be skilled.
  - MCSE is a paper-only test. It does not test applied skills.
- Still, there is a need for measurable skills.
Certification – continued

As system administration progresses from an "art" to an engineering discipline, there is a need for:

- Standardization
- Discipline
- Consistency
- Assurance
Certification – cont.

What other professions have certification?

- Doctors
- Lawyers
- Engineers
- Architects

Why?

- Safety concerns
- Professionalism
- A way for the government to regulate
Certification

SAGE has had system administrator job descriptions for a long time.
SAGE is now releasing a quality system administrator certification.

- Paper component
- Applied component

SANS has their GIAC certifications

Both of these follow the CISCO model for CCII
Documentation

Documentation is a critical part of system administration. It's also the most often overlooked.

Documenting what you do is a large part of being a professional.

- You are being paid to do it.
- Your employer expects it.
- It is your duty

It might even be a legal requirement.

- Quality systems as defined by the FDA
Change Control

- Process is your friend.
- It lets other people know you are a professional that plans
- It sets expectations
- It is self-documenting. Following change control processes allows you to go back and see what you've done.
- Revision control
References


The Practice of System and Network Administration. Limoncelli, Thomas. 2001

Principles of Network and System Administration. Burgess, Mark. 2000