SI5 – Administration des Réseaux

Monitoring and Managing Computer Networks

Dr. Quentin Jacquemart
quentin.jacquemart@unice.fr

http://www.qj.be/teaching/

Outline

Reminder

- SLA, NOC
- Network troubleshooting
- ICMP
- Packet sniffers (Wireshark), ping, traceroute

Outline

- Introduction
- ⇒ **SNMP**
- MRTG
- collectd
- NetData
- ELK
- Bibliography

Simple Network Management Protocol (SNMP) I

[K&R]

- Design goal: generic management tool for (growing) networks
- *Simple Network Management Protocol* (**SNMP**)
  - Name of *protocol* **but also** of global management solution
  - Drafted at the end of 1980's, as an evolution of SGMP
    (Simple Gateway Management Protocol)
- Supported by the Internet Architecture Board (IAB)...
  - but only as a **short term** solution!
  - CMIP was being standardized, and envisioned as the *long term* solution
    (*Common Management* Information Protocol)
  - SNMP and CMIP were to be developed in parallel to ease transition

Simple Network Management Protocol (SNMP) II

[K&R]

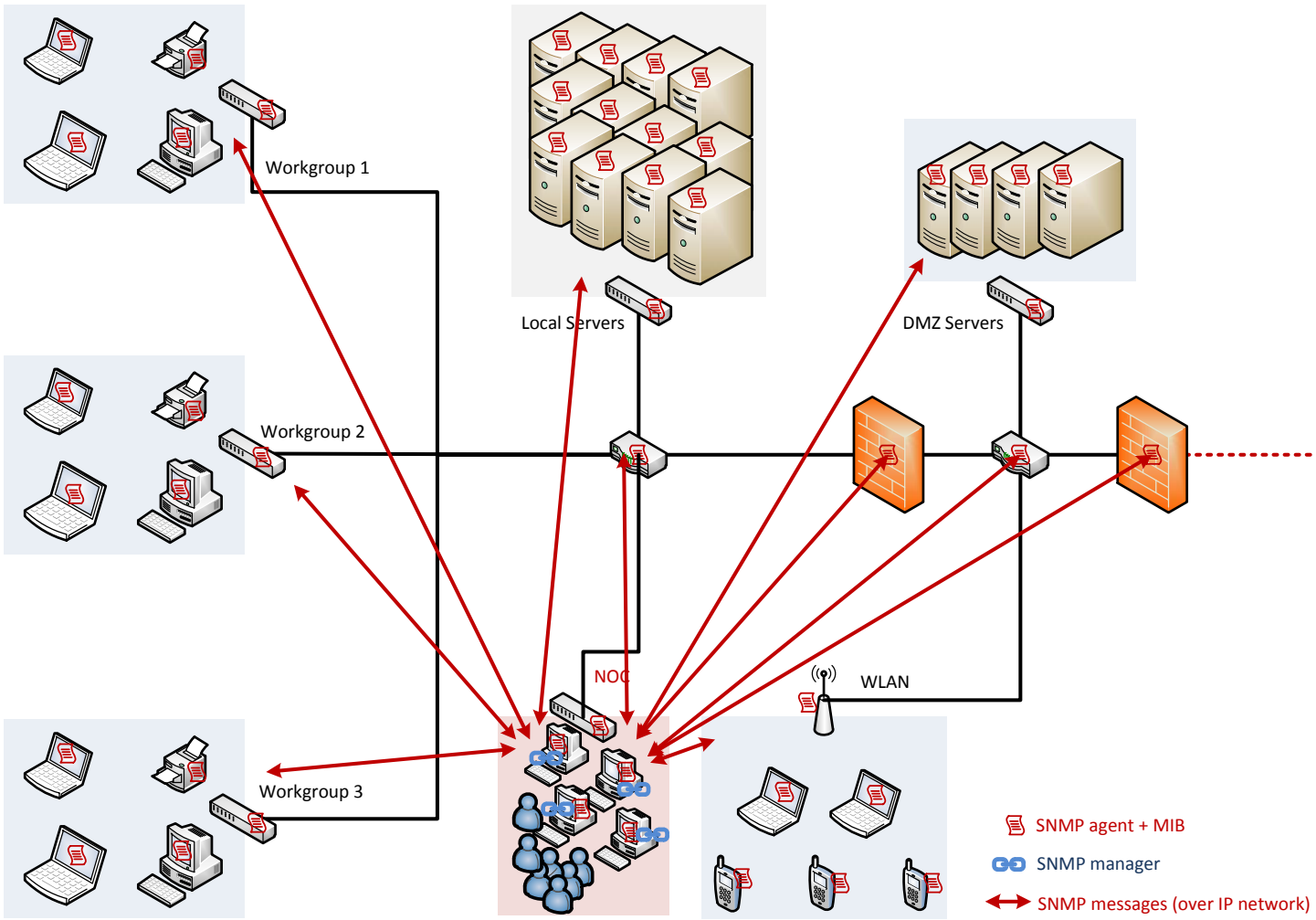
- Due to *divergent* conceptual choices, IAB relaxes interoperability conditions
  - SNMP's more simplistic and pragmatic approach leads to a *faster* development
  - and also faster **implementation** (including industry support)
  - SNMP has be come the *de facto* standard, due to its ubiquitousness

SNMP: Key Concepts

[K&R]

1. **MIB**: Management Information Base
   — Distributed information database, stored *on each* managed device
2. **SMI**: Structure of Management Information
   — Definition language, used to describe objects included in the MIB
3. The SNMP **protocol**
   — Enables **communications** between the *manager* and the managed device (*agents*)
4. **Security**
   — Concept of *communities* in SNMPv1 and SNMPv2 (but mostly lacking)
   — Major addition of SNMPv3

An SNMP Deployment



MIB: Management Information Base

[K&R]

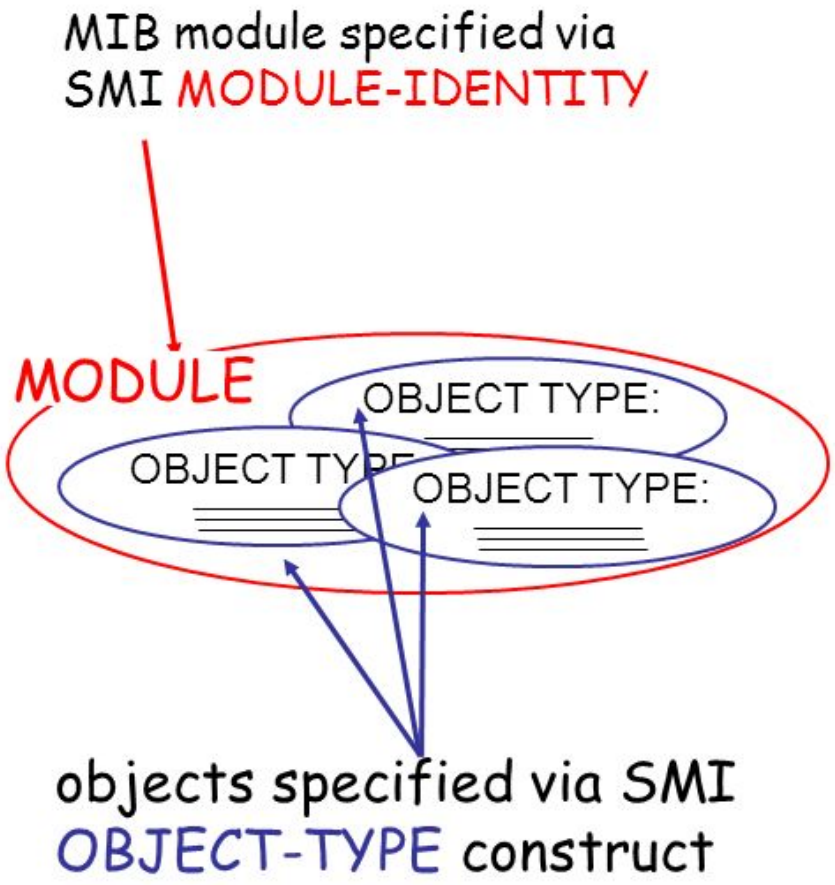
- Database that includes **information** about *agents*
- *Each agent* **maintains** its **own** MIB
- This MIB reflects the **current** device status
- 2 constraints:
  1. The **same objects** need to reflect the **same resource**, *across devices*
     $\Rightarrow$ need for **uniformity** (e.g. *total* packet count VS *hourly* packet count)
  2. A common **representation** language needs to be used
     $\Rightarrow$SMI

SMI: Structure of Management Information I

- Specifies how *resources* are **named** and **represented** within the MIB
- Purpose of SMI within the MIB:
  - Define the **structure** of a MIB
    - **module** → relation among objects within the MIB (e.g. related to a device or protocol)
  - Define **individual objects**, their syntax and meanings of the values
    - **object-type** → semantics
  - Define the **encoding** of each object
    - **scalars**: int/int32/unsigned32, octet string, object ID, IP/network address, counter, gauge, timetick
    - **2D arrays**: sequence-of

SMI: Structure of Management Information II

[K&R]



SMI Example: A Module and an Object

[K&R]

```
ipMIB MODULE-IDENTITY
    LAST-UPDATED "941101000Z"
    ORGANZATION
        "IETF SNPv2 Working Group"
    CONTACT-INFO
        "Keith McCloghrie..."
    DESCRIPTION
        "The MIB module for managing
        IP and ICMP implementations,
        but excluding their management
        of IP routes."
    REVISION "019331000Z"
    ...
::= {mib-2 48}
```

```
ipInDelivers OBJECT TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The total number of input
        datagrams successfully
        delivered to IP user-protocols
        (including ICMP)"
::= { ip 9}
```

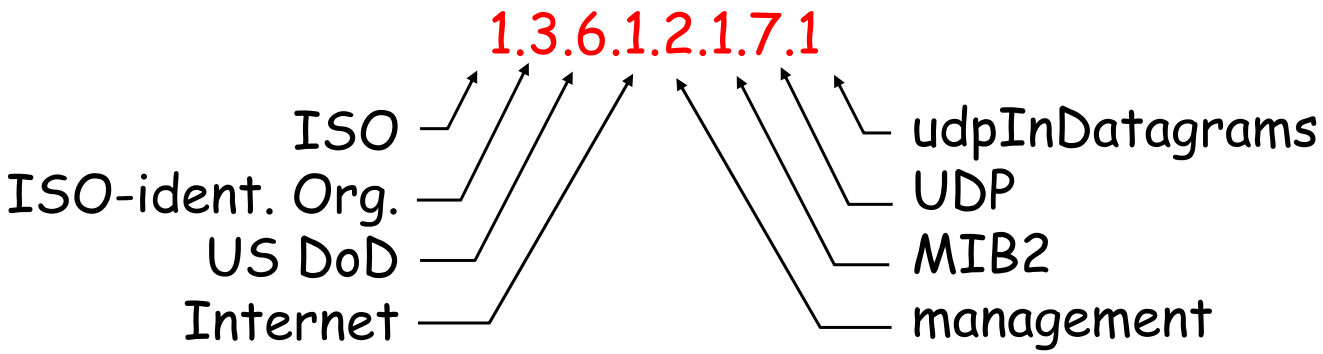
The UDP Module

[K&R]

ObjectID	Nom	Type	Description
1.3.6.1.2.1.7.1	udpInDatagrams	Counter32	total number of received datagrams
1.3.6.1.2.1.7.2	udpNoPorts	Counter32	total number of undeliverable datagrams (no application at port)
1.3.6.1.2.1.7.3	udpInErorrs	Counter32	total number of undeliverable datagrams (other reason)
1.3.6.1.2.1.7.4	udpOutDatagrams	Counter32	total number of sent datagrams
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	one entry per port in use: {port, IP}

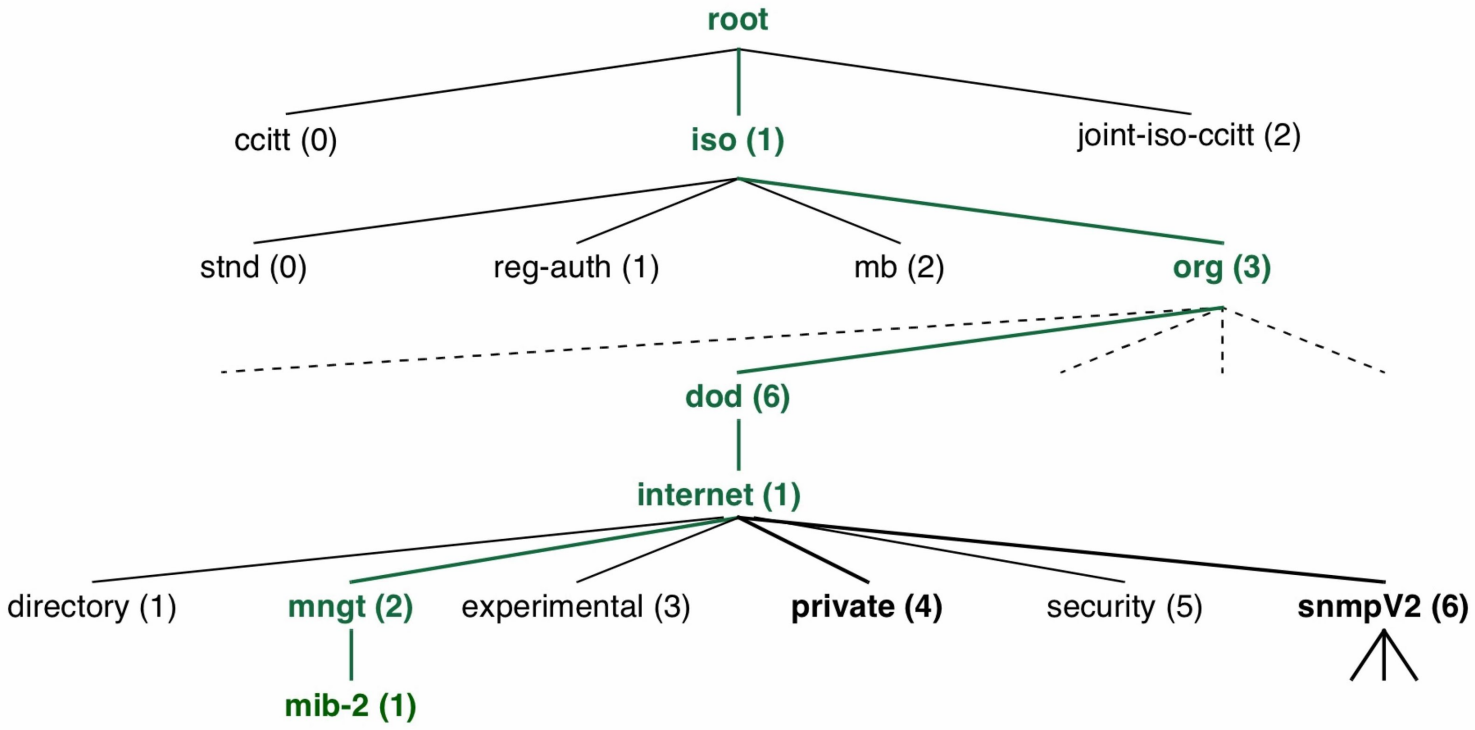
Object Naming within the MIB

- Problem: how to **name all** common **objects**/attributes related to all protocols/data/... from **all possible standards** on any possible network?
- Hierarchical tree **OSI ObjectIdentifier**
  - Each branch corresponds to a **name** and a **number**



The OSI Tree

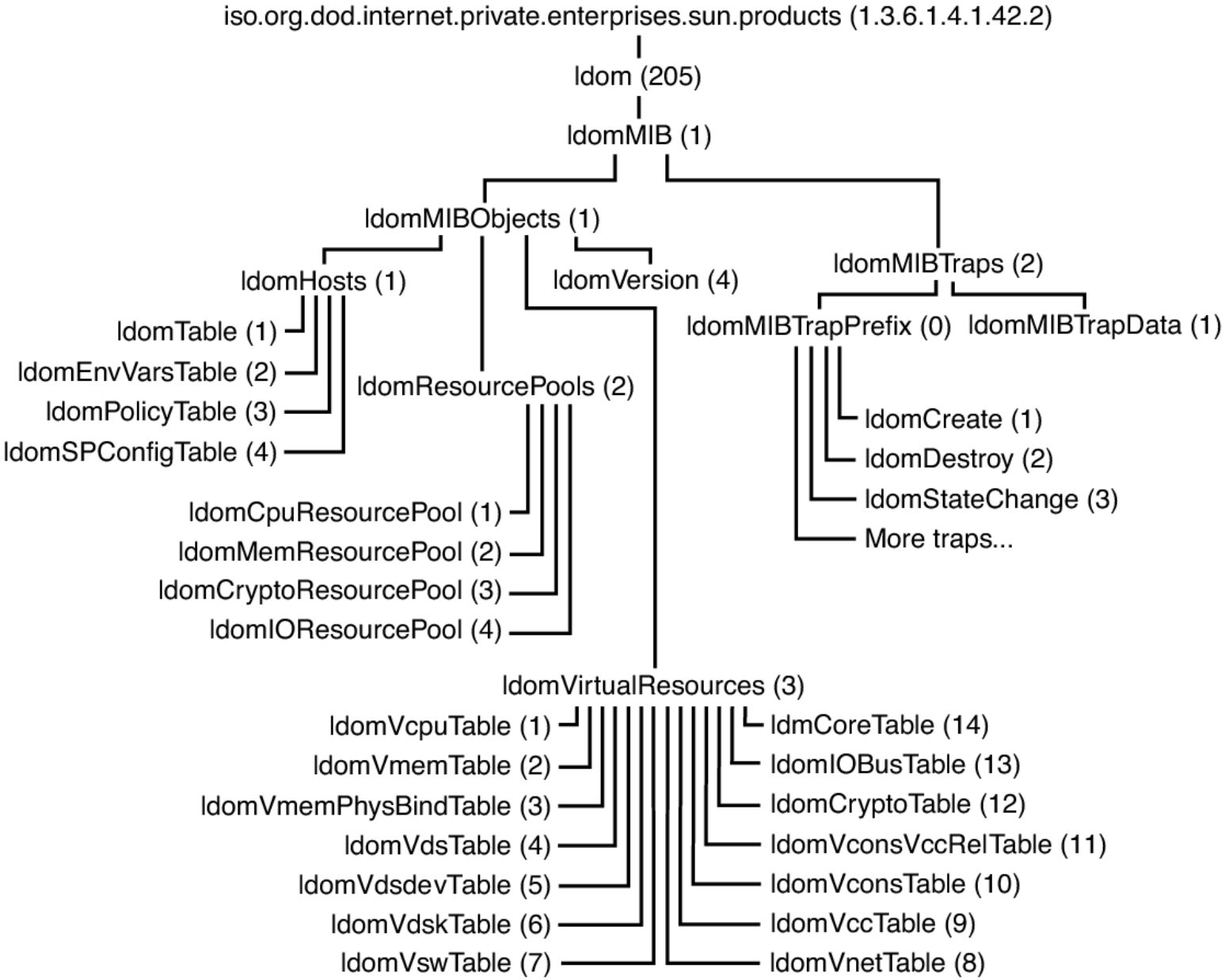
[Pras 2013; K&R]



Plus de MIBs: http://www.alvestrand.no/objectid/

Proprietary MIB in the OSI tree

[Oracle 2014]



MIBs available from an Agent

- It is **mandatory** to implement the MIB-2 [RFC1213]
  - Interfaces statistics (speed, MTU, sent/received bytes)
  - System information (location, contact details)
- An agent implements *standardized MIBs* wrt. its **network services**
  - MIB BGPv4 (RFC 1657), MIB Radius Server (RFC 2619), ...
- An agent can implement proprietary MIBs (e.g. constructor)

The SNMP Protocol I

- Application-layer protocol, relies on UDP datagrams
  - port #161: requests to agents
  - port #162: notifications to managers (InformRequest et Trap)
- An **SNMP agent** runs on each managed device
  - collect data to fill in MIB
  - exchange data/information with the manager

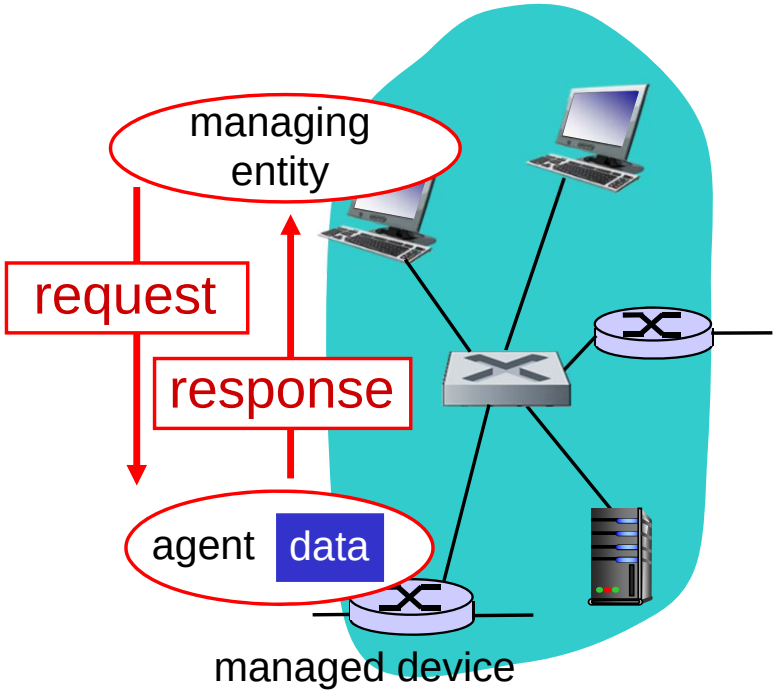
The SNMP Protocol II

- Possible messages between a manager and an agent:
  - GetRequest/GetNextRequest/GetBulkRequest: manager requests information from agent
  - Response: response to a request (agent towards manager)
  - SetRequest: manager sends a new value to agent to enact behaviour change
  - InformRequest: disseminates an MIB value (either manage-to-manager, or agent-to-manager)
  - Trap: agent informs manager of exceptional circumstances

SNMP operation mode: request and response

[K&R]

The manager requests information from agents by actively polling



Q: what is the main pitfall of this operation mode?

Clue: think about network size, real-time operations, . . .

SNMP operation mode: trap

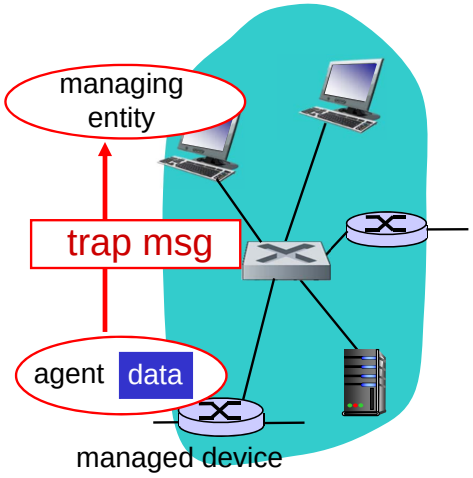
[K&R]

- Large number of agents $\leftrightarrow$ large number of requests
- The network is not there to convey management information!

  (particularly when it is not needed)
- Favoured approach:
  - initially, poll agents directly
  - make agent **responsible** to **notify** the manager upon exceptional cicumstances

    (e.g. agent crashed and rebooted, link is down, overload, . . .)
  - upon receipt of an alert, the manager can choose to **take an action**

    (typically, probe/poll alerting agent and its neighborhood



SNMP Access Control

- SNMPv1 et SNMPv2: **Communities**
  - can be considered as plain-text passwords...
  - correspond to data access rights (read-only, read-write, write-only, not accessible)
- Usual default communities:
  - public: read-only
  - private: read-write
  - an *authentication trap* exists to notify about password errors
- SNMPv3 brings user authentication, but seldom use
- In SNMPv2, each agent knows its manager's IP address to "avoid" impersonation

Configuring an Agent

- Important to configure
  - MIB-2: SysLocation, SysContact, SysName
  - Communities: read-write et read-only
  - Limit the IP address (range) from which a manager can connect
  - Trap destination: the manager's IP address

SNMP Manager Example: Observium

- PHP application, available for almost all platforms
- Displays informations obtained with SNMP
  - system: CPU/memory/disk stats
  - network: traffic per interface, packets, errors
  - hardware: temperature, fan speed, power information
  - users: processes, average load, uptime
- Real-time graphs
- http://demo.observium.org/

SNMP Managers

- SNMP managers are a front-end to data collected from SNMP agents
  - They are more about UI than monitoring
- Generally: mix between SNMP and plug-ins
- Observium (simple) vs. Nagios (complex)
  - templates
  - alarm management in case of cascaded failure
    $\Rightarrow$ relies on topology to figure out dependencies
  - ease of scaling up
    $\Rightarrow$ customization of notifications (e.g. per service type)
  - tighter integration with the underlying system
    $\Rightarrow$ enables directly acting on the system

SNMP Manager Example: [Nagios] I

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
- Configuration

Current Network Status
Last Updated: Fri Oct 17 18:51:18 UTC 2014
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

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

Host Status Totals

Up	Down	Unreachable	Pending
11	0	0	0

All Problems	All Types
0	11

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	1	4	0

All Problems	All Types
6	39

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
NOAA	Auroral Activity	OK	10-17-2014 18:51:09	535d 4h 28m 6s	1/3	Aurora OK: Activity level is 2
	Weather Carteret North Carolina	WARNING	10-17-2014 18:43:15	0d 0h 46m 57s	3/3	Weather Warning: Beach Hazards
	Weather King Washington	OK	10-17-2014 18:45:25	737d 1h 52m 46s	1/3	Weather OK: No watches or warni area.
	Weather Ramsey Minnesota	OK	10-17-2014 18:46:45	59d 20h 47m 12s	1/3	Weather OK: No watches or warni area.
	Weather San Bernardino California	OK	10-17-2014 18:41:45	0d 0h 48m 40s	1/3	Weather OK: No watches or warni area.
	Weather Strafford New Hampshire	OK	10-17-2014 18:43:45	0d 0h 46m 51s	1/3	Weather OK: No watches or warni area.
	Weather Tulsa Oklahoma	OK	10-17-2014 18:45:53	737d 1h 53m 51s	1/3	Weather OK: No watches or warni area.
localhost	Current Load	OK	10-17-2014 18:49:08	0d 0h 46m 9s	1/4	OK - load average: 0.29, 0.49, 0.5
	Current Users	OK	10-17-2014 18:51:02	1710d 15h 36m 24s	1/4	USERS OK - 0 users currently logg
	HTTP	OK	10-17-2014 18:48:25	1019d 2h 7m 58s	1/4	HTTP OK: HTTP/1.1 200 OK - 21 response time
	PING	OK	10-17-2014 18:50:20	1710d 15h 35m 9s	1/4	PING OK - Packet loss = 0%, RTA
	Root Partition	OK	10-17-2014 18:48:32	938d 2h 32m 35s	1/4	DISK OK - free space: / 20300 MB
	SSH	OK	10-17-2014 18:46:38	1704d 7h 35m 15s	1/4	SSH OK - OpenSSH_4.3 (protocol
	Swap Usage	OK	10-17-2014 18:48:54	1710d 15h 33m 17s	1/4	SWAP OK - 100% free (255 MB ou
	Total Processes	OK	10-17-2014 18:50:49	1706d 8h 22m 2s	1/4	PROCS OK: 147 processes with S

SNMP Manager Example: [Nagios] II

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
- Configuration

Current Network Status
Last Updated: Tue Jun 9 15:56:07 CDT 2015
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

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

Host Status Totals

Up	Down	Unreachable	Pending
41	9	0	1

All Problems	All Types
9	51

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
338	11	9	141	1

All Problems	All Types
161	500

Service Status Details For All Hosts

Limit Results: 100

Results 300 - 400 of 500 Matching Services

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ScottsServer	Page File Usage	OK	06-09-2015 15:54:55	36d 4h 35m 32s	1/5	Paging File usage is 0.00 %
	Ping	OK	06-09-2015 15:55:30	4d 6h 4m 36s	1/5	OK - 192.168.5.15: rta 1.011ms, lost 0%
	SQL Server	CRITICAL	06-09-2015 15:51:43	36d 4h 31m 32s	5/5	MSSQLSERVER: Not found
	Server Work Queues	OK	06-09-2015 15:51:41	26d 4h 13m 36s	1/5	Current work queue (an indication of processing load) is 0
	Uptime	OK	06-09-2015 15:51:55	4d 6h 2m 8s	1/5	System Uptime - 4 day(s) 6 hour(s) 0 minute(s)
abc.com	DNS IP Match	OK	06-09-2015 15:52:18	26d 15h 15m 11s	1/5	DNS OK: 0.007 seconds response time. abc.com returns 199.181.132.250
	DNS Resolution	OK	06-09-2015 15:51:08	26d 15h 16m 25s	1/5	DNS OK: 0.011 seconds response time. abc.com returns 199.181.132.250
	HTTP	OK	06-09-2015 15:55:42	5d 14h 11m 15s	1/5	HTTP OK: HTTP/1.1 301 Moved Permanently - 428 bytes in 0.144 second response time
	Ping	OK	06-09-2015 15:54:58	4d 21h 21m 47s	1/5	OK - abc.com: rta 57.127ms, lost 0%
	Web Page Content	CRITICAL	06-09-2015 15:55:39	390d 21h 17m 29s	5/5	HTTP CRITICAL: HTTP/1.1 301 Moved Permanently - string 'ABC' not found on 'http://abc.com:80/' - 504 bytes in 0.123 second response time
conference.nagios.local	NetBIOS	CRITICAL	06-09-2015 15:51:08	63d 0h 51m 18s	5/5	connect to address 192.168.5.10 and port 139: No route to host
	Ping	CRITICAL	06-09-2015 15:51:06	63d 0h 50m 45s	5/5	CRITICAL - 192.168.5.10: Host unreachable @ 192.168.5.60. rta nan, lost 100%
	RDP	CRITICAL	06-09-2015 15:54:20	63d 0h 53m 4s	5/5	connect to address 192.168.5.10 and port 3389: No route to host
exchange.nagios.org	/ Disk Usage	OK	06-09-2015 15:53:39	0d 1h 56m 46s	1/5	DISK OK - free space: / 72815 MB (92% inode=98%):
	Apache Web Server	OK	06-09-2015 15:54:26	0d 1h 56m 0s	1/5	httpd (pid 2286) is running...
	CPU Stats	OK	06-09-2015 15:54:50	3d 4h 17m 5s	1/5	CPU STATISTICS OK: user=5.11% system=2.60% iowait=0.00% idle=92.22%
	Cron Scheduling Daemon	OK	06-09-2015 15:54:29	0d 1h 55m 57s	1/5	crond (pid 2296) is running...
	DNS IP Match	OK	06-09-2015 15:51:25	18d 18h 48m 0s	1/5	DNS OK: 0.270 seconds response time. exchange.nagios.org returns 66.228.58.94
	DNS Resolution	OK	06-09-2015 15:51:11	467d 11h 59m 56s	1/5	DNS OK: 0.015 seconds response time. exchange.nagios.org returns 66.228.58.94
	HTTP	OK	06-09-2015 15:54:58	6d 23h 52m 1s	1/5	HTTP OK: HTTP/1.1 301 Moved Permanently - 572 bytes in 0.085 second response time
	Load	OK	06-09-2015 15:54:05	8d 1h 35m 37s	1/5	OK - load average: 0.15, 0.20, 0.22
	Memory Usage	OK	06-09-2015 15:53:54	0d 1h 56m 30s	1/5	OK - 7624 / 8107 MB (94%) Free Memory, Used: 483 MB, Shared: 0 MB, Buffers: 21 MB, Cached: 229 MB
	MySQL Server	OK	06-09-2015 15:53:40	3d 23h 15m 19s	1/5	mysqld (pid 2127) is running...
	Open Files	OK	06-09-2015 15:53:33	1d 16h 8m 41s	1/5	OK: 1184 open files (0% of max 830107)
	Ping	OK	06-09-2015 15:54:14	0d 1h 56m 11s	1/5	OK - exchange.nagios.org: rta 40.931ms, lost 0%
	SSH Server	OK	06-09-2015 15:54:36	0d 0h 56m 12s	1/5	openssh-daemon (pid 1961) is running...
	Swap Usage	OK	06-09-2015 15:55:48	1d 4h 20m 34s	1/5	SWAP OK - 100% free (255 MB out of 255 MB)
	System Logging Daemon	OK	06-09-2015 15:53:50	0d 1h 56m 35s	1/5	rsyslogd (pid 1933) is running...
	Total Processes	OK	06-09-2015 15:51:54	0d 0h 4m 13s	1/5	PROCS OK: 145 processes
	Users	OK	06-09-2015 15:53:58	26d 15h 14m 20s	1/5	USERS OK - 1 users currently logged in
	Yum Updates	WARNING	06-09-2015 15:52:22	0d 1h 53m 6s	5/5	YUM WARNING: O/S requires an update.
firewall	Ping	OK	06-09-2015 15:54:37	206d 3h 56m 47s	1/5	OK - 192.168.5.1: rta 2.772ms, lost 0%
gateway.nagios.local	HTTPS	OK	06-09-2015 15:54:32	85d 3h 20m 48s	1/5	TCP OK - 0.002 second response time on 192.168.5.1 port 443
	Ping	OK	06-09-2015 15:54:26	85d 3h 20m 43s	1/5	OK - 192.168.5.1: rta 2.250ms, lost 0%
	Telnet	OK	06-09-2015 15:54:49	85d 3h 21m 6s	1/5	TCP OK - 0.002 second response time on 192.168.5.1 port 23
	bgroup0 Bandwidth	OK	06-09-2015 15:53:53	0d 11h 57m 16s	1/5	OK - Current BW in: .49Mbps Out: 6.70Mbps
	bgroup0 Status	OK	06-09-2015 15:51:58	85d 3h 21m 37s	1/5	OK: Interface bgroup0 (index 9) is up.
	bgroup1 Bandwidth	OK	06-09-2015 15:55:42	286d 17h 2m 4s	1/5	OK - Current BW in: 0Mbps Out: 0Mbps
	bgroup1 Status	CRITICAL	06-09-2015 15:51:45	85d 3h 17m 6s	5/5	CRITICAL: Interface bgroup1 (index 10) is down.
	bgroup2 Bandwidth	OK	06-09-2015 15:53:17	286d 17h 1m 0s	1/5	OK - Current BW in: 0Mbps Out: 0Mbps
	bgroup2 Status	WARNING	06-09-2015 15:51:25	265d 22h 47m 42s	5/5	WARNING: Interface bgroup2 (index 11) is administratively down.
	bgroup3 Bandwidth	OK	06-09-2015 15:51:09	18d 18h 48m 0s	1/5	OK - Current BW in: 0Mbps Out: 0Mbps
	bgroup3 Status	WARNING	06-09-2015 15:52:59	18d 18h 44m 15s	5/5	WARNING: Interface bgroup3 (index 12) is administratively down.

SNMP Manager Example: [Nagios] III

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
- Configuration

Alert History
Last Updated: Tue Jun 9 15:00:11 CDT 2015
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

View Status Detail For All Hosts
View Notifications For All Hosts

All Hosts and Services

Latest Archive

Log File Navigation
Tue Jun 9 00:00:00 CDT 2015 to Present..

File: /usr/local/nagios/var/nagios.log

State type options:
All state types
History detail level for all hosts:
All alerts
Hide Flapping Alerts
Hide Downtime Alerts
Hide Process Messages
Older Entries First
Update

June 09, 2015 15:00

[06-09-2015 15:59:48] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;4;PROCS WARNING: 154 processes
[06-09-2015 15:58:49] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;3;PROCS WARNING: 175 processes
[06-09-2015 15:57:50] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;2;PROCS WARNING: 152 processes
[06-09-2015 15:56:52] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;1;PROCS WARNING: 174 processes
[06-09-2015 15:54:42] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;OK;HARD;5;OK - Current BW in: 0Mbps Out: .81Mbps
[06-09-2015 15:51:54] SERVICE ALERT: exchange.nagios.org;Total Processes;OK;SOFT;2;PROCS OK: 145 processes
[06-09-2015 15:50:55] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;1;PROCS WARNING: 163 processes
[06-09-2015 15:50:48] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;OK;SOFT;4;OK - Current BW in: 0Mbps Out: .81Mbps
[06-09-2015 15:49:50] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;3;CRITICAL - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:49:43] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;HARD;5;WARNING - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:48:53] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;OK;HARD;5;OK - Current BW in: 8.38Mbps Out: 4.35Mbps
[06-09-2015 15:48:51] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;2;CRITICAL - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:48:45] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;SOFT;4;WARNING - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:47:51] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;1;CRITICAL - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:47:46] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;SOFT;3;WARNING - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:46:46] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;SOFT;2;WARNING - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:46:05] SERVICE ALERT: Office Backbone;Trusted One Bandwidth;OK;SOFT;2;OK - Current BW in: 4.28Mbps Out: 8.45Mbps
[06-09-2015 15:45:58] SERVICE ALERT: exchange.nagios.org;Total Processes;OK;HARD;5;PROCS OK: 147 processes
[06-09-2015 15:45:48] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;SOFT;1;WARNING - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:45:06] SERVICE ALERT: Office Backbone;Trusted One Bandwidth;WARNING;SOFT;1;WARNING - Current BW in: 1.02Mbps Out: 21.23Mbps
[06-09-2015 15:43:54] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;WARNING;HARD;5;WARNING - Current BW in: 21.50Mbps Out: 1.09Mbps
[06-09-2015 15:42:55] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;WARNING;SOFT;4;WARNING - Current BW in: 21.50Mbps Out: 1.09Mbps
[06-09-2015 15:42:52] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;OK;HARD;5;OK - Current BW in: .14Mbps Out: 0Mbps
[06-09-2015 15:41:57] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;WARNING;SOFT;3;WARNING - Current BW in: 21.50Mbps Out: 1.09Mbps
[06-09-2015 15:40:58] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;WARNING;SOFT;2;WARNING - Current BW in: 21.50Mbps Out: 1.09Mbps
[06-09-2015 15:40:00] SERVICE ALERT: 192.168.5.42;Port 1 Bandwidth;WARNING;SOFT;1;WARNING - Current BW in: 16.86Mbps Out: .78Mbps
[06-09-2015 15:37:55] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;HARD;5;CRITICAL - Current BW in: 14.17Mbps Out: 0Mbps
[06-09-2015 15:35:11] SERVICE FLAPPING ALERT: localhost;MySQL Table Cache Hit Rate;STARTED; Service appears to have started flapping (20.9% change >= 20.0% threshold)
[06-09-2015 15:35:11] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;OK;HARD;5;OK - table cache hitrate 0.02%, 67.19% filled
[06-09-2015 15:20:18] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;CRITICAL;HARD;5;CRITICAL - table cache hitrate 0.03%
[06-09-2015 15:19:21] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;CRITICAL;SOFT;4;CRITICAL - table cache hitrate 0.03%
[06-09-2015 15:18:22] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;CRITICAL;SOFT;3;CRITICAL - table cache hitrate 0.03%
[06-09-2015 15:17:23] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;CRITICAL;SOFT;2;CRITICAL - table cache hitrate 0.03%
[06-09-2015 15:16:24] SERVICE ALERT: localhost;MySQL Table Cache Hit Rate;CRITICAL;SOFT;1;CRITICAL - table cache hitrate 0.03%
[06-09-2015 15:08:02] SERVICE FLAPPING ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;STARTED; Service appears to have started flapping (22.0% change >= 20.0% threshold)
[06-09-2015 15:08:02] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;WARNING;HARD;5;WARNING - Current BW in: 6.29Mbps Out: 0Mbps
[06-09-2015 15:07:04] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;WARNING;SOFT;4;WARNING - Current BW in: 6.29Mbps Out: 0Mbps
[06-09-2015 15:06:16] SERVICE ALERT: vs1.nagios.com;Memory Usage;WARNING;HARD;5;WARNING - 1442 / 8107 MB (17%) Free Memory, Used: 6665 MB, Shared: 28 MB, Buffers: 81 MB, Cached: 2788 MB
[06-09-2015 15:06:06] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;WARNING;SOFT;3;WARNING - Current BW in: 6.29Mbps Out: 0Mbps
[06-09-2015 15:06:01] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;OK;SOFT;2;OK - Current BW in: 6.29Mbps Out: 0Mbps
[06-09-2015 15:05:18] SERVICE ALERT: vs1.nagios.com;Memory Usage;WARNING;SOFT;4;WARNING - 1439 / 8107 MB (17%) Free Memory, Used: 6668 MB, Shared: 28 MB, Buffers: 80 MB, Cached: 2786 MB
[06-09-2015 15:05:08] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;2;CRITICAL - Current BW in: 59.23Mbps Out: 0Mbps
[06-09-2015 15:05:03] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;WARNING;SOFT;1;WARNING - Current BW in: 59.23Mbps Out: 0Mbps
[06-09-2015 15:04:18] SERVICE ALERT: vs1.nagios.com;Memory Usage;WARNING;SOFT;3;WARNING - 1474 / 8107 MB (18%) Free Memory, Used: 6633 MB, Shared: 28 MB, Buffers: 80 MB, Cached: 2784 MB
[06-09-2015 15:04:12] SERVICE ALERT: 192.168.5.41;Port-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;1;CRITICAL - Current BW in: 59.23Mbps Out: 0Mbps
[06-09-2015 15:03:22] SERVICE ALERT: vs1.nagios.com;Memory Usage;WARNING;SOFT;2;WARNING - 994 / 8107 MB (12%) Free Memory, Used: 7113 MB, Shared: 28 MB, Buffers: 79 MB, Cached: 2780 MB
[06-09-2015 15:02:23] SERVICE ALERT: vs1.nagios.com;Memory Usage;WARNING;SOFT;1;WARNING - 1635 / 8107 MB (20%) Free Memory, Used: 6472 MB, Shared: 28 MB, Buffers: 109 MB, Cached: 3380 MB
[06-09-2015 15:01:13] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;HARD;5;PROCS WARNING: 156 processes
[06-09-2015 15:00:16] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;4;PROCS WARNING: 152 processes

SNMP Manager Example: [Nagios] IV

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
- Configuration

Current Event Log
Last Updated: Tue Jun 9 16:06:28 CDT 2015
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

Latest Archive

Log File Navigation
Tue Jun 9 00:00:00 CDT 2015
to
Present

File: /usr/local/nagios/var/nagios.log

June 09, 2015 16:00

[06-09-2015 16:05:43] GLOBAL SERVICE EVENT HANDLER: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;1;xi_service_event_handler
[06-09-2015 16:05:43] SERVICE ALERT: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;1;CRITICAL - Current BW in: 58.32Mbps Out: .92Mbps
[06-09-2015 16:00:57] GLOBAL SERVICE EVENT HANDLER: vs1.nagios.com;Memory Usage;CRITICAL;HARD;5;xi_service_event_handler
[06-09-2015 16:00:57] SERVICE ALERT: vs1.nagios.com;Memory Usage;CRITICAL;HARD;5;CRITICAL - 888 / 8107 MB (10%) Free Memory, Used: 7219 MB, Shared: 29 MB,
[06-09-2015 16:00:46] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;HARD;5;xi_service_event_handler
[06-09-2015 16:00:46] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;HARD;5;PROCS WARNING: 167 processes

June 09, 2015 15:00

[06-09-2015 15:59:48] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;SOFT;4;xi_service_event_handler
[06-09-2015 15:59:48] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;4;PROCS WARNING: 154 processes
[06-09-2015 15:58:49] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;SOFT;3;xi_service_event_handler
[06-09-2015 15:58:49] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;3;PROCS WARNING: 175 processes
[06-09-2015 15:57:50] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;SOFT;2;xi_service_event_handler
[06-09-2015 15:57:50] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;2;PROCS WARNING: 152 processes
[06-09-2015 15:56:52] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;SOFT;1;xi_service_event_handler
[06-09-2015 15:56:52] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;1;PROCS WARNING: 174 processes
[06-09-2015 15:54:42] GLOBAL SERVICE EVENT HANDLER: 192.168.5.41;Port 1 Bandwidth;OK;HARD;5;xi_service_event_handler
[06-09-2015 15:54:42] SERVICE NOTIFICATION: nscott;192.168.5.41;Port 1 Bandwidth;OK;xi_service_notification_handler;OK - Current BW in: 0Mbps Out: .81Mbps
[06-09-2015 15:54:42] SERVICE ALERT: 192.168.5.41;Port 1 Bandwidth;OK;HARD;5;OK - Current BW in: 0Mbps Out: .81Mbps
[06-09-2015 15:53:29] SERVICE NOTIFICATION: nscott;192.168.5.41;Port 4 Status;CRITICAL;xi_service_notification_handler;CRITICAL: Interface Port: 4 Gigabit - Level (index
[06-09-2015 15:51:58] SERVICE NOTIFICATION: nscott;192.168.5.41;Port 18 Status;CRITICAL;xi_service_notification_handler;CRITICAL: Interface Port: 18 Gigabit - Level (inc
[06-09-2015 15:51:54] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;OK;SOFT;2;xi_service_event_handler
[06-09-2015 15:51:54] SERVICE ALERT: exchange.nagios.org;Total Processes;OK;SOFT;2;PROCS OK: 145 processes
[06-09-2015 15:51:01] SERVICE NOTIFICATION: nscott;192.168.5.41;Port 14 Status;CRITICAL;xi_service_notification_handler;CRITICAL: Interface Port: 14 Gigabit - Level (inc
[06-09-2015 15:50:55] GLOBAL SERVICE EVENT HANDLER: exchange.nagios.org;Total Processes;WARNING;SOFT;1;xi_service_event_handler
[06-09-2015 15:50:55] SERVICE ALERT: exchange.nagios.org;Total Processes;WARNING;SOFT;1;PROCS WARNING: 163 processes
[06-09-2015 15:50:48] GLOBAL SERVICE EVENT HANDLER: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;OK;SOFT;4;xi_service_event_handler
[06-09-2015 15:50:48] SERVICE ALERT: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;OK;SOFT;4;OK - Current BW in: 0Mbps Out: .81Mbps
[06-09-2015 15:49:50] GLOBAL SERVICE EVENT HANDLER: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;3;xi_service_event_handler
[06-09-2015 15:49:50] SERVICE ALERT: 192.168.5.41;Port:-1-Gigabit---Level Bandwidth;CRITICAL;SOFT;3;CRITICAL - Current BW in: 0Mbps Out: 57.57Mbps
[06-09-2015 15:49:43] GLOBAL SERVICE EVENT HANDLER: 192.168.5.41;Port 1 Bandwidth;WARNING;HARD;5;xi_service_event_handler

SNMP Manager Example: [Nagios] V

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
- Configuration

All Host and Service Scheduled Downtime
Last Updated: Tue Jun 9 16:35:23 CDT 2015
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

[Host Downtime | Service Downtime]

Scheduled Host Downtime

Schedule host downtime

Host Name	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
ScottsServer	06-09-2015 00:01:02	nagiosadmin	AUTO: Automatically scheduled for host	06-10-2015 00:00:00	06-10-2015 01:00:00	Fixed	0d 1h 0m 0s	4069	N/A	
ScottsServer	06-05-2015 18:01:02	nagiosadmin	AUTO: windows update	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4065	N/A	
ScottsServer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4052	N/A	
ScottsServer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4039	N/A	
ScottsServer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4026	N/A	
ScottsServer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4013	N/A	
ScottsServer	06-09-2015 00:01:02	nagiosadmin	AUTO: Automatically scheduled for host	06-15-2015 00:00:00	06-15-2015 01:00:00	Fixed	0d 1h 0m 0s	4070	N/A	

Scheduled Service Downtime

Schedule service downtime

Host Name	Service	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
ScottsServer	CPU Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4064	N/A	
ScottsServer	Drive C: Disk Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4063	N/A	
ScottsServer	Drive D: Disk Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4062	N/A	
ScottsServer	Explorer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4061	N/A	
ScottsServer	IIS Web Server	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4060	N/A	
ScottsServer	Logon Errors	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4059	N/A	
ScottsServer	Memory Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4058	N/A	
ScottsServer	Page File Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4057	N/A	
ScottsServer	Ping	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4056	N/A	
ScottsServer	SQL Server	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4055	N/A	
ScottsServer	Server Work Queues	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4054	N/A	
ScottsServer	Uptime	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4053	N/A	
ScottsServer	CPU Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4051	N/A	
ScottsServer	Drive C: Disk Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4050	N/A	
ScottsServer	Drive D: Disk Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4049	N/A	
ScottsServer	Explorer	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4048	N/A	
ScottsServer	IIS Web Server	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4047	N/A	
ScottsServer	Logon Errors	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4046	N/A	
ScottsServer	Memory Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4045	N/A	
ScottsServer	Page File Usage	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4044	N/A	
ScottsServer	Ping	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4043	N/A	
ScottsServer	SQL Server	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4042	N/A	
ScottsServer	Server Work Queues	06-05-2015 18:01:02	nagiosadmin	AUTO: Down for patching...again...!	06-12-2015 18:00:00	06-12-2015 20:00:00	Fixed	0d 2h 0m 0s	4041	N/A	

SNMP Manager Example: [Nagios] VI

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
- Configuration

Hostgroup Availability Report
Last Updated: Tue Jun 9 16:32:02 CDT 2015
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

All Hostgroups

06-02-2015 16:32:02 to 06-09-2015 16:32:02
Duration: 7d 0h 0m 0s

First assumed host state: Unspecified
First assumed service state: Unspecified
Report period: Last 7 Days
Backtracked archives: 4
Update

[Availability report completed in 0 min 0 sec]

Hostgroup 'all_emc_hosts' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
abc.com	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'firewalls' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
firewall	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'linux-servers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
ScottsServer	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
esx2.nagios.local	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
exchange.nagios.org	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
lmitchev.nagios.local	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
vs1.nagios.com	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'new group' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
192.168.5.33	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
ScottsServer	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
esx2.nagios.local	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
exchange.nagios.org	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
firewall	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
hp-1536dnf	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
hp-4100dtn	62.991% (62.991%)	0.000% (0.000%)	37.009% (37.009%)	0.000%
hp-cp2025	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
lmitchev.nagios.local	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
localhost	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
vs1.nagios.com	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	96.636% (96.636%)	0.000% (0.000%)	3.364% (3.364%)	0.000%

Hostgroup 'printers' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
hp-1536dnf	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
hp-4100dtn	62.991% (62.991%)	0.000% (0.000%)	37.009% (37.009%)	0.000%
hp-cp2025	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	87.664% (87.664%)	0.000% (0.000%)	12.336% (12.336%)	0.000%

Hostgroup 'switches' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
192.168.5.42	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
192.168.5.43	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Hostgroup 'websites' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
exchange.nagios.org	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
support.nagios.com	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

SNMP Manager Example: [Nagios] VII

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

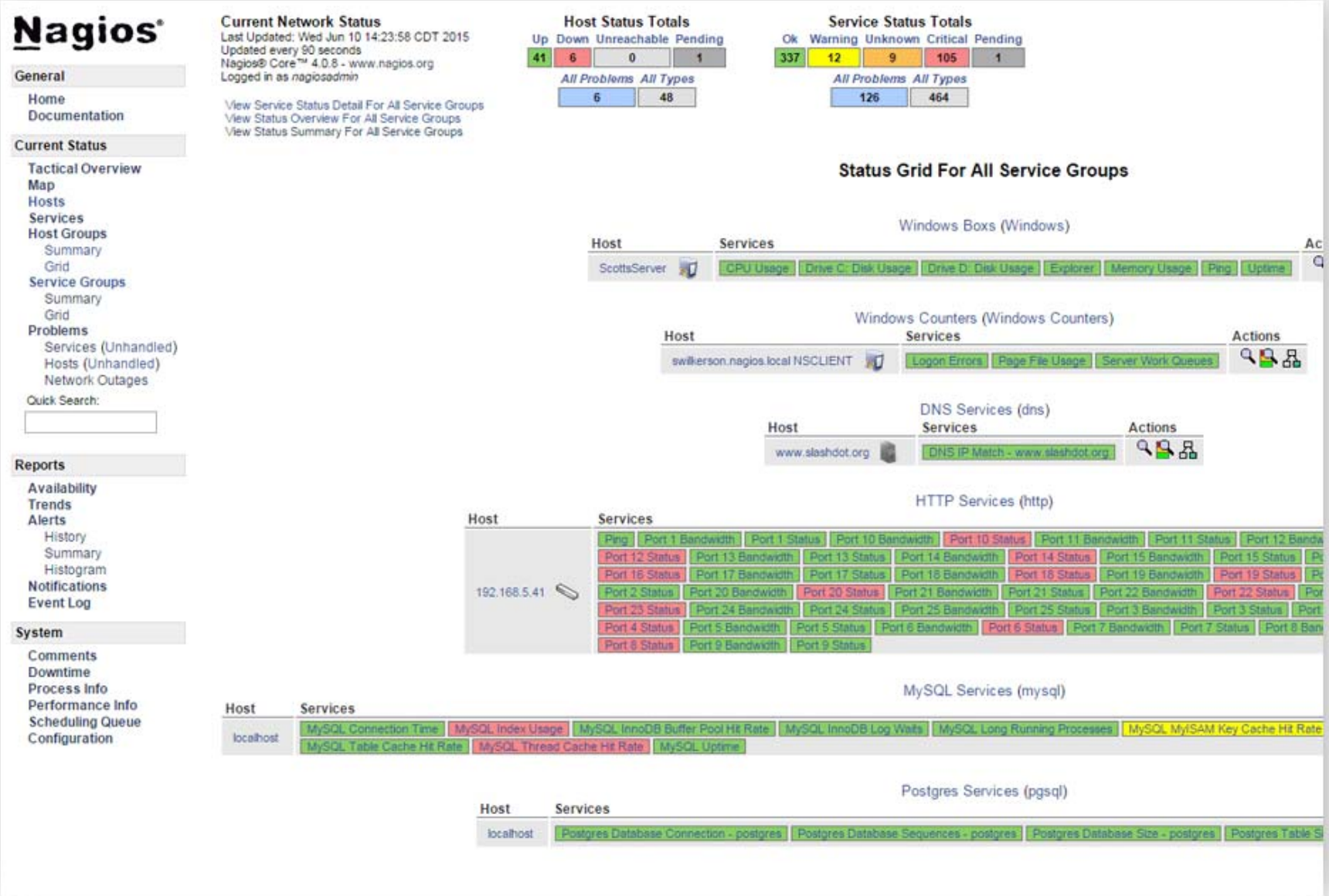
System
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Check Scheduling Queue
Last Updated: Wed Jun 10 12:54:54 CDT 2015
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

Entries sorted by **next check time** (ascending)

Host	Service	Last Check	Next Check	Type	Active Checks	Actions
192.168.5.43	gigabitethernet9 Status	06-10-2015 12:49:55	06-10-2015 12:54:52	Normal	ENABLED	
192.168.5.41	Port:-4-Gigabit—Level Status	06-10-2015 12:49:54	06-10-2015 12:54:52	Normal	ENABLED	
NNA Source - Source One - Roberts PC	Abnormal Behavior	06-10-2015 12:49:55	06-10-2015 12:54:53	Normal	ENABLED	
swilkerson.nagios.local SNMP	CPU Usage	06-10-2015 12:49:57	06-10-2015 12:54:54	Normal	ENABLED	
exchange.nagios.org	Yum Updates	06-10-2015 12:49:56	06-10-2015 12:54:54	Normal	ENABLED	
exchange.nagios.org		06-10-2015 12:49:57	06-10-2015 12:54:55	Normal	ENABLED	
abc.com	DNS IP Match	06-10-2015 12:49:58	06-10-2015 12:54:56	Normal	ENABLED	
192.168.5.41	Port:-22-Gigabit—Level Bandwidth	06-10-2015 12:49:58	06-10-2015 12:54:56	Normal	ENABLED	
192.168.5.43	gigabitethernet3 Status	06-10-2015 12:49:59	06-10-2015 12:54:57	Normal	ENABLED	
localhost	Postgres Table Sizes - postgres	06-10-2015 12:50:00	06-10-2015 12:54:58	Normal	ENABLED	
google.com	Ping	06-10-2015 12:50:00	06-10-2015 12:54:58	Normal	ENABLED	
vs1.nagios.com	Open Files	06-10-2015 12:50:01	06-10-2015 12:54:59	Normal	ENABLED	
gateway.nagios.local	ethernet0 3 Status	06-10-2015 12:50:02	06-10-2015 12:54:59	Normal	ENABLED	
support.nagios.com	_forum URL Status	06-10-2015 12:50:02	06-10-2015 12:55:00	Normal	ENABLED	
vs1.nagios.com	/ Disk Usage	06-10-2015 12:50:03	06-10-2015 12:55:01	Normal	ENABLED	
192.168.5.42	Port 8 Status	06-10-2015 12:50:03	06-10-2015 12:55:01	Normal	ENABLED	
NNA Source - Source One - Roberts PC	Bytes	06-10-2015 12:50:03	06-10-2015 12:55:02	Normal	ENABLED	
www.google.com	Ping	06-10-2015 12:50:04	06-10-2015 12:55:03	Normal	ENABLED	
192.168.5.41	Port 9 Status	06-10-2015 12:50:04	06-10-2015 12:55:03	Normal	ENABLED	
192.168.5.42	Port 101 Bandwidth	06-10-2015 12:50:05	06-10-2015 12:55:04	Normal	ENABLED	
mstarr.nagios.local	NetBIOS	06-10-2015 12:50:06	06-10-2015 12:55:05	Normal	ENABLED	
192.168.5.43	gigabitethernet7 Bandwidth	06-10-2015 12:50:06	06-10-2015 12:55:05	Normal	ENABLED	
vs1.nagios.com	Ping	06-10-2015 12:50:07	06-10-2015 12:55:06	Normal	ENABLED	
swilkerson.nagios.local WMI	Ping	06-10-2015 12:50:08	06-10-2015 12:55:07	Normal	ENABLED	
192.168.5.41	Port:-19-Gigabit—Level Bandwidth	06-10-2015 12:50:07	06-10-2015 12:55:07	Normal	ENABLED	
localhost	Total Processes	06-10-2015 12:50:09	06-10-2015 12:55:08	Normal	ENABLED	
192.168.5.42	Port 1 Bandwidth	06-10-2015 12:50:09	06-10-2015 12:55:08	Normal	ENABLED	
192.168.5.23	IIS Web Server	06-10-2015 12:50:10	06-10-2015 12:55:09	Normal	ENABLED	
swilkerson.nagios.local WMI	Explorer	06-10-2015 12:50:11	06-10-2015 12:55:10	Normal	ENABLED	
192.168.5.41	Port:-2-Gigabit—Level Status	06-10-2015 12:50:11	06-10-2015 12:55:10	Normal	ENABLED	
192.168.5.43	gigabitethernet22 Bandwidth	06-10-2015 12:50:12	06-10-2015 12:55:11	Normal	ENABLED	
gateway.nagios.local	bgroup3 Status	06-10-2015 12:50:13	06-10-2015 12:55:12	Normal	ENABLED	
192.168.5.43	gigabitethernet2 Status	06-10-2015 12:50:13	06-10-2015 12:55:12	Normal	ENABLED	

SNMP Manager Example: [Nagios] VIII



Outline

- Introduction
- SNMP
- ⇒ **MRTG**
- collectd
- NetData
- ELK
- Bibliography

MRTG – Multi Router Traffic Grapher

- Relies on SNMP
- Creates **graph data** (ex. network load)
- Fast and dynamic visualization
- Qualitative result

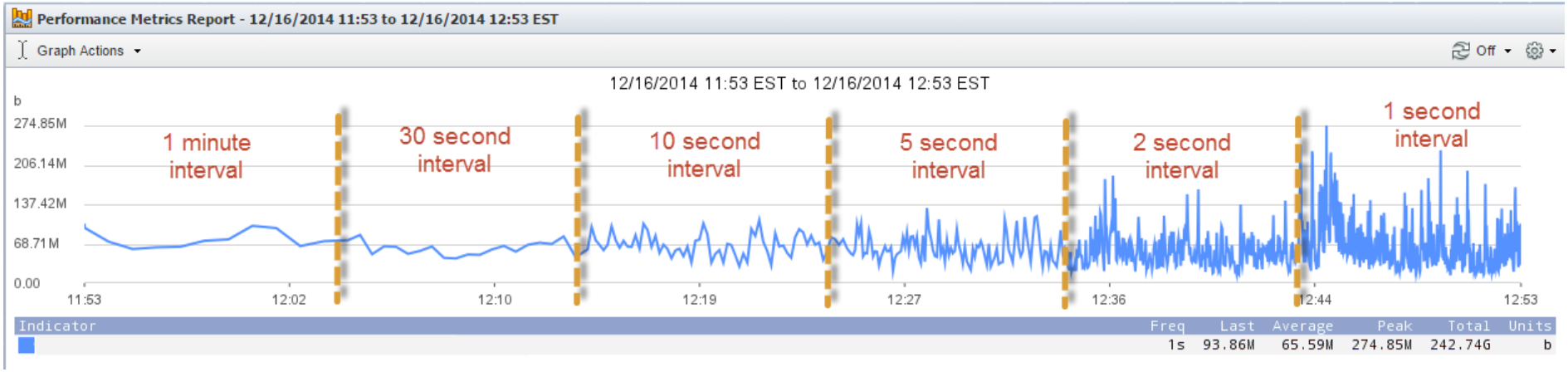
For UNice ⇒ http://nephi.unice.fr/Router/

SNMP Pros and Cons

- Pros:
  - Stood the test of time
  - Supported by default by all networking hardware (and a lot of software)
  - Centralized management with alerting mechanism
  - Cross-platform
- Cons:
  - Configuration can be cumbersome
  - Actions only based on changes in values
  - Granularity of data can be too coarse
    - Refresh time not always changeable
    - More and more reliance on virtual appliances and commodity hardware

SNMP Data Granularity

[Farmer 2014]



Outline

- Introduction
- SNMP
- MRTG
- ⇒ **collectd**
- NetData
- ELK
- Bibliography

collectd

- Unix/Linux Daemon responsible for collecting system and application metrics
  - Windows port available
- Able to store retrieved values on a variety of database back ends

  (e.g. time-series database)
- Ability to transmit data on network, including using multicast
- Lightweight (usually embedded with DD-WRT)
- Based on plug-ins
  - Easy to write
  - More than 100 plug-in available
- High data granularity

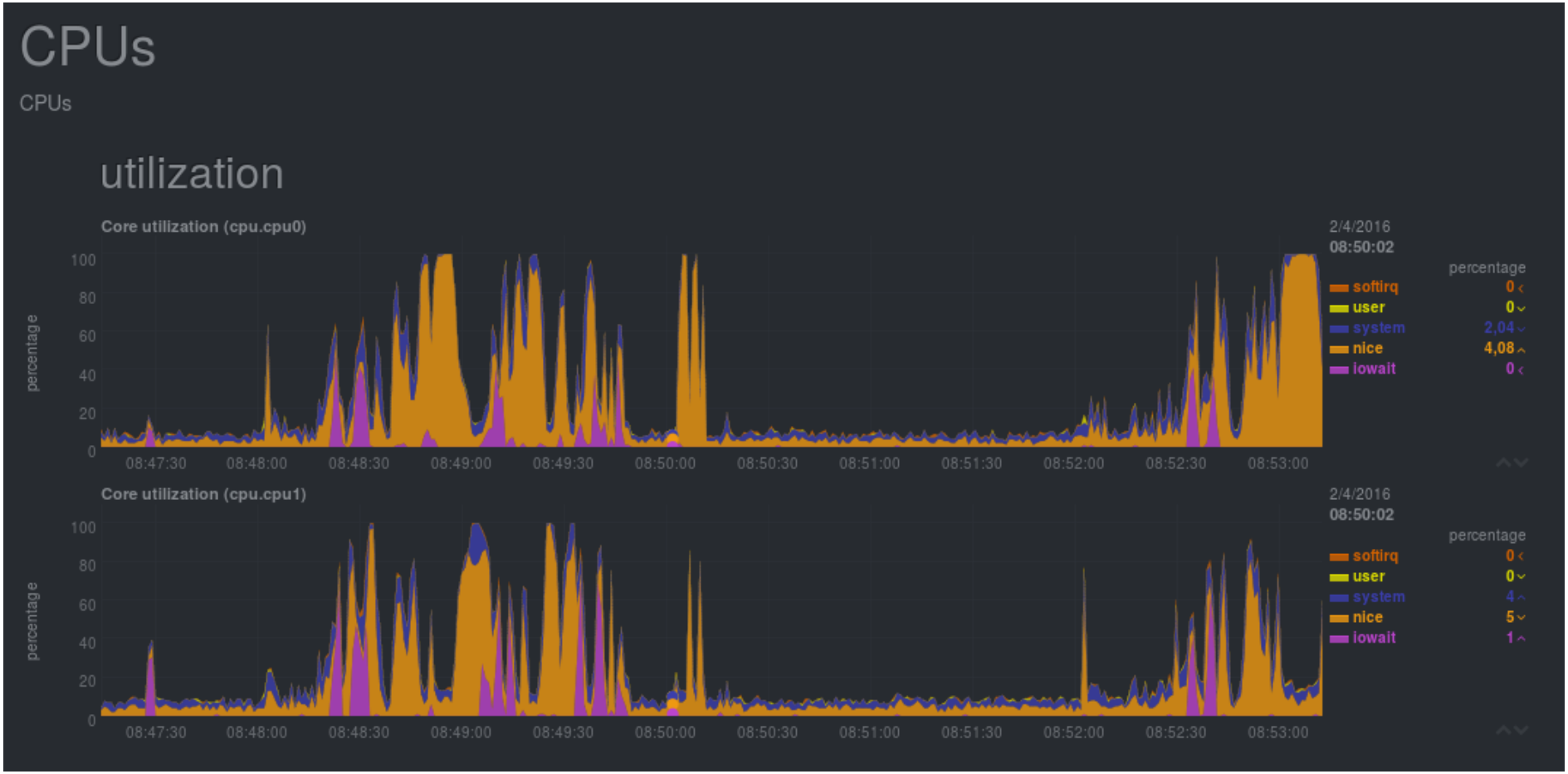
Outline

- Introduction
- SNMP
- MRTG
- collectd
- ⇒ **NetData**
- ELK
- Bibliography

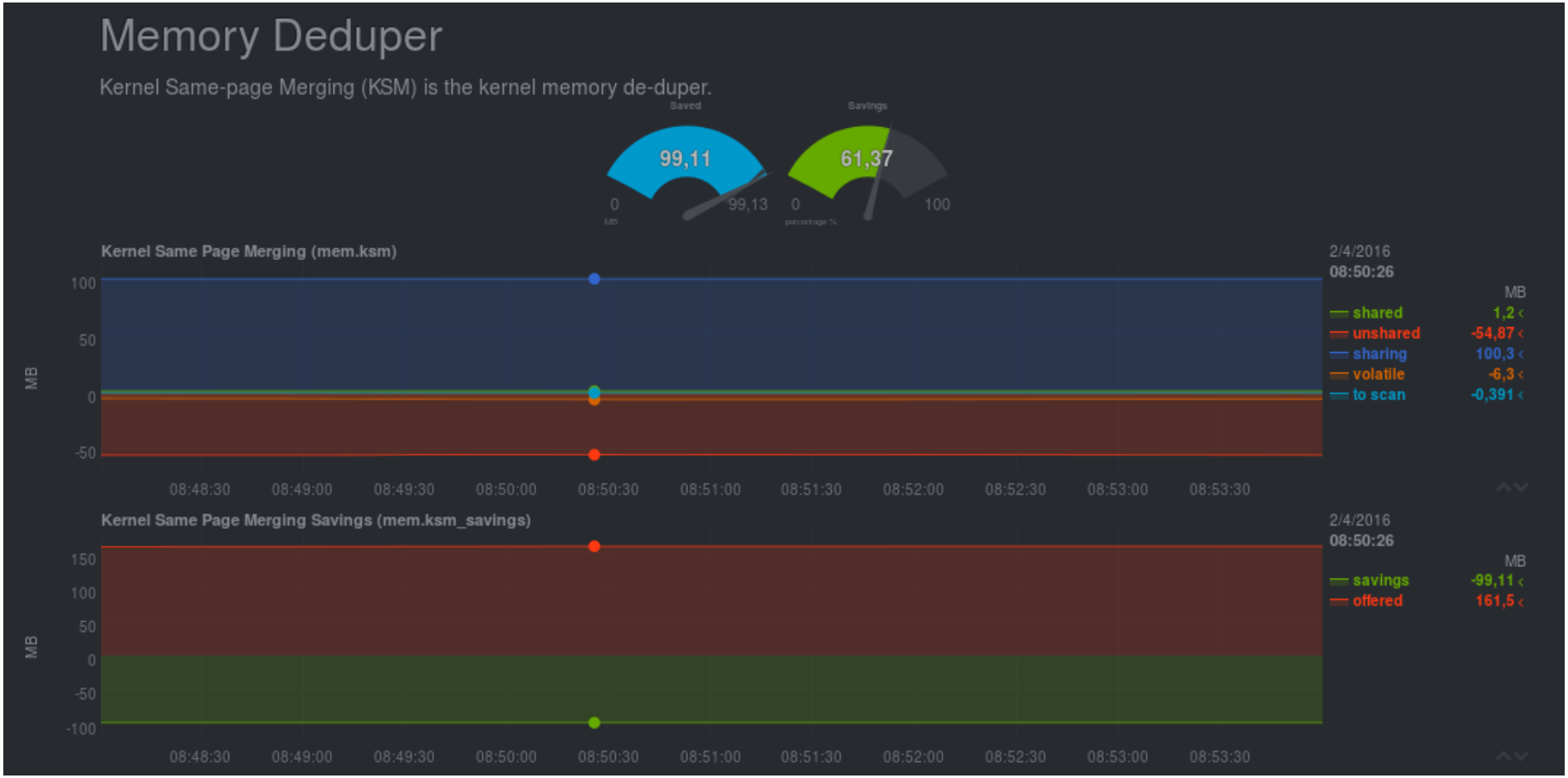
NetData

- Linux/BSD application for real-time monitoring
- Metric collection back-end in C
- Front-end UI in JS.node
- Very easily installed (just one package/container), self aware
- Needs to be installed on every monitored device
- Only localized view
- Demo: http://my-netdata.io/#demosites

Netdata


CPUs
CPUs
utilization
Core utilization (cpu.cpu0)
percentage
100
80
60
40
20
0
08:47:30
08:48:00
08:48:30
08:49:00
08:49:30
08:50:00
08:50:30
08:51:00
08:51:30
08:52:00
08:52:30
08:53:00
2/4/2016
08:50:02
percentage
softirq 0
user 0
system 2,04
nice 4,08
iowait 0
Core utilization (cpu.cpu1)
percentage
100
80
60
40
20
0
08:47:30
08:48:00
08:48:30
08:49:00
08:49:30
08:50:00
08:50:30
08:51:00
08:51:30
08:52:00
08:52:30
08:53:00
2/4/2016
08:50:02
percentage
softirq 0
user 0
system 4
nice 5
iowait 1

Netdata


Memory Deduper
Kernel Same-page Merging (KSM) is the kernel memory de-duper.
Saved
99,11
0
99,13
Savings
61,37
0
100
Kernel Same Page Merging (mem.ksm)
2/4/2016
08:50:26
MB
shared 1,2
unshared -54,87
sharing 100,3
volatile -6,3
to scan -0,391
100
50
0
-50
MB
08:48:30
08:49:00
08:49:30
08:50:00
08:50:30
08:51:00
08:51:30
08:52:00
08:52:30
08:53:00
08:53:30
Kernel Same Page Merging Savings (mem.ksm_savings)
2/4/2016
08:50:26
MB
savings -99,11
offered 161,5
150
100
50
0
-50
-100
MB
08:48:30
08:49:00
08:49:30
08:50:00
08:50:30
08:51:00
08:51:30
08:52:00
08:52:30
08:53:00
08:53:30

Outline

- Introduction
- SNMP
- MRTG
- collectd
- NetData
- ⇒ **ELK**
- Bibliography

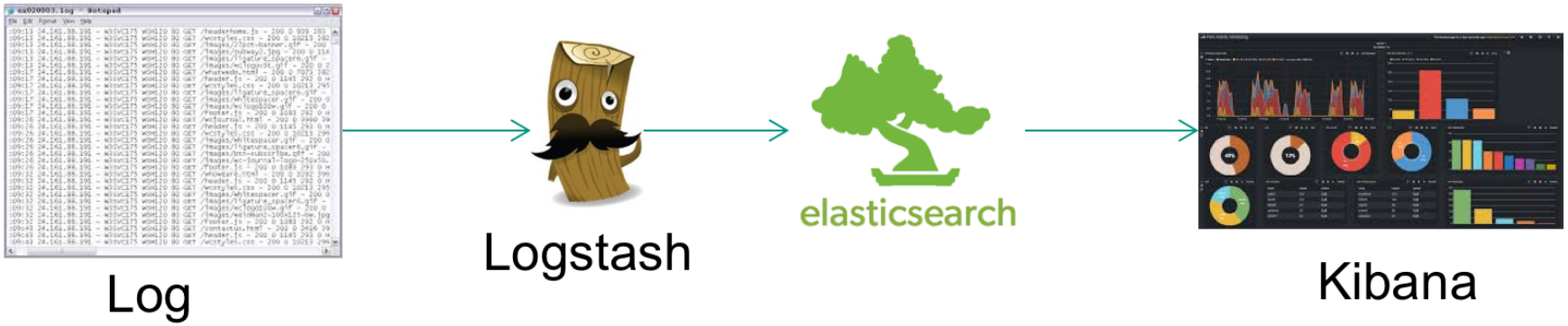
Log Consolidation

- Motivation:
  - A lot of physical/virtual machines, and/or containers
  - Fuse/archive all logs
  - To search/browse these logs

ELK Stack

- Elasticsearch, Logstash, Kibana
  — https://www.elastic.co/fr/

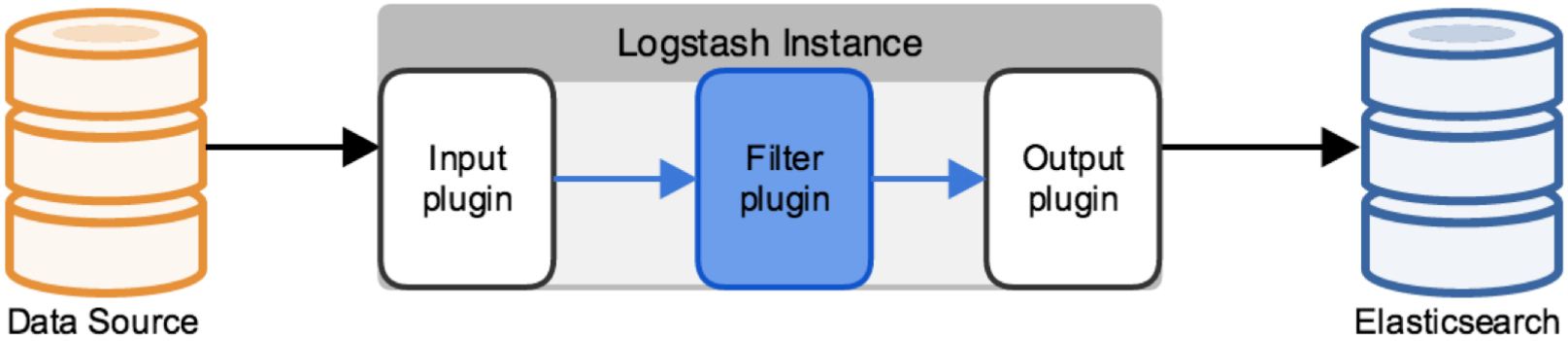
1. Logstash: data/log collection, filtering, parsing, and formatting to JSON format
2. Elasticsearch: search engine
3. Kibana: exploration and visualization



Logstash

- Implemented in JRuby, runs within a JVM
- Collects data by opening a port for each type of data

  (e.g. a port for syslog, a port for Apache logs,. . .)
- Once collected, data can be filtered and enriched
- Augmented data is passed onto next tool (e.g. Elasticsearch, Graphite)



Logstash: a Configuration File I

Three parts corresponding to the 3 operations:

```
input {
  file {
    path => "/tmp/access_log"
    start_position => "beginning"
  }
}

filter {
  if [path] =~ "access" {
    mutate { replace => { "type" => "apache_access" } }
    grok {
      match => { "message" => "%{COMBINEDAPACHELOG}" }
    }
  }
  date {
    match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]
  }
}

output {
  elasticsearch {
    host => localhost
  }
  stdout { codec => rubydebug }
}
```

Logstash: a Configuration File II

Notice TCP and UDP port numbers per log type, and filter:

```
input {
  tcp {
    port => 5000
    type => syslog
  }
  udp {
    port => 5000
    type => syslog
  }
}

filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_h
_program}(?:\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }
      add_field => [ "received_at", "%{@timestamp}" ]
      add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
    date {
      match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}

output {
  elasticsearch { host => localhost }
  stdout { codec => rubydebug }
}
```

Configuration for parsing syslog messages

Input filter receives messages directly from tcp and udp ports

Filter splits messages and adds fields

Logstash: Filter Example

The filter `grok` splits a string into fields that can be indexed by Elasticsearch

grok usage example

- Input: 55.3.244.1 GET /index.html 15824 0.043
- grok filter

```
filter {
    grok { match => { "message" => "%{IP:client}
%{WORD:method} %{URIPATHPARAM:request}
%{NUMBER:bytes} %{NUMBER:duration}" }
}
```

- Then the output will contain fields like:
  - client: 55.3.244.1
  - method: GET
  - request: /index.html
  - bytes: 15824
  - duration: 0.043

Elasticsearch

- Written in Java, based on Apache Lucene indexing engine
- Similar to a database: schemas can be added
- Can run on a cluster for scaling up
- Able to select stored data, and indexed data
- Indexed data speeds up searches, but requires storage and memory

Elasticsearch: Indexation I

Writing an object in an index through the REST API

```
PUT /megacorp/employee/1
{
    "first_name" : "John",
    "last_name" :  "Smith",
    "age" :        25,
    "about" :      "I love to go rock climbing",
    "interests": [ "sports", "music" ]
}
```

Here: an object of type `employee` written in index `megacorp`

Elasticsearch: Indexation II

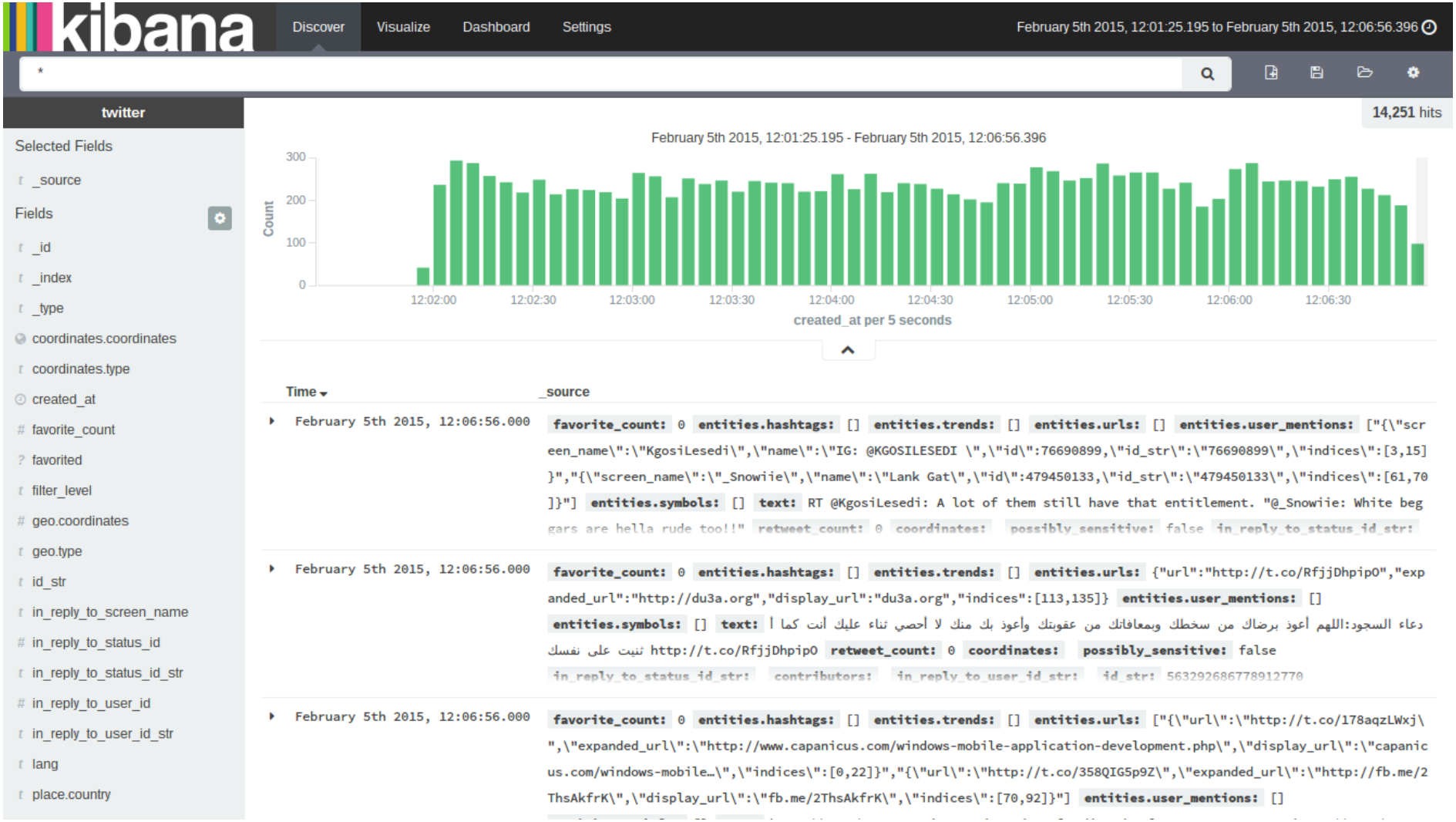
The same object after insertion/search:

GET /megacorp/employee/_search?q=last_name:Smith

```
{
   ...
   "hits": {
      "total":      2,
      "max_score":  0.30685282,
      "hits": [
         {
            ...
            "_source": {
               "first_name":  "John",
               "last_name":   "Smith",
               "age":         25,
               "about":       "I love to go rock climbing",
               "interests": [ "sports", "music" ]
            }
         },
         {
            ...
            "_source": {
               "first_name":  "Jane",
               "last_name":   "Smith",
               "age":         32,
               "about":       "I like to collect rock albums",
               "interests": [ "music" ]
            }
         }
      ]
```

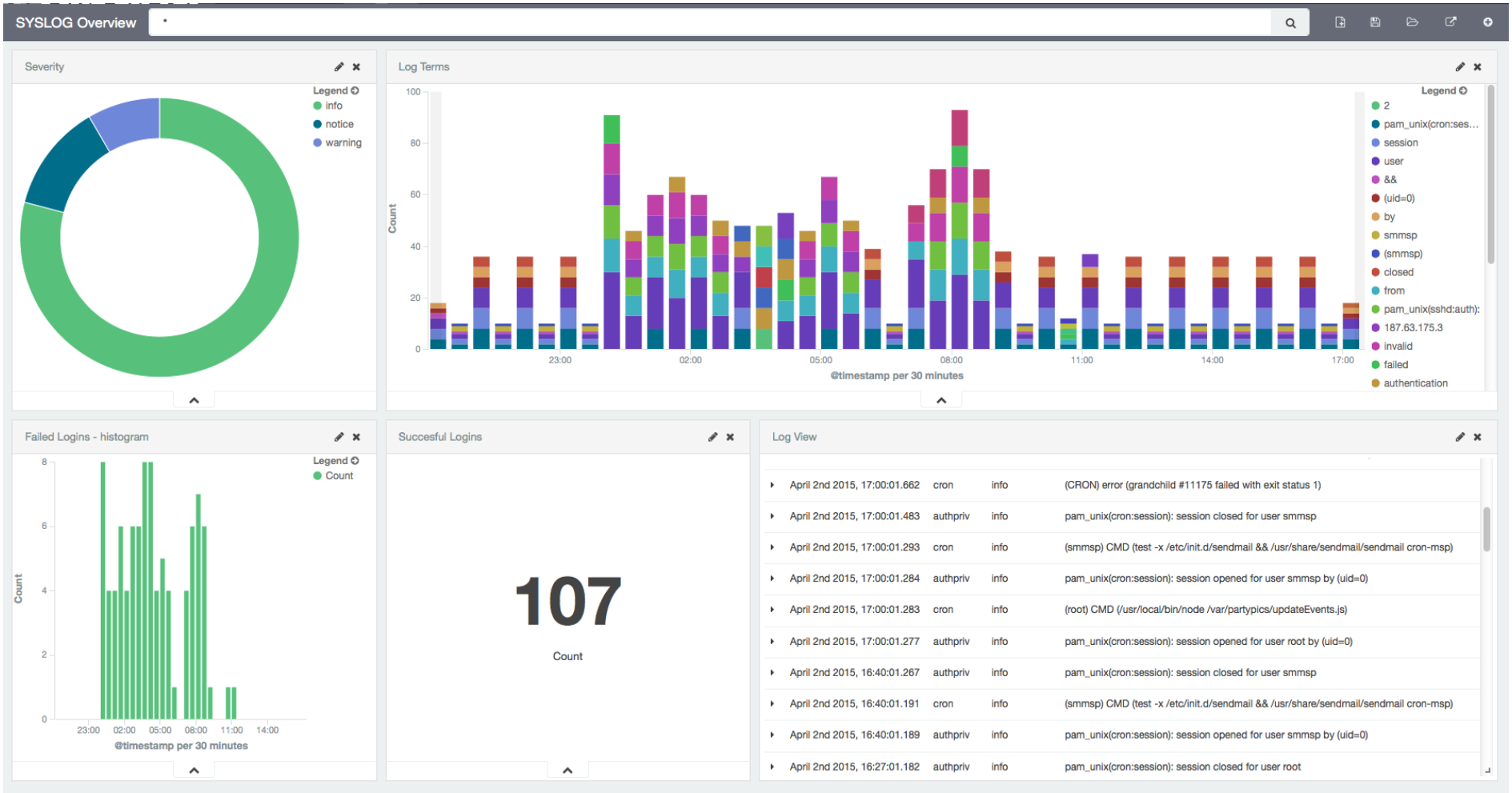
Kibana I

Useful graphical rendering tool for browsing Elasticsearch indexes



Kibana

Ability to create *dashboards* by picking within Elasticsearch indexes




I DON'T HAVE A BUDGET FOR THE NET-WORK MONITORING SOFTWARE YOU NEED, SO YOU'LL HAVE TO WRITE IT YOURSELF.
Dilbert.com DilbertCartoonist@gmail.com
GOOD PLAN. I'LL CHECK BACK WITH YOU WHEN I'M DONE DOING THAT.
9-4-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
WHAT'S YOUR CAL-ENDAR LOOK LIKE IN THE YEAR 2040?
SORT OF A GRID WITH SQUARE BOXES.

Outline

- Introduction
- SNMP
- MRTG
- collectd
- NetData
- ELK

⇒ **Bibliography**

Bibliography I

[Farmer 2014]
B. Farmer, *SNMP polling interval granularity*, https://brandonfarmer.com/2014/12/16/snmp-polling-interval-granularity/, Dec. 2014.

[K&R]
J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 6th. Addison-Wesley, 2012.

[Nagios]
Nagios, *Screenshots*, http://www.nagios.org/about/screenshots.

[Oracle 2014]
Oracle, *Oracle vm server for sparc 3.1 administration guide*, https://docs.oracle.com/cd/E38405_01/html/E38406/, 2014.

Bibliography II

[Pras 2013]
A. Pras, *Introduction to snmp management information bases*, https://www.youtube.com/watch?v=LxTKnjHpYMM, 2013.

[RFC1213]
M. T. Rose and K. McCloghrie, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, RFC 1213, Mar. 1991.