Africa Network Operator's Group

Application NOC et Service

AFNOG 2003
Alain AINA

Qu'est-ce qu'un NOC?

Centre d'opération réseau

- Observer et gérer les services d'un fournisseur de service.
  - Recueillir et gérer les disfonctionnements
  - Statistique sur l'état opérationnel du réseau
  - Historique sur le fonctionnement du système.
  - Coordination du travail des Ingénieurs à travers le COR (NOC).

L'administration réseau – Qu'est ce que c'est?

"Afin de mettre en oeuvre un service efficace et sure, 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

Les composantes de l'administration réseau

- Gestions des erreurs et disfonctionnements
- Gestion des configurations/modifications
- Gestion de la performance
- Gestion de la sécurité
- Gestion des comptes.

Gestion des incidents et disfonctionnements

- Identifier les problèmes
- Sonder/vérifier régulièrement le réseau.
- Isoler les disfonctionnements
- Diagnostique des équipements du réseau.
- Résoudre les disfonctionnements.
  - Allouer des ressources pour résoudre les problèmes
  - Priorité les interventions
  - Interventions technique par pallier.
- Informer
- notification

Gestion des Incidents

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

Gestion des incidents Détection de dysfonctionnement

Qui signale un problème sur le réseau?

- Équipe du centre d'opération (7/24/24)
  - ouvre des tickets d'Incidents pour suivre les problèmes
  - Procède au Diagnostique préliminaire
  - Assigne le problème à un ingénieur, ou met à jour le statut des ticket.
  - Appel les clients
- Les Autre ISPs

7

Gestion des incidents - Détection de dysfonctionnement (suite)

Comment identifier les problèmes sur le réseau

- Outil d'observation réseau
  - Outils communs
    - ping
    - traceroute
    - Snmp
  - Observation Système
    - NOCol/Snips
    - Big Brother
    - NetSaint

8

Gestion des incidents - Détection de dysfonctionnement (suite)

- NMIS
- HP Openview, etc…

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

9

Gestion des incidents – Système de Tickets

- Très Importants
- Besoins de mécanisme pour le suivi:
  - Défaut de fonctionnement
  - État actuel de saturation
  - Ticket de trafic

10

Gestion des incidents – Système de Tickets

- Le système doit:
  - Favoriser l'archivage des incidents sur du long terme
  - Faire la programmation des taches.
  - Aider à la surveillance
  - Analyse statistiques
  - Comptabilité de donnée sur du long terme

11

Gestion des incidents – Utilisation des tickets

- Créer un ticket pour TOUS les appels
- Créer un ticket pour chaque problèmes signalés
- Créer un ticket pour chaque évènement planifié
  Distribuer le ticket à la mailling list des techniciens
- Toutes les étapes de la résolution d'un problème doit garder le même numéro de ticket.
- Les tickets doivent rester ouvert jusqu'à résolution du problème tel que signale.

12

Fault Management - Ticket Example

Users on the laptop station minihub are not getting correct DHCP responses. No gateway or DNS entries are returned.

Thanks, - Hervey

-- CUSTOMER INFORMATION ----------

'inst' (AFNOG Instructors) –

----

*There have been several issues. First, the Cisco config-switch was set so the box would forget it's config on a power cycle (and we've had a few). Second, I made a typo when I cleaned up a DNS file. Things *should* be working now (famous last words). Resolving this till I hear otherwise.*

GJ ----------

>otherwise.

>>GJ

Many thanks!

- Hervey

13

Gestion des incidents – Incidents Typiques

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

14

Gestion de performance

Avoir un niveau de performance consistent

- 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 l'accounting (comptabilité)
- diagnostique
- Analyse pour l'évolution à long terme
- Planification de capacité
- Deux type de mesure
  - Mesure actives
  - Mesures passives
- Les outils de gestion réseau ont des fonctionnalités de statistiques

16

Outils de gestion de performance

- netflow
  - cflowd (http://www.caida.org/Tools/Cflowd)
  - Collecte les information sur le flux réseau a travers des routeurs cisco
  - Information AS to AS.
  - Information ip/ports source et destination useful 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

Outils de gestion de performance

- netflow
  - cflowd (http://www.caida.org/Tools/Cflowd)
  - Collecte les information sur le flux réseau a travers des routeurs cisco
  - Information AS to AS.
  - Information ip/ports source et destination useful 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?

18

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                  output
port     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
```


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 ou les souris les souris passent au sans que vous les voyiez.

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!

Gestion de la sécurité - Outils

- Outils
  - cops – Teste la configuration des machines (www.cert.org)
  - swatch – rapport sur l'activité des machines par e-mail
  - Tcpwrappers – restriction des accès et log des connexions
  - Tripwire – observe les changement sur les fichiers système

    http://www.cert.org/tech_tips/security_tools.html
- Soyez informe sur les dernières mises a jours sur la sécurité

Gestion de la sécurité - Outils

- Information sur les bugs
  - liste de diffusion CERT :
    - http://www.cert.org./contact_cert/certmaillist.html
- Correction des bugs
- Alerte d'intrusion

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-isp.net)
- Contrôle de vos gateway interne et externe
- Gérer les logs de sécurité
  - Avoir une machine qui centralise les logs

Gestion de configuration

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

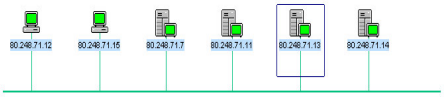
Observer l'état du réseau

- Consigner la topologie de votre réseau
  - Statique
    - Qu'est ce qui est installe?
    - Ou est-il installe?
    - Comment sont-ils connecte?
  - Dynamique
    - État opérationnel des équipements du réseau

25

Gestion de configuration

Ecran de collecte SNMP



26

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.
- Mise a jour matériel et Logiciel
- Méthode d'accès
  - SNMPGet / SNMPSet

27

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 donne des serveurs de nom
- Gestion des machines et du nomage
  - "Une information n'est perd sa valeur si on ne sait pas ou elle se trouve."

28

Qu'est ce que SNMP?

- Simple Network Management Protocole
- 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

29

Pourquoi utiliser SNMP?

- Interroger les routeurs pour avoir:
  - Le nombre d'octet en entre 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
  - ….

30

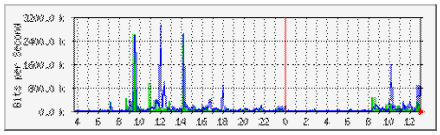
Outils d'administration reseau

- MRTG http://www.ee-staff.ethz.ch/~oetiker/webtools/mrtg/
- RRDtool http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/
- Cricket http://cricket.sourceforge.net/
- HP OPenview
- **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

31

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.



32

Comptabilité Technique des données

- Pourquoi cette comptabilité?
  - Utilisation du réseau et des services fournies
- 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 model commercial
  - Facturer a l'utilisation?
  - Facturer au forfait?

33

NOC en Pratique

- Observation du réseau – NOCOL/SNIPS
  - http://www.netplex-tech.com/software/snips/
- Observe l'état du réseau
  - Signale les problèmes
  - Observe le changement d'état des problèmes
  - Résoudre les problèmes
- Statistiques?

34

NOC en pratique

- Systeme de ticket - WebRT
  - description
  - Création de tickets
    - En temps que client
    - En temps qu'ingénieur
  - Consulter les tickets
  - Prendre/Assigner des tickets

35

References

- http://www.merit.edu/ipma/docs/isp.html
- http://www.nanog.org
- http://www.caida.org
- http://www.nlanr.net
- http://www.cisco.com
- http://www.amazing.com/internet/
- http://www.isp-resource.com/
- http://www.merit.edu/ipma
- http://www.ripe.net

36

D'autres outils!

- http://www.caida.org/Tools/
  - OC3Mon/Coral
- http://www.merit.edu/~ipma
  - RouteTracker
  - IRRj
  - ASExplorer
- http://www.geektools.com/
- http://www.merit.edu/ipma/tools/other.html
- www.cidr-report.org

37

Outils miroir

```
BGP routing table entry for 80.248.64.0/20, version 41826462
Paths: (2 available, best #1)
  Not advertised to any peer
  6461 16631 16631 16631 22241 19686
    195.22.211.248 (metric 91) from 195.22.208.248 (195.22.208.248)
      Origin IGP, metric 8161, localpref 90, valid, internal, best
      Community: 6762:49 6762:99
      Originator: 195.22.211.248, Cluster list: 0.0.0.1, 0.0.0.4
  6461 16631 16631 16631 22241 19686
    195.22.211.248 (metric 91) from 195.22.208.249 (195.22.208.249)
      Origin IGP, metric 8161, localpref 90, valid, internal
      Community: 6762:49 6762:99
      Originator: 195.22.211.248, Cluster list: 0.0.0.1, 0.0.0.4
```

38

Outils miroir

- Serveurs traceroute
- http://www.merit.edu/ipma/tools/trace.html

```
                    Query: trace
                    Addr: www.isoc.org
Translating "www.isoc.org"...domain server (206.205.242.132) [OK]
Type escape sequence to abort.
Tracing the route to info.isoc.org (198.6.250.9)
  1 iad1-core2-fa5-0-0.atlas.digex.net (165.117.129.2) 0 msec 0 msec 4 msec
  2 dca5-core2-s5-0-0.atlas.digex.net (165.117.53.41) 0 msec 4 msec 0 msec
  3 dca5-core1-fa5-1-0.atlas.digex.net (165.117.56.117) 4 msec 0 msec 4 msec
  4 Hssi3-1-0.BR1.DCA1.ALTER.NET (209.116.159.98) 0 msec 0 msec 4 msec
  5 101.ATM2-0.XR1.DCA1.ALTER.NET (146.188.160.226) [AS 701] 4 msec 0 msec 4 msec
  6 195.ATM7-0.XR1.TCO1.ALTER.NET (146.188.160.102) [AS 701] 4 msec 0 msec 0 msec
  7 193.ATM8-0-0.GW1.TCO1.ALTER.NET (146.188.160.33) [AS 701] 4 msec 4 msec 4 msec
  8 charlie.isoc.org (198.6.250.1) [AS 701] 8 msec 8 msec 8 msec
  9 info.isoc.org (198.6.250.9) [AS 701] 8 msec *  12 msec
```

39

Reference d'outils SNMP

- MON - http://www.kernel.org/software/mon/
- NOCol – Snips
- Sysmon - ftp://puck.nether.net/pub/jared
- Rover - http://www.merit.edu/~rover
- Concord - http://www.concord.com
- http://www.merit.net/~netscarf

40