Nagios® Core™

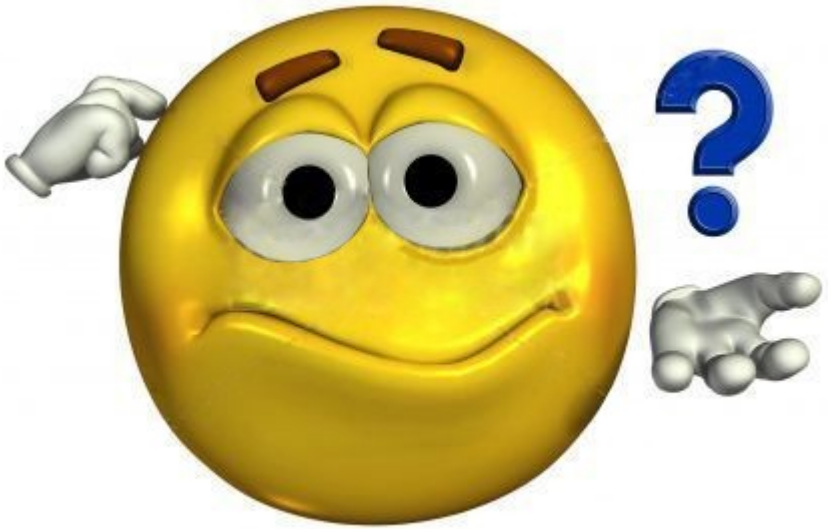
BMO 2015

2nd July 2015

Nyanjau Kimani

NSRC Network Startup Resource Center

kenet Kenya Education Network



kenet

Kenya Education Network

Nagios: a measurement tool that actively monitors availability of devices and services:

- **Popular:** One of the most used open source network monitoring software packages.
- **Fast:** Uses CGI functionality written in C for faster response and scalability.
- **Scalable:** Can support up to thousands of devices and services.
- **Modular**

kenet
Kenya Education Network

Nagios Core - Google Chrome

Nagios Core

localhost/nagios/

Nagios

General
- Home
- Documentation

Current Status
- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

Reports
- Availability
- Trends
- Alerts
  - History
  - Summary
  - Histogram
- Notifications
- Event Log

System
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Nagios® Core™

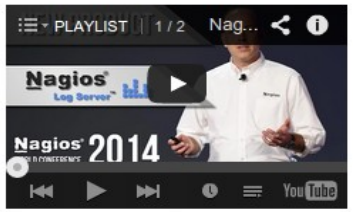
✔ **Process running with PID 11188**

http://www.2daygeek.com

Nagios® Core™
Version 4.0.8
August 12, 2014
Check for updates

Get Started
- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links
- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)



Latest News
- NCPA 1.7.2 Released
- NCPA 1.7.1 Released
- Nagios Core 4.0.8 Released
- More news...

Don't Miss...
- **Want to Learn More about Nagios Log Server?** - Register for an upcoming live webinar!
- **2014 Nagios World Conference Proves Biggest Success Yet** - Read More
- **Nagios Extends IT Management Capabilities with Launch of Log Management Solution** - Read More

kenet
Kenya Education Network

Features: 1

- Comprehensive Monitoring

Capabilities to monitor applications, services, operating systems, network protocols, system metrics and infrastructure components with a single tool

- Visibility

Centralized view of entire monitored IT infrastructure

Detailed status information available through web interface

kenet
Kenya Education Network

Features: 2

- Awareness

Fast detection of infrastructure outages

Alerts can be delivered to technical staff via email or SMS

Escalation capabilities ensure alert notifications reach the right people

kenet
Kenya Education Network

Features: 3

- Uses “intelligent” checking capabilities.
  - » Attempts to distribute the server load of running Nagios (for larger sites) and the load placed on devices being checked.
- Configuration is done in simple, plain text files, that can contain much detail and are based on templates.
- Nagios reads it's configuration from an entire directory. You decide how to define individual files.

Features: 4

Topology Aware: To determine dependencies.

Differentiates between what is down vs. what is not available. This way it avoids running unnecessary checks. This is done using parent-child relationships between devices.

Notifications: How they are sent is based on combinations of:

Contacts and lists of contacts.

Devices and groups of devices

Services and groups of services

Defined hours by persons or groups.

The state of a service.

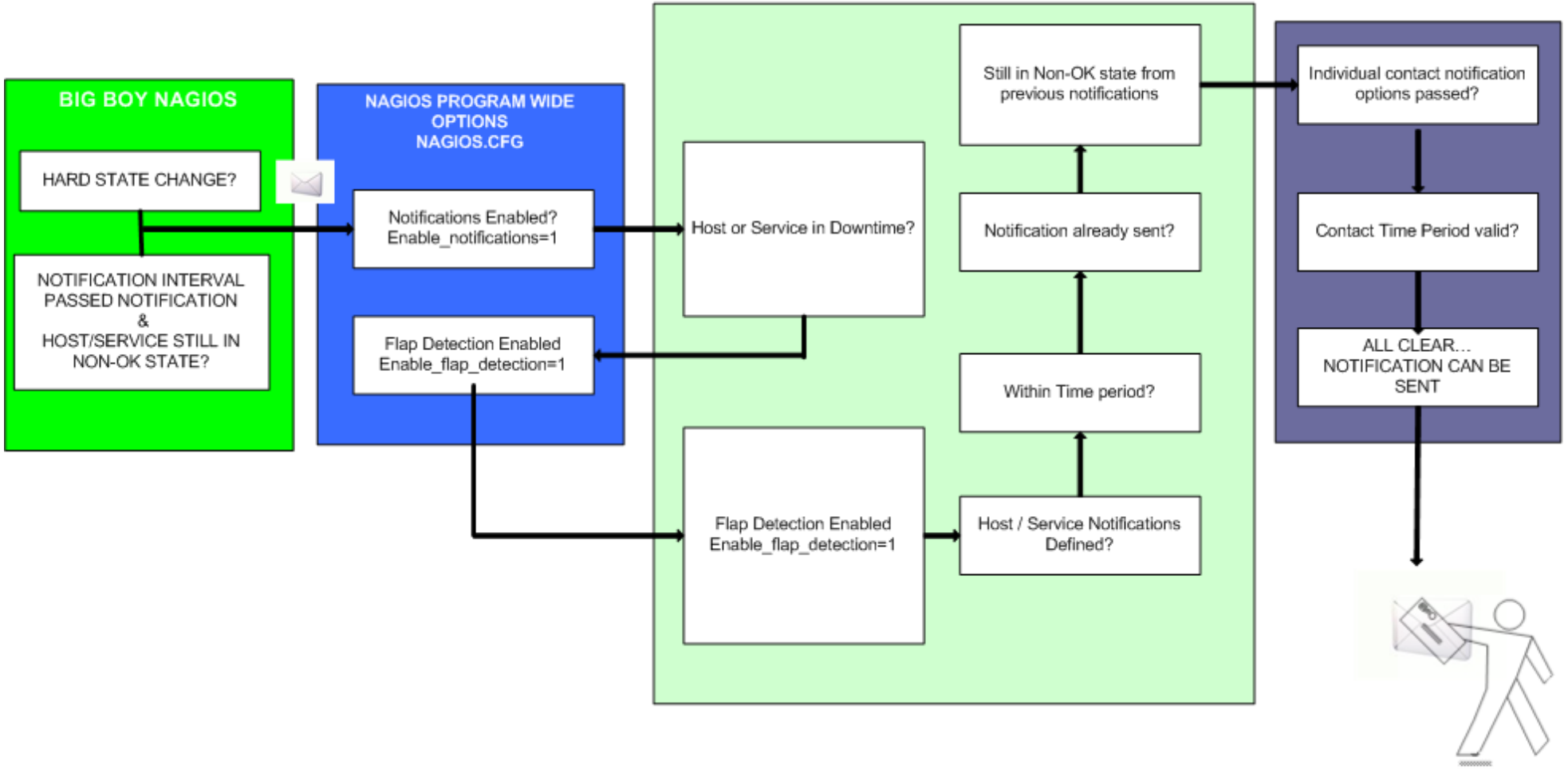
kenet
Kenya Education Network

Features: 5

Service state:

- When configuring a service you have the following notification options:
  - **d:** DOWN: The service is down (not available)
  - **u:** UNREACHABLE: When the host is not visible
  - **r:** RECOVERY: (OK) Host is coming back up
  - **f:** FLAPPING: When a host first starts or stops or it's state is undetermined.
  - **n:** NONE: Don't send any notifications

NAGIOS - NOTIFICATION FLOW DIAGRAM



NOTE: The flow will only continue when each of the listed filters are satisfied.

CONTACT GETS THE NOTIFICATION MESSAGE

kenet
Kenya Education Network

How Checks Work

- A node/host/device consists of one or more service checks (PING, HTTP, MYSQL, SSH, etc)
- Periodically Nagios checks each service for each node and determines if state has changed. State changes are:
  - CRITICAL
  - WARNING
  - UNKNOWN
- For each state change you can assign:
  - Notification options (as mentioned before)
  - Event handlers (scripts, actions to take)

How Checks Work contd.

- **Parameters:** Set in /etc/nagios3/nagios.cfg:
  - Normal checking interval
  - Re-check interval
  - Maximum number of checks.
  - Period for each check
- Services check(s) only happen when a node responds (ping check or “is alive = yes”):
  - Remember a node can be:
    - DOWN
    - UNREACHABLE

(What's the difference?)

kenet
Kenya Education Network

How Checks Work 2

- **Parameters:** Set in /etc/nagios3/nagios.cfg:
  - Normal checking interval
  - Re-check interval
  - Maximum number of checks.
  - Period for each check
- Services check(s) only happen when a node responds (ping check or “is alive = yes”):
  - Remember a node can be:
    - DOWN
    - UNREACHABLE

(What's the difference?)

kenet
Kenya Education Network

The Concept of “Parents”

- Nodes can have parents.
  - For example, the parent of a PC connected to the switch *mgmt-sw1* would be *mgmt-sw1*.
  - This allows us to specify the network dependencies that exist between machines, switches, routers, etc.
  - This avoids having Nagios send alarms when a parent does not respond.
  - **Note:** A node can have multiple parents.

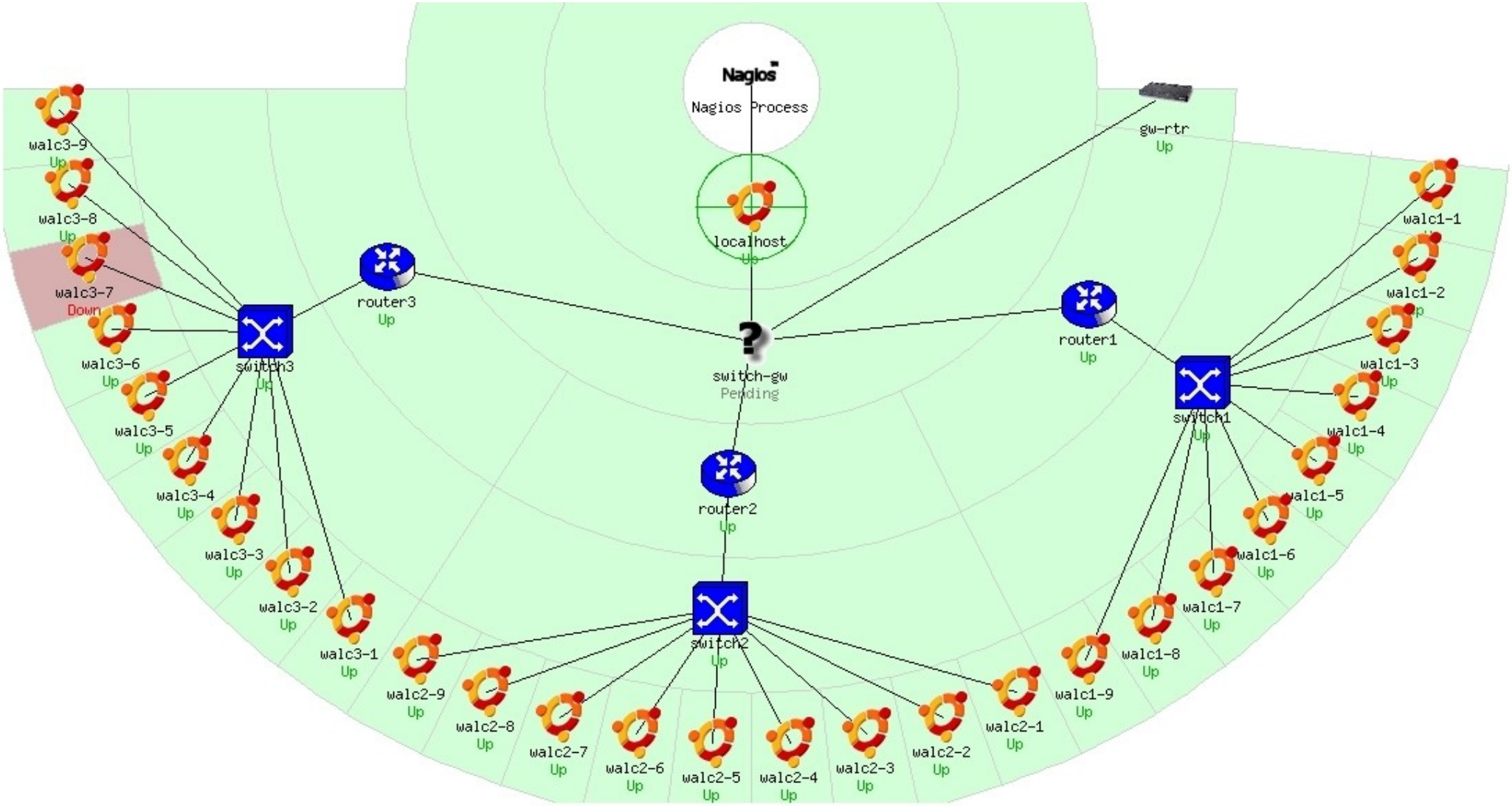
kenet
Kenya Education Network

The Idea of Network Viewpoint

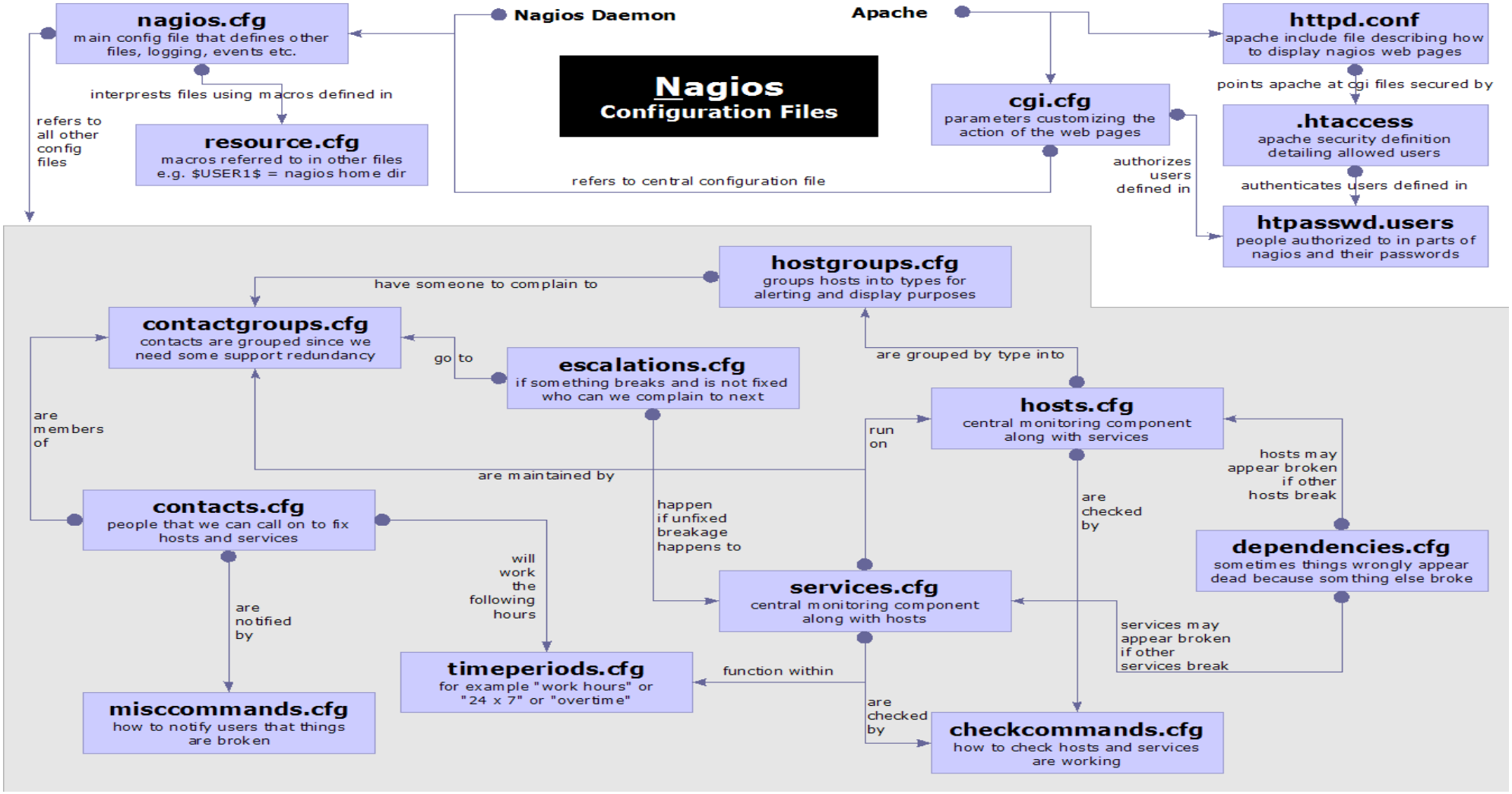
- Where you locate your Nagios server will determine your point of view of the network.
- Nagios allows for parallel Nagios boxes that run at other locations on a network.
- Often it makes sense to place your Nagios server nearer the border of your network vs. in the core, or...

Have someone else run checks for you from an external location as well.

Network Viewpoint



Nagios Configuration Files



kenet
Kenya Education Network

Nagios Configuration Files

Located in /usr/local/nagios/etc/ (in Ubuntu)

Important files include:

cgi.cfg	Controls the web interface and security options.
commands.cfg	The commands that Nagios uses for notifications (i.e. sending email)
nagios.cfg	Main configuration file.
conf.d/*	All other configuration goes here!

kenet
Kenya Education Network

Nagios Configuration Files contd.

Under conf.d/* (*sample only*)

contacts_nagios3.cfg	users and groups
generic-host_nagios2.cfg	default host template
generic-service_nagios2.cfg	default service template
hostgroups_nagios2.cfg	groups of nodes
services_nagios2.cfg	what services to check
timeperiods_nagios2.cfg	when to check and who to notifiy

kenet
Kenya Education Network

Nagios Configuration Files contd.

Under conf.d some other possible configfiles:

host-gateway.cfg	Default route definition
extinfo.cfg	Additional node information
servicegroups.cfig	Groups of nodes and services
localhost.cfg	Define the Nagios server itself
pcs.cfg/servers.cfg	Sample definition of PCs (hosts)
switches.cfg	Definitions of switches (hosts)
routers.cfg	Definitions of routers (hosts)

kenet
Kenya Education Network

Main Configuration Details

Global settings

File: /usr/local/nagios/etc/nagios.cfg

CGI Configuration

/usr/local/nagios/etc/cgi.cfg

- You can change the CGI directory if you wish
- Authentication and authorization for Nagios use.
  - Activate authentication via Apache's .htpasswd mechanism, or using RADIUS or LDAP.
  - Users can be assigned rights via the following variables:
    - authorized_for_system_information
    - authorized_for_configuration_information
    - authorized_for_system_commands
    - authorized_for_all_services
    - authorized_for_all_hosts
    - authorized_for_all_service_commands
    - authorized_for_all_host_commands

Time Periods

`conf.d/timeperiods_nagios2.cfg`: defines the base periods that control checks, notifications, etc.

- Defaults: 24 x 7
- Could adjust as needed, such as work week only.
- Could adjust a new time period for “outside of regular hours”, etc.

```
# '24x7'
define timeperiod{
        timeperiod_name 24x7
        alias           24 Hours A Day, 7 Days A Week
        sunday          00:00-24:00
        monday          00:00-24:00
        tuesday         00:00-24:00
        wednesday       00:00-24:00
        thursday        00:00-24:00
        friday          00:00-24:00
        saturday        00:00-24:00
        }
```

kenet
Kenya Education Network

Configuring Service/Host Checks

Define how you are going to test a service.

```
# 'check-host-alive' command definition
define command{
        command_name    check-host-alive
        command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c
5000.0,100% -p 1 -t 5
 }
```

Located in /etc/nagios-plugins/config, then adjust in /etc/nagios3/conf.d/services_nagios2.cfg

kenet
Kenya Education Network

Notification Commands

```
# 'notify-by-email' command definition
define command{
        command_name    notify-by-email
        command_line    /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost:
$HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail -s
'$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
        }
```

```
From:     nagios@nms.localdomain
To:           grupo-redes@localdomain
Subject:  Host DOWN alert for switch1!
Date:     Thu, 29 Jun 2006 15:13:30 -0700


Host: switch1
In: Core_Switches
State: DOWN
Address: 111.222.333.444
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds
```

kenet
Kenya Education Network

Nodes and Services Configuration

- Based on templates
  - This saves lots of time avoiding repetition
  - *Similar to Object Oriented programming*
- Create default templates with default parameters for a:
  - generic node
  - generic service
  - generic contact

kenet
Kenya Education Network

Generic Node Configuration

```
define host{
        name                            generic-host
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        check_command                   check-host-alive
        max_check_attempts              5
        notification_interval           60
        notification_period             24x7
        notification_options            d,r
        contact_groups                  nobody
        register                         0
        }
```

kenet
Kenya Education Network

Individual Node Configuration

```
define host{
        use                     generic-host
        host_name               switch1
        alias                   Core_switches
        address             192.168.1.2
        parents                 router1
        contact_groups          switch_group
}
```

kenet
Kenya Education Network

Generic Service Configuration

```
define service{
        name                            generic-service
        active_checks_enabled           1
        passive_checks_enabled          1
        parallelize_check               1
        obsess_over_service             1
        check_freshness                 0
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information 1
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              5
        normal_check_interval        5
        retry_check_interval            1
        notification_interval           60
        notification_period             24x7
        notification_options            c,r
        register                        0
        }
```

kenet
Kenya Education Network

Individual Service Configuration

```
define service{
        host_name                    switch1
        use                           generic-service
        service_description           PING
        check_command                 check-host-alive
        max_check_attempts            5
        normal_check_interval         5
        notification_options          c,r,f
        contact_groups                switch-group
}
```

kenet
Kenya Education Network

Beeper/SMS Messages

- It's important to integrate Nagios with something available outside of work
  - Problems occur after hours... (unfair, but true)
- A critical item to remember: an SMS or message system should be independent from your network.
  - You can utilize a modem and a telephone line
  - Packages like sendpage, qpage, gnoki can help.

Some References

- http://www.nagios.org/
- http://sourceforge.net/projects/nagiosplugins
- http://www.nagiosexchange.org/
- http://www.debianhelp.co.uk/nagios.htm
- http://www.nagios.com/: Commercial Nagios support
- *Nagios,* by O'Reilly Media, Inc.
- *Nagios. System and Network Monitoring,* by Wolfgang Barth.

kenet
Kenya Education Network

kenet
Kenya Education Network