Introduction to Systems Administration

Systems Administration

School of Information Technology
Otago Polytechnic
Dunedin, New Zealand

February 19, 2013

A little history

- Systems Administration emerged as a discipline in the 1970s.
- Computers were making the transition from special purpose machines and research subjects to *infrastructure*.
- Early sysadmins were programmers who took on responsibility for configuring and maintaining servers.

So what do sysadmins do?

- Whatever is takes.
- It's still not completely well defined. Different organisations have different needs.
- The list of possible duties is always changing. More and more things are converging into the ICT domain.
  - VOIP
  - Mobile devices
  - Video conferencing

Oh, come on.

Fine, then.

- Adding and removing users
- Adding and removing hardware
- Performing backups
- Installing new software
- Monitoring the system
- Troubleshooting
- Maintaining local documentation
- Auditing security
- Helping users

The Stereotypical Sysadmin

Sysadmins have a reputation for being

- Grumpy
- Overworked
- Scornful towards users, management, and humans in general

The Stereotypical Sysadmin

Sysadmins have a reputation for being

- Grumpy
- Overworked
- Scornful towards users, management, and humans in general

The Operations Report Card

- http://opsreportcard.net
- Tom Limoncelli[1] and Peter Grace
- A set of 32 yes/no questions that gauge the strength of an organisations's ICT operations

[1] You should read his book, *The Practice of System and Network Administration*.

Public Facing Practices

1. Are user requests tracked via a ticket system?

Public Facing Practices

2. Are “the three empowering policies” defined and published?

    1. How do users get help?
    2. What is an emergency?
    3. What is supported?

Public Facing Practices

3. Does the team record monthly metrics?

Modern Team Practices

4. Do you have a policy and procedure wiki?

Modern Team Practices

5. Do you have a password safe?

Modern Team Practices

6. Is your team's code kept in a source code control system?

Modern Team Practices

7. Does your team use a bug tracking system for it's own code?

Modern Team Practices

8. In your bugs/tickets, does stability have a higher priority than new features?

- Security
- Stability
- Bugs
- Performance
- New features

Modern Team Practices

9. Does your team write “design docs”?

Modern Team Practices

10. Do you have a “post mortem process”?

Operational Practices

11. Does each service have an OpsDoc?

1. Overview
2. Build
3. Deploy
4. Common Tasks
5. Pager Playbook
6. Disaster Recovery
7. Service Level Agreement (SLA)

Operational Practices

12. Does each service have appropriate monitoring?

Operational Practices

12. Do you have a password safe?

Operational Practices

13. Do you have a pager rotation schedule?

Operational Practices

14. Do you have separate development, QA, and production systems?

Operational Practices

15. Do roll-outs to many machines have a “canary process”?

Automation Practices

16. Do you use configuration management tools like cfengine/puppet/chef?

Automation Practices

17. Do automated administration tasks run under role accounts?

Automation Practices

18. Do automated processes that generate email only do so when they have something to say?

Fleet Management Practices

19. Is there a database of all machines?

Fleet Management Practices

20. Is OS installation automated?

Fleet Management Practices

21. Can you automatically patch software across your entire fleet?

Fleet Management Practices

22. Do you have a PC refresh policy?

Disaster Preparation Practices

23. Can your servers keep operating even if one disk dies?

Disaster Preparation Practices

24. Is the network core N+1?

Disaster Preparation Practices

25. Are your backups automated?

Disaster Preparation Practices

26. Are your disaster recovery plans tested periodically?

Disaster Preparation Practices

27. Do machines in your data center have remote power/console access?

Security Practices

28. Do desktops, laptops, and servers run self-updating, silent, anti-malware software?

Security Practices

29. Do you have a written security policy?

Security Practices

30. Do you submit to periodic security audits?

Security Practices

31. Can a user's account be disabled on all systems in one hour?

Security Practices

32. Can you change all privileged passwords in one hour?

The rest of it

Let's wrap up by talking about what we'll do this semester.