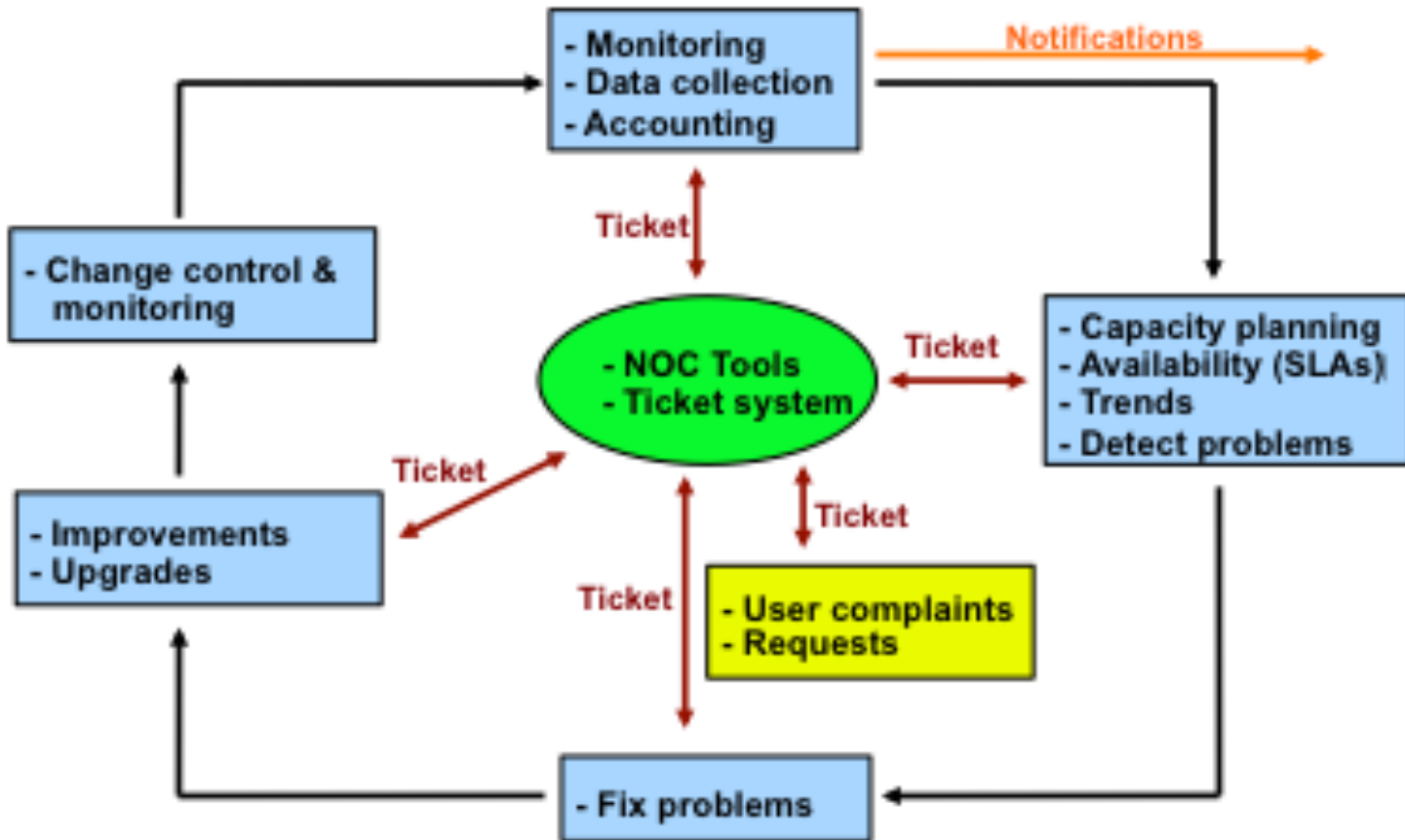


WACREN DNS/DNSSEC Regional Workshop

Monitoring

The Big Picture of Monitoring



Monitoring DNS

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

Monitoring DNS

- Logging
- Monitoring Availability
- Monitoring Reliability

Monitoring Tools for DNS

- 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

Monitoring DNS

- 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 the lab, you will:
 - Add DNS host
 - Create dns-servers hostgroup
 - Use check_ping, check_dns, check_dig plugin to monitor your master, slave, and cache servers for you domain
- Configuration will be kept simple.

dns-servers.cfg

```
define host{
    use                generic-service
    host_name          master
    alias              master
    address            10.10.31.1
}

define host{
    use                generic-service
    host_name          cache
    alias              cache
    address            10.10.31.2
}

define host{
    use                generic-service
    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.google.com
}
```

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 are available on
 - www.nagios.org
 - www.smokeping.org
- 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

Some Useful Websites

- www.zonemaster.fr
- www.intodns.com

Questions ?