Lecture 1

What is this subject about in a nutshell?

The subject is designed to introduce you to the *practice* of systems administration (SA).

- You will learn about the range of jobs SAs do
- You will also learn about the challenges facing SAs
- Teach you concepts that will help you to communicate with other SAs
- Provide you with technical skills to make you useful when you graduate from university

Topics

- Operating system fundamentals, structure and management
- Networking basics, routing and protocols
- System administration in the Enterprise
- System security and monitoring
- Storage concepts and technologies
- Services, infrastructure and protocols
- Backup and disaster recovery
- System Administration: Ethics and Policy

Who is a systems administrator?

- **Drink lots of coke and pizza?**
- **Likes playing solitaire?**
- **Devoted family man?**
- **Business savvy?**

- These are some traits for sure based on experience but they are generally technical in their background, are able to effectively manage people and have a good understanding of business value.

Who is a systems administrator?

- A system administrator is a person who manages one or more computer systems.
- In some cases administrators have close relationships with
  - Database administrators
  - Network administrators
  - Security administrators
  - Web administrators
  - Computer operators

What is a system?

- A computer system is any system running an operating system and capable of providing services to a user base or other hosts.
- In this course operating systems discussed will be multi-user and enforce security. They are also configurable and tunable to an extent.

The role of the systems administrator

- The role of a system administrator is to maximize a system:
  - Reliability
  - Integrity
  - Security
  - Performance
  - Efficiency
  - Ease of use
  - Order

Reliability

- Reliability is a measure of the percentage of time a machine, service and network is usable by the respective user base.
- User perception of reliability may not match measurable indicators.
- Common services such as mail, web and file sharing suffer from this ‘perception’ problem.

- In some environments certain levels of reliability MUST be achieved.

- Reliability and service level agreements (SLA's) go hand in hand.

- The easiest measure of reliability is *uptime* which shows how long a system has been up.

- It should be noted however that even though a system is up - it may be inaccessible for a number of reasons *e.g. no network connectivity.*

- Measuring service and network reliability is similar.

- It is common practice to install *monitoring* solutions such as *nagios (formerly netsaint)* (www.nagios.org) and *Cacti* (www.cacti.net) to monitor services such as POP/IMAP, HTTP and FTP. Other examples include HP *OpenView*, *StatSeeker*, *CiscoWorks*.
- Such tools can be used to monitor networks too and provide an indication of reliability.
- Some integrate with SNMP and/or use Shell Scripts

Four 9’s = 99.99% = 52 minutes downtime per year.

Five 9’s = 99.999% = 5 minutes downtime per year.

- In the case of Five 9’s a single crash/ reboot would destroy the reliability requirement.

- This measure usually does not include scheduled downtime.

Integrity

- Integrity is the degree to which data stored on a computer system can be trusted not to be lost or damaged.

- Integrity is largely effected by;
  - Storage (file system) design e.g. disk failures.
  - Administration procedures e.g. backup.
  - Protocol and hardware design e.g. security

- It is *harder* today for administrators to ensure integrity of data - this is largely due to;
  - The sheer amount of data being stored.
  - Complex systems interactions.
  - Bugs and other problems in software/hardware from vendors.
  - The list goes on.

- A number of solutions exist to help ensure integrity e.g;
  - Bacula *www.bacula.org*
  - Amanda (The Amanda Backup Program) *www.amanda.org*
  - *Commercial offerings such as Legato, Tivoli etc.*
  - TripWire (Filesystem checksum tool) *www.tripwire.org*
- However preserving the integrity of data is largely a procedural problem where we use the tools above to get it implemented.
- *First rule of thumb with system administration is tools are useless without procedure or policy.*

Security

- As you know Integrity and Security go together.

- Security is the degree to which data stored or in transit through a computer network can be relied upon not to be;
  - Destroyed
  - Altered
  - Disclosed to unauthorized parties.

- Security is effected by procedures and policy.
- For example High Security often means Lower Useability for the user. This in turn effects work flows and procedures in the organisation.
- Administrators need to understand this -- it is often their job to help design and/or advise on this.

- Security can be achieved through a number of network and host based technologies.

- Excellent examples of such technologies include *snort* (Open Source Network Intrusion Detection System) *www.snort.org*

- There are even tools to assess how vulnerable you are e.g. Nessus.

- Check out http://sectools.org/ for a listing of them all.

Performance

- From time to time the following are said;
  - Email is really slow . . .
  - My computer is not very responsive.
  - Moodle and SOLS run like a *dog.*
- Administrators are responsible for this as well.

- Within some set of constraints, systems should run as efficiently as possible and as fast as possible.

- Performance can be improved through
  - Capital expenditure
  - Procedures and Policies
  - Users

- It should be noted that performance is typically associated with networks and machines which in turn effects user services. Again the sheer complexity of modern systems makes it difficult to get the best performance out of everything.
- Things that influence performance include;
  - Underlying hardware.
  - Operating System.
  - Software design and bugs in software.
  - Tuning of operating system.
  - Administration and End User practices.
- Never fall into the habit of saying *a bigger box* or *faster network* will solve the problem.

Efficiency

- Systems should be managed in a way which maximizes the productivity of the administration staff.
- Administration staff should not have to worry about ‘small’ things but well that never really happens.
- This aim OFTEN conflicts with the other aims of an administrator.

For example:

- Centralizing a service may make it easier to administer but it may also have a detrimental effect on performance.

- Automating account creation may be efficient but can also influence security and integrity if not done correctly.

It is very hard to balance efficiency with anything else.

Ease of Use

- Ease of use is the degree to which a system allows the user base to perform their tasks in the way they desire.

- This is affected by policies and procedures

Consider the following scenario;

As users wish to change their password so they instinctively go for their car registration number.

Unfortunately the system administrators have rules on passwords.

The user cries that this system is NOT intermittently easy to use.

- The problem with ease of use is that it conflicts with what the administrator tries to do. Areas where the conflict largely occurs are;
  - Security
  - Performance
  - Integrity
- People with disabilities have specific usability requirements that SAs are required to deal with (see Legal). Ensuring accessibility features are available on all devices including phones and photocopiers. Specific support may need to given to assistive technologies (hardware such as screen readers and software such as Dragon Dictate)

- Again it is really hard to balance ease of use because administrators have to work within the bounds of organisational policies and procedures.

- An administrator can hopefully influence these but in some organisational settings it is near impossible.

Order

- Order is the degree to which the layout, operation or management of a computer system conforms to a set of regulatory policies or guidelines.
- For example consider an ISP and how they need to adhere to the Broadcasting Services Amendment (Online Services) Bill 1999 (originally from Broadcasting Service Act 1992).
- Other acts include Suicide Related Materials Offences Act 2006, Copyright Legislation Amendment 2005
- You need to think carefully how these laws will affect you and your processes.

- Company policies are often used to ensure compliance with these laws (user agreements, privacy policy, intellectual property policy and so on)

- There are other areas of policy such as
  - ethics
  - equal opportunity (gender, ethnic origins, sexual orientation, people with disabilities)
  - harassment bullying

A system administrator would typically have these skills

- Programming
  - Administrators will be expected to cut code from time to time. The code will typically be small programs either written in C or an interpreted language like Perl.
- Systems
  - Typically administrators have a strong knowledge of operating systems, systems, services and even protocols. Some administrators know RFC numbers by heart.
- Support
  - Support is fundamental to being an administrator. You need to be able to diagnose and fix problems.

You can expect administrators to do these tasks

- Install hardware.
  - Install disk, raid arrays, tape, memory.
  - Install of a cluster.
- Install and maintain software.
  - Install operating system
  - Install applications either binaries or compiles.
- Set and maintain configurations.
  - Manage users and profiles.
  - Patch and update operating system.
  - Configure services as requirements change.

- Capacity Planning and Performance Tuning.
  - Tune the operating system to perform with certain applications correctly.
  - Evaluate resource requirements such as storage, CPU, memory and networks.
  - Evaluate requirements for infrastructure environments.
- Monitoring the systems.
- Diagnose and fix problems.
  - Yes administrators must do a degree of end user support, application support and systems support.
- Maintain or increase knowledge and skills.
- Evaluate and recommend products.

- Maintain local documentation.
  - What happens if the administrator gets hit by a bus?
- Write procedures and policy.
  - Acceptable use policy.
  - Security policy.
  - Specific resource policies.
  - Disaster recovery plan.
  - Administration policies and guidelines.
- Enforcement and arbitration.
  - Include executing policies e.g. performing backups and executing audits in accordance with security policy.
- Advise and educate users and managements.

Related Fields

- Database administrator
  - integrity of the data and the efficiency and performance of the database system
- Network administrator
  - Maintenance of network infrastructure such as switches and routers
- Security administrator
  - administration of security devices such as firewalls, as well as consulting on general security measures
- Web administrator
  - Maintenance of web servers for internal or external access to web sites. Tasks include managing multiple sites, administering security, and configuring necessary components and software

SysAdmin Day

- Friday, July 26, 2019, is the 20th annual System Administrator Appreciation Day
  - System Administrator Appreciation Day is on the Last Friday of July
- System Administrators get no respect 364 days a year.
- On this special international day, give your System Administrator something that shows that you truly appreciate their hard work and dedication

  - http://www.sysadminday.com.au
  - http://sysadminday.com

Questions?