Operations Management and Open Source Tools

Jeremiah Jackson - jjackson@mcnc.org

Gonzalo Guzman — gonz@mcnc.org
WHAT IS FCAPS?

- Framework for managing telecommunication and network resources.
- Developed by the ISO when similar management needs were noticed between the OSI and SMO models.

**FCAPS is:**
- Fault Detection
- Configuration
- Accounting
- Performance
- Security
Goal of Fault Management:
Recognize, isolate, correct and log faults that occur.

Components:
- Fault Detection: *Ability to recognize a error when it occurs*
- Notification: *Ability to notify when fault occurs.*
- Trending: *Setting up a series of baselines of normal operation.*
- Logging: *Keep track of faults for future review*
- Response: *Either human or automated*
FCAPS – Fault Management

Solutions:

- Nagios - http://www.nagios.org/
- OpenNMS - http://www.opennms.org/
- Vendor Specific Switch Programs:
  - HP Procurve Manager
  - CiscoWorks, etc.
- HP OpenView / EMC Smarts / IBM Tivoli
Nagios - www.nagios.org

Pros:

• Open Source
• Polls actual services for response. (HTTP, SMTP, etc)
• Flexible Addons for specialized testing
• Good Trending data and Uptime Statistics

Cons:

• Configuration is done via text files.
• Linux only
Goal of Configuration Management:
Establish and maintain consistency of performance by controlling changes, and documenting configurations throughout the life cycle of an information system.

Components:
- Gather: Collect configurations on a scheduled basis.
- Store: Store those configurations for backup purposes
- Track: Monitor and report changes to configurations.
- Automate: Ability to make mass changes with limited user input.
FCAPS – Configuration Management

Solutions:

- Rancid - http://www.shrubbery.net/rancid/
  “Really Awesome New Cisco config Differ”
  Utilizes CVS to maintain a database of configuration changes.
  Configurations can be generated for any date in time since the device was first added to Rancid.
  Linux based command-line only product.

- NetCanner - http://bangj.com

- Vendor Specific Switch Programs:
  HP Procurve Manager
  CiscoWorks, etc.
FCAPS – Configuration Management

NetCannery

Pros:
• Graphical Front End
• Troubleshooting tools such as:
  IP address analyzer
  Finds devices with unsaved changes
• Ability to create custom reports

Cons:
• Graphical Front End requires MacOS
• Sometimes has difficulty logging into older devices.
• Retail Product, fee based
FCAPS – Accounting

What is the goal of Accounting management?

To gather usage statistics for users and use those statistics, to bill users and enforce usage quotas.

For non-billed networks, "administration" replaces "accounting".

To administer a set of resources in such a way as to provide availability and accessibility to authorized users.
Components:

- Managing Accounts, passwords and permissions.
- Auditing system logs.
- Performing backups of critical data.
FCAPS – Accounting

Managing Accounts, passwords and permissions.

- LDAP
  - Microsoft Active Directory
  - Novell eDirectory
  - OpenLDAP

- TACACS
  - CiscoACS

- RADIUS
  - Steelbelted Radius
  - FreeRadius

- Diameter
Password Guidelines

- length should be a minimum of 7 characters
- should contain a mix of lower-case, upper-case, numeric and punctuation
- names, birthdays, holidays should be prohibited
- words from any language should be prohibited
- expire every 30-90 days
- Remembered the last 6 passwords
- lock out accounts after 3-5 failed attempts
Password Guidelines

- Educate your users on using Mnemonic to remember complex passwords
- 3vi1hax0r
- 2$3cur34u
- ow&uP@k12
Auditing system logs

Basic Auditing in Windows

- Enable auditing in Local Security Settings > Audit Policy or use a Group policy
- Failed logon attempts can be found in the “Security log”

Basic Auditing in *nix

- Is enabled by default
- Look for failed logon attempts
Performing backups of critical data

- Microsoft System Center Data Protection Manager
- Symantec Backup Exec and Veritas Netbackup
- Windows backup and restore
- Amanda (www.Zamanda.com)
Windows backup and restore

Pros:

• Free
• Easy to use
• Bare metal restore capable (ASR)

Cons:

• Windows only
• Reliance on legacy technology
FCAPS – Accounting

Amanda

Pros:
• Freeware
• Clients for most OS
• Easy to setup

Cons:
• Server is Linux only
• CLI intensive
FCAPS – Performance Management

**Goal of Performance Management:**
Prepare the network for the future by monitoring current network trends, utilization, error rates, and response times.

**Components:**
- Data Collection – Store performance information for retrieval.
- Visualization – Turn data into images for quick comprehension.
- Trend Analysis – Monitor data over time to recognize patterns.
- Summarization – Consolidate data in larger time blocks.
Types of Performance Measurement:

- Performance Measurement – Cacti, PRTG, MRTG, Smokeping,
- Forensics Analysis – Wireshark, NTOP, Netstumbler, TCPDump
- Load Generation – Iperf, D-ITG, Internet 2 NDT
FCAPS – Performance Management

Cacti - http://www.cacti.net/

- Open Source Visualization Tool
- Monitors all types of statistics from SNMP or custom scripts.
- Web Based administration / viewing
- Module support for scripts to handle additional types of monitoring.
- Based on RRDTool.
- Automatically summarizes data as time goes on.
FCAPS – Performance Management

WireShark - http://www.wireshark.org/

- Forensic Analysis of data on a network.
- Determine network issues like retransmissions.
- Statistics feature can playback IM sessions, and VoIP calls.
- Open Source
What is the goal of Security management?

- The process of controlling access to assets in the network
FCAPS – Security

Components:

- Policies and Procedures
- Physical security
- Firewalls
- Anti-virus, Trojan and Malware protection
FCAPS – Security

Policies and Procedures:

- "Acceptable Use Policy" and "Network Connection Policy."
- Procedure for requesting security changes.
- These documents should be very straightforward, easy to understand.
Physical Security:

- Servers should be kept in temperature and humidity controlled, locked rooms with keyboards and monitors hidden from plain sight if possible.
- Access to these rooms should be limited to key personnel.
- Don't forget a good chemical fire extinguisher.
FCAPS – Security

Firewalls:

- Host firewalls
  - Windows firewall
  - Iptables

- Network firewall
  - Cisco ASA/Pix
  - Fortigate
  - Sonicwall
  - Juniper Netscreen
  - Iptables
Anti-virus, Trojan and Malware Protection/Removal:

- Trend micro AV (www.antivirus.com)
- Symantec AV (www.symantec.com)
- ClamAV (www.clamav.net)
- Malwarebytes (http://www.malwarebytes.org)
- HijackThis (http://www.download.com/Trend-Micro-HijackThis/3000-8022_4-10227353.html)