Robust & Reliable DNS Operations

Logging & Monitoring

Logging & 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

Network Management Details

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

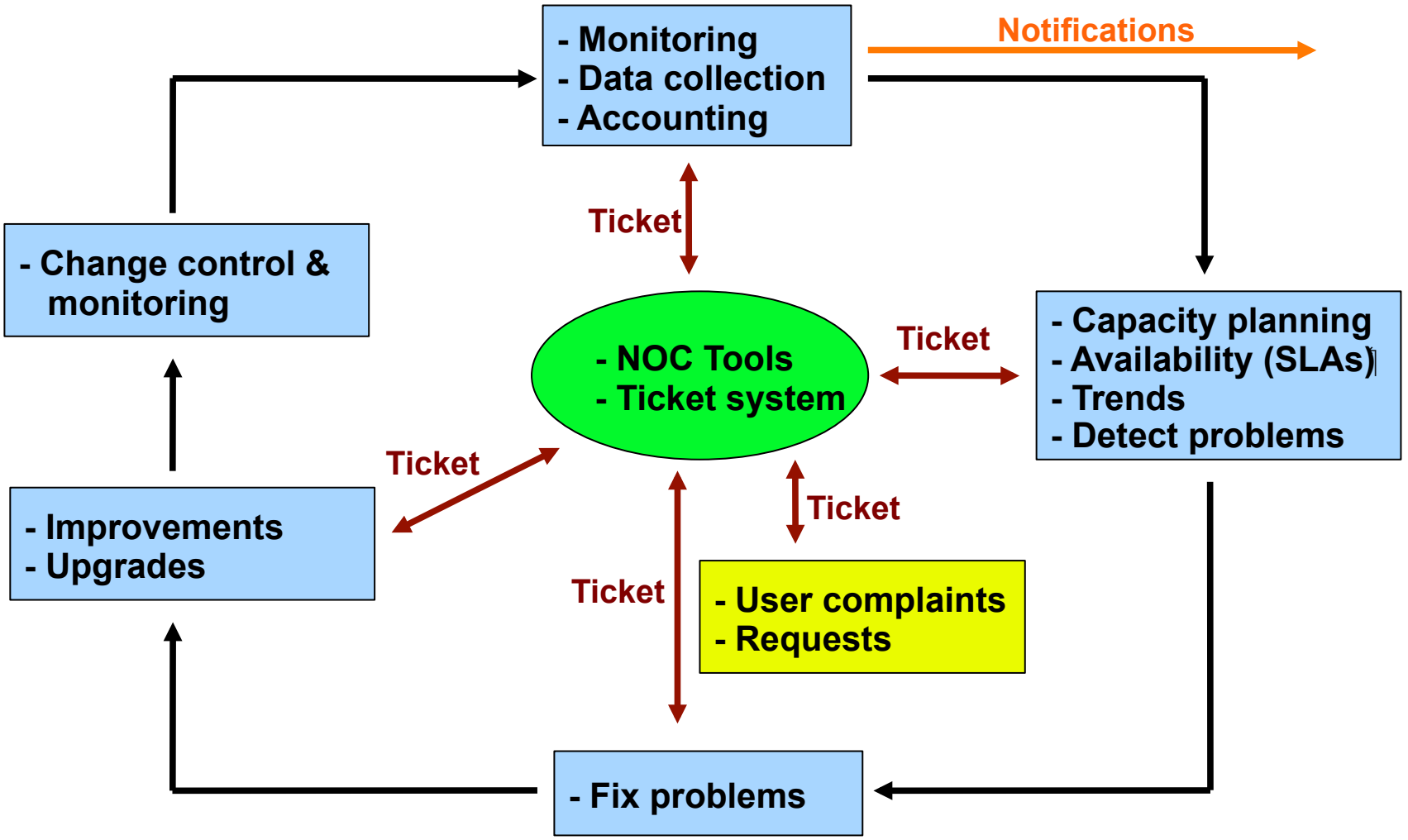
Attack Detection

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

Logging and DNS

- DNS logs are useful for troubleshooting
- Understand what is happening with the DNS service
- Statistics collector

Logging Categories

- client, config, database, default, delegation-only, dispatch, dnssec, general, lame-servers, network, notify, queries, resolver, security, unmatch, update, update-security, xfer-in, xfer-out

Logging Categories cont.

Commonly used:

- *dnssec*
- *general*
- *lame-servers*
- *notify*
- *queries*
- resolver
- *security*
- *xfer-in and xfer-out*

Logging Samples

```
10-Feb-2011 17:31:42.748 dispatch: dispatch
0x2bb3c3e0: shutting down due to TCP receive error:
12.34.56.78#53: unexpected end of input
10-Feb-2011 19:07:43.647 client: client
12.34.56.78#58216: error sending response: not
enough free resources
10-Feb-2011 17:21:28.703 general: the working
directory is not writable
14-Feb-2011 13:02:05.623 queries: info: client
120.50.62.74#37899: query: 139.134.110.10.in-
addr.arpa IN PTR + (10.20.0.56)
17-Feb-2011 11:18:15.331 client 127.0.0.1#61235:
transfer of 'MYTLD/IN': AXFR started
17-Feb-2011 11:18:15.331 client 127.0.0.1#61235:
transfer of 'MYTLD/IN': AXFR ended
```

Logging Management: part 1

```
logging {
        // Channels

        channel transfers {
            file "/etc/namedb/log/transfers" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
        channel notify {
            file "/etc/namedb/log/notify" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
        channel dnssec {
            file "/etc/namedb/log/dnssec" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
        channel query {
            file "/etc/namedb/log/query" versions 5 size 10M;
            print-time yes;
                        severity info;
        };
        channel general {
            file "/etc/namedb/log/general" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
```

Logging Management: part 2

Assign categories to logging **channels**:
- i.e. to what log file to write category-specific messages

```
// Categories

        category xfer-out { transfers; };
        category xfer-in { transfers; };
        category notify { notify; };

        category lame-servers { general; };
        category config { general; };
        category default { general; };
        category security { general; };
        category dnssec { dnssec; };

        // category queries { query };

}; // end of logging section
```

Logging with syslog-ng/rsyslog

- Syslog-ng or rsyslog for remote logging
- Aggregate to central logging server
- Analyze log data (swatch, tenshi, many other tools)

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/

Nagios®

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.

Monitoring with Nagios

In dns-servers.cfg (sample):

```
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
}
```

Monitoring with Nagios

Add hostgroup to dns-servers.cfg:

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

Monitoring with Nagios

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

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

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

Monitoring

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
```