NAGIOS

Tim Shaw

Clinical School Information Management Services Unit

tim.shaw@imsu.ox.ac.uk

NAGIOS

What is it? & what can it do for you?
Architecture
Demo
Installation
Configuration
Advanced stuff

NAGIOS

Problems facing sysadmins

- Increasing numbers of systems

NAGIOS

Problems facing sysadmins

- Increasing numbers of systems
- Increasing complexity of systems

NAGIOS

Problems facing sysadmins

- Increasing numbers of systems
- Increasing complexity of systems
- More systems + More services = more stuff to break

NAGIOS

Problems facing sysadmins

- Increasing numbers of systems
- Increasing complexity of systems
- More systems + More services = more stuff to break
- More time spent monitoring and maintaining

NAGIOS

More problems facing sysadmins

- Heterogeneous systems

NAGIOS

More problems facing sysadmins

- Heterogeneous systems
- User expectations of higher availability.

NAGIOS

More problems facing sysadmins

- Heterogeneous systems
- User expectations of higher availability.
- The need to do more but spend less.

NAGIOS

A solution would ...

Monitor whether servers and devices are online.

NAGIOS

A solution would ...

Monitor whether servers and devices are online.

Monitor all "services" and "resources" to see if they are functioning properly.

NAGIOS

A solution would also...

Define fine-grain thresholds
for what is and isn't right.

NAGIOS

A solution would also...

Define fine-grain thresholds
for what is and isn't right.

Be easily extensible and customizable,
so we can run our own checks

NAGIOS

A solution would also...

Let the right person know of a problem.

NAGIOS

A solution would also...

Let the right person know of a problem.

Allow the person to acknowledge the problem.

NAGIOS

A solution would also...

Let the right person know of a problem.

Allow the person to acknowledge the problem.

Notify someone else if someone doesn't respond to the problem, (escalation).

NAGIOS

A solution might even...

- Be able to take action to try to rectify the problem

NAGIOS

The good news is...

Nagios can do all this.

NAGIOS

What is it?

An open-source, Unix-based enterprise monitoring package with a web-based console

It can monitor hosts,
networks and services via TCP/IP

NAGIOS

Its free!

In the sense that it is free to use
but will cost time to implement.

NAGIOS

Its free!

In the sense that it is free to use
but will cost time to implement.

And of course it has value!

NAGIOS

What is it?

- System for monitoring things.
- System for taking action when "things" aren’t working right.
- System for reporting problems to someone who can fix them.

NAGIOS

Why NAGIOS?

Originally NetSaint

NAGIOS

Why NAGIOS?

Originally NetSaint

now (yet another) recursive acronym:

NAGIOS Ain't Gonna Insist On Sainthood

NAGIOS

Why NAGIOS?

Originally NetSaint

now (yet another) recursive acronym:

NAGIOS Ain't Gonna Insist On Sainthood

Is it a hard 'G' or not?!

NAGIOS

What can it do for you?

- Monitoring and reporting on hosts and services running Windows, Linux, NetWare and other operating systems as well as printers, switches and anything else talking TCP/IP.

Nagios

Features

- Nagios supports both active and passive checks.
- Hosts can have hierarchical relationships.
- Nagios runs plugins that do the actual checks.
- Status information is displayed through a web interface.
- Nagios sends notifications, typically email or SMS/Pager.
- Nagios uses an object and template based definition.
  and configuration system.

Nagios

Architecture

- Nagios Daemon

Nagios

Architecture

- Nagios daemon
- Web interface

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

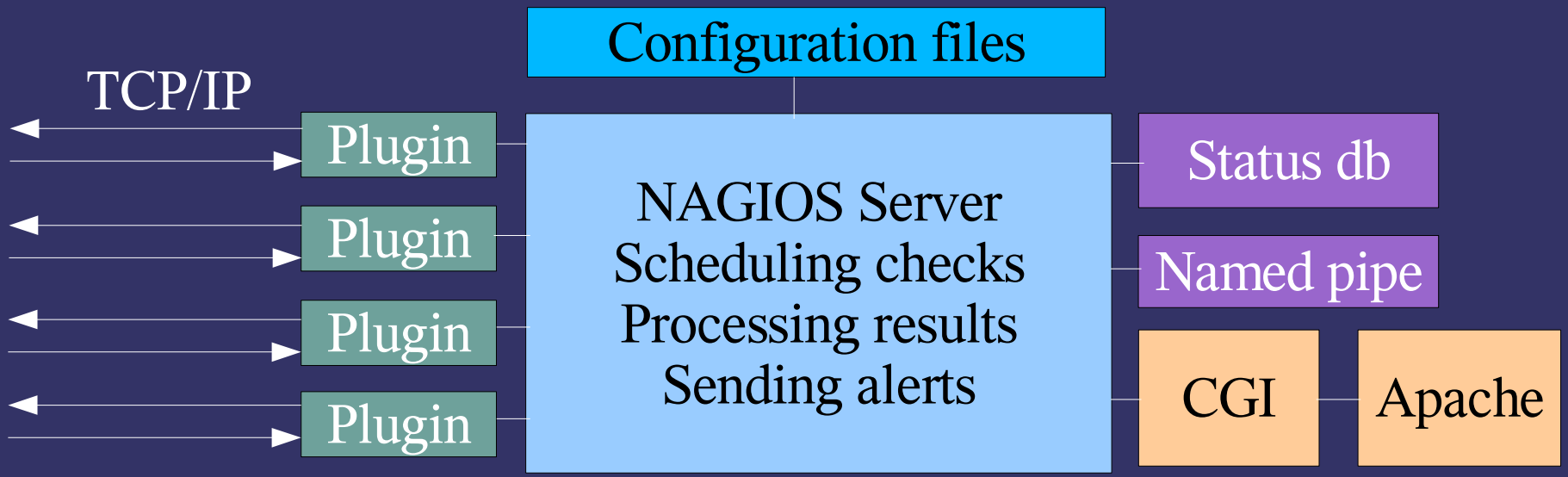
Nagios

Architecture

- Monitors host/service availability
- Maintains status database
- Provides named pipe
- Intelligent scheduling of service checks
- Event handling
- Handles notifications

Nagios

Architecture



Nagios

Alerts

- Primarily email but also SMS
- Also possible to use IM and Pagers
- Configured using notification commands in config - eg:

```
•# 'host-notify-by-email' command definition
define command {
        command_name    host-notify-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios  *****\n\n \
                Notification Type: $NOTIFICATIONTYPE$\nHost: \
                $HOSTNAME$\n State: $HOSTSTATE$\n Address: $HOSTADDRESS$\n \
                Info: $HOSTOUTPUT$\n\n Date/Time: $LONGDATETIME$\n" \
                | /usr/bin/mail -s "Host $HOSTSTATE$ alert for $HOSTNAME$!" $CONTACTEMAIL$
        }
```

Nagios

File layout

/usr/local/nagios/

/bin	Server files
/etc	Configuration files
/libexec	Plugins
/sbin	cgi-bin directory
/share	html files
/var	named pipe, log files, status data, runtime info

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

Nagios

Status database

Stores all host and service related history.

- In Nagios 1.x can be text, or to MySQL, or Postgres.
- In Nagios 2.x can be text and/or handled by Nagios Event Broker.

Nagios

Object states

- Host states

Nagios

Object states

- Host states
  - OK DOWN UNREACHABLE

Nagios

Object states

- Host states
  - OK DOWN UNREACHABLE
- Service states

Nagios

Object states

- Host states
  - OK DOWN UNREACHABLE
- Service states
  - OK WARNING CRITICAL UNKNOWN

Nagios

Object states

- Host states
  - OK DOWN UNREACHABLE
- Service states
  - OK WARNING CRITICAL UNKNOWN
- Hard and soft states

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

Nagios

Plugins

- Collection of standalone programs (check_http, check_smtp, etc...).
- Nagios uses output of programs to determine status.
- Managed as a separate project from Nagios core (nagiosplug.sourceforge.net).
- Some plugins require external software (nrpe, snmpd,sshd) to obtain information

Nagios

Remote Checks

- What about checking remote systems?

Nagios

Remote Checks

- What about checking remote systems?
- MRTGEXT.NLM for Netware

Nagios

Remote Checks

- What about checking remote systems?
- MRTGEXT.NLM for Netware
- NSCLIENT for Windows
  - uses NRPE (Nagios Remote Program Executor)

Nagios

Architecture

- Nagios daemon
- Web interface
- Status database
- Plugins and remote "helpers"
- Configuration files

Nagios

Configuration files

- Runtime Configuration
  - cgi configuration (cgi.cfg) Configuration of authorisation, statusmaps etc.
  - daemon configuration (nagios.cfg) Main global configurations

Nagios

Configuration files

- Runtime Configuration
  - cgi configuration (cgi.cfg) Configuration of authorisation, statusmaps etc.
  - daemon configuration (nagios.cfg) Main global configurations
- Basic Objects
  - check commands (checkcommands.cfg)
  - contacts (contacts.cfg)
  - hosts (hosts.cfg)
  - services (services.cfg)

Nagios

Configuration files

- Runtime Configuration
  - cgi configuration (cgi.cfg) Configuration of authorisation, statusmaps etc.
  - daemon configuration (nagios.cfg) Main global configurations
- Basic Objects
  - check commands (checkcommands.cfg)
  - contacts (contacts.cfg)
  - hosts (hosts.cfg)
  - services (services.cfg)
- Advanced Objects
  - host groups (hostgroups.cfg)
  - contact groups (contactgroups.cfg)
  - escalations (escalations.cfg)
  - time periods (timeperiods.cfg)

Nagios

Configuration files

- nagios.cfg
  - Contains global settings
  - Pointers to other config files
  - Pointers to config directories

Nagios

Configuration files : examples

```
# 'check_smtp' command definition
# goes into checkcommands.cfg
#
define command {
    command_name check_smtp
    command_line /usr/local/nagios/libexec/check_smtp \
        -H $HOSTADDRESS$
}
```

Nagios

Configuration files : examples

```
# 'check_smtp' command definition
# goes into checkcommands.cfg
#
define command {
    command_name check_smtp
    command_line /usr/local/nagios/libexec/check_smtp \
        -H $HOSTADDRESS$
}
```

- Notice the use of macros – see docs for full list

Nagios

Configuration files : examples

```
# 'check_smtp' command definition
# goes into checkcommands.cfg
#
define command {
    command_name check_smtp
    command_line /usr/local/nagios/libexec/check_smtp \
        -H $HOSTADDRESS$
}
```

This is a simple example – some check commands will include detailed definitions of warning and critical thresholds and more specific checking criteria defined as part of the command line.

Nagios

Configuration files : examples

```
# 'tim' contact definition – goes in contacts.cfg
#
define contact {
    contact_name                    tim
    alias                           Tim Shaw
    service_notification_period     24x7
    host_notification_period        24x7
    service_notification_options    w,u,c,r
    host_notification_options       d,u,r
    service_notification_commands   notify-by-email
    host_notification_commands      host-notify-by-email
    email                           tim.shaw@imsu.ox.ac.uk
}
```

Nagios

Configuration files : examples

Notification options

d	Send notification when host DOWN
c	Send notification when service is in CRITICAL state
f	Sends notification when service or host is flapping
n	Send no notifications
r	Send notification when host or service recovers
w	Send notification when service is in WARNING state
u	Send notification when service is in UNKNOWN state or host is UNREACHABLE

Nagios

Configuration files : examples

```
# this group contains all the people responsible
# for smtp servers
#
define contactgroup {
    contactgroup_name  smtp-admins
    alias smtp mail    Mail Administrators
    members            tim,mark,john
}
```

Nagios

Configuration files : examples

```
# smtp1 host definition
#
define host   {
    host_name                smtp1.company.com
    alias                    primary smtp server
    parents                  primary-gw
    address                  10.0.0.1
    checks_enabled           1
    notifications_enabled 1
    check_command            check-host-alive
    max_check_attempts    20
    notification_interval 60
    notification_period   24x7
    notification_options  d,u,r
}
```

Nagios

Configuration files : examples

```
define service   {
    name                        smtp
    notifications_enabled       1
    process_perf_data           1
    notification_interval       60
    check_period                24x7
    check_command               check_smtp
    max_check_attempts          3
    normal_check_interval       3
    retry_check_interval        1
    notification_options        w,u,c,r
    notification_period         24x7
    host_name                   smtp1
    contacts                    tim
}
```

Nagios

Configuration files : examples

```
# this group contains all the servers running
# an smtp daemon
#
define hostgroup {
    hostgroup_name  smtp-servers
    alias           Mail Servers
    contact_groups  smtp-admins
    members         smtp1,smtp2,smtp3
}
```

Hostgroups are a way to group together a set of hosts which can then be assigned services, contacts, etc.
Servicegroups can be similarly defined.

Nagios

Configuration files : templates

Declare a template by setting register = 0

```
define host   {
...
    register          0 ; DON'T REGISTER THIS DEFINITION
...

}
```

This will prevent Nagios from treating the template as an ordinary host definition.

Nagios

Configuration files : templates

```
define host   {
    name                generic-host
    check_command       check-host-alive
    register            0 ; DON'T REGISTER THIS DEFINITION
    notifications_enabled       1
    event_handler_enabled       0
    process_perf_data           1
    max_check_attempts          20
    notification_interval       60
    notification_period         24x7
    notification_options        d,u,r
    checks_enabled              1
}
```

Nagios

Configuration files : templates

```
# Use host template definition
#
define host   {
    use             generic-host
    host_name       smtp1
    alias           primary smtp server
    parents         primary-gw
    address         10.0.0.149
}

define host   {
    use             generic-host
    host_name       smtp2
    alias           secondary smtp server
    parents         primary-gw
    address         10.0.0.169
}
```

Nagios

Configuration files : summary

- Use templates for objects, especially services and hosts
- Use hostgroups and macros to avoid duplication.
- Use timeperiods and notification intervals
  to define when to be contacted.
- Don’t flood yourself with notifications!

Nagios

Sizing – large deployment

Brookhaven National Laboratory

Nagios

Sizing – large deployment

Brookhaven National Laboratory

1963 hosts & ~7 services per host

= 13958 service checks!

Nagios

Sizing – large deployment

Brookhaven National Laboratory

1963 hosts & ~7 services per host

= 13958 service checks

A dual 2.4Ghz Nagios server

was rendered unusable by this load

Nagios

Sizing – average

IMSU

1 server (at present)

Single 1.6GHz processor

500Mb RAM

Nagios

Sizing – average

IMSU

200 hosts & on average 2 services

per host = 400 service checks

Many people find 1000 checks to be

a working limit for one server

Nagios

Installation

- Nagios server has few dependencies
- gcc etc. (if compiling)
- libgd libjpeg libpng (devel)
- Apache web server

Nagios

Installation

- Nagios plugins - multiple dependencies
- Plugins will not be built unless supporting libraries are present.
  eg. check_mysql requires mysql-devel

Nagios

Events

- Nagios can act on events by using Event Handlers
- Event handlers can do things like:
  - Shut down services,
  - Restart failed services
  - Start applications
  - Restart failed applications
  - Run custom scripts

Nagios

Events

```
define service {
    hostname                smtp1
    service_description     smtp
...other config settings ....
    event_handler           restart-smtp
}

define command {
    command_name restart-smtp
    command_line /usr/local/bin/restart-smtp \
       $HOSTADDRESS$ $SERVICESTATE$ $STATETYPE$
}
```

Nagios

Escalations

- Provides a way to escalate a problem when a problem persists
- Based on Notification Count – starts at 3 and ends at 5

```
define serviceescalation {
    hostgroup_name              smtp-servers
    service_description         * ; All services
    first_notification          3
    last_notification           5
    notification_interval       60
    contact_groups              smtp-admins
}
```

Nagios

Configuration managers

NagiosQL

- Web server (Apache 1.3.x/2.0.x)
- PHP Version 4.1 or higher / 5.0 or higher
- MySQL Version 4.0 or higher / 4.1 or higher
- Pear module HTML_Template_IT Version 1.1
- Nagios Version 2.x (1.x is not supported)

Nagios

Configuration managers

NagioSQL

- LAMP product
- Web interface
- Code comments in German ...

Nagios

Configuration managers

Fruity

http://sourceforge.net/projects/fruity

Looks promising ...

Nagios

Reporting

- Useful for uptime reports
- Useful for Service Level Agreements
- Useful for giving clients or managers pretty pictures

Nagios

What to check

- Consider a switch restart ...
- at 08:59 Nagios checks switch by ping – status OK
- at 09:00 switch crashes and restarts
- at 09:02 switch is back online
- at 09:04 Nagios checks switch by ping – status OK
- No record of failure but users will have noticed ...

Nagios

What to check

- An alternative method ...
- at 08:59 Nagios checks switch uptime – status OK 32657853
- at 09:00 switch crashes and restarts
- at 09:02 switch is back online
- at 09:04 Nagios checks switch uptime – WARNING 2160
- at 10:04 Nagios checks switch uptime – OK 64801
- We know the switch restarted and when.

Nagios

What to check

- Service degradation
- Not so easy to check but arguably more commonly seen
- Internal failure of process
  - Still listening but not functioning correctly
  - Functioning but not completing processes
- Need for shared wisdom

Nagios

Futures: Event Broker

- Working in Nagios 2.x, minor changes for Nagios 3.x
- Documentation:
  - http://www.nagios.org/developerinfo/
- Examples:
  - NDOUtils addon

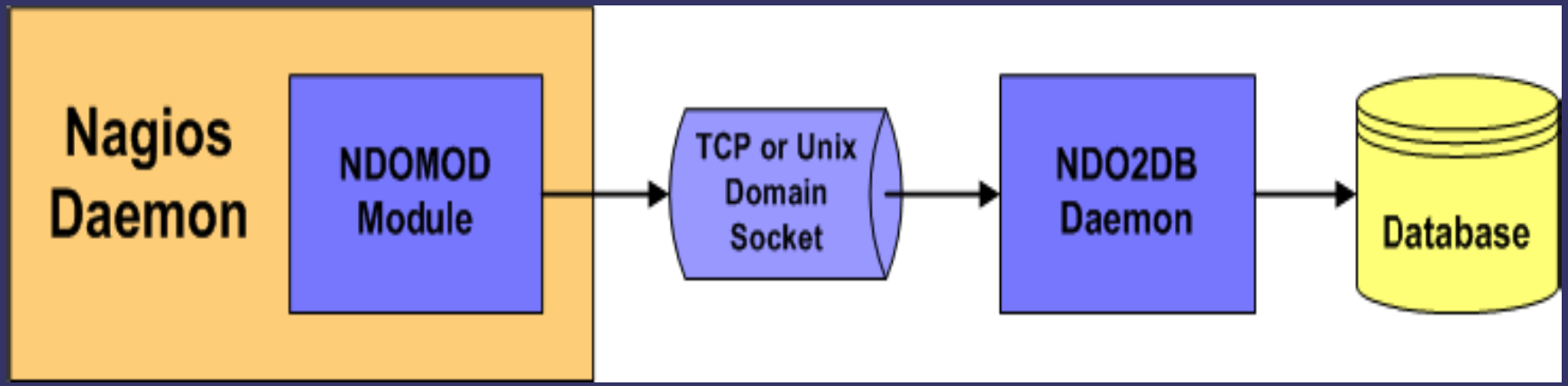
Nagios

Futures: NDOutils Addon

- Event broker module and daemon
- Nagios config, status, and event information stored in DB
- Ability to import historical NetSaint/Nagios logs
- MySQL supported now, Postgres in future
- Current log, status files unaffected
- Works with both Nagios 2.x and 3.x
- Currently in development – bugs to fix, docs to write

Nagios

Futures: NDOutils Addon



- NDOMOD module is loaded into Nagios
- Data is sent to TCP or UNIX domain socket
- NDO2DB daemon reads data from socket
- Data is processed and stored in a DB

Nagios

Futures: Nagios 3.x

- Nagios 3.x
  - New check logic
  - Custom variables for use in macros
  - Changes to plugin output format
  - Config changes inc. Multiple inheritance

Nagios

Futures: Nagios 4.x

- Nagios 4.x
  - DB integration (MySQL/Postgres) – NDOUtils addon
  - PHP-based GUI with
    - Multiple instance support
    - Internationalization
    - Easier addon integration
  - Community website for news, events, etc.
  - Documentation wiki – of, by, and for the community.

Nagios

Links

http://www.nagios.org

http://nagiosplug.sourceforge.net

http://www.nagiosql.org

http://www.nagiosexchange.org

Nagios

Recommended reading

Nagios documentation

Pro Nagios 2.0 Turnbull, J. Apress 2006

(ISBN-10: 1-59059-609-9)

Nagios

Questions?