

Africa Network Operators Group

La gestion réseau et le NOC:
concepts, pratiques, et outils

AfNOG 2010

Jean-Robert Hountomey

origine: Afnog T2-2003 by Brian Longwe & Sunday Folayan, Afnog T3-2003 Alain Aina, Afnog T3 2004 Phil Regnaud – Alain Aina

1

La gestion du réseau – Qu'est ce que c'est?

“ Afin de mettre en oeuvre un service efficace et fiable, le réseau doit être géré avec une véritable discipline en utilisant une structure cohérente pour la gestion des informations recueillies”.

Geoff Huston, ISP Survival Guide
Traduit de l'Anglais

2

Qu'est-ce qu'un NOC?

Centre d'Opération Réseau

- ♦ Observer et gérer les services d'un fournisseur de service.
 - Recueillir et gérer les dysfonctionnements
 - Statistique sur l'état opérationnel du réseau
 - Historique sur le fonctionnement du système.

Coordination du travail des Ingénieurs à travers le COR (NOC).

Les composantes de l'administration réseau

- ♦ Gestion des erreurs et dysfonctionnements
- ♦ Gestion des configurations/modifications
- ♦ Gestion de la performance
- ♦ Gestion de la sécurité

Gestion des incidents et dysfonctionnements

- ♦ Identifier les problèmes
- ♦ Sonder/vérifier régulièrement le réseau.
- ♦ Isoler les dysfonctionnements
- ♦ Diagnostic des équipements du réseau.
- ♦ Résoudre les dysfonctionnements.
 - Allouer des ressources pour résoudre les problèmes
 - Priorité des interventions
 - Interventions technique par pallier (escalation)
- ♦ Informer
- ♦ Alerter

5

Gestion des Incidents

- ♦ Mécanisme d'alerte
 - Lien vers le NOC
 - Alerte Téléphonique/Mail
- ♦ Mettre en oeuvre et contrôler les procédures d'alarme.
- ♦ Procédure de récupération
- ♦ Système de Ticket

6

Gestion des incidents Détection de dysfonctionnement

Qui signale un problème sur le réseau?

- Équipe du centre d'opération (24x7)
 - ouvre des tickets d'incidents pour suivre les problèmes
 - Procède au diagnostic préliminaire (1st level)
 - Assigne le problème à un ingénieur, ou met à jour le statut des tickets.
 - Contacte les clients
- Les autres FAI

7

Gestion des incidents - Détection de dysfonctionnement (suite)

Comment identifier les problèmes sur le réseau

- Outil d'observation réseau
 - Outils communs
 - Ping (test de disponibilité)
 - Traceroute (topologie, atteignabilité)
 - outils snmp (collecte de données, pour statistiques)
 - Observation Système
 - Nagios
 - Big Brother
 - Analyse de logs (syslog)

8

Gestion des incidents - Détection de dysfonctionnement (suite)

- ◆ Signaler les incidents et les inaccessibilités
- ◆ Détecter les nœuds qui ne répondent pas
- ◆ Problèmes de routage

9

Gestion des incidents – Système de Tickets

- ◆ Très importants
- ◆ Besoin de mécanismes pour le suivi:
 - Défaut de fonctionnement
 - État actuel
 - Perturbation de trafic

10

Gestion des incidents – Système de Tickets

- ◆ Le système doit:
 - Favoriser l'archivage des incidents sur du long terme
 - Faciliter la programmation des tâches (fenêtre de maintenance)
 - Aider à la surveillance
 - Permettre des analyse statistiques (incidents / période, type, temps moyen de résolution, etc...)
 - Servir de base de connaissances (knowledge base): RT, RTFM

11

Gestion des incidents – Utilisation des tickets

- ◆ Créer un ticket pour TOUS les appels
- ◆ Créer un ticket pour chaque problème signalé
- ◆ Créer un ticket pour chaque évènement planifié
- ◆ Distribuer le ticket à tous les techniciens
- ◆ Durant toutes les étapes de la résolution d'un problème, on doit garder le même numéro de ticket.
- ◆ Les tickets doivent rester ouverts jusqu'à résolution du problème tel que signalé.

12

Gestion d'incident – Exemple de ticket

History

```
Thu Sep 23 18:11:34 2003 mattias@oncotype.dk - Ticket created
Date: Tue, 23 Sep 2003 18:06:23 +0200 (CEST)
Subject: wyeth.dk
From: "Mattias Bodlund" <mattias@oncotype.dk>
To: <support@catpipe.net>
Cc: <seant@oncotype.dk>
```

```
Mi
The wyeth server has not come up after the power failure'.
Can you take a look at it.
```

```
cheers,
mattias .i oncotype
```

```
Thu Sep 23 18:38:18 2003 regnauld - Correspondence added
```

```
Date: Tue, 23 Sep 2003 18:38:16 +0200
From: Phil Regnauld <regnauld@catpipe.net>
To: mattias bodlund via RT <support@catpipe.net>
Cc: undisclosed-recipients: ;
Subject: Re: [catpipe.net #884] wyeth.dk
```

```
mattias bodlund via RT (support) writes:
> Mi
>
> The wyeth server has not come up after the power failure'.
>
> Can you take a look at it.
```

```
Am on it.
```

```
--
| regnauld@catpipe.net | catpipe Systems ApS |
| "BSD solutions, consulting, development" |
| Tlf.: +45 7021 0050 | http://www.catpipe.net/ |
```

```
Thu Sep 23 20:00:57 2003 regnauld - Status changed from new to resolved
```

13

Gestion des incidents – Incidents Typiques

- Réseau non joignable par "ping"
- Pas de connectivité IP sur le routeur
- Raisons possibles
 - Liaison Série tombée
 - Appeler votre fournisseur
 - Routeur inactif/problème matériel
 - Appeler les ingénieurs
 - Problème de routage
 - Diagnostique avec traceroute / mtr
 - Ou utiliser des utilitaires de diagnostique de routage

14

Gestion de performance

Avoir un niveau de performance consistant

- Collecte de Données
 - États des interfaces
 - Trafic de sortie
 - Taux d'erreur
 - utilisation
 - Pourcentage de disponibilité
- Analyse des données pour évaluer les performances
- Établir les seuils de performance
- Planifier l'évolution de la capacité

15

Importance des statistique réseau

- Pour la comptabilité
- Diagnostique (erreur récurrentes, corrélation)
- Analyse pour l'évolution à long terme
- Planification de capacité
- Deux type de mesure
 - Mesure actives (ping, traceroute, telnet, snmpget ifStatus)
 - Mesures passives (traps SNMP, logs syslogs, netflow)
- Les outils de gestion réseau ont des fonctionnalités de statistiques

16

Outils de gestion de performance

- netflow
 - cflowd (<http://www.caida.org/tools/measurement/cflowd/>)
 - Collecte les information sur le flux réseau au travers des routeurs Cisco (et certains autres)
 - Information AS <-> AS.
 - Information IP/ports source et destination utiles pour une comptabilité de donnée et les statistiques.
 - Quel part de mon trafic a rapport avec le port 80?
 - Quel part de mon trafic va vers l'AS237?

17

Exemple Netflow

```
##### Top 5 AS's based on number of bytes #####
srcAS  dstAS      pkts      bytes
6461   237         4473872   3808572766
 237   237         22977795  3180337999
3549   237         6457673   2816009078
2548   237         5215912   2457515319

##### Top 5 Nets based on number of bytes #####
Net Matrix
-----
number of net entries: 931777
SRCNET/MASK DSTNET/MASK      PKTS      BYTES
165.123.0.0/16 35.8.0.0/13      745858   1036296098
207.126.96.0/19 198.108.98.0/24  708205   907577874
206.183.224.0/19 198.108.16.0/22  740218   861538792
 35.8.0.0/13   128.32.0.0/16    671980   467274801

##### Top 10 Ports #####
input
port   packets  bytes      output
      packets  bytes      packets  bytes
119    10863322 2808194019 5712783  427304556
80     36073210 862839291  17312202 1387817094
20     1079075  1100961902 614910   62754268
7648   1146864  419882753  1147081  414663212
25     1532439  97294492  2158042  722584770
```

18

Gestion de la sécurité

- Ne laissez pas des aliments qui peuvent intéresser les souris sur votre table de cuisine la nuit
- Bouchez les trous susceptible d'être utiliser par les souris pour entrer dans votre maison.
- Ne fournissez pas aux souris de l'espace dans votre maison pour qu'il y installent leur nid
- Installer des pièges le long des murs par où les souris passent sans que vous les voyiez.

19

Gestion de la sécurité

- Vérifier régulièrement l'efficacité de vos pièges. Utiliser des appâts différents....
- Éviter d'utiliser des pièges commerciaux . Les pièges traditionnels sont souvent plus efficace.
- Ayez un chat!

20

Gestion de la sécurité - Outils

- Outils pour serveurs
 - cops – Teste la configuration des machines (www.cert.org)
 - Tcpwrappers – restriction des accès et log des connexions
 - AIDE – observe et rapporte les changements sur des fichiers
- <http://www.cs.tut.fi/~rammer/aide.html>
- Analyse de logs
 - Swatch, logsurger, logcheck – analyse de logs (syslog ou autre) et alertes
 - Soyez informés sur les dernières mises à jour de sécurité

21

Gestion de la sécurité - Outils

- Information sur les bugs
 - liste de diffusion CERT :
 - ♦ http://www.cert.org/contact_cert/certmaillist.html
 - Bugtraq
 - ♦ <http://www.securityfocus.com/archive/1>
- Correction des bugs
- Alerte d'intrusion (SNORT - <http://www.snort.org>)

22

Gestion de la sécurité – les Bonnes manières

- ◆ Procédure de rapport pour les problèmes de sécurité
 - Ex: Intrusion
 - Une adresse d'abus pour permettre aux clients de signaler les abus (abuse@votre-fai.net)
- ◆ Contrôle de vos passerelles internes et externes
- ◆ Gérer les logs de sécurité
 - Avoir une machine qui centralise les logs (syslog-ng)

23

Gestion de configuration

Maintenir les information sur l'architecture de votre réseau et sa config. courante.

Observer l'état du réseau

- Consigner la topologie de votre réseau
 - Statique
 - ◆ Qu'est ce qui est installé?
 - ◆ Où est-ce installé?
 - ◆ Comment sont-ils connectés?
 - Dynamique
 - ◆ État opérationnel des équipements du réseau

24

Gestion de configuration

Control opérationnel de votre réseau

- Arrêt et démarrage individuel des éléments de votre réseau.
- Charger et sauvegarder différentes versions de vos configuration.
 - Chaque nuit, rapatrier via SNMP (ou autre) la configuration et la stocker dans un endroit sûr
- Mise a jour matériel et logiciel
- Méthode d'accès
 - SNMPGet / SNMPSet

25

Gestion de configuration

- Inventaire de votre réseau
 - Base de donnée des éléments du réseau
 - Historique des changements & problèmes
 - Toutes les machines et les applications qui y tournent
 - Base de donnée: les serveurs de nom (LOC, HINFO, RP, TXT)
- Gestion des machines et du nommage
 - "Une information perd sa valeur si on ne sait pas où elle se trouve."

26

Qu'est ce que SNMP?

- Simple Network Management Protocol
- Système de requête - réponse
- Peut obtenir des informations sur l'état d'un élément réseau
 - Requête standard
 - Requêtes spécifiques a une entreprise
- Utiliser les données de la MIB
 - management information base

27

Pourquoi utiliser SNMP?

- Interroger les routeurs pour avoir:
 - Le nombre d'octet en entrée et sortie par seconde.
 - Charge du Processeur.
 - Le temps total de marche.
 - État des sessions BGP.
- Interroger des machines pour avoir:
 - L'état du réseau
 - Web trafic
 - La charge du proxy Squid
 - Les logiciels installés, ...

28

Outils d'administration reseau

- MRTG <http://www.ee-staff.ethz.ch/~oetiker/webtools/mrtg/>
- RRDtool <http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/>
- Cricket <http://cricket.sourceforge.net/>
- **Avantage**
 - Simple à utiliser et à configurer
 - Identifier rapidement les pointes et les creux du trafic
 - Afficher n'importe quelle information transmis a travers SNMP

29

MRTG

Traffic Analysis for 2 -- noc.ws.afnog.org

Maintainer: postmaster@localhost

Description: fxp1

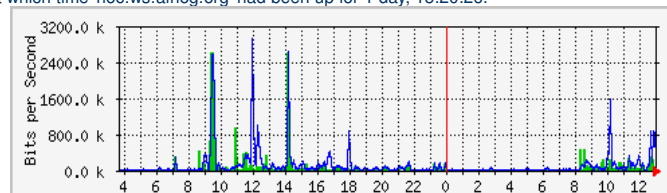
ifType: ethernetCsmacd (6)

ifName:

Max Speed: 100.0 Mbits/s Ip: 81.199.109.1 (host-81-199-109-1)

The statistics were last updated Thursday, 12 June 2003 at 13:50,

at which time 'noc.ws.afnog.org' had been up for 1 day, 15:20:26.



30

Comptabilité Technique des données

- Pourquoi cette comptabilité?
 - Utilisation du réseau et des services fournis
- Type de comptabilité de données
 - RADIUS/TACACS comptabilité des données venant des serveurs d'accès.
 - Statistique des interfaces
 - Statistiques des protocoles
- A comptabilité des données a un effet sur votre modèle commercial
 - Facturer a l'utilisation?
 - Facturer au forfait?

31

NOC en Pratique: les outils

- ♦ **Observation du réseau et services - Nagios**
 - <http://www.nagios.org/>
- ♦ Observe l'état du réseau
 - Signale les problèmes
 - Observe le changement d'état des problèmes
 - Résoudre les problèmes
- ♦ Statistiques

32

Nagios

Current Network Status
 Last Updated: Fri May 21 04:18:23 CEST 2004
 Updated every 90 seconds
 Real-time Network Monitor - www.nagios.org
 Logged in as **admin**
 - Nagios process is running
 - Notifications can be sent out (active mode)
 - Service checks are actively being executed

[View History For All Hosts](#)
[View Notifications For All Hosts](#)
[View Status Details For All Host Groups](#)
[View Status Summary For All Host Groups](#)

Host Status Totals			
Up	Down	Unreachable	Pending
27	0	0	0
All Problems		All Types	
0		27	

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
88	2	0	1	0
All Problems		All Types		
3		88		

Service Overview For All Host Groups

Home ADSIs (ads)			
Host	Status	Services	Actions
testad	UP	1 OK	

ISP DK servers (isp-dk)			
Host	Status	Services	Actions
bobbes.hst-dk.dk	UP	1 OK	

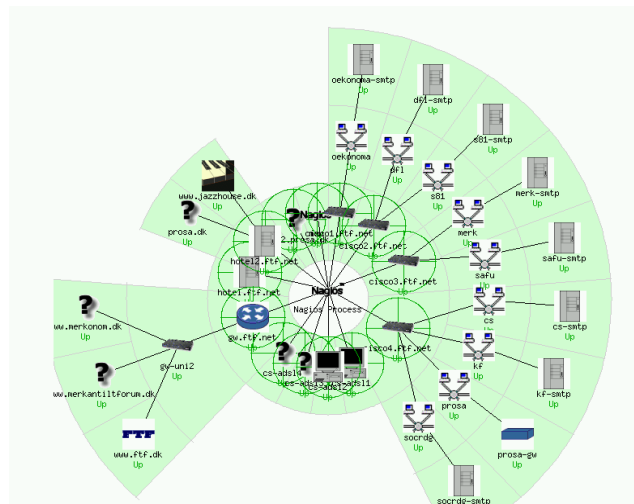
Hosted CMS servers (cmsrtr)			
Host	Status	Services	Actions
bcprod	UP	1 OK	
bcstest	UP	1 OK	
bobbes.hst-dk.dk	UP	1 OK	
www.nyweb.dk	UP	1 OK	

Home Capacity (hp)			
Host	Status	Services	Actions
bcprod	UP	1 OK	
bcstest	UP	1 OK	

H.S.DNS (adsn)			
Host	Status	Services	Actions
DNS1.hosp.dk	UP	1 OK	
DNS2.hosp.dk	UP	1 OK	
ns1-int.hosp.dk	UP	1 OK	
ns1-int.hosp.dk	UP	1 OK	
ns2-int.hosp.dk	UP	1 OK	
ns2-int.hosp.dk	UP	1 OK	

hls (hls)			
Host	Status	Services	Actions
mdo.dk	UP	1 OK	
denochdetail	UP	1 OK	
gotstak	UP	1 OK	
psbille	UP	1 OK	
www.sasnapr.dk	UP	1 OK	

Nagios



NOC en pratique

♦ Systeme de ticket – RT (www.fsck.com/rt/)

- Création de tickets
 - En temps que client
 - En temps qu'ingénieur
- Consulter les tickets
- Prendre/Assigner des tickets
- Suivi par mail et Web
- Base de connaissances RTfm

35

RT

History

Tue Sep 23 18:11:34 2003 **mattias@oncotype.dk - Ticket created**

```
Date: Tue, 23 Sep 2003 18:06:23 +0200 (CEST)
Subject: wyeth.dk
From: "mattias bodlund" <mattias@oncotype.dk>
To: <support@catpipe.net>
Cc: <seant@oncotype.dk>
```

Mi

The wyeth server has not come up after the power failure'.

Can you take a look at it.

cheers,
mattias .: oncotype

Tue Sep 23 18:38:18 2003 **regnauld - Correspondence added**

```
Date: Tue, 23 Sep 2003 18:38:16 +0200
From: Phil Regnauld <regnauld@catpipe.net>
To: mattias bodlund via RT <support@catpipe.net>
Cc: undisclosed-recipients: ;
Subject: Re: [catpipe.net #84] wyeth.dk
```

mattias bodlund via RT (support) writes:

> Mi

>

> The wyeth server has not come up after the power failure'.

>

> Can you take a look at it.

>

Am on it.

--

```
catpipe | regnauld@catpipe.net | catpipe Systems ApS |
  BSD solutions, consulting, development |
  Tlf.: +45 7021 0050 | http://www.catpipe.net/ |
```

Tue Sep 23 20:00:57 2003 **regnauld - Status changed from new to resolved**

36

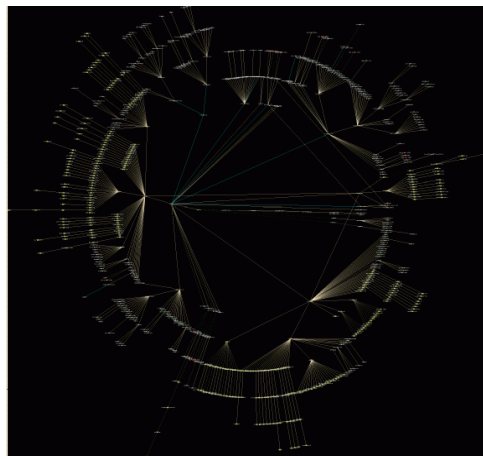
NOC en pratique

♦ Gestion de configuration

- Ciscoconf – récupère automatiquement les configuration Cisco
 - <http://software.automagic.org/ciscoconf/>
- RANCID – pareil, mais bien plus avancé, et plusieurs fabricants
 - <http://www.shrubbery.net/rancid/>
- Netdisco – gestion de configuration via cdp et SNMP, cisco et autres. Fait aussi la cartographie des équipements réseau
 - <http://www.netdisco.org/>

37

Netdisco



38

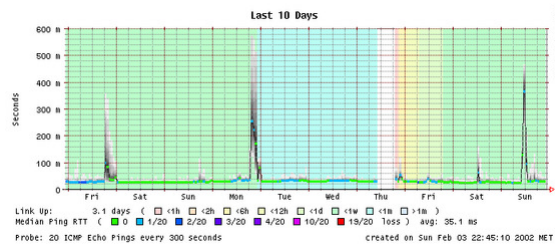
NOC en pratique

- ◆ Stockage de logs
 - Syslog-ng http://www.balabit.com/products/syslog_ng/
- ◆ Analyse et rapports de logs
 - Swatch - <http://www.oit.ucsb.edu/~eta/swatch/>
 - Logsurfer - <http://www.cert.dfn.de/eng/logsurfi/>
 - Logcheck - <http://www.astro.uiuc.edu/~r-dass/logcheck/>

39

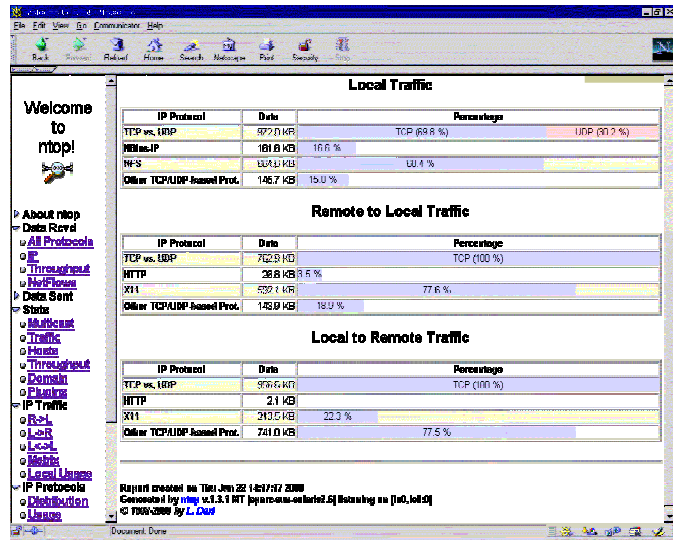
NOC en pratique

- ◆ Outils de collecte de données et mesures
 - MRTG, RRD, Cricket, Cflowd
 - NTOP2 - <http://www.ntop.org/>
 - SmokePing - <http://people.ee.ethz.ch/~oetiker/webtools/smoeping/>

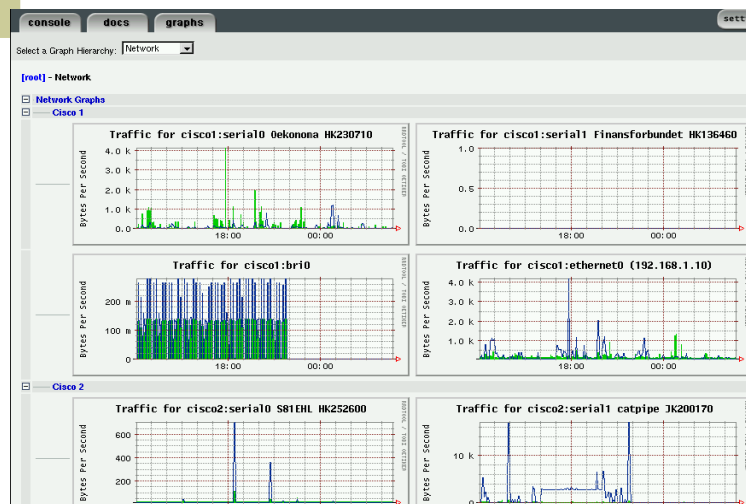


40

NTOP



Cacti - <http://raxnet.net/products/cacti/>



Securité

IDS: SNORT - <http://www.snort.org/>

43

Outils de diagnostic

- ◆ Mtr - <http://www.bitwizard.nl/mtr/>
 - Traceroute et ping à la fois
- ◆ Nmap - <http://www.insecure.org/nmap/>
 - Scanner ICMP/UDP/TCP pour découvrir les réseaux
- ◆ Bing - <http://www.freenix.fr/freenix/logiciels/bing.html>
 - Mesurer la bande passante entre deux points

44

