Monitoring Systems and Services

Alwin Brokmann
DESY-IT
March 24 – 28 ,2003
CHEP 2003 San Diego

Requirements

Host Monitoring
Service Monitoring
Navigation
User specific Parameter s
WEB Interface
Alarming
Escalation
Simple Configuration
Reporting
Interface to Trouble Ticket System
Fault Isolation

Why NAGIOS

There are several reasons for us to select NAGIOS .

a. Fulfills most of our requirements

b. Possibility to submit our own test`s
   (Plug In Concept)

c. Scalability

d. Design (WEB Interface)

e. Out of the Box functionality

e. Price

History

Test

Starting Oct. 2001

One PC running NetSaint -- Monitoring 50 Hosts

March 2002

3 PC`s running NetSaint -- Monitoring ~300 Hosts, several Proc`s

Jun 2002

Testing logsurfer

Nov 2002

Production

NAGIOS 1.0 available

4 PC`s running NAGIOS ~ growing Number of Hosts and Services

LogHost is running /connecting to NAGIOS

Feb 2003

New Service Checks for AFS

Monitoring Policy

Every Host in the Computer Center will be monitored and also Centrally Supported Printer`s

Host	*Check by*
Network Device	PING
Farm PC	PING
Printer	SNMP
Workgroup Server	Load Disk Process
Mail	POP IMAP
WEB Server	HTTP
AFS Server	Service Monitoring

Monitoring Service for Clusters

Hardware Cluster:

Mail cluster, consisting of 2 computers.

Service Cluster:

YP cluster which consists of several computers for the YP Service

To make the check of a cluster possible we need a Check Cluster Plug In.

We can define for each cluster how many components may fail before an alarm is triggered

Monitoring AFS

With the introduction of OpenAFS at DESY we experienced, that a simple process monitoring gives no reliable answers.

Therefore we added some new tests in NAGIOS to ensure the operation of the AFS Servers.

For these tests we use afs tools like rxdebug, vos etc..

The result is then transferred to NAGIOS.

Host Statistics

(Feb. 2003)

Host	*Services*
~630	~1300

Type	*Quantity*
Printer	17
Network	37
UNIX	550
Windows	26

Configuration

At present we use simple flat files to describe host and services. This means a very high effort, but makes it simply possible to distribute the checks

For the future we plan to produce the tests automatically over our AMS.

For an automatic configuration of NAGIOS we will extract the informatios such as computer name , interface and naturally which service runs on the computer from the AMS database.

Perhaps we will hold the data in a data base

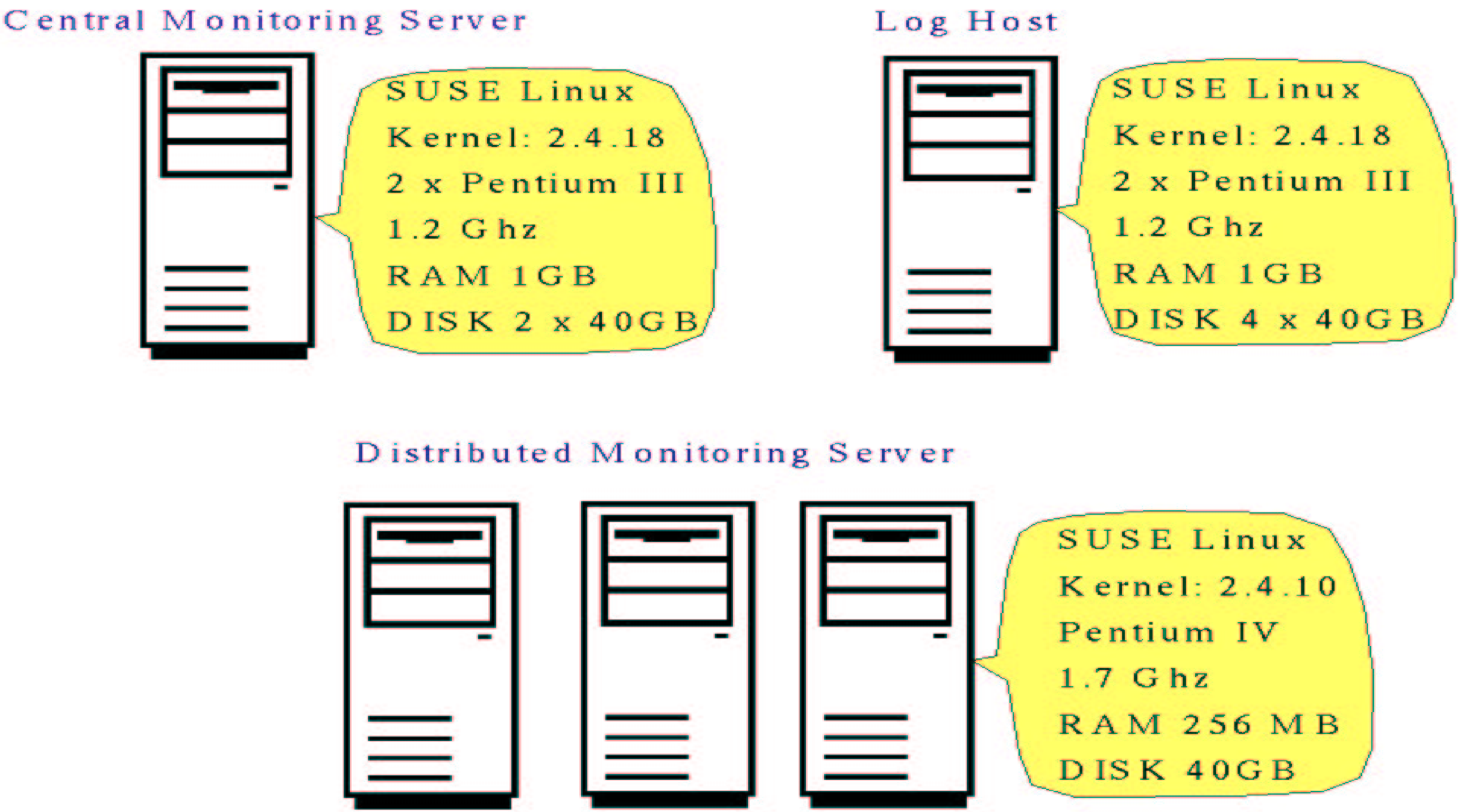
Configuration Example

```
define  hostgroup{
        name                    night
        hostgroup_name          night
        alias                   night
        contact_groups      sgi-admins,night-admins
        members             netra8,test1,test2
        }
define  host{
        host_name               netra8
        alias                   netra AFS Server
        address                 131.169.40.109
        parents                 route-194,route-40
        use                     hostcheck
        }
define  service{
        use                     fileserver
        host_name               netra8,test1,test2
        contact_groups        afs-admins,night-admins
        }
```

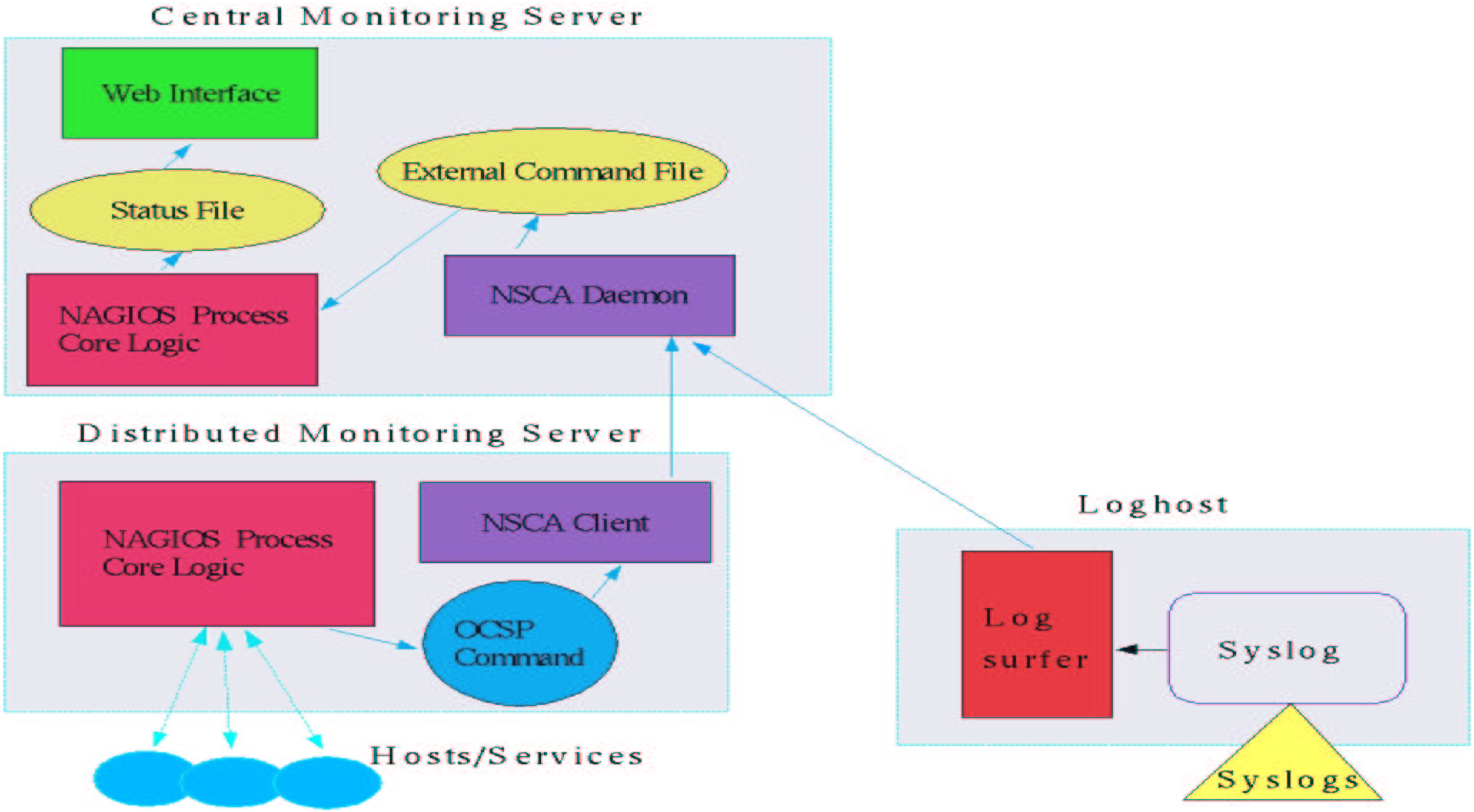
Configuration Example

```
define  service{
        name                        fileserver
        service_description         fileserver
        is_volatile                 0
        active_checks_enabled       0
        passive_checks_enabled      1
        check_period                24x7
        max_check_attempts          10
        normal_check_interval       1
        retry_check_interval        5
        notification_interval       2200
        notification_period         24x7
        notification_options        w,u,c,r
        check_command          check_named_proc!' '!' '!fileserver
        register                    0
        }
```

Monitoring Setup @ DESY IT



Monitoring Server Setup



Operator Console

Current Network Status
Last Updated: Wed Mar 19 09:46:41 MET 2003
Updated every 60 seconds
Nagios® - www.nagios.org
Logged in as *brokmann*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
621	2	0	1

All Problems	All Types
2	624

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1247	1	3	6	105

All Problems	All Types
10	1362

Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
adsm-s1	PING P	CRITICAL	19-03-2003 09:46:34	0d 0h 21m 23s	1/10	CRITICAL - Plugin timed out after 10 seconds
cosmos07	AFSD RUNNING P	UNKNOWN	19-03-2003 09:46:18	0d 0h 0m 20s	1/10	No Answer from Client
	CHECK_Procs P	UNKNOWN	19-03-2003 09:46:21	0d 0h 0m 18s	1/10	No Answer from Client
	syslogd P	UNKNOWN	19-03-2003 09:46:21	0d 0h 0m 18s	1/10	No Answer from Client
h1desy01	CHECK_ALL_DISK P	WARNING	19-03-2003 09:45:48	0d 0h 21m 10s	10/10	Warning: /wgsmount/x01/h1desy01(97%)
h1raid05	CHECK_ALL_DISK P	CRITICAL	19-03-2003 09:46:29	0d 0h 19m 31s	10/10	Critical: /var(100%)
solar08	AFSD RUNNING P	CRITICAL	19-03-2003 09:46:28	0d 0h 16m 54s	1/10	(Service Check Timed Out)
	CHECK_ALL_DISK P	CRITICAL	19-03-2003 09:45:54	0d 0h 26m 49s	1/10	(Service Check Timed Out)
	SSHD Running P	CRITICAL	19-03-2003 09:46:17	0d 0h 21m 23s	1/10	(Service Check Timed Out)
	syslogd P	CRITICAL	19-03-2003 09:45:33	0d 0h 16m 40s	1/10	(Service Check Timed Out)

10 Matching Service Entries Displayed

Problem Notification

```
**** Nagios 1.0 *****
Notification Type: PROBLEM Service: IT Web Server
Host: WWW Server WEB
Address: 131.169.40.38
State: CRITICAL
Date/Time: Tue Mar 19 08:35:59 MET 2003
Additional Info: Connection refused by host
```

Recovery Notification

***** Nagios 1.0 *****

Notification Type: RECOVERY

Service: IT Web Server

Host: WWW Server WEB

Address: 131.169.40.38

State: OK Date/Time: Wed Mar 19 08:37:46 MET 2003

Additional Info: HTTP ok: HTTP/1.1 200 OK - 0 second response time

LOGSURFER

* Works on any textfile (or text from standard input)
* Matching of lines is done by two regular expression (logline must match the first expression but must not match the optional second regular expression). So you are able to specify exceptions.
* Uses contexts (collection of messages) instead single lines
* Flexible but easy configuration
* Timeouts and resource limits included
* Handles "shifting" of logfiles
* Dynamic rules can change the actions associated with logmessages (something might happen that makes you interested in messages you would usually drop)
* Multiple reactions on one logline possible

References

NAGIOS
www.nagios.org

SNMP
www.net-snmp.org

logsurfer
www.dfn-cert.de/eng/logsurf/index.html