Administration de Systèmes d'Information

Luiz Angelo Steffenel

Université de Reims Champagne-Ardenne

Cours 3

- Surveillance d'un Réseau
  - Logrotate et Syslog
  - MRTG & RRDTools
  - GANGLIA
  - NAGIOS

Syslog et les fichiers de Log

Quelles informations enregistrer dans un log ?

- Les informations relatives aux connexions des utilisateurs
- Les informations issues du noyau
- Les application
  - Presque toutes produisent des données qui peuvent être enregistrées
  - La plupart des données a une durée de vie limitée, et on doit analyser, compresser, supprimer ces informations selon leur importance

Les politiques de log

- Plusieurs choix
  - Effacer les données immédiatement
  - Supprimer les logs à des périodes régulières
  - Faire la rotation des logs, tout en gardant les données pour un temps fixé
  - Compresser et archiver les logs sur d'autres supports de sauvegarde
- Laquelle utiliser ?
  - Combien d'espace en disque nous avons ?
  - Quel est le niveau de "paranoïa" de l'administrateur ?
- Dans tous les cas, il est fortement recommandé d'automatiser la manipulation des logs avec des commandes telles que cron

Où trouver les fichiers de log

- Cherchant directement dans les scripts de démarrage : /etc/rc* or /etc/init.d/*
  - Si le log est activé, bien sûr
- Certains programmes et signaux sont gérés directement par **Syslog**
  - Vérifier la liste dans /etc/syslog.conf
- Différents systèmes d'exploitation stockent les logs dans des répertoires divers
  - /var/log/*
  - /var/cron/log
  - /usr/adm
  - /var/adm …
- Sous Linux, les fichiers log se trouvent dans le répertoire /var/log

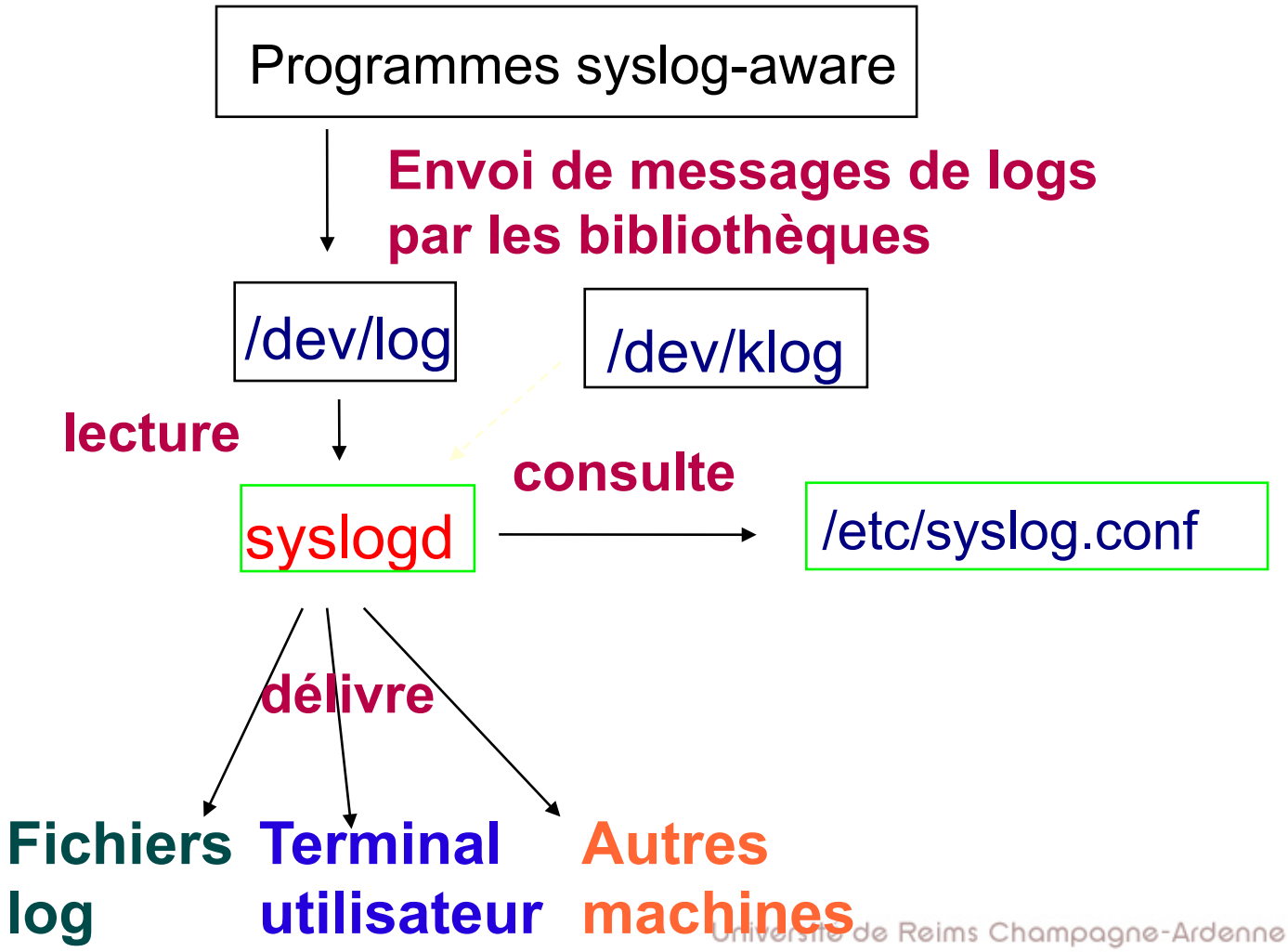
Syslog

- Syslog
  - Un sous-système Unix spécialement dédié à la gestion des informations créer par le noyau et par les utilitaires du système
  - Implémente toutes les fonctionnalités d'archivage et de rotation

- Permet le tri des messages par leurs sources et importance, de même que le routage des logs à différentes destinations
  - Fichiers de log, terminal de l'utilisateur, serveurs distants

Syslog : les trois composants

- Syslogd et /etc/syslog.conf
  - le daemon du service de gestion des logs
  - Son fichier de configuration
- openlog, syslog, closelog
  - Des bibliothèques de programmation qui permettent l'envoi de messages à syslogd
- logger
  - Commande utilisateur qui permet aussi la soumission de messages log


Programmes syslog-aware
Envoi de messages de logs par les bibliothèques
/dev/log
/dev/klog
lecture
consulte
syslogd
/etc/syslog.conf
délivre
Fichiers log
Terminal utilisateur
Autres machines

Configuration de syslogd

- Le fichier /etc/syslog.conf contrôle le comportement de syslogd
- C'est un fichier texte simple, où les lignes en blanc et les ligne commençant par # sont ignorées
- ATTENTION : le séparateur est un <TAB>
  - ***Selector*** <TAB> ***action***
- mail.* /var/log/mail.log
- ftp.* /var/log/ftp.log

La configuration – le sélecteur

- Le premier champs est le sélecteur
- Il est composé de
  - Source - le programme (‘facility’) qui est à l’origine du message de log
  - importance – le niveau d’importance du message
  - Ex. : mail.info /var/log/maillog
- La syntaxe
  - facility.niveau
  - Les noms de "facility" et les niveaux doivent être choisis à partir d’une liste de valeurs définies
  - Plusieurs sélecteurs peuvent être alignées, séparés par des virgules

Noms des "facilities"

Facility	Programme qui l'utilise
kern	Le noyau
user	Processus utilisateur, c'est le défaut
mail	Le système de mail
daemon	Les daemons du système
auth	Commandes liées à la sécurité et l'autorisation
lpr	Le système d'impression
news	Le système Usenet

Noms des "facilities"

Facility	Programme qui l'utilise
uucp	Les échanges de message UUCP
cron	Le daemon cron
mark	Des "tics" d'horloge crées régulièrement
local0-7	Huit "parfums" de messages locaux
syslog	Les messages internes à Syslog
authpriv	Messages privés
ftp	Le daemon ftp
*	Toutes facilities à l'exception de "mark"

Niveaux de priorité

Niveau	Ce qui veut dire
emerg (panic)	Situation de panique
alert	Situations urgents
crit	Condition critique
err	Autres conditions d'erreur
warning	Messages d'alerte
notice	Situations qui méritent une investigation postérieure
info	Messages d'information
debug	Messages pour le débogage
none	Tout message sera ignoré

Les actions

Action	Ce qu'elle fait
filename	Écrit le message sur le fichier indiqué
@hostname @ipaddress	Transfère le message au daemon syslogd de la machine indiquée
user1, user2,…	Affiche le message dans les terminaux des utilisateurs, lorqu'ils sont connectés
*	Affiche le message à tout utilisateur connecté

```
# network client, typically forwards serious messages to
# a central logging machine
# emergencies: tell everyone who is logged on
*.emerg;user.none                       *

#important messages, forward to central logger
*.warning;lpr,local1.none               @netloghost
daemon,auth.info                        @netloghost

# local stuff to central logger too
local0,local2,local7.debug              @netloghost

# card syslogs to local1 - to boulder
local1.debug                            @boulder.colorado.edu

# printer errors, keep them local
lpr.debug                               /var/log/lpd-errs

# sudo logs to local2 - keep a copy here
local2.info                             /var/log/sudolog
```

Comment activer le log à distance ?

- Machines plus anciennes
  - syslogd <= version 3
  - Il suffit de configurer le daemon syslogd du serveur
    - Éditer `/etc/default/syslogd`
      - Activer l'entrée `SYSLOGD = "-r"`
      - Redémarrer le service `syslog`
    - Si nécessaire, le pare-feu doit laisser passer les données par le port UDP 514

Comment activer le log à distance ?

- Machines plus récentes
  - Rsyslogd
    - Permet l'utilisation de UDP et TCP
    - Fichier de configuration `/etc/rsyslog.conf`
    - Activer les options

```
$modload imtcp
$InputTCPServerRun 10514
```

    - ou

```
$modload imudp
$UDPServerRun 514
```

Rotation des logs

- Le principe : garder des copies des logs, réparties selon leur ancienneté
  - Exemple : les logs des 7 derniers jours, avec un fichier par jour
  - logfile, logfile.1 , logfile.2, … logfile.6
- Chaque jour, il faut renommer les fichiers afin de les "pousser" vers la fin de la chaîne

```
#! /bin/sh
cd /var/log
mv logfile.2 logfile.3
mv logfile.1 logfile.2
mv logfile logfile.1
cat /dev/null > logfile
```

Logrotate

- Logrotate est un service qui permet de rendre plus simple la rotation des logs
- Normalement, executé comme tâche régulière par cron
- Exemple de fichier /etc/logrotate

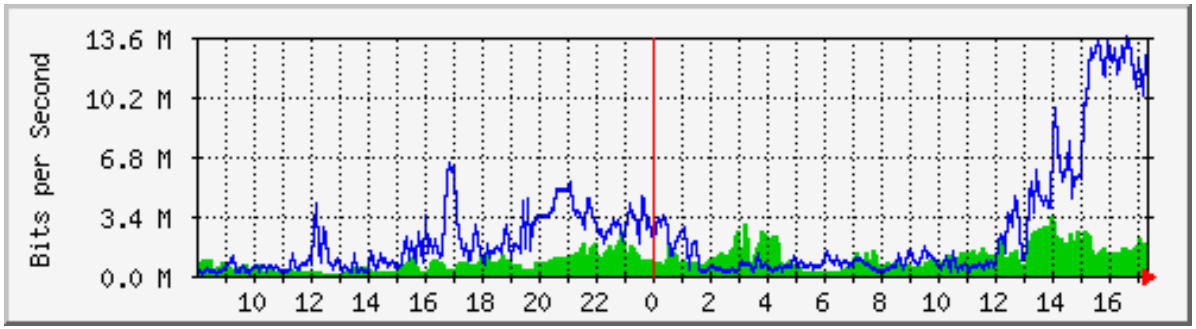
```
errors sysadmin@my.org
compress
/var/log/messages {
   rotate 5
   weekly
   postrotate
                /sbin/killall -HUP syslogd
   endscript }

/var/log/httpd/access.log {
   rotate 5
   mail www@my.org
   errors www@my.org
   size=100k
   postrotate
                /sbin/killall -HUP httpd
   endscript }
```

MRTG/RRDTool

MRTG...

- Le Multi Router Traffic Grapher (MRTG) est un outil de surveillance du trafic sur les liens d'un réseau
- MRTG permet de créer des pages HTML contenant des courbes qui affichent l'évolution de ce trafic, presque en temps réel



- MRTG est un outil simple, très utilisé par les FAI
- MRTG utilise des requêtes SNMP régulières afin de créer les courbes

Autres utilisations de MRTG

- Des applications externes peuvent interpréter les graphiques MRTG et fournir des services supplémentaires
- MRTG peut aussi être utilisé pour construire des courbes à partir d'autres informations disponibles dans les MIB
  - Charge de la CPU
  - Espace en disque
  - Température, etc...
- Les données peuvent aussi être issus d'autres sources que SNMP, tant qu'on puisse les quantifier (comme un compteur ou une jauge)
  - par exemple, utiliser PING pour estimer le RTT dans le réseau
- D'ailleurs MRTG est d'habitude étendu avec RRDTool

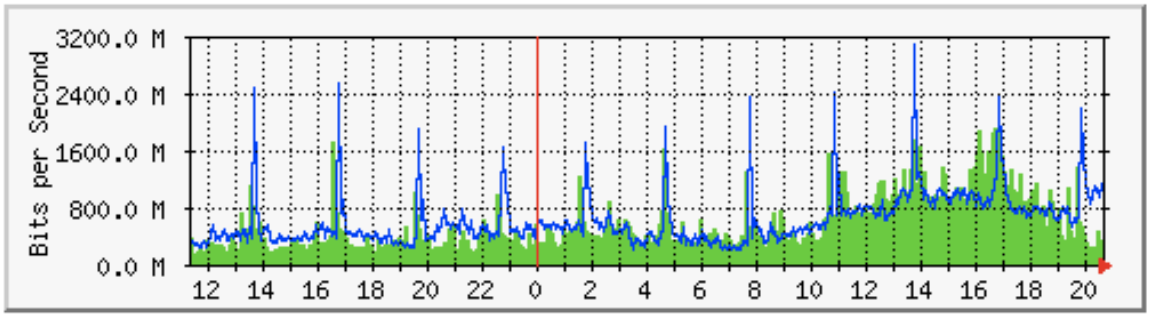
Déploiement de MRTG

- Installation des paquets
- Élaboration des fichiers cfg pour les interfaces réseau à l'ide de cfgmaker
- Création des pages html pages à partir des fichiers cfg en utilisant indexmaker
- Déclencher MRTG périodiquement avec Cron ou l'exécuter en mode daemon

Usage of the Connection to GEANT2

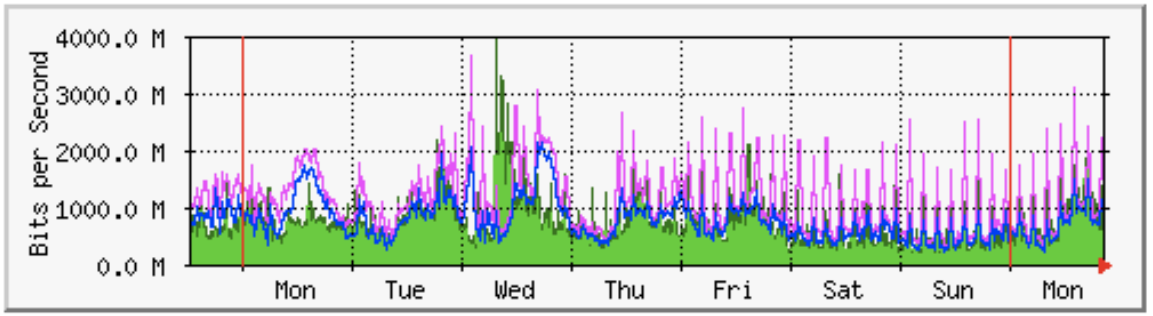
The statistics were last updated **Monday, 20 October 2008 at 20:40**

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	1894.3 Mb/s (18.9%)	550.6 Mb/s (5.5%)	223.2 Mb/s (2.2%)
Out	3058.3 Mb/s (30.6%)	602.9 Mb/s (6.0%)	901.9 Mb/s (9.0%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	3972.3 Mb/s (39.7%)	608.0 Mb/s (6.1%)	290.0 Mb/s (2.9%)

Terminé

RRDtool

- Round Robin Database – outil de stockage de données en série
- Outil non-graphique (ligne de commande)
- Du même auteur de MRTG
- Construit pour être plus rapide et flexible que MRTG seul
- Contient une API d'intégration ainsi que des outils de génération de pages CGI et des outils de manipulation graphique

Définition des sources de données

- DS:speed:COUNTER:600:U:U
- DS:fuel:GAUGE:600:U:U
  - DS = source de données (Data Source)
  - speed, fuel = nom des “variables”
  - COUNTER, GAUGE = type des variables (compteur, jauge)
  - 600 = intervalle entre les échantillons
    - UNKNOWN est retourné si rien n'est reçu
  - U:U = valeurs limites minimum et maximum pour les variables
    - (U veut dire "unknown" donc toutes les valeurs sont permises)

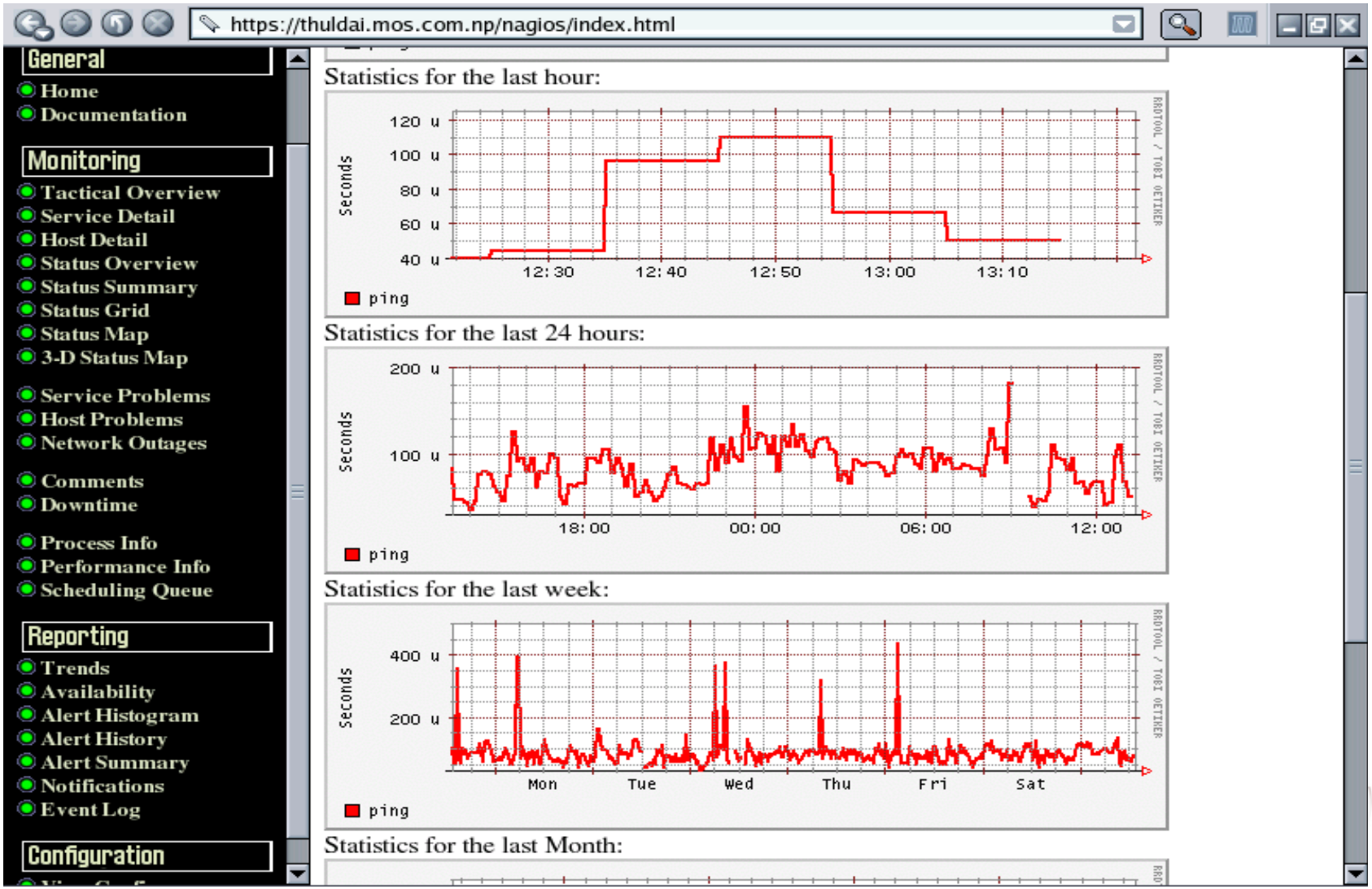
Définition des Sorties (archivage)

- RRA:AVERAGE:0.5:1:24
- RRA:AVERAGE:0.5:6:10
  - RRA = flux de sortie (Round Robin Archive)
  - AVERAGE = fonction statistique de consolidation
  - 0.5 = jusqu'à 50% des points consolidés peut être de type UNKNOWN
  - 1:24 = cet archive garde des échantillons (moyenne sur une intervalle "défaut" de 5 minutes), 24 fois (24*5 minutes = 2 heures)
  - 6:10 = l'archive garde la moyenne de six périodes défaut (6*5 = 30 minutes), au plus 10 fois (donc au plus 5 heures)
- Facile à comprendre, non ? **;)**
  - En fait, tout dépend de l'intervalle par défaut de 5 minutes

Voilà comme c'est simple !

- `rrdtool create /var/nagios/rrd/host0_load.rrd -s 600 DS:1MIN-Load:GAUGE:1200:0:100 DS:5MIN-Load:GAUGE:1200:0:100 DS:15MIN-Load:GAUGE:1200:0:100 RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- `rrdtool create /var/nagios/rrd/host0_disk_usage.rrd -s 600 DS:root:GAUGE:1200:0:U DS:home:GAUGE:1200:0:U DS:usr:GAUGE:1200:0:U DS:var:GAUGE:1200:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- `rrdtool create /var/nagios/rrd/apricot-INTL_Ping.rrd -s 300 DS:ping:GAUGE:600:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`
- `rrdtool create /var/nagios/rrd/host0_total.rrd -s 300 DS:IN:COUNTER:1200:0:U DS:OUT:COUNTER:600:0:U RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800`

Courbes de Latence d'un PING



Ganglia

Ganglia Monitoring

- Introduction
- L'architecture Ganglia
- Le frontend Apache
- Gmond & Gmetad
- Déploiement des agents Ganglia

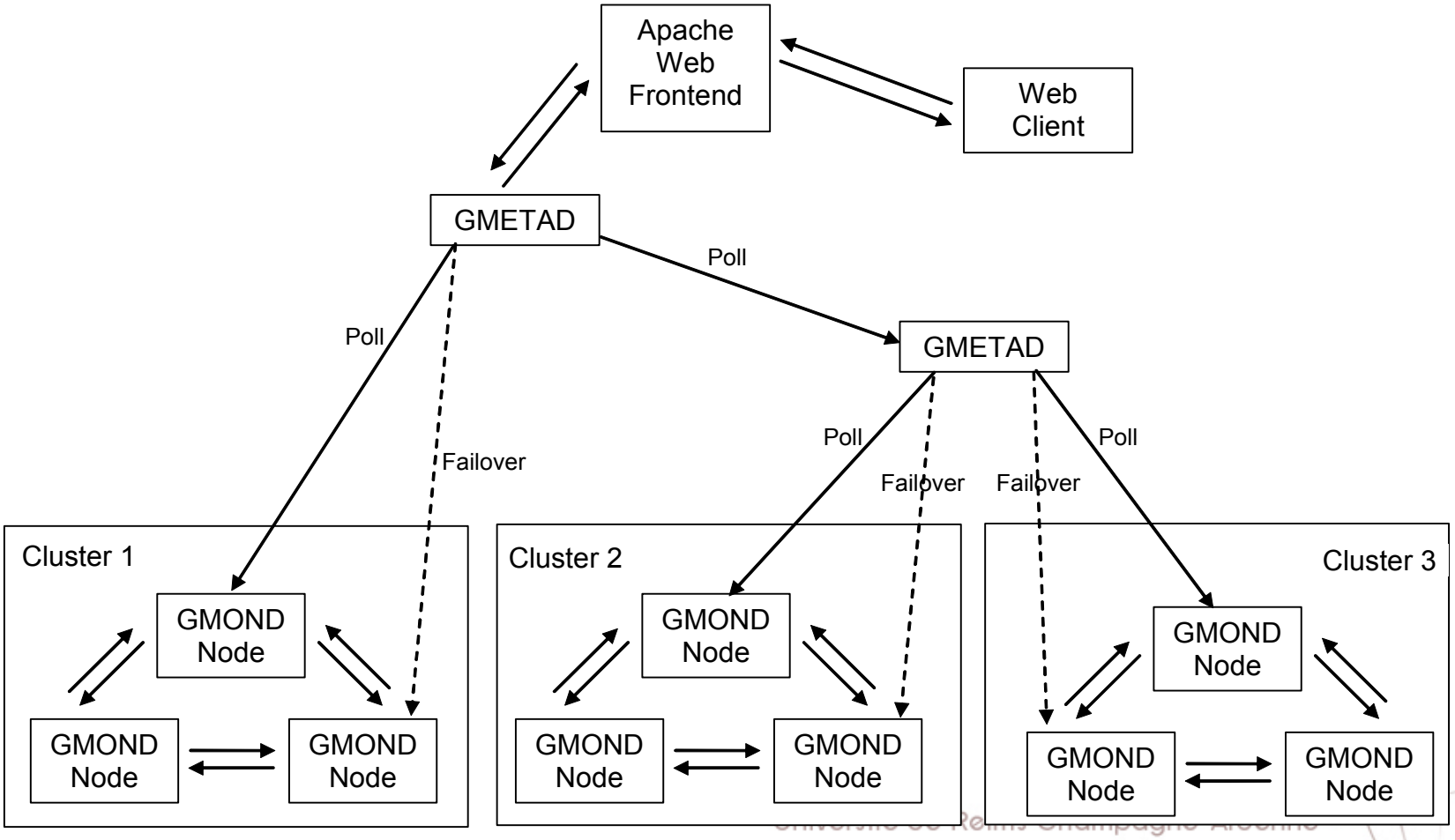
Introduction

- Système de surveillance orienté clusters et grilles
- Protocole basé sur le multicast
- Construit à partir de technologies ouvertes
  - XML
  - XDR (protocole de transport de données compact)
  - RRDTool - Round Robin Database
  - APR – Apache Portable Runtime
  - Apache HTTPD Server
  - Interface web PHP
- **http://ganglia.sourceforge.net** ou **http://www.ganglia.info**

L'Architecture Ganglia

- **Gmond** – Agents installés dans les clients
- **Gmetad** – Serveur d'agrégation
  - Installé en un ou plusieurs serveurs
- **Frontend Apache** – Présentation et analyse des métriques
- Attributs
  - Multicast – Les nœuds *gmond* surveillent et rapportent des défaillances sur la totalité du cluster
  - Failover – Lors d'une défaillance, *Gmetad* peut changer automatiquement le nœud utilisé pour les requêtes
  - Outils de mesure peu invasifs et transport léger sur le réseau

L'Architecture Ganglia



Le frontend Ganglia

- Utilise un serveur Apache et le module mod_php
- Des templates permettent la customisation du site
  - Adaptation à la charte graphique de l'entreprise
- Différents niveaux de visualisation
  - Les clusters dans une grille
  - Les nœuds dans un cluster
    - Mais aussi les nœuds dans toute la grille
  - Les caractéristiques de chaque nœud

Ganglia Customized Web Front-end

Grid'5000

Grid5000 Grid Report for Mon, 20 Oct 2008 20:33:55 +0200 Get Fresh Data

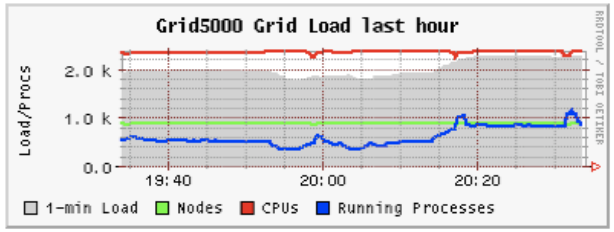
Last hour Sorted descending

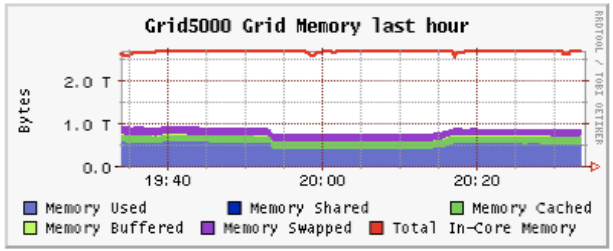
Grid5000 Grid > --Choose a Source

Grid5000 Grid (7 sources) (tree view)

CPUs Total:	2365
Hosts up:	896
Hosts unknown:	216
Hosts down:	58

Avg Load (15, 5, 1m):
88%, 95%, 96%
Localtime:
2008-10-20 20:33

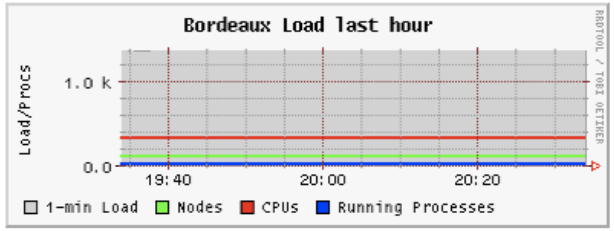


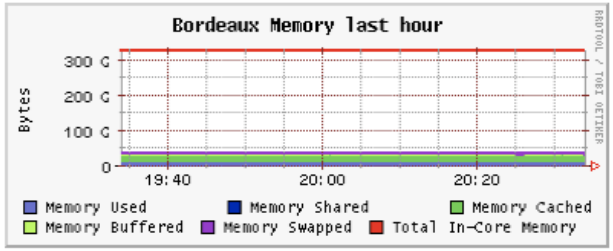


Bordeaux (physical view)

CPUs Total:	336
Hosts up:	102
Hosts unknown:	20
Hosts down:	23

Avg Load (15, 5, 1m):
407%, 408%, 408%
Localtime:
2008-10-20 20:33





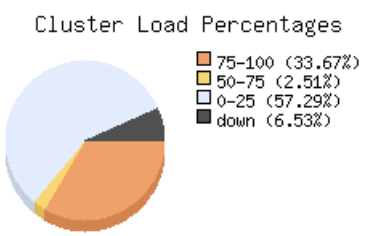
Lyon (physical view)

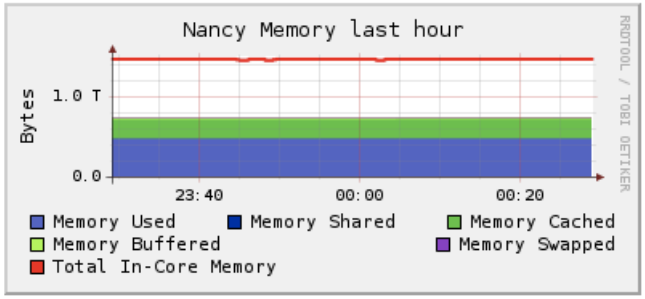
CPUs Total: 197

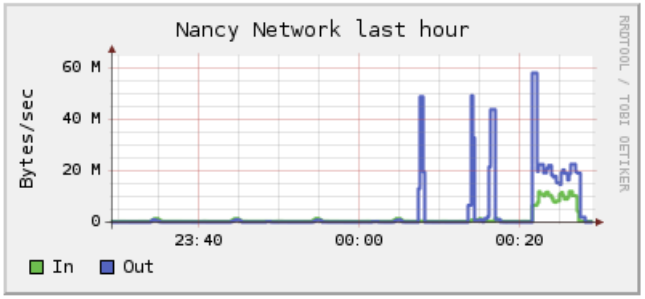
Lyon Load last hour

Lyon Memory last hour

Ganglia Customized Web Front-end







Show Hosts: yes ◉ no ○ | **Nancy load_one last hour sorted descending** | Columns 4

grelon-37.nancy.grid5000.fr *load_one:* **down** Last heartbeat 19 days, 6:48:25 ago	**grelon-38.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 19 days, 6:48:19 ago	**grelon-39.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 19 days, 6:48:17 ago	**grelon-113.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 14:47:48 ago
griffon-40.nancy.grid5000.fr *load_one:* **down** Last heartbeat 0 days, 6:40:05 ago	**griffon-69.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 1:55:11 ago	**griffon-72.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 1:40:43 ago	**griffon-73.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 1:40:38 ago
griffon-74.nancy.grid5000.fr *load_one:* **down** Last heartbeat 1 day, 1:40:40 ago	**griffon-75.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 1:40:41 ago	**griffon-76.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 12:01:45 ago	**griffon-77.nancy.grid5000.fr** *load_one:* **down** Last heartbeat 1 day, 1:40:45 ago
griffon-78.nancy.grid5000.fr *load_one:* **down** Last heartbeat 1 day, 1:40:42 ago	griffon-86.nancy.grid5000.fr load_one last hour (now 6.27	griffon-3.nancy.grid5000.fr load_one last hour (now 6.22	griffon-24.nancy.grid5000.fr load_one last hour (now 6.06

Déploiement de Ganglia

- http://ganglia.sourceforge.net/docs/ganglia.html
- Installer Gmond dans tous les noeuds à surveiller
  - Editer le fichier de configuration
    - Personnaliser les information des clusters et des noeuds
      - Configurer network upd_send_channel, udp_recv_channel, tcp_accept_channel
    - Lancer gmond
- Installer Gmetad dans un noeuds d'agrégation
  - Editer le fichier de configuration
    - Rajouter les sources de données et les remplaçants failover
    - Start gmetad
- Installer le frontend web
  - Installer les pages PHP dans le répertoire choisi
  - Entrer les informations d'authentification nécessaires

Nagios®

Quel est le plus de Nagios

- Nagios, d'une certaine manière, associe tous les outils suivants :
  - SNMP
  - MRTG
  - RRDTool
  - Rancid
  - Cacti
  - Smokeping

Les raisons pour utiliser Nagios

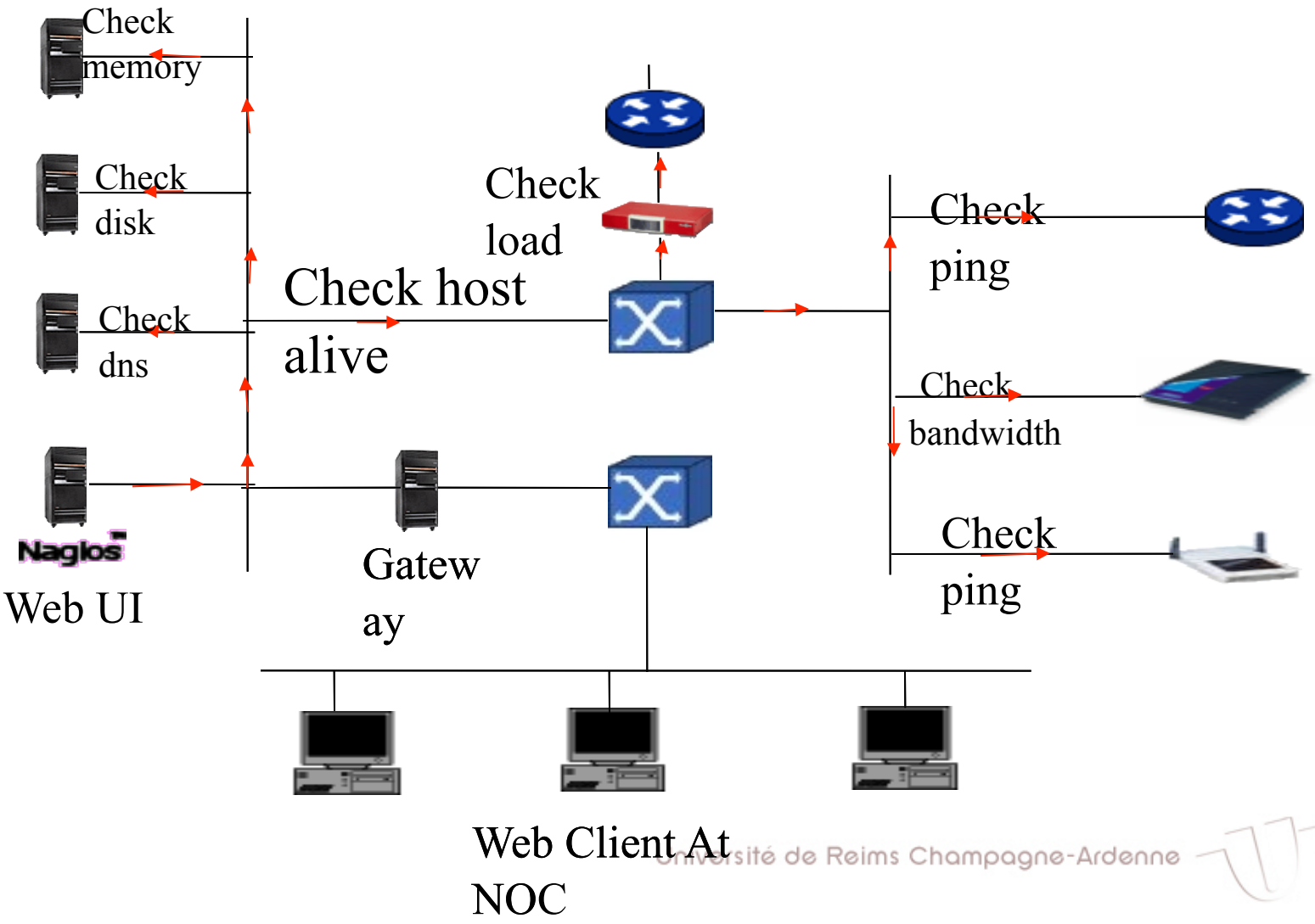
- Open source (même si la société fait du "commercial")
- Passe bien à l'échelle, facile à gérer, sécurisé
- Bien documenté
- Flexible – on peut créer nos propres sondes
- Effectue des alertes automatiques selon des paramètres de surveillance
- Plusieurs modalités de contact
  - Email, téléphone portable, etc

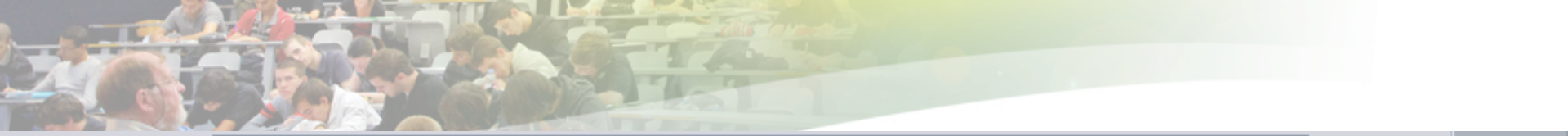
Les raisons pour utiliser Nagios

- Philosophie “**minimiser les de voyants rouges**”
  - “uniquement les faits” – affiche les événements qui ont donné origine au problème, au lieu d'inonder le serveur avec des alertes des défaillances qui suivent
- Gestion intelligente des sondes
  - Ex : si le HTTP répond, faire un ping n'est pas nécessaire
  - Ex : si une panne de courant est détectée, ça ne sert à rien de lancer d'autres sondes
  - En gros, si les services se portent bien, il n'y a pas besoin de vérifier si la machine est active

Les possibilités

- Nagios permet de répondre à plusieurs questions grâce à l'association de différents outils de surveillance :
- L'état individuel des nœuds
  - Sont-ils actifs ?
  - Quelle est leur charge ?
  - Combien de mémoire et d'espace en disque sont disponibles ?
  - NFS et les interfaces réseau sont actifs ?
  - Quelle est la température des machines ?
  - Toutes les applications tournent correctement ?
  - Quel est le temps d'un ping (latence) ?
- L'état d'un ensemble de nœuds
  - Mêmes informations, mais sur l'ensemble des machines


Check memory
Check disk
Check dns
Check host alive
Check load
Check ping
Check bandwidth
Check ping
Nagios
Web UI
Gatew ay
Web Client At NOC



https://thuldai.mos.com.np/nagios/index.html

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications

Current Network Status
Last Updated: Sun Feb 1 12:17:48 NPT 2004
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as *dhruba*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
226	5	0	16	0

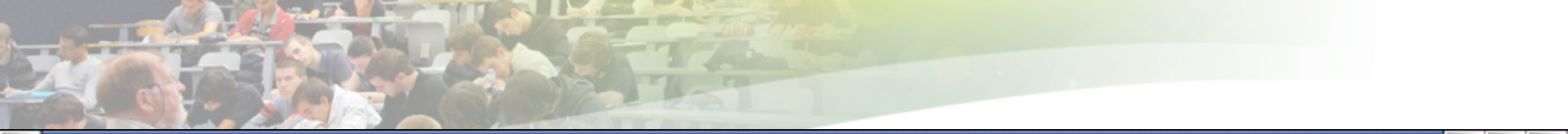
All Problems	All Types
21	247

Display Filters:

Host Status Types:	All problems
Host Properties:	Any
Service Status Types:	All
Service Properties:	Any

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
CHILDREN-FIRST	DOWN	02-01-2004 12:13:59	1d 19h 10m 33s	PING CRITICAL - Packet loss = 100%
DANIDA	DOWN	02-01-2004 12:15:55	1d 0h 43m 12s	PING CRITICAL - Packet loss = 100%
DASS	DOWN	02-01-2004 12:08:59	4d 0h 40m 42s	PING CRITICAL - Packet loss = 100%
FNCCI	DOWN	02-01-2004 12:12:38	4d 0h 40m 2s	PING CRITICAL - Packet loss = 100%
ITLINK	DOWN	02-01-2004 12:15:55	0d 1h 37m 12s	PING CRITICAL - Packet loss = 100%
Laz-cnet	DOWN	02-01-2004 12:12:38	4d 0h 38m 53s	PING CRITICAL - Packet loss =



Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all

Search

Current Network Status
Last Updated: Sun Feb 1 09:57:47 NPT 2004
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as *dhruba*

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

Host Status Totals

Up	Down	Unreachable	Pending
155	15	0	0

All Problems	All Types
15	170

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
228	3	0	16	0

All Problems	All Types
19	247

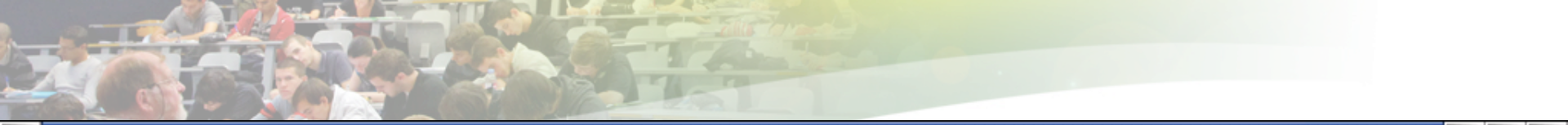
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
ACTIONAID	Ping	OK	02-01-2004 09:53:07	0d 12h 20m 9s	1/3	PING OK - Packet loss = 0%, RTA = 2 ms
AFP	Ping	OK	02-01-2004 09:55:38	0d 13h 40m 29s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
AGNIPAGE	Ping	OK	02-01-2004 09:55:27	0d 0h 0m 59s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
BRTSCHOOL	Ping	OK	02-01-2004 09:54:06	1d 18h 7m 39s	1/3	PING OK - Packet loss = 0%, RTA = 8 ms
Ban-cat	Ping	OK	02-01-2004 09:56:11	0d 22h 44m 39s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms

Transferring data from thuldai.mos.com.np...

Current S [root@dhr

Sun Feb 01, 9:26 PM



Current Service Status - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?host=all

Search

Kailash	Cpu-usage	OK	02-01-2004 10:21:38	3d 22h 48m 34s	1/3	SNMP OK: usr-cpu:1, sys-cpu:1,
	FTP	OK	02-01-2004 10:23:48	3d 22h 46m 38s	1/3	FTP OK - 0.007 second response time port 21 [220 kailash.mos.com.np FTP server ready.]
	Free-Memory	OK	02-01-2004 10:22:15	3d 22h 48m 34s	1/3	SNMP OK: Ram-Free:3100,
	HTTP	OK	02-01-2004 10:22:59	3d 22h 46m 38s	1/3	HTTP ok: HTTP/1.1 200 OK - 0.021 second response time
	Load	OK	02-01-2004 10:25:17	3d 22h 48m 34s	1/3	SNMP OK: 1MIN-Load:0.08, 5MIN-Load:0.05, 15MIN-Load:0.00,
	Ping	OK	02-01-2004 10:25:07	0d 5h 7m 33s	1/3	PING OK - Packet loss = 0%, RTA = 0 ms
	disk_usage	OK	02-01-2004 10:22:51	3d 22h 48m 34s	1/3	Disk utilization: All disks OK
Karnali	Ping	OK	02-01-2004 10:25:58	0d 17h 48m 53s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
Kopila	Cpu-usage	OK	02-01-2004 10:24:07	3d 22h 48m 34s	1/3	SNMP OK: usr-cpu:0, sys-cpu:1,
	Free-Memory	OK	02-01-2004 10:22:51	3d 22h 46m 38s	1/3	SNMP OK: Ram-Free:3808,
	Load	OK	02-01-2004 10:22:18	3d 22h 48m 34s	1/3	SNMP OK: 1MIN-Load:0.18, 5MIN-Load:0.19, 15MIN-Load:0.18,
	POP	OK	02-01-2004 10:23:07	3d 22h 46m 38s	1/3	POP OK - 0.028 second response time port 110 [+OK <8832.1075610415@kopila.mos.com
	Ping	OK	02-01-2004 10:25:58	3d 15h 7m 15s	1/3	PING OK - Packet loss = 0%, RTA = 1 ms
Koshi	Ping	OK	02-01-2004 10:22:37	1d 13h 37m 43s	1/3	PING OK - Packet loss = 0%, RTA = 9 ms

Done

Mozilla-bi [root@dhr

Sun Feb 01, 9:56 PM

https://thuldai.mos.com.np/nagios/cgi-bin/status.cgi?hostgroup=all

All Routers @Durbar Marg-KTM (Routers@DMG)

Host	Status	Services	Actions
Dmg-3640	UP	1 OK	
Dmg-rt2	UP	1 OK	
Gw-7206	UP	1 OK	

All Routers @Kantipath-KTM (Routers@KP)

Host	Status	Services	Actions
Ktp-rt1	UP	1 OK	
Ktp-rt2	UP	1 OK	

All Routers @Lazim

Host	Status	Serv
Laz-nxl-link1	UP	1 O
Laz-rt1	UP	1 O

All Routers @POPs w/ Lease Link (Routers@POPsL)

Host	Status	Services	Actions
Brj-gw	UP	1 OK	
Brt-gw	UP	1 OK	
Brt-link1	UP	1 OK	
Brt-link2	UP	1 OK	
Htd-lease	DOWN	1 CRITICAL	

All Routers @POPs w/ VSAT Link (Routers@POPsV)

Host	Status	Services	Actions
Brj-2501	UP	1 OK	
Btl-vsat	UP	1 OK	
Htd-vsat	UP	1 WARNING	
Nam-gw	UP	1 OK	

All Routers @Sundh

Host	Status	Services
Ptn-rt1	UP	1 OK

All Routers @Pulchowk-KTM (Routers@PUL)

Host	Status	Services	Actions
Pul-2610	UP	1 OK	
Pul-ptn-link1	UP	1 OK	
Pul-ptn-link2	UP	1 OK	
Pul-rt2	UP	1 OK	

All Routers @Sundhara (Routers@SDR)

Host	Status	Services	Actions
Sdr-rt1	UP	1 OK	

All Routers @Xpressway (Routers@X

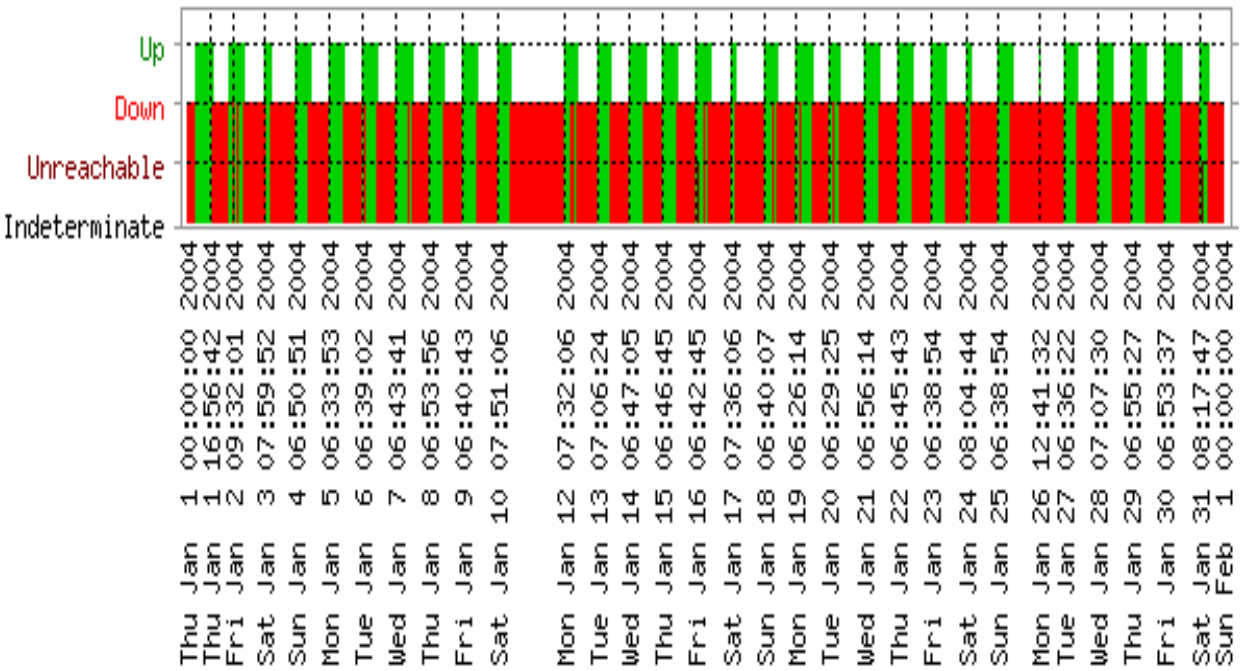
Host
AGNIPAGE
BRTSCHOOL

Historique des événements

Trends

State History For Host 'Don_Bosco'

Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004

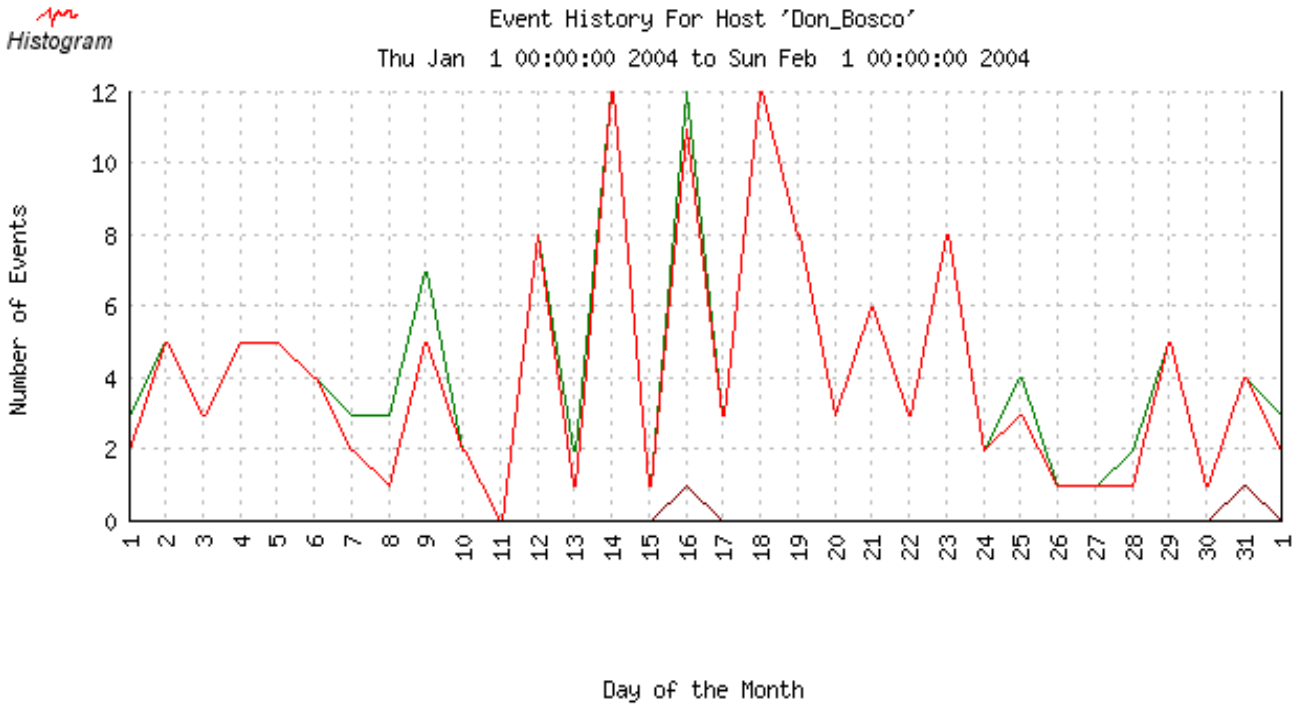


State Breakdowns:

Up	:	(32.6%) 10d 2h 21m 41s
Down	:	(67.1%) 20d 19h 17m 27s
Unreachable	:	(0.3%) 0d 2h 5m 12s
Indeterminate	:	(0.0%) 0d 0h 15m 40s

Report Produced By:
Nagios®
http://www.nagios.org

Histogramme d'une machine



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06

Report Produced By:
Nagios®
http://www.nagios.org

https://thuldai.mos.com.np/nagios/cgi-bin/showlog.cgi

Current Event Log
Last Updated: Sun Feb 1 12:15:31 NPT 2004
Nagios® - www.nagios.org
Logged in as *dhruba*

Latest Archive

Log File Navigation
Sun Feb 1 00:00:00 NPT 2004 to Present..

Older Entries First:
Update

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

February 01, 2004 12:00

[02-01-2004 12:14:28] HOST NOTIFICATION: Amod;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28] HOST NOTIFICATION: Amod;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28] HOST NOTIFICATION: DeepakA;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:28] HOST NOTIFICATION: Krishna;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27] HOST NOTIFICATION: NirajS;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27] HOST NOTIFICATION: Prabhu;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27] HOST NOTIFICATION: Ravin;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27] HOST NOTIFICATION: Ravin;WORLDBANK-R;DOWN;host-notify-by-epager;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:14:27] HOST NOTIFICATION: Upendra;WORLDBANK-R;DOWN;host-notify-by-email;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:12:16] SERVICE ALERT: SDC;Ping;WARNING;HARD;1;PING WARNING - Packet loss = 60%, RTA = 23.73 ms
[02-01-2004 12:12:16] HOST ALERT: SDC;DOWN;HARD;1;PING CRITICAL - Packet loss = 100%
[02-01-2004 12:11:09] SERVICE ALERT: Htd-vsat;Ping;WARNING;HARD;3;PING WARNING - Packet loss = 40%, RTA = 674.22 ms
[02-01-2004 12:10:26] SERVICE ALERT: Htd-lease;Ping;WARNING;HARD;3;PING WARNING - Packet loss = 40%, RTA = 385.85 ms
[02-01-2004 12:08:58] SERVICE FLAPPING ALERT: WORLDBANK-R;Ping;STOPPED; Service appears to have stopped flapping (3.8% change < 5.0% threshold)
[02-01-2004 12:08:49] HOST NOTIFICATION: Gyanu;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48] HOST NOTIFICATION: Ishwar;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48] HOST NOTIFICATION: Kedar;Htd-lease;UP;host-notify-by-epager;PING OK - Packet loss = 30%, RTA = 357.24 ms
[02-01-2004 12:08:48] HOST NOTIFICATION: MSurya;Htd-lease;UP;host-notify-by-email;PING OK - Packet loss = 30%, RTA = 357.24 ms

https://thuldai.mos.com.np/nagios/cgi-bin/notifications.cgi?contact=all

Contact Notifications
Last Updated: Sun Feb 1 12:07:59 NPT 2004
Nagios® - www.nagios.org
Logged in as *dhruba*

All Contacts

Latest Archive

Log File Navigation
Sun Feb 1 00:00:00 NPT 2004 to Present..

Notification detail level for all contacts:
All notifications

Older Entries First:

Update

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

Host	Service	Type	Time	Contact	Notification Command	Information
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:12	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	NirajS	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:11	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:10	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
WORLDBANK-R	N/A	HOST DOWN	02-01-2004 11:13:08	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Amod	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	DeepakA	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Krishna	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:49	Prabhu	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Ravin	host-notify-by-epager	PING CRITICAL - Packet loss = 100%
Laz-cnet	N/A	HOST DOWN	02-01-2004 11:07:48	Upendra	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Gyanu	host-notify-by-email	PING CRITICAL - Packet loss = 100%
Htd-lease	N/A	HOST DOWN	02-01-2004 10:56:06	Ishwar	host-notify-by-email	PING CRITICAL - Packet loss = 100%