The Seventh Annual
Southern California Linux Expo
Los Angeles, California

Getting Started with System Monitoring

Æleen Frisch
aefrisch@lorentzian.com
www.aeleen.com

e^{x}ponential Consulting, LLC
Wallingford, Connecticut, USA

Itinerary

- Brief Intro
- Nagios
- SNMP Interlude
- Munin

Why Monitor?

- "I'm not Big Brother!!"

Reasons to Monitor

- Status
- Security
- Performance

You Don't Always Need Special Software ...

```
# find /home -type f \( -perm 2000 -o -perm -4000 \)
```

```
# ps aux | egrep "(httpd|nfs|smb|crond)"
# ps aux | grep telnetd
```

- cron is your friend

.. But It Is Often Very Helpful

- Status:
  - Nagios
  - Xenoss
- Security:
  - Nessus
  - nmap
  - Tripwire
- Performance:
  - Munin
  - Many more …
- General:
  - RRDTool
  - Cfengine
- Data Storage:
  - MySQL
  - More …

Nagios

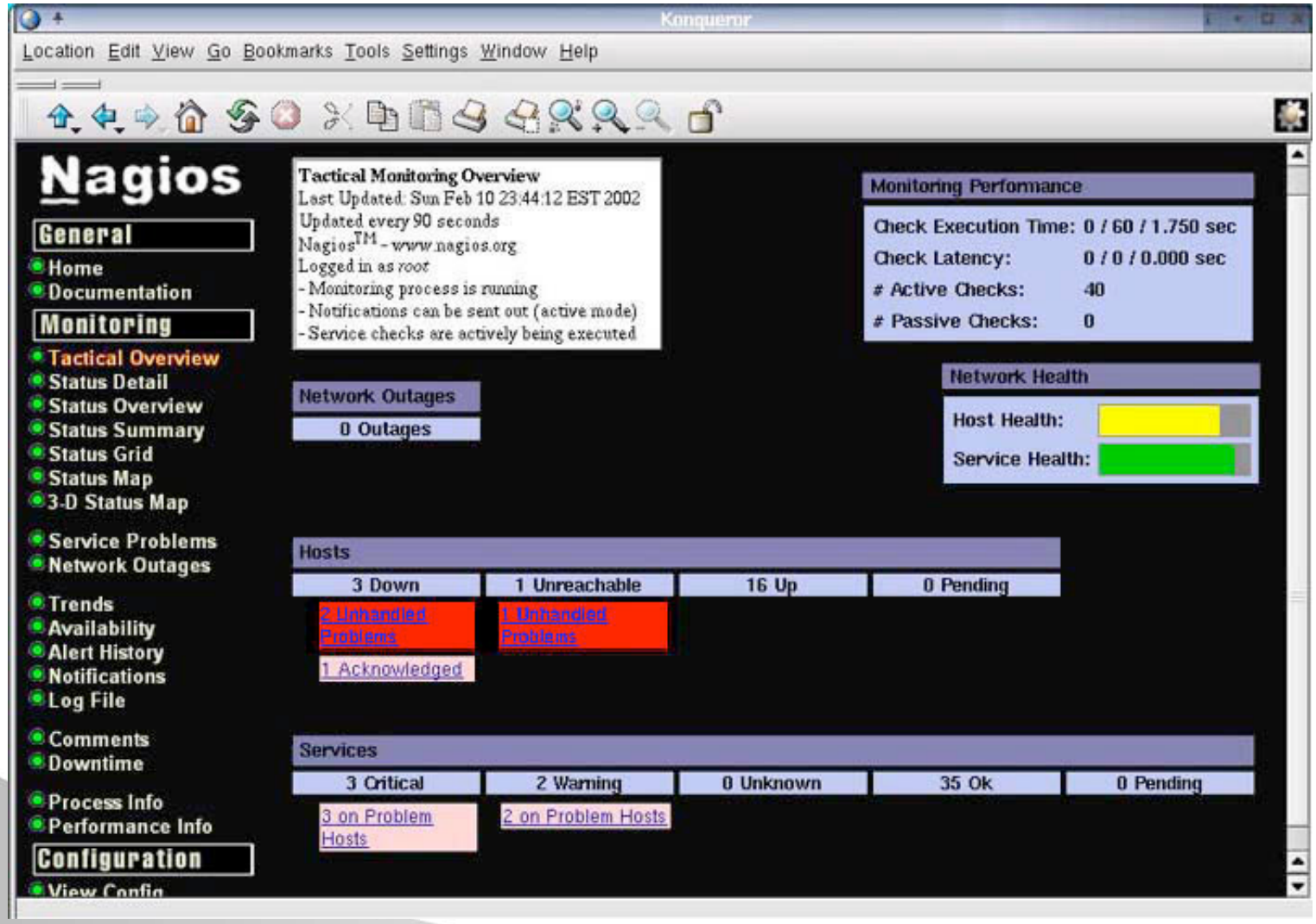
- Ethan Galstad
- www.nagios.com
- nagios.sourceforge.net/docs/3_0/toc.html

What Nagios Can Do

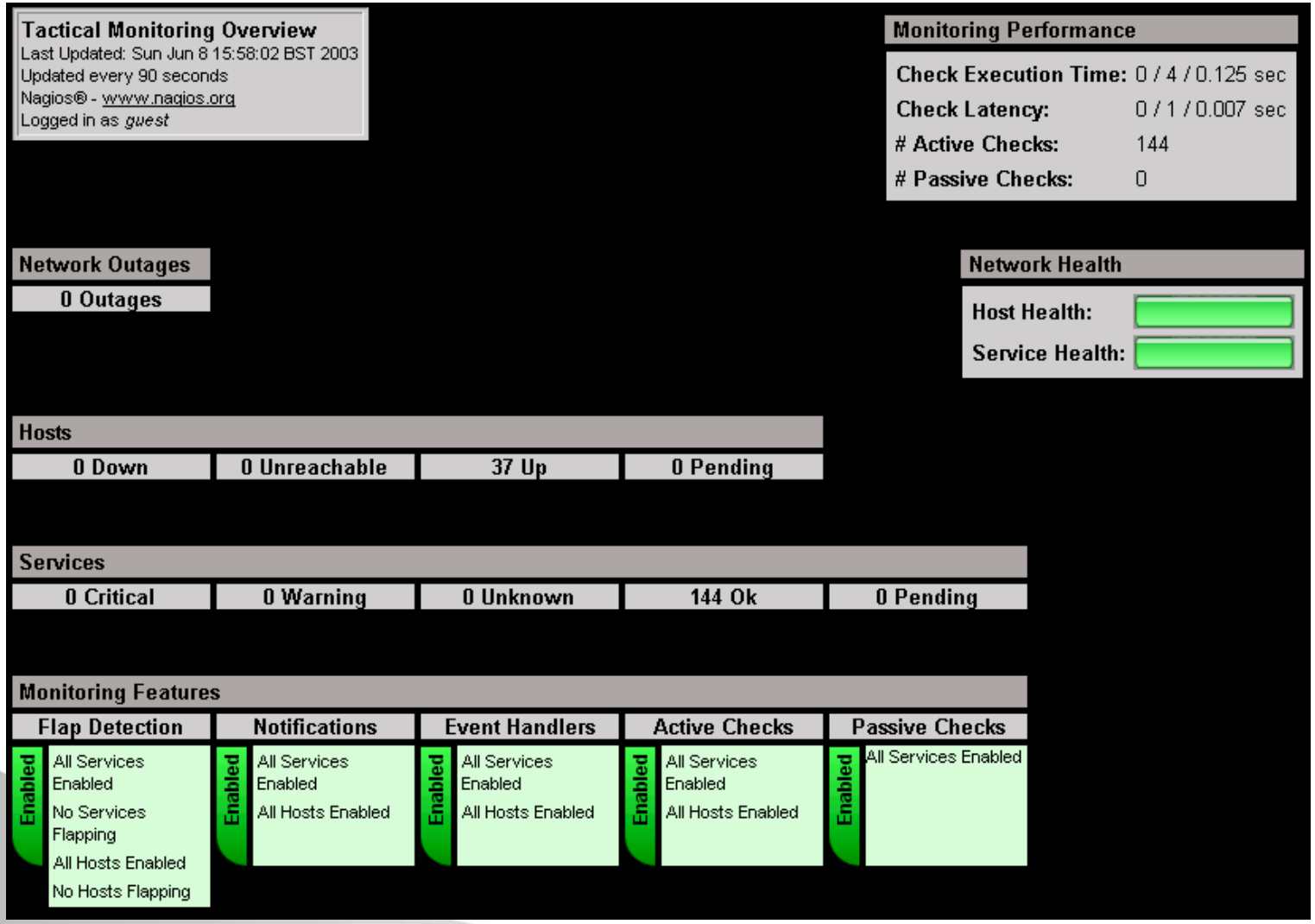
- Monitor all hosts and devices across a network
- Monitor services running on hosts
- Gather data for trend analysis

- Demo: nagios.demo.netways.de
  - guest, guest

Control Center



Another Look



Status Information at a Glance

Host Status Totals

Up	Down	Unreachable	Pending
13	5	2	0

All Problems	All Types
7	20

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
54	2	0	6	0

All Problems	All Types
8	62

Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
Annex (Annex)	3 UP 2 UNREACHABLE	9 OK 2 CRITICAL
Bldg1 (Bldg1)	6 UP	27 OK
Bldg2 (Bldg2)	2 UP 4 DOWN	16 OK 2 WARNING 3 CRITICAL
Printers (Printers)	3 UP 1 DOWN	3 OK 1 CRITICAL

Printers (Printers)

Host	Status	Services	Actions
catprt	UP	1 OK	
ingres	DOWN	1 CRITICAL	
lomein	UP	1 OK	
turtle	UP	1 OK	

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
ariadne	PROCS	WARNING	02-10-2002 22:26:14	0d 1h 6m 53s	1/4	WARNING - 292 processes running
beulah	FTP	WARNING	02-10-2002 22:25:10	0d 1h 21m 52s	1/4	Invalid FTP response received from host

Host Based View

leah
192.168.0.77

Host State Statistics

State	Time	% Time
UP	0d 2h 39m 36s	51.8%
DOWN	0d 2h 28m 46s	48.2%
UNREACHABLE	0d 0h 0m 0s	0.0%
All States	0d 5h 8m 22s	100.0%

Host State Information

Variable	Value
Host Status	YES
Status Information	/bin/ping -n -c 1 192.168.9.7
Last Status Check	02-10-2002 23:35:42
Host Checks Enabled?	YES
Last State Change	02-10-2002 21:07:39
Current State Duration	0d 2h 34m 43s
Last Host Notification	02-10-2002 23:07:39
Current Notification Number	2
Host Notifications Enabled?	YES
Event Handler Enabled?	YES
Flap Detection Enabled?	YES
Is This Host Flapping?	N/A
Percent State Change	N/A
In Scheduled Downtime?	NO
Last Update	02-10-2002 23:42:11

Host Commands

- Disable checks of this host
- Acknowledge this host problem
- Disable notifications for this host
- Delay next host notification
- Schedule downtime for this host
- Cancel scheduled downtime for this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule an immediate check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host

Host Comments

Add a new comment
Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Actions
02-10-2002 23:36:05	root	needed new disk drive	1	Yes	

Installing Nagios 3

- Claim: 15 minute install
- Took me 32 minutes this morning, but a typo was to blame for 5 and hubris for another 5!
- You have to build it from source code
- Great quick installation guides

Lots of Steps, but Very Easy

- Go to nagios.org and download 2 items
- Find Fedora install guide (fine for RHEL5)
- Prerequisites:

```
$ sudo yum install gd gd-devel
```

- Create user and groups:

```
$ sudo useradd -m nagios --password nagios
$ sudo groupadd nagcmd
$ sudo usermod -G nagcmd nagios
$ sudo usermod -G nagcmd apache
$ sudo useradd -m nagiosadmin --password xxx
```

Finally We Compile …

- Unpack and compile Nagios:

```
$ cd /whereever
$ tar xvfz nagios-3.0.6.tar.gz
$ cd nagios-3.0.6
$ ./configure --with-command-group=nagcmd
$ make all
$ sudo make install
$ sudo make install-init
$ sudo make install-config
$ sudo make install-commandmode
```

- Edit /usr/local/nagios/etc/objects/contacts.cfg:

```
email nagios@localhost ; <<***** CHANGE ******
```

Just a Few More …

- Hook up to Apache:

```
$ sudo make install-webconf
$ sudo htpasswd -c \
  /usr/local/nagios/etc/htpasswd.users nagiosadmin
$ sudo service httpd restart
```

- Unpack and build the plugins
- Configure the Nagios service:

```
$ sudo chkconfig --add nagios
$ sudo chkconfig nagios on
$ sudo service nagios start
```

- SELinux considerations if not disabled

Liftoff!

- Point your browser at http://localhost/nagios

Under the Hood

- /usr/local/nagios directory is Nagios' default home
  - Executables in ./bin
  - CGI files in ./sbin
  - Configuration files in ./etc/objects
  - Command scripts in ./libexec
  - Log and lock files in ./var

Important Configuration Files

- etc/nagios.cfg: Global settings
- etc/objects/*: *Object configuration files* specify which hosts and services are monitored.

Selections from nagios.cfg

```
# File locations
log_file=/usr/local/nagios/var/nagios.log
resource_file=/usr/local/nagios/etc/resource.cfg
lock_file=/usr/local/nagios/var/nagios.lock

cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/hosts.cfg


# Global settings
nagios_user=nagios
nagios_group=nagios
date_format=us
admin_email=nagadmin@ahania.com
```

Configuring Features

```
retain_state_information=1
retention_update_interval=60
use_retained_program_state=1
```

Retained status information

```
enable_event_handlers=1
global_host_event_handler=global-event-cmd
global_service_event_handler=global-svc-cmd
```

Global event handlers

```
max_concurrent_checks=0
service_check_timeout=60
host_check_timeout=30
event_handler_timeout=30
notification_timeout=30
```

Concurrent checks & time-outs

Fundamental Objects

- Hosts: Computers and other network devices.
- Host Groups : Named groups of hosts.
- Services: Important daemons providing specific services.
- Contacts: User to be contacted in the event of a problem.
- Contact Groups: Named groups of contacts.
- Time Periods: Day and/or time ranges within a week, used to specify when checks are to be performed, notifications are to be sent, and the like.
- Commands: Commands to be run for all purposes (host/service checking, notifications, event handling, and so on).

The Pieces

- host
  - hostgroup
  - hostdependency
  - hostescalation
- service, servicegroup, servicedependency, serviceescalation,
- contact, contactgroup
- timeperiod
- command

Defining Hosts to Monitor

Host template

```
define host {
    name normal                         ; Template name
    register 0                          ; This is only a template (not a monitored host)
    notifications_enabled 1             ; Host notifications are enabled
    check_command check-host-alive      ; Command to check if host is available
    max_check_attempts 4                ; Recheck failures this many times
    notification_interval 120           ; Repeat failure notifications every 2 hours
    notification_period 24x7            ; When to check (time period name)
    notification_options d,u,r          ; Notify when down, unreachable and on recovery
    }
```

An Actual Host

```
define host {
    use normal                      ; Template on which to base host
    host_name beulah                ; Note the attribute is not "name" as above
    alias beulah: RHEL5             ; Longer description
    address 192.168.1.44            ; IP address
    max_check_attempts 8            ; Overrides template value
    }
```

Host Groups

```
define hostgroup{
   hostgroup_name bldg2
   alias Building 2
   contact_groups admins1
   members beulah,callisto,ariadne,leah,lovelace,valley
   }
```

Services

```
define service{                          ; Define defaults for all services
    name generic
    register 0
    normal_check_interval 30             ; Check service every 30 minutes
    retry_check_interval 3               ; Retry failing checks every 3 minutes …
    max_check_attempts 5                 ; … up to 5 times
    check_period 24x7
    notification_interval 120            ; Repeat notifications for failures every 2 hours
    notification_period 6to22
    notification_options c,r             ; Notify contacts about critical failures/recoveries
    notifications_enabled 1
    contact_groups admins
    }
```

Specific & Actual Service

```
define service{                          ; Template for SMTP Mail service
   use generic
   name generic-smtp
   register 0
   service_description Check SMTP
   check_command check_smtp
   contact_groups mailadmins
   }

define service{                          ; Define service to be monitored
          use generic-SMTP
          host_groups mailhosts          ; Hosts to monitor SMTP
          }
```

Time Periods

```
define timeperiod{
    name weekends
    timeperiod_name weekends
    saturday 00:00-24:00
    sunday 00:00-24:00
}

define timeperiod{
    timeperiod_name we_hate_ae
    use weekends,holidays
    exclude weekdays
}
```

Commands

```
define command{
    command_name check_smtp
    command_line $USER1$/check_smtp -H $HOSTADDRESS$
    }

define command{
    command_name eh_smtp
    command_line /usr/local/nagios/eh/fix_mail $HOSTADDRESS$ $STATETYPE$
    }
```

Contacts

```
define contact{
    contact_name aeleen
    alias Aeleen Frisch
    host_notifications_enabled 1
    service_notifications_enabled 1
    service_notification_options w,u,c,r
    host_notification_options d,u,r
    host_notification_period we_hate_ae
    service_notification_period we_hate_ae
    service_notification_commands notify-by-email-page
    host_notification_commands notify-by-email-page

    email aefrisch@lorentzian.com
    pager 555-5555@pagergateway.ahania.com
    address1 aefrisch@lorentzian.com
    address2 555-555-5555

    can_submit_commands 1
}
```

Dependencies

```
define hostdependency{
   host_name taurus                        ; can also use a hostgroup
   dependent_host_name marco               ; taurus is unreachable when marco is
   notification_failure_criteria d         ; don't check taurus when marco is down


define servicedependency{
   host_name taurus
   service_description report_svc
   dependent_host_name marco
   dependent_service_description db_svc
   execution_failure_criteria w,u          ; when not to run checks on report_svc
   notification_failure_criteria c         ; when to suppress notifications about report_svc
```

Notification Escalations

```
define serviceescalation{
    host_name ariadne
    service_description payroll_svc
    first_notification 3
    last_notification 5
    notification_interval 90
    escalation_period non-holidays
    contact_groups senior-adms,managers
}
```

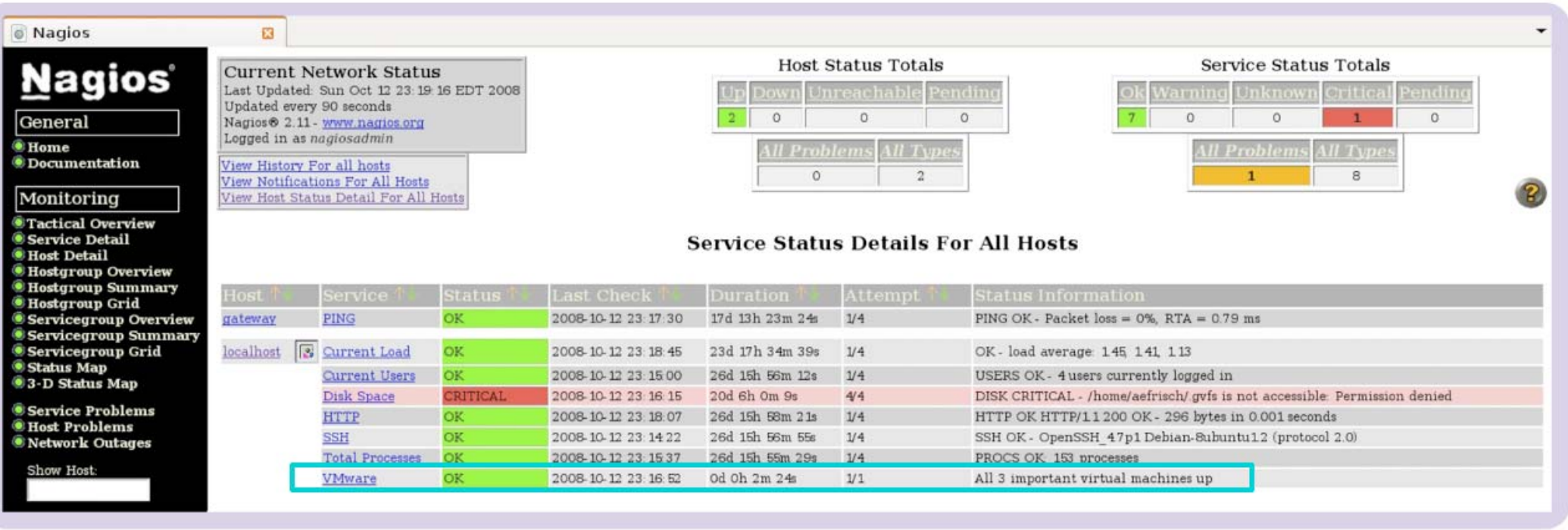
Access Control: cgi.cfg

```
use_authentication=1
authorized_for_configuration_information=nagiosadmin,root,chavez
authorized_for_all_services=nagiosadmin,root,chavez,begnum
```

More Features

- Passive service checks
- External commands
- Log rotation
- Data can be written to external files or DB
- Infinitely customizable

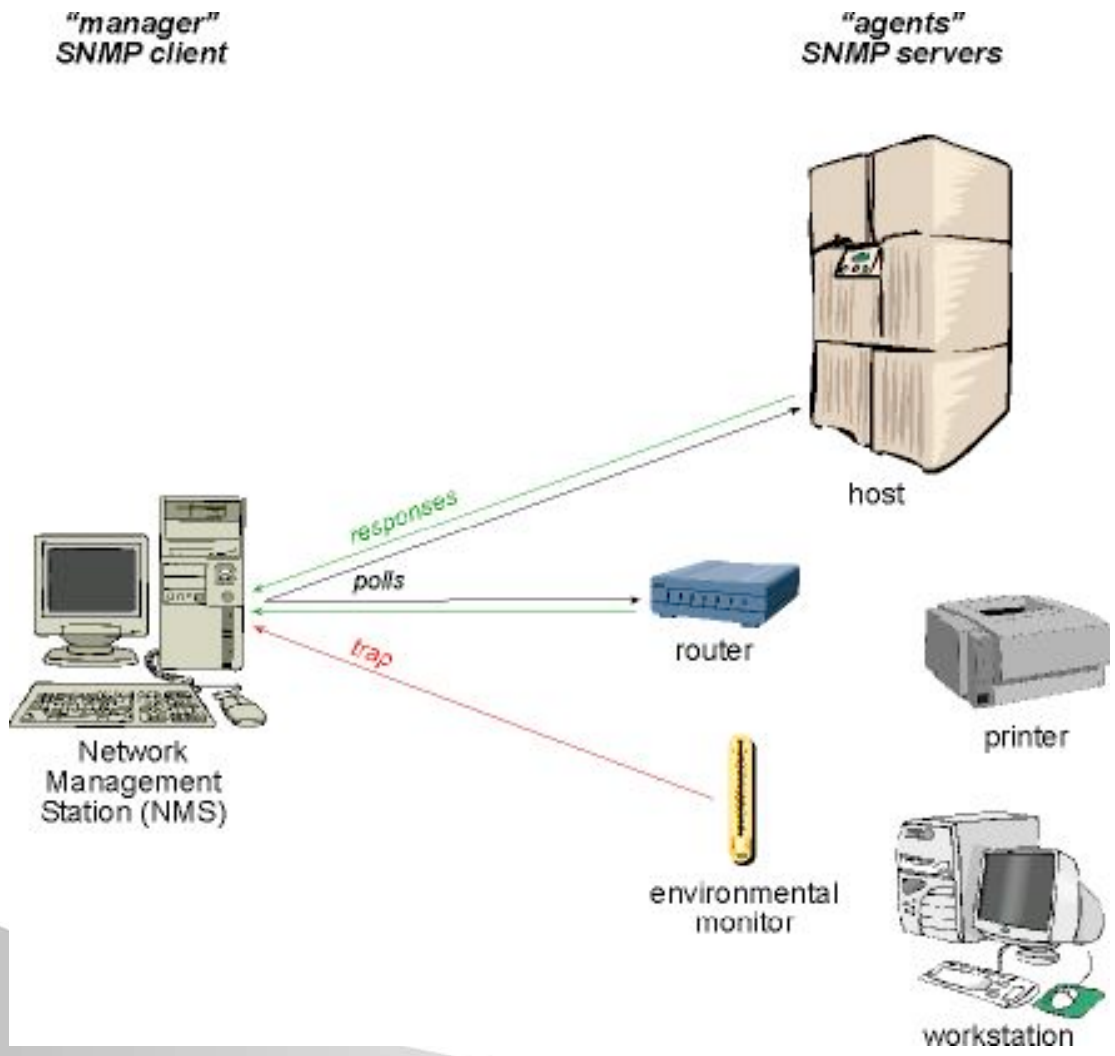
My Plug-in: Check for VMs



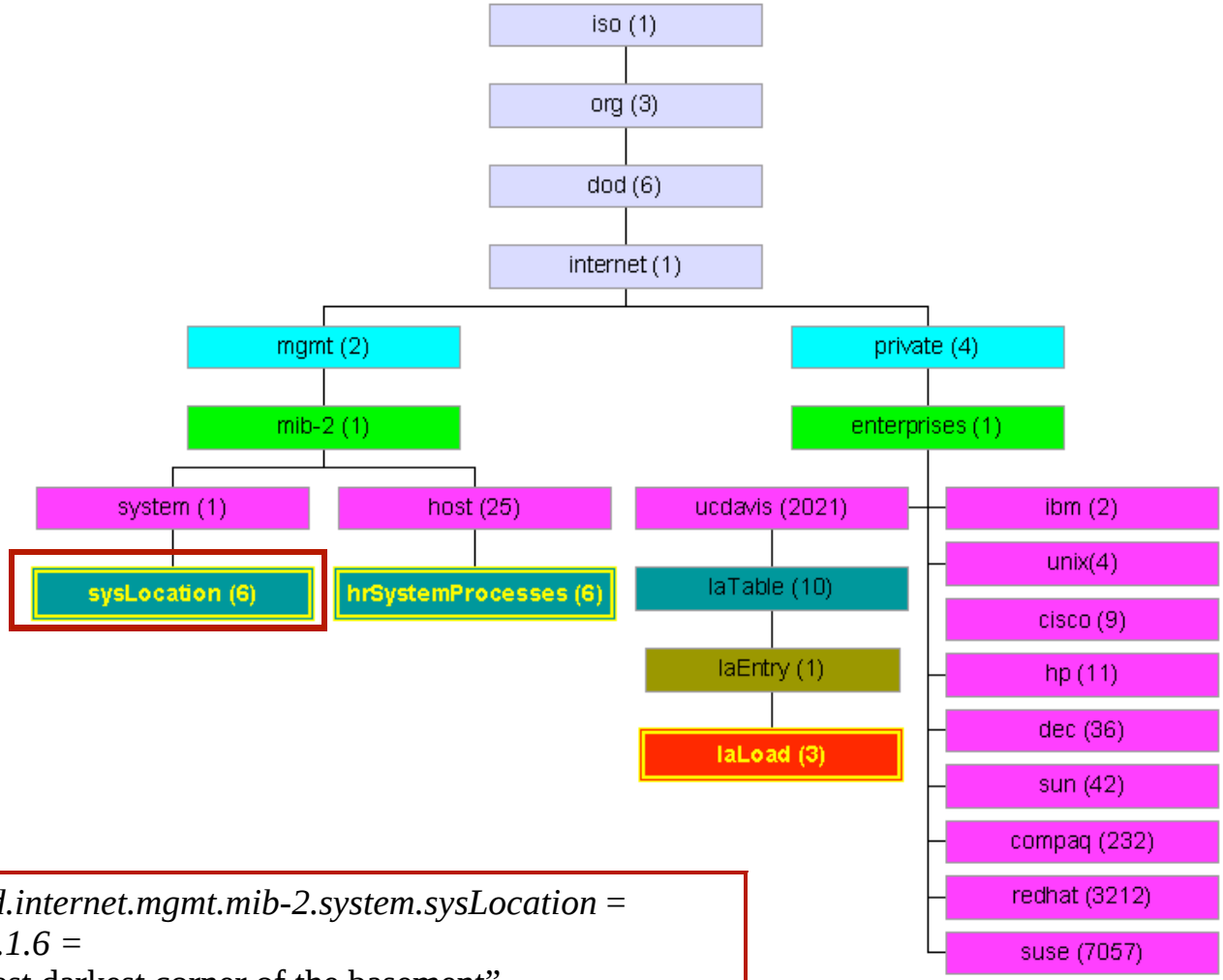
2 Minutes of SNMP

- Simple Network Management Protocol
  - Protocol for device communication and management
  - Structured data hierarchy: "management information base"
- Terms
  - MIB
  - Polls and responses
  - Traps

SNMP Concepts



MIBs



iso.org.dod.internet.mgmt.mib-2.system.sysLocation = 1.3.6.1.2.1.1.6 =
"The deepest darkest corner of the basement"

SNMP Components

- Daemon
- Community string => password
- Net-SNMP Utilities
  - **snmptranslate**: describe MIB entries
  - **snmpget**: poll device for data value
  - **snmpwalk**: retrieve data for a MIB subtree

SNMP Security

- Disable where you're not using it!
- Use version 3
- Block or restrict access to ports
- Choose good community strings

Munin

- Performance-oriented monitoring
  - Lots of functionality out of the box
- munin.projects.linpro.no
- See munin.ping.uio.no for a demo

Munin Advantages

- Very fast to get going
- Lightweight agent
- Elementary auto-service discovery
- Very customizable via plug-ins

Munin Displays

Overview

- vlab :: [day week month year]
  - Overview :: [Other]
  - gjovik.vlab :: [Other]
  - huldra.vlab :: [Disk Exim Network Other Processes System]
  - min1.vlab :: [Other]
  - min2.vlab :: [Other]
  - min3.vlab :: [Other]
  - min4.vlab :: [Other]
  - min5.vlab :: [Disk Exim Network Other Processes System]
  - min6.vlab :: [Other]
  - min7.vlab :: [Other]
  - sanity.vlab :: [Disk Network Other Processes System]
  - shadowfax.vlab :: [Disk Mysql Network Other Postfix Processes Sensors System]

This page was generated by Munin version 1.2.5 at 2008-11-12 T 07:58:19

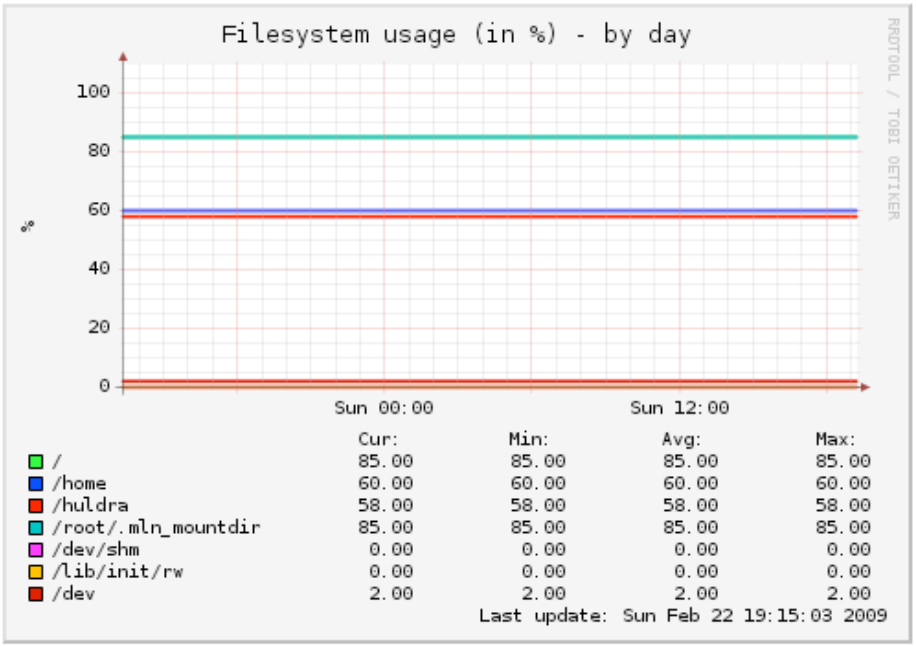
Host View

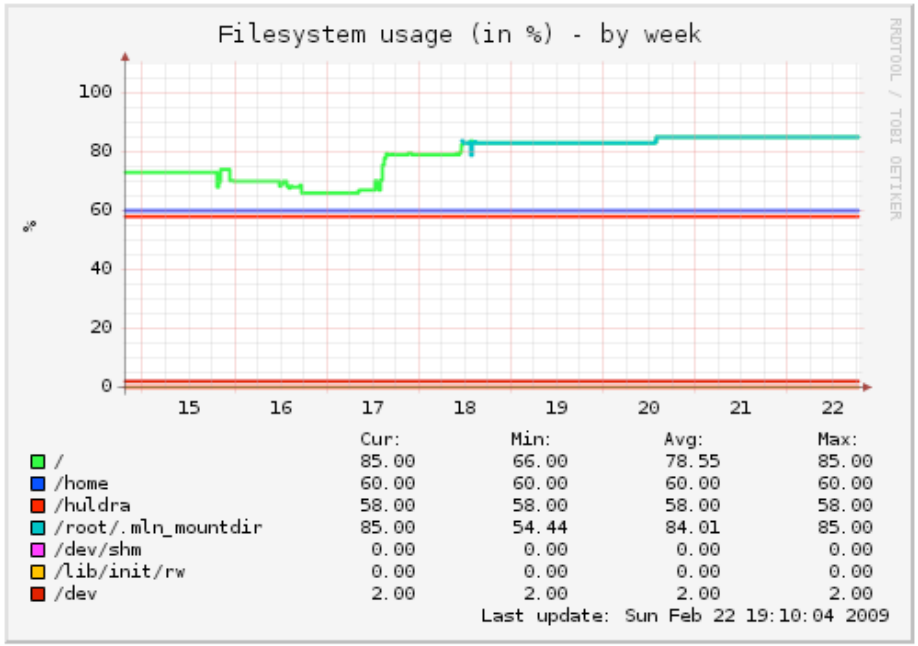
Overview :: vlab :: huldra.vlab

huldra.vlab :: [Disk Exim Network Other Processes System]

Disk

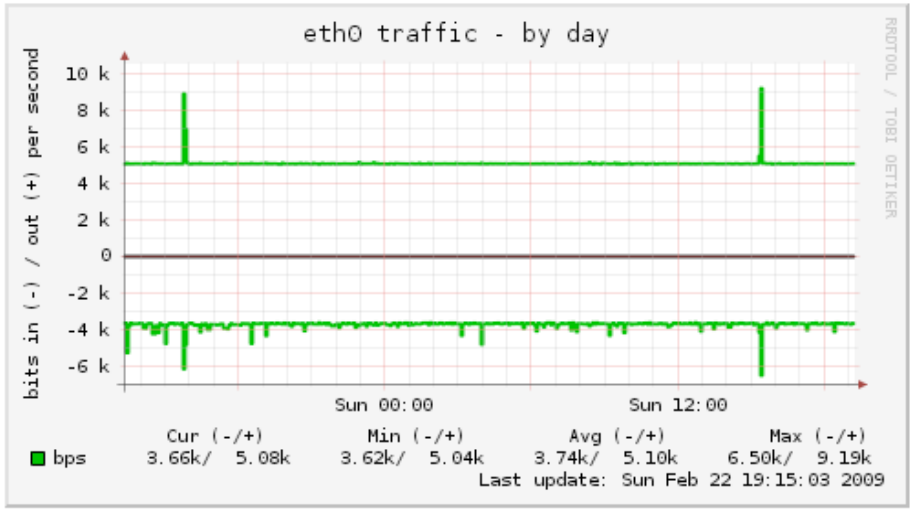
:: Filesystem usage (in %)

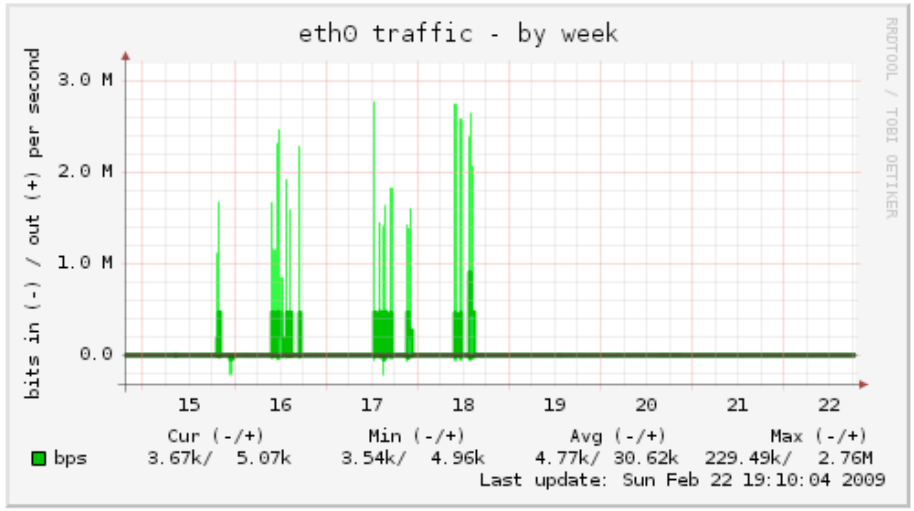




Continues …

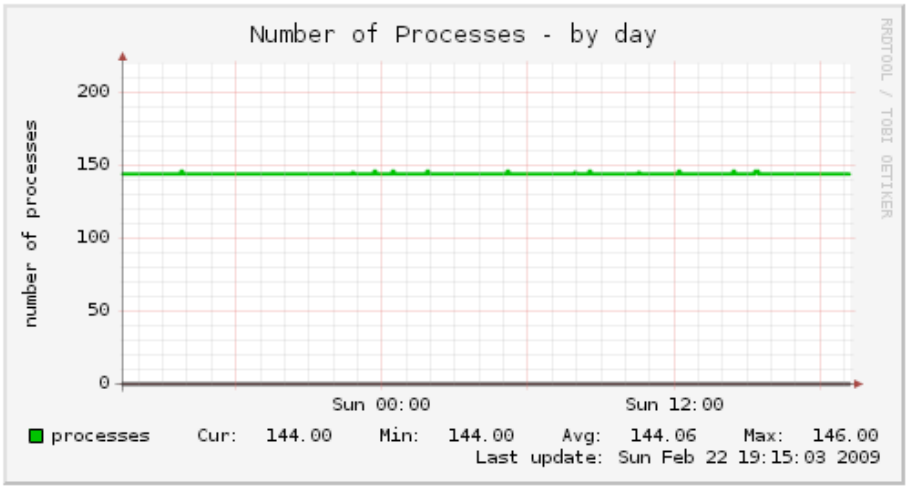
:: eth0 traffic

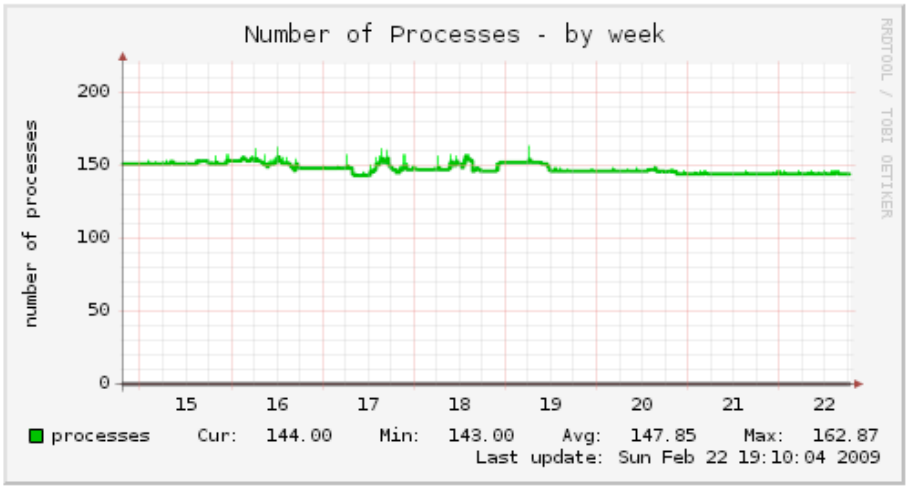




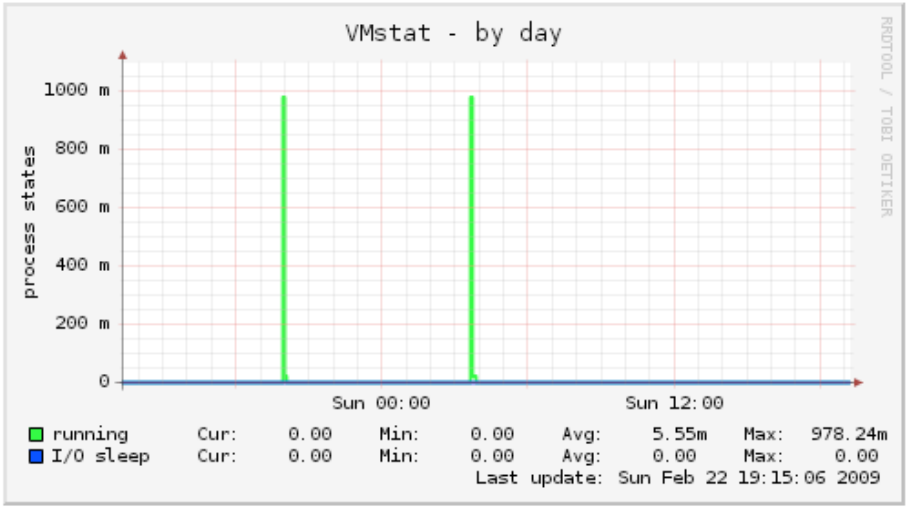
More ...

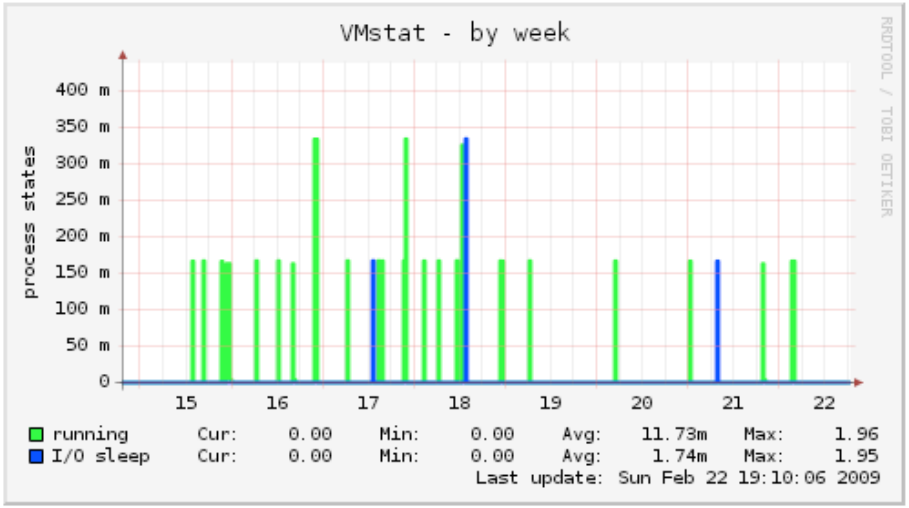
:: Number of Processes



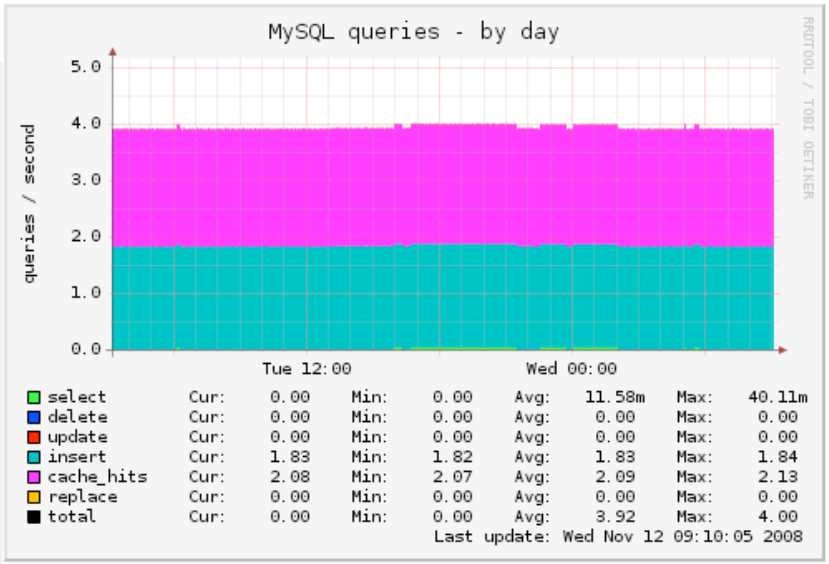


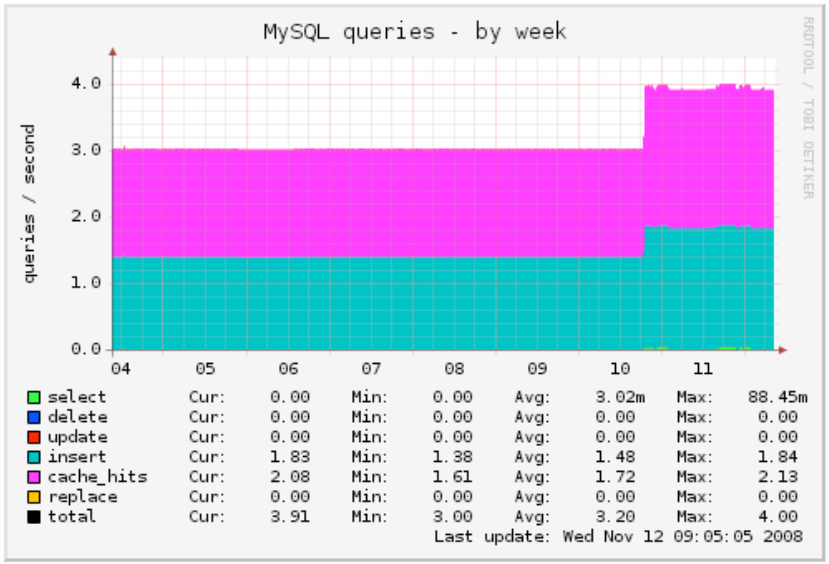
:: VMstat

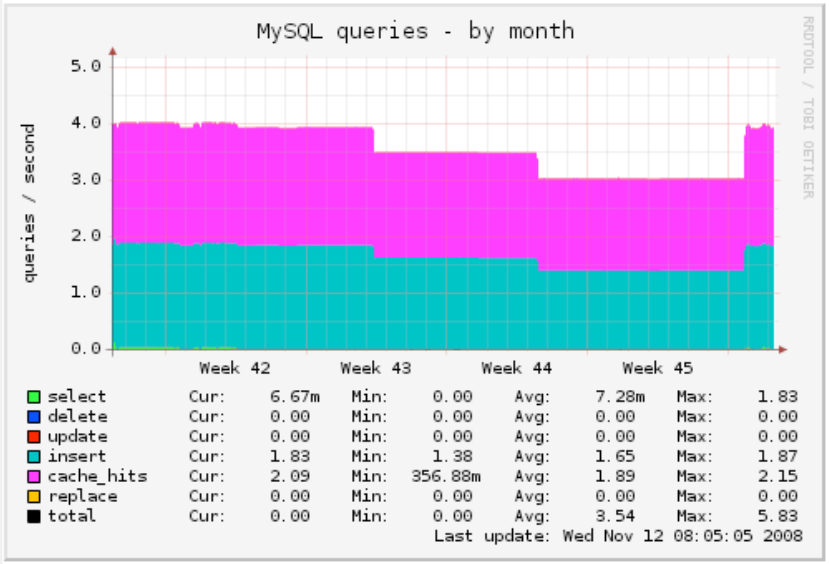


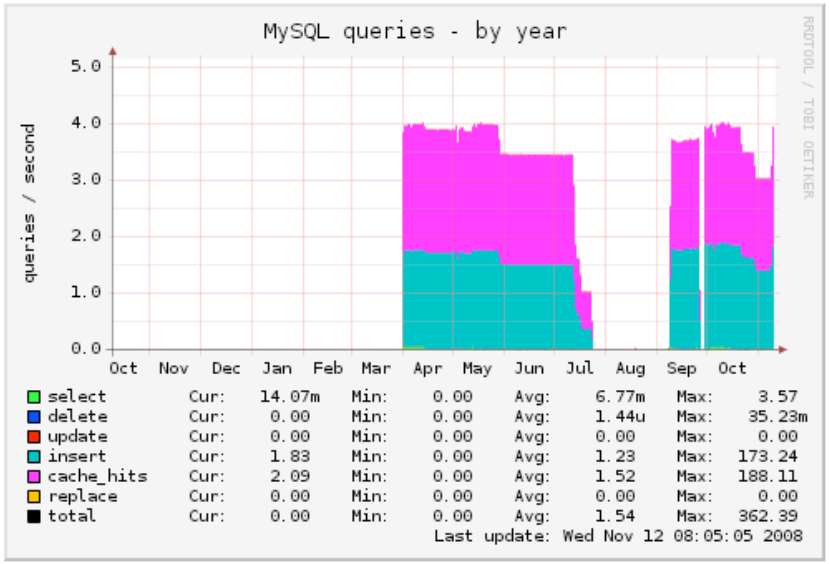


Detail View


MySQL queries - by day
queries / second
5.0
4.0
3.0
2.0
1.0
0.0
Tue 12:00
Wed 00:00
RRDTOOL / TOBI OETIKER
select Cur: 0.00 Min: 0.00 Avg: 11.58m Max: 40.11m
delete Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
update Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
insert Cur: 1.83 Min: 1.82 Avg: 1.83 Max: 1.84
cache_hits Cur: 2.08 Min: 2.07 Avg: 2.09 Max: 2.13
replace Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
total Cur: 0.00 Min: 0.00 Avg: 3.92 Max: 4.00
Last update: Wed Nov 12 09:10:05 2008


MySQL queries - by week
queries / second
4.0
3.0
2.0
1.0
0.0
04
05
06
07
08
09
10
11
RRDTOOL / TOBI OETIKER
select Cur: 0.00 Min: 0.00 Avg: 3.02m Max: 88.45m
delete Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
update Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
insert Cur: 1.83 Min: 1.38 Avg: 1.48 Max: 1.84
cache_hits Cur: 2.08 Min: 1.61 Avg: 1.72 Max: 2.13
replace Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
total Cur: 3.91 Min: 3.00 Avg: 3.20 Max: 4.00
Last update: Wed Nov 12 09:05:05 2008


MySQL queries - by month
queries / second
5.0
4.0
3.0
2.0
1.0
0.0
Week 42
Week 43
Week 44
Week 45
RRDTOOL / TOBI OETIKER
select Cur: 6.67m Min: 0.00 Avg: 7.28m Max: 1.83
delete Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
update Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
insert Cur: 1.83 Min: 1.38 Avg: 1.65 Max: 1.87
cache_hits Cur: 2.09 Min: 356.88m Avg: 1.89 Max: 2.15
replace Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
total Cur: 0.00 Min: 0.00 Avg: 3.54 Max: 5.83
Last update: Wed Nov 12 08:05:05 2008


MySQL queries - by year
queries / second
5.0
4.0
3.0
2.0
1.0
0.0
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
RRDTOOL / TOBI OETIKER
select Cur: 14.07m Min: 0.00 Avg: 6.77m Max: 3.57
delete Cur: 0.00 Min: 0.00 Avg: 1.44u Max: 35.23m
update Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
insert Cur: 1.83 Min: 0.00 Avg: 1.23 Max: 173.24
cache_hits Cur: 2.09 Min: 0.00 Avg: 1.52 Max: 188.11
replace Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
total Cur: 0.00 Min: 0.00 Avg: 1.54 Max: 362.39
Last update: Wed Nov 12 08:05:05 2008

Installing Munin

- Needs RRDTool + Perl + web server
- Install munin on the master
- Install munin-node on master and clients

Simple to Configure

- /etc/munin/munin.conf

```
[troll.vlab]
   address troll
   cpu.user.warning 200
   cpu.user.critical 250
   sensors_temp.temp1.warning 55
```

- /etc/munin/munin-node

```
allow ^192\.168\.0\.22$
```

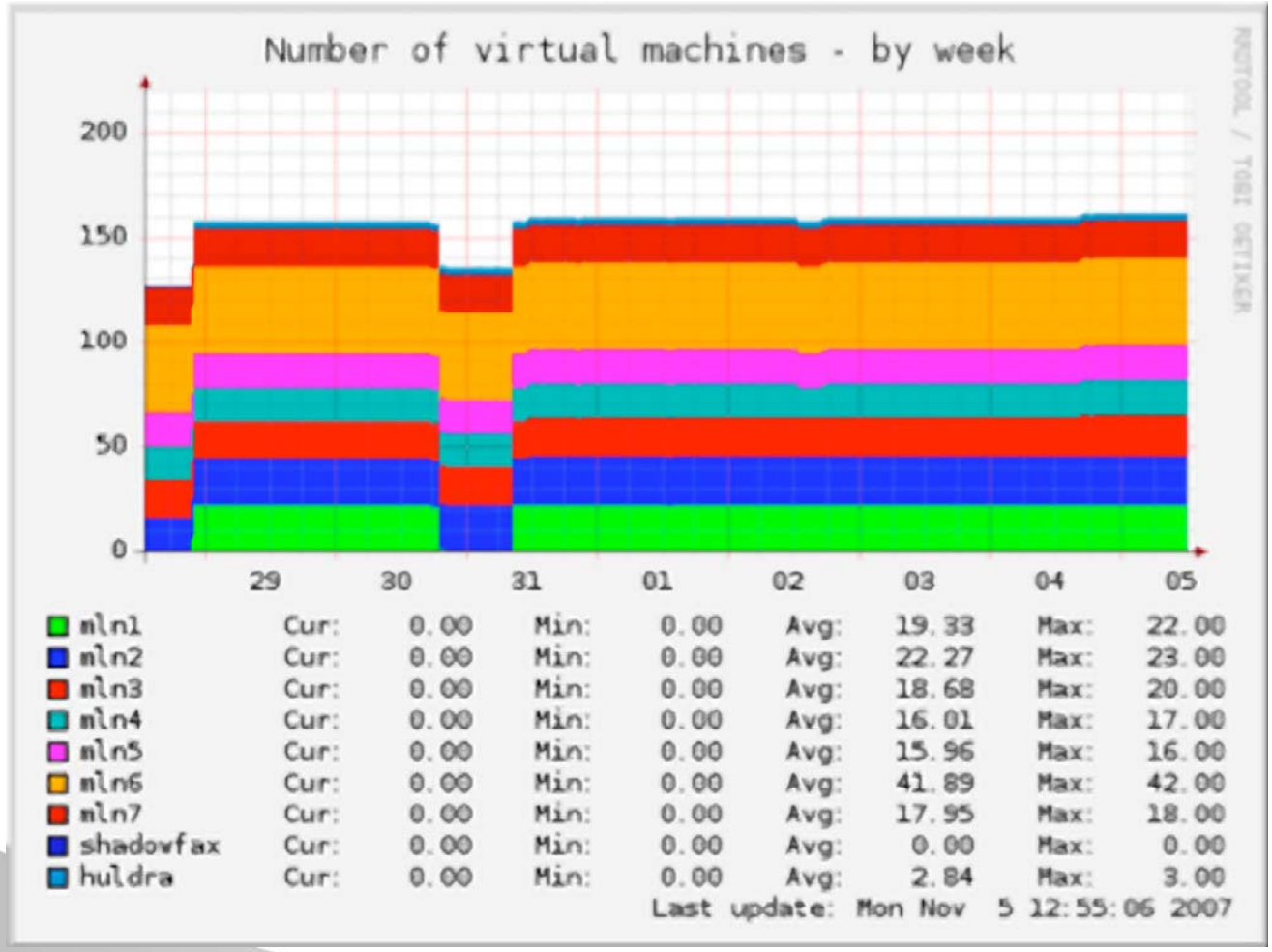
- Page definitions are in /etc/munin/templates

Munin Plug-ins

- Installed in /usr/share/munin/plugins
- Active ones are linked to /etc/munin/plugins
  - Add your own here
- Configured in /etc/munin/plugin-conf.d/munin.node:

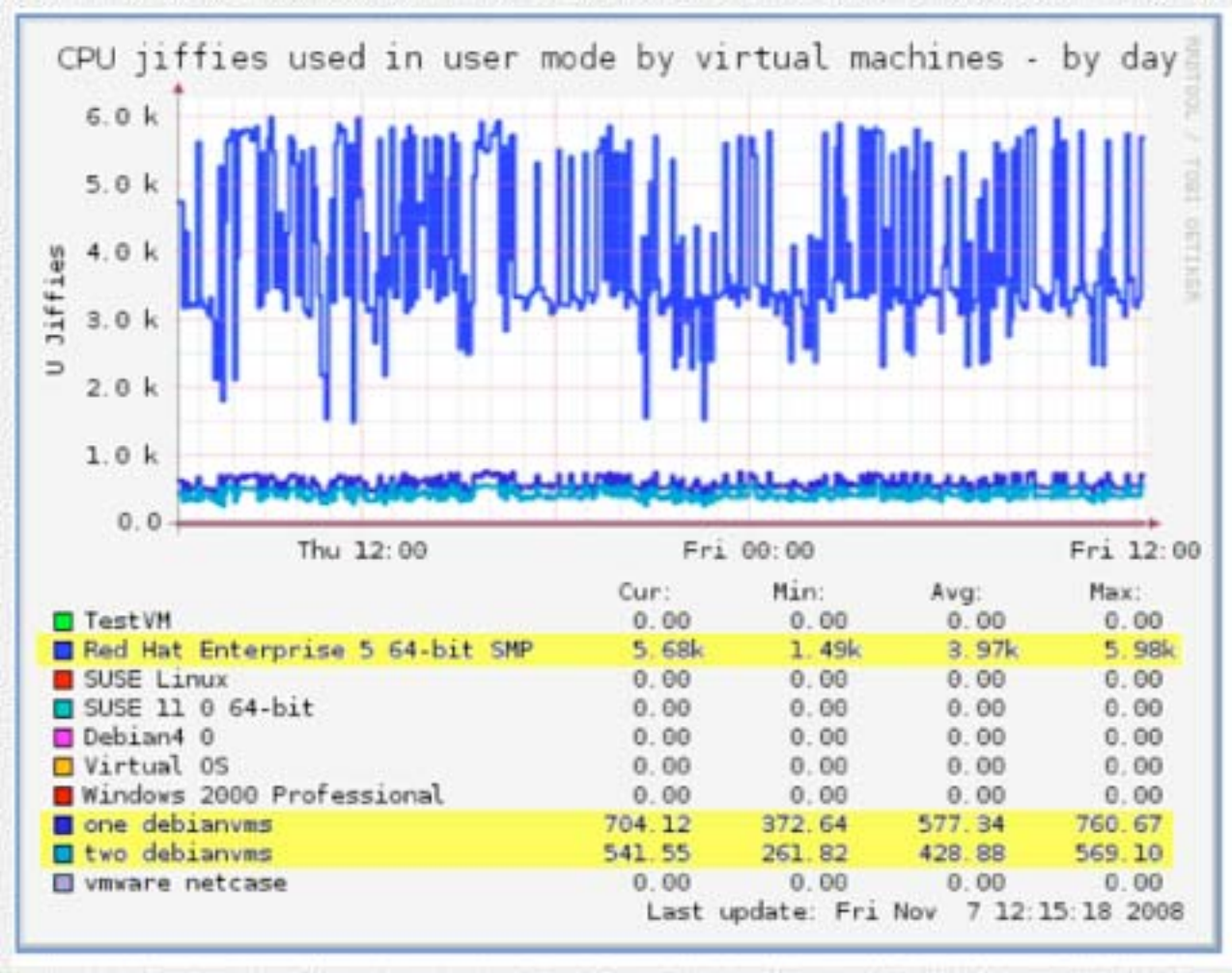
```
[vmware*]
user root
```

Plug-ins are Easy



Plug-in Code

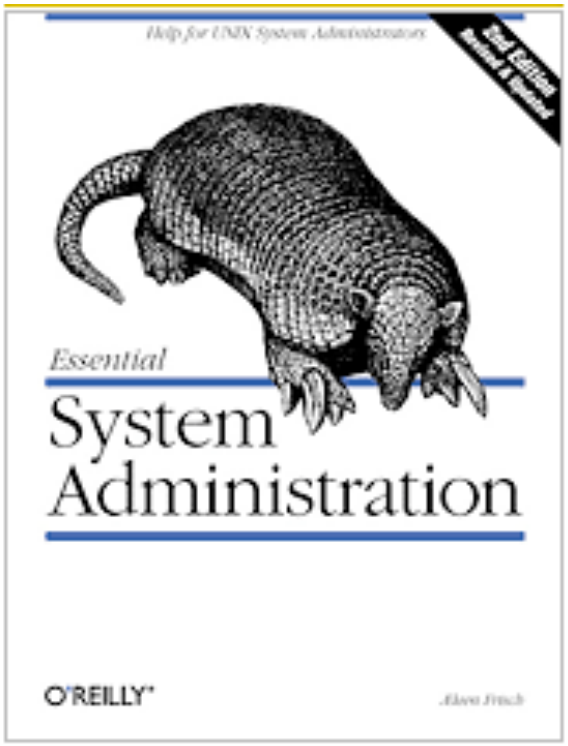
```
#!/usr/bin/perl

if ($ARGV[0] eq "config"){
   print "graph_title Xen virtual machines\n";
   print "graph_vlabel domains\n";
   print "graph_info The number of virtual machines running Xen\n";
   print "domains.label domains\n";

} else {

    $return = `/usr/sbin/xm list | wc -l 2>&1`;

    print "got result: $return\n";
    chomp $return;
    print "domains.value " . ($return - 2) . "\n";
}
```


CPU jiffies used in user mode by virtual machines - by day
U Jiffies
6.0 k
5.0 k
4.0 k
3.0 k
2.0 k
1.0 k
0.0
Thu 12:00
Fri 00:00
Fri 12:00
Cur: Min: Avg: Max:
TestVM 0.00 0.00 0.00 0.00
Red Hat Enterprise 5 64-bit SMP 5.68k 1.49k 3.97k 5.98k
SUSE Linux 0.00 0.00 0.00 0.00
SUSE 11 0 64-bit 0.00 0.00 0.00 0.00
Debian4 0 0.00 0.00 0.00 0.00
Virtual OS 0.00 0.00 0.00 0.00
Windows 2000 Professional 0.00 0.00 0.00 0.00
one debianvms 704.12 372.64 577.34 760.67
two debianvms 541.55 261.82 428.88 569.10
vmware netcase 0.00 0.00 0.00 0.00
Last update: Fri Nov 7 12:15:18 2008

Want to Learn More?

- Both packages have lots of online info
- Many books on Nagios

Shameless Plugs



USENIX | Conferences | Join/Renew | Who We Are | Contact Us | ;login: | Site Map

The Advanced Computing Systems Association

23rd Large Installation System Administration Conference (LISA '09)

November 1–6, 2009, Baltimore, MD

LOPSA

the league of professional system administrators

Thanks for Listening!