DNS/DNSSEC Workshop

Monitoring

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Monitoring

The DNS Service is now running, so we can think about monitoring and managing this service:

- Troubleshoot with logs
- Analyze performance via statistic logs
- Monitor service Availability
- Monitor service Performance

Network Management Details

In General We Monitor…

- System & Services
  - Available, reachable, responding as expected
- Resources
  - Expansion planning, maintaining availability
- Performance
  - Round-trip-time, throughput, latency
- Changes and configurations
  - Documentation, revision control, logging

We Keep Track Of:

- Statistics
  - For purposes of accounting and metering
- Faults (Intrusion Detection)
  - Detection of issues,
  - Troubleshooting issues and tracking their history
  - Ticketing systems are good at this
  - Help Desks are a useful to critical component
- The above are topics for a full-fledged Network Monitoring and Management course

Expectations

- A network in operation needs to be monitored in order to:
  - Deliver projected SLAs (Service Level Agreements) for services being provided
  - SLAs depend on policy
    - What does your management expect?
    - What do your users expect?
    - What do your customers expect?
    - What does the rest of the Internet expect?
  - What's good enough? 99.999% Uptime?
    - Defining uptime (maintenance windows)

Baselining

What is normal for your network?

- If you've never measured or monitored your network you will need to know things like:
  - Typical load on links => Cacti
  - Level of jitter between endpoints => Smokeping
  - Typical availability of services => Nagios
  - Typical percent usage of resources
  - Typical amounts of "noise":
    - Network scans
    - Dropped data
    - Reported errors or failures

Monitoring Tools We'll Configure

- Logging

bind	zone transfers, config changes queries, security issues
Swatch	realtime regex checks on logs

- Availability

Nagios	Services, servers, routers, switches

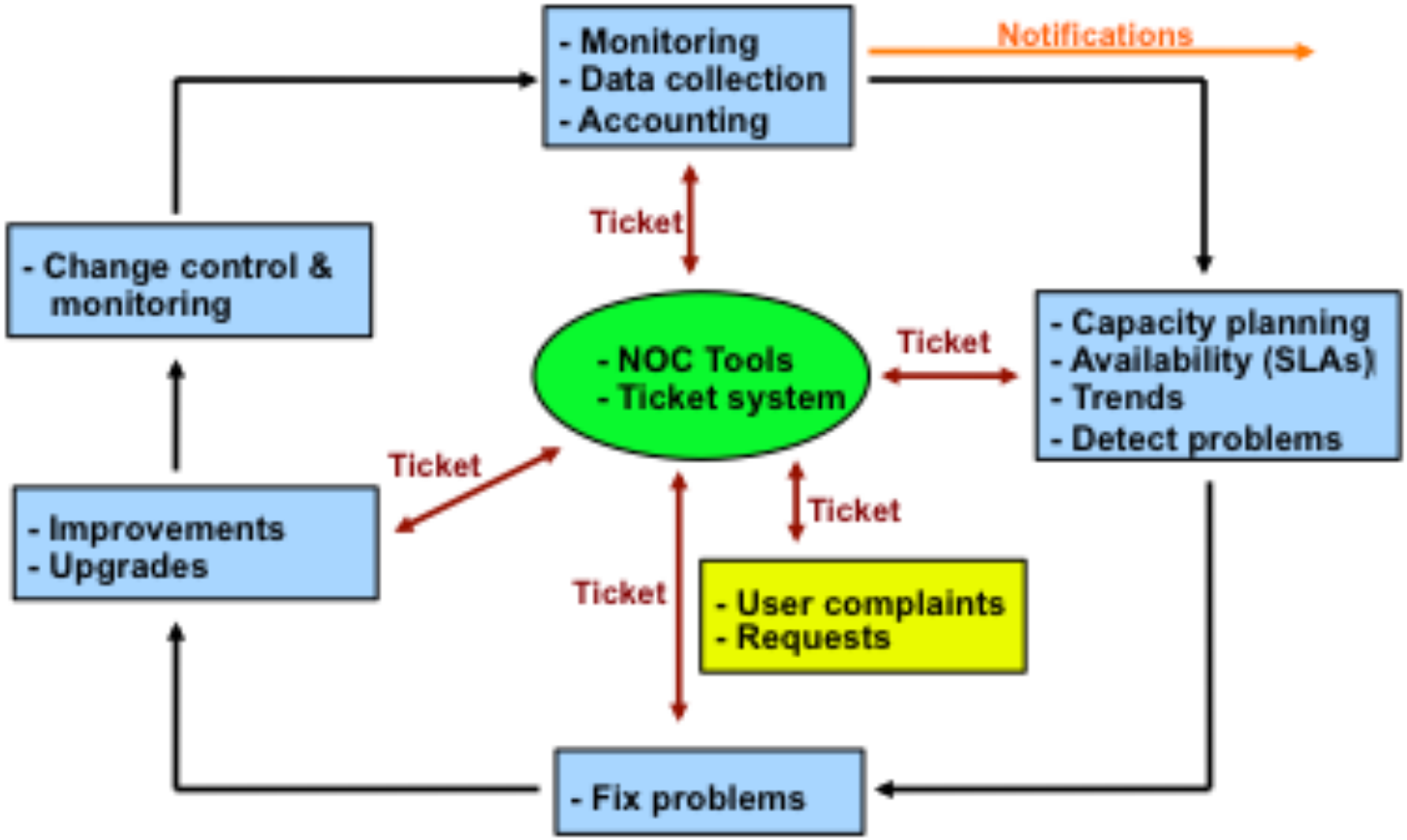
- Reliability

Smokeping	Connection health, rtt, service response time, latency

Attack Detection

- Trends and automation allow you to know when you are under attack.
- The tools in use can help you to mitigate attacks:
  - Flows across network interfaces (NetFlow)
  - Load on specific servers and/or services (Cacti)
  - Multiple service failures (Nagios)

The Big Picture



A *few* Open Source Options

- Performance
  - Cricket
  - dnstop
  - dsc
  - mrtg
  - NetFlow
  - NfSen
  - ntop
  - perfSONAR
  - pmacct
  - rrdtool
  - SmokePing
- Ticketing
  - Request Tracker
  - Trac
  - Redmine
- Change Mgmt
  - Mercurial
  - Rancid (routers)
  - CVS
  - Subversion
  - git
- Security/NIDS
  - Nessus
  - OSSEC
  - Prelude
  - Samhain
  - SNORT
  - Untangle
- Logging
  - swatch
  - syslog/rsyslog
  - tenshi
- Net Management
  - Big Brother
  - Big Sister
  - Cacti
  - Hyperic
  - Munin
  - Nagios
  - OpenNMS
  - Sysmon
  - Zabbix
- Documentation
  - IPplan
  - Netdisco
  - Netdot
  - Rack Table

Protocols/Utilities

- SNMP, Perl, ping

Monitoring DNS

- Logging
- Monitoring Availability: Nagios
- Monitoring Reliability: SmokePing
- More Monitoring

Monitoring

- What can we monitor about DNS service?

- DNS service running on TCP/UDP port 53
- Monitor service port
- Service availability
- Query response time
- Latency graphing
- All the specifics of types of queries:
  - Most common types
  - Most popular zones
  - Most popular domains
  - Etc…

Monitoring with Nagios

- Nagios
- Very popular monitoring software
- Open source
- check_ping
- check_dns
- check_zone_auth
- Hundreds of plug-ins
- Availability reports auto-generated
- Modular configuration
- http://www.nagios.org/

Monitoring with Nagios

- In our exercises we will:

- Add DNS host
- Create dns-servers hostgroup
- Use check_ping and check_dns plugin to monitor our master, cache and slave servers for MYTLD

- Configuration will be kept simple.

dns-servers.cfg

```
define host{
        use                     freebsd-server
        host_name               master
        alias                   master
        address                 10.10.31.1
}

define host{
        use                     freebsd-server
        host_name               cache
        alias                   cache
        address                 10.10.31.2
}

define host{
        use                     freebsd-server
        host_name               slave
        alias                   slave
        address                 10.10.22.1
}
```

Add hostgroup to dns-servers.cfg

```
define hostgroup {
        hostgroup_name  dns-servers
        alias           DNS Servers
        members         cache,master,slave
}
```

Add service monitoring to dns-servers.cfg

```
define service {
        use                             generic-service
        hostgroup_name                  dns-servers
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
}

define service {
        use                             generic-service
        hostgroup_name                  dns-servers
        service_description             Check DNS
        check_command                   check_dns!www.oregon.ducks
}
```

Monitoring with SmokePing

- SmokePing, an open source software
- Monitor latency
- Provide performance graph
- DNS probe is available and will be used
- Configuration file uses hierarchies
- For service, server and connection latency monitoring probably #1 product in use worldwide.

SmokePing and Nagios In Depth

- Complete presentations and exercises are available on class website reference section.

- Nagios is large, complex and includes a world-class notification system.

Some More Tools

- DNSTOP
  http://dns.measurement-factory.com/tools/dnstop/
- DSC (DNS Statistics Collector)
  http://dns.measurement-factory.com/tools/dsc/
- Nagios check_zone_auth Plugin
  http://dns.measurement-factory.com/tools/nagios-plugins/check_zone_auth.html
- SOA Compare
  dig +nssearch MYTLD