Operations Management – Network Monitoring and Management

Dave Furiness/MCNC - dfuriness@mcnc.org
Gonzalo Guzman/MCNC - gonz@mcnc.org
Damien Ball/Granville County Schools - balld@gcs.k12.nc.us

March 9, 2010
Agenda

- Network monitoring and management – the FCAPS framework
- Open source tools
  - Nagios
  - Syslog
  - RANCID
  - Cacti
  - SmokePing
  - ntop
- Low cost commercial tools
  - NetCrunch/SolarWinds/WhatsUp Gold
  - SolarWinds demonstration
FCAPS is a network management functional model defined by ITU-T and ISO.

**FCAPS is:**
- **Fault** - Recognize, isolate, correct and log faults that occur
- **Configuration** – Manage device configurations
- **Accounting** - Gather usage statistics and use those statistics to bill users and enforce usage quotas
- **Performance** – Monitor and track short-term and long-term network and server statistics to identify trends and for capacity planning
- **Security** - Control access to assets in the network and audit security violations
## FCAPS Functional Examples

<table>
<thead>
<tr>
<th>Fault</th>
<th>Configuration</th>
<th>Accounting</th>
<th>Performance</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault detection</td>
<td>System turn-up</td>
<td>Track service usage</td>
<td>Performance data collection</td>
<td>Selective resource access</td>
</tr>
<tr>
<td>Fault correction</td>
<td>Network provisioning</td>
<td>Bill for services</td>
<td>Utilization and error rates</td>
<td>Access logs</td>
</tr>
<tr>
<td>Alarm handling</td>
<td>Auto-discovery</td>
<td></td>
<td>Data analysis</td>
<td>Security alarm/event reporting</td>
</tr>
<tr>
<td>Trouble notification</td>
<td>Backup and restore</td>
<td></td>
<td>Report generation</td>
<td>Security audit trail log</td>
</tr>
<tr>
<td>Error/event logging</td>
<td>Change management</td>
<td></td>
<td>Capacity planning</td>
<td></td>
</tr>
<tr>
<td>Network recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Open Source or Commercial Tools?

Considerations

- Cost
- Functionality, e.g. event correlation, dashboards
- Integrated solutions - open source tools are typically point solutions
- Level of effort and skills required to implement open source solutions
FCAPS – Fault Management

Solutions:

- Nagios - http://www.nagios.org/
- OpenNMS - http://www.opennms.org/
FCAPS – Fault Management

Nagios - www.nagios.org

Pros:
- Open Source
- Polls actual services for response. (HTTP, SMTP, etc)
- Flexible Add-ons for specialized testing
- Good Trending data and Uptime Statistics

Cons:
- Configuration is done via text files.
- Linux only
Nagios Demo
FCAPS – Fault Management

System logging

- Syslog – Redhat, CentOS, Fedora Core
- Klogd – Ubuntu
- Kiwi Syslog - http://www.kiwisyslog.com/
- Splunk – http://www.splunk.com/
**ASA**

```
conf t
logging enable
logging host <interfacename> <ip or hostname of syslog server>
no logging timestamp
no logging device-id
logging trap debug
logging facility 20
exit
write mem

**Add to syslog.conf file**

local3.debug /var/log/ciscofw
```
FCAPS – Fault Management

Splunk – http://www.splunk.com

- Search and analysis engine
- Works on live or historical data
- Windows, Linux, Mac
FCAPS – Configuration Management

Solutions:

- NetCanner - http://bangj.com
RANCID- http://www.shrubbery.net/rancid/

Pros:
- Automates configuration collection process
- Stores configuration files in a revision control system
- Alerts to configuration changes via email
- Supports most switches and routers

Cons:
- Linux only
- Text configuration file
- No GUI interface
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
**Types of Performance Measurement:**

- Performance Measurement – Cacti, PRTG, MRTG, Smokeping,
- Forensics Analysis – Wireshark, NTOP, Netstumbler, TCPDump
- Load Generation – Iperf, D-ITG, Internet 2 NDT
Cacti - http://www.cacti.net/

Pros:
- Open Source
- Web based configuration and viewing
- Good Trending data and Statistics
- Large open source community support

Cons:
- Linux only
SmokePing - http://oss.oetiker.ch/smokeping/

Pros:
- Open Source
- Web based viewing
- Good Trending data and Statistics

Cons:
- Linux only
- Text configuration file.
FCAPS – Performance Management

ntop - http://www.ntop.org/

Pros:
- Open Source
- Web based viewing
- Good Trending data and Statistics

Cons:
- Linux only
- Text configuration file.
Performance Tools Demo
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
Commonly Used Commercial Tools

- **Vendor agnostic**

- **Vendor Specific**
  - HP Procurve Manager
  - CiscoWorks, etc.

- **Considerations**
  - Understand the vendor pricing model
    - Interfaces…..nodes…..volumes…..etcetera
  - Base package versus options
  - Understand product functionality
<table>
<thead>
<tr>
<th>Tool</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>adrem software</strong></td>
<td></td>
</tr>
<tr>
<td>NetCrunch 6.x Premium 300 + 10 Remote Access</td>
<td>$4,500</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>????:</td>
</tr>
<tr>
<td>1 Year Service Agreement and Upgrade Protection (Yr. 2+)</td>
<td>$1,575</td>
</tr>
<tr>
<td><strong>SolarWinds</strong></td>
<td></td>
</tr>
<tr>
<td>Orion Network Performance Monitor SL250</td>
<td>$5,474</td>
</tr>
<tr>
<td>Orion Network Configuration Manager DL200</td>
<td>$4,995</td>
</tr>
<tr>
<td>1 Year Service Agreement and Upgrade Protection (Yr. 2+)</td>
<td>$2,000</td>
</tr>
<tr>
<td><strong>WhatsUp Gold</strong></td>
<td></td>
</tr>
<tr>
<td>WhatsUp Gold Premium – up to 300 devices</td>
<td>$3,895</td>
</tr>
<tr>
<td>WhatsConfigured – up to 300 devices</td>
<td>$5,395</td>
</tr>
<tr>
<td>1 Year Service Agreement and Upgrade Protection (Yr. 2+)</td>
<td>$1,720</td>
</tr>
</tbody>
</table>
SolarWinds Products Used - Granville County Schools

Orion Network Performance Monitor
Device Monitoring
Fault Monitoring
Bandwidth (Interface) Monitoring
Condition-based Alerting
Syslog Collection
Cisco Energywise Support

Orion Network Configuration Manager
Network Device Configuration
Granular Network Inventory (Device and Data)
Network Policy Management and Remediation

Orion Application Performance Monitor
Application Monitoring
Application Fault Alerting
Forum container dedicated to network monitoring and management at:

https://www.mcnc.org/forums