Robust & Reliable DNS Operations

Logging & Monitoring

Logging & Monitoring

DNS Service is running now, and we can:-

- Troubleshooting with logs
- Analyze performance via statistic logs
- Monitoring service Performance
- Monitoring service Availability

Logging

- DNS logs are useful when come to troubleshooting
- Understand what is happening on DNS service
- Statistic 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

Commonly see:-

- 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)
```

Logging Management

```
logging {
    channel bind_logging {
        file "/var/log/bind.log" versions 3;
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;
};

        channel query_logging {
                file "/var/log/query.log" versions 10 size 100m;
                severity debug 3;
                print-time yes;
                print-severity yes;
                print-category yes;
        };

       category default { bind_logging; };
       category queries { query_logging; };
}
```

Logging Management

```
logging {
    channel security_logging {
        file "/var/log/security.log" versions 3;
        severity warning;
        print-time yes;
        print-severity yes;
        print-category yes;
};

        channel lameservers_logging {
                file "/var/log/lameservers.log" versions 10 size 100m;
                severity debug 3;
                print-time yes;
                print-severity yes;
                print-category yes;
        };

       category security { security_logging; };
       category lame-servers { lameservers_logging; };
}
```

Logging with Syslog-ng

- Syslog-ng for remote logging
- Aggregate to central logging server
- Analyze log data

Logging with Syslog-ng

TUTORIAL

Monitoring

What can we monitor on DNS service?

- DNS service running on TCP/UDP port 53
- Monitor service port
- Service availability
- Query response time
- Latency graphing

Monitoring with Nagios

Nagios

- Popular monitoring software
- Open source software
- check_ping
- check_dns
- Availability report

Monitoring with Nagios

Tutorial We will:-

- Add DNS host
- Create DNS hostgroup
- Use check_ping and check_dns plugin to monitor service

Monitoring with Nagios

TUTORIAL

Monitoring with Nagios

Add host:-

```
define host{
        use                     generic-server
        host_name               ns1.apricot.org
        alias                   ns1-apricot
        address                 10.10.10.10
}

define host{
        use                     generic-server
        host_name               ns2.apricot.org
        alias                   ns2-apricot
        address                 10.10.10.20
}
```

Monitoring with Nagios

Add hostgroup:-

```
define hostgroup{
        hostgroup_name  dns-servers
        alias           Apricot DNS Server
        members         ns1.apricot.org, ns2.apricot.org
}
```

Monitoring with Nagios

Add service monitoring:-

```
define service{
       use                 generic-service
       host_name           ns1.apricot.org
       service_description PING Check
       check_command       check_ping!100.0,20%!500.0,60%
}

define service{
       use                    generic-service
       host_name              ns1.apricot.org
       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

Monitoring with Smokeping

TUTORIAL

Monitoring

Other useful tools

- DSC
- SOA Compare