Monitoring, Accounting

(Traçabilité).

Introduction

Deux notions importantes pour un administrateur de réseau, la première pour la bonne marche du système, la seconde pour la tranquillité des administrateurs :)

Plan de la présentation

- Monitoring
  - Définition
  - Outils
  - Exemple
  - Conclusion
- Accounting (Traçabilité)
  - Définition
  - Pourquoi, pour qui
  - Les enregistrements
  - La loi
  - Exemples
  - Conclusion
- Conclusion (et ébauche d'un projet)

Monitoring

- Définition : C'est l'opération qui consiste à suivre méticuleusement le fonctionnement d'un système, d'un processus en temps réel.

  Dans notre cas deux buts
  - Assurer le bon fonctionnement du réseau et prévenir si possible les problèmes. (au moins les résoudre)
  - Garantir la sécurité sur le réseau.

Monitoring

- Les outils propriétaires
  Ils sont souvent liés au matériel que l'on a déployé, par exemple dans le cadre d'AP légères reliées à un switch «wifi», ou d'un manager vendu avec les bornes.

- Les outils libres
  Pour n'en citer qu'un celui que l'on utilise Nagios, qui peut faire du simple PING au manager SNMP. Si on excepte la partie radio, tout logiciel de monitoring de réseaux filaires peut être adapté à un réseau wifi. Pour faire du monitoring radio on pourra utiliser n'importe quel logiciel de scan de réseau Wifi.

Monitoring

- Notre architecture, un mélange propriétaire-libre.

  Nous utilisons Nagios comme outil de monitoring de notre dorsale réseau. Nous avons décidé de le garder pour la partie Wifi. Il Ping les différentes bornes et envoie un mail en cas de problème. Il s'agit là du monitoring le plus basique, à savoir est-ce que mon équipement est bien présent sur le réseau.

Monitoring

On utilise également un outil propriétaire, fourni par Cisco, le WLSE. (Wireless LAN Solution Engine) Il s'agit d'un outil de monitoring complet dont je vais présenter les principales caractéristiques. Nous n'utilisons pour notre part que certaines fonctionnalités que j'expliciterai.

Monitoring

- Wlse un outil complet
  - Un système de détection d'intrusion Wifi.
  - Un manager radio complet couplé à un système de plans qui donne une bonne vision de sa couverture radio, permet de l'améliorer et le la corriger.
  - Un système d'alertes pour la sécurité et la disponibilité.
  - Un outil de reporting complet qui permet de voir l'état de son réseau Wifi : radio, SSID, utilisation des bornes , et qui permet également de générer des rapports.
  - Un gestionnaire des configurations et des IOS.

Monitoring

C'est sans doute la partie qui facilite le plus la vie que ce soit pour mettre à jour les IOS des bornes, sauvegarder l'ensemble des configurations, passer une modification sur une ou plusieurs bornes. Dans notre cas, nous l'utilisons pour charger, puis supprimer, à la demande, des SSID pour des colloques sur une partie de l'infrastructure. C'est également très pratique quand on veut tester de nouvelles configurations sur une ou plusieurs bornes.

Monitoring

- Wlse, un outil qui peut vite devenir trop lourd.
  - Beaucoup (trop ?) d'information par défaut. Toute la partie réglage des seuils d'alertes que ce soit au niveau de la sécurité (IDS) ou de la disponibilité doit être bien paramétrée avant d'être mise en service sous peine d'être rapidement inutilisée. (et de voir sa messagerie exploser si on a réglé les alertes pour arriver par mail)

Monitoring

- Wlse un système qui demande du temps. Il en faut en effet pour par exemple utiliser à plein toute la partie management radio ou bien encore éplucher l'ensemble des possibilités de reporting qu'il offre.

  (petite présentation de l'interface)

Monitoring

- Conclusion sur le Wlse.
  - Pratique pour la maintenance du réseau.
  - Nous utilisons la partie reporting et alertes ponctuellement quand un problème survient.
  - Nous n'utilisons pas le système de détection d'intrusion par manque de temps.
  - La partie radio est utile pour améliorer les performances de l'ensemble du réseau.

Monitoring

- Conclusion sur le monitoring
  - On surveille à hauteur du degré de disponibilité que l'on souhaite atteindre.
  - On peut utiliser des outils les plus simples aux plus élaborés. (méfiance toutefois au trop plein d'informations)
  - Finalement pas de bonne méthode, on fait en fonction de son temps, de ses besoins et aussi de ses moyens.

Accounting (traçabilité)

- Définition : Pour lutter contre les usurpations de droits, il est souhaitable de suivre les accès aux ressources informatiques sensibles. (heure de connexion, suivi des actions)
  On retiendra principalement la fin de la phrase car le but peut être plus ambitieux, et je compléterai en disant : les accès nominatifs, car il s'agit bien de savoir qui fait quoi.

Accounting (traçabilité)

- Pourquoi ?
  - Avoir des éléments à analyser en cas de problème.
  - Pour respecter la loi. En tant que fournisseur d'accès internet le gestionnaire du réseau Wifi se doit de garder des traces des connexions au cas ou une action malveillante serait entreprise depuis ce réseau wifi.
  - Pour mieux monitorer. Les informations d'accounting se retrouvent d'ailleurs (en partie) dans un outil comme le Wlse.
- Pour qui ?
  - Soi-même. (l'administrateur du réseau) (renvoi aux points 1 et 3 ci-dessus)
  - La police et/ou la justice si elles en font la demande.

Accounting (traçabilité)

- Ce qu'on enregistre
  - Les logs des bornes.
  - Les logs radius.
  - Les logs de la passerelle. (nat, dhcp, ids)
  - Accounting radius des bornes.

Accounting (traçabilité)

- Comment on l'enregistre.
  - Les méthodes d'enregistrement
    - Syslog. (les bornes, tout ce qui concerne la passerelle)
    - Trap ou interrogations Snmp. (les bornes)
    - Radius. (l'accounting des bornes et logs du serveur)
  - Les supports d'enregistrements.
    - Fichiers. (on y envoie les logs de la passerelle : nat, logs des bornes)
    - Bases de données. (accounting radius, logs dhcp)

Accounting (traçabilité)

- Présentation de la mise en oeuvre de ces différentes techniques d'accounting, on envoie les logs dans des fichiers.
  - Le NAT iptables log les paquets autorisés (en tête) dans un fichier. (directive iptables -J LOG)
  - Le dhcp log les requêtes dans un fichier. (fichier de configuration)
  - On active les différents sections de logs radius dans le fichier radiusd.conf. (pour freeradius)
  - On configure l'accounting radius sur les bornes et le radius pour qu'il soit envoyé dans /var/log/radius/radacct/adresseipborne.
  - On configure les bornes pour qu'elles loggent vers un serveur syslog

Accounting (traçabilité)

- Présentation de la mise en oeuvre de ces différentes techniques d'accounting, utilisation d'une base mysql.
  - On commence par créer un table mysql ACCOUNTING qui va rassembler l'ensemble des informations.
  - On configure le fichier sql.conf (freeradius) et on active sql dans radiusd.conf pour que l'accounting des bornes aille dans la base. A ce stade, l'accounting radius se trouve dans la base mysql. On va maintenant lui ajouter les logs dhcp, c'est à dire les adresses ip des clients.

Accounting (traçabilité)

- Ajout des adresses dhcp dans la base.
  On utilise le script monitor_eduroam.pl pour envoyer également dans la base mysql les logs dhcp. Il faut pour cela créer une nouvelle table avec les adresses ip des bornes et les communautés SNMP. Ensuite on déclare les quelques variables au début du script (le chemin du fichier de logs dhcp, l'adresse de la base ...) puis on lance le script qui est un démon qui va parser le fichier de logs dhcp et insérer les adresses dans la base après interrogation SNMP des bornes.

Accounting (traçabilité)

Je vais maintenant donner quelques exemples des différents types de logs que l'on est amené à traiter.

Accounting (traçabilité)

Logs des bornes :

Jan 9 12:51:39 195.220.107.35 10612: Jan 9 11:51:38.995: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 000e.9b44.1d00 Associated KEY_MGMT[NONE]
Jan 9 12:52:02 195.220.107.78 7269: Jan 9 11:52:01.673: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 0018.de6d.0502 Reason: Disassociated because sending station is leaving (or has left) BSS

Accounting (traçabilité)

Les logs radius :

Packet-Type = Access-Accept
Tue Jan 9 10:58:26 2007
User-Name := "anonymous@siris.sorbonne.fr"
User-Name := "lemoan@siris.sorbonne.fr"
Service-Type = Framed-User
Session-Timeout = 1200
Tunnel-Type:1 = VLAN
Tunnel-Medium-Type:1 = IEEE-802
Tunnel-Private-Group-Id:1 = "4"
MS-MPPE-Recv-Key =
0x719e22226abc74ccee5eef686447952cb9f2abcfba49da41e24191062423 93f8
MS-MPPE-Send-Key =
0x2dd1d3069815d17d3cc6855483753e78854dd2ece4e336c096d58347b9ee2ed5

Accounting (traçabilité)

Les logs de la passerelle :

Jan 9 12:54:01 rethel kernel: IN=eth2 OUT=eth1 SRC=192.168.115.239 DST=207.46.109.69 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=12898 DF PROTO=TCP SPT=1067 DPT=1863 WINDOW=63395 RES=0x00 ACK URGP=0

Jan 9 12:49:17 rethel dhcpd: DHCPDISCOVER from 00:13:72:3e:4a:94 via eth0
Jan 9 12:49:18 rethel dhcpd: DHCPOFFER on 195.220.107.191 to 00:13:72:3e:4a:94 via eth0
Jan 9 12:51:09 rethel dhcpd: DHCPRELEASE of 192.168.116.231 from 00:16:cf:61:4d:bc (valued-12ef4461) via eth2 (found)
Jan 9 12:51:26 rethel dhcpd: DHCPREQUEST for 192.168.116.232 from 00:18:de:24:ac:ea (nom-7ecd37cbf2b) via eth2
Jan 9 12:51:26 rethel dhcpd: DHCPACK on 192.168.116.232 to 00:18:de:24:ac:ea (nom-7ecd37cbf2b) via eth2

Accounting (traçabilité)

User-Name	Calling-Station-Id	Client-IP-Address	Called-Station-Id	NAS-IP-Address	NAS-Port	Timestamp Start	Timestamp Dhcp
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3230	2007-01-04 09:39:17	2007-01-11 10:55:51
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3230	2007-01-04 09:39:15	2007-01-11 10:55:51
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3230	2007-01-04 09:39:07	2007-01-11 10:55:51
fboivent@univ-rennes1.fr	0040.96ad.b361	195.220.94.239	0012.d942.a460	195.220.94.225	9668	2007-01-11 10:55:48	2007-01-11 10:55:51
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3161	2007-01-03 16:52:20	2007-01-11 10:55:51
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3070	2007-01-03 14:55:42	2007-01-11 10:55:51
fboivent@univ-rennes1.fr	0040.96ad.b361	195.220.94.239	0012.d942.a460	195.220.94.225	9504	2007-01-03 11:37:22	2007-01-03 11:37:23
arredu@cru.fr	0040.96ad.b361	195.220.94.239	0012.dabf.90b0	129.20.1.1	3230	2007-01-04 09:39:07	2007-01-11 10:55:51
anonymous	0040.96ad.b361	195.220.94.239	0012.d942.a460	195.220.94.225	9500	2007-01-03 11:34:50	2007-01-03 11:34:59

Accounting (traçabilité)

Timestamp Stop	Acct-Unique-Session-Id	Acct-Session-Time	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets	Acct-Terminate-Caus
1970-01-01 01:00:00	375a92393f53ed81	0	0	0	0	0	
1970-01-01 01:00:00	375a92393f53ed81	0	0	0	0	0	
1970-01-01 01:00:00	375a92393f53ed81	0	0	0	0	0	
2007-01-11 10:56:16	f888174221f47e08	27	10936	11767	175	33	Lost-Carrier
1970-01-01 01:00:00	e8535cea3218c957	0	0	0	0	0	
1970-01-01 01:00:00	cbc3e1c1bd5d29ca	0	0	0	0	0	
2007-01-03 11:40:58	4d4183deef36bbe4	216	13005	5904	344	24	Lost-Carrier
1970-01-01 01:00:00	375a92393f53ed81	0	0	0	0	0	
2007-01-03 11:35:34	dfc7d28fec9df263	44	4206	1554	63	9	Lost-Carrier

Accounting (traçabilité)

- Ce qui dit la loi du 29 novembre 2005 (décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques) Il faut conserver pendant un an
  - Les informations permettant d'identifier l'utilisateur.
  - Les données relatives aux équipements terminaux de communication utilisés.
  - Les caractéristiques techniques ainsi que la date l'horaire et la durée de chaque communication.
  - Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.
  - Les données permettant d'identifier le ou les destinataires de la communication.
    Le code des postes et communications électroniques interdit par contre de garder le corps des paquets .

Accounting (traçabilité)

- Qui peut y accéder :
  - La police ou les renseignements généraux en en faisant simplement la demande à une « personne qualifiée » qui sera nommée « auprès du ministère de l'intérieur ». Il n'y aura donc plus besoins de l'autorisation d'un juge pour que la police se saisisse de ces données.

    Cette loi est valable pour une durée de trois ans.

Accounting (traçabilité)

- Ce que dit la CNIL : elle a demandé des précisions pour savoir qui était contraint de conserver ces données outre les FAI (cybercafé , hotel , université etc ....) . Pas de réponse à cette question.
- En conclusion , craignant plus la police que la CNIL je garde mes logs un an :)

Accounting (traçabilité)

- Trois exemples d'applications
  - Détection de vol d'identifiant par la détection des connexions simultanées. En recherchant systématiquement les demandes de connexions simultanées on peut très facilement découvrir des identifiants qui ont été volés.
  - Détection d'un problème de handhover trop fréquent. Quelqu'un qui sans bouger ne cesse de faire du handhover est tout de suite vu dans la table d'accounting mysql.
  - Plainte d'un organisme et remontée de traces. C'est cet exemple que l'on va plus détailler.

Accounting (traçabilité)

- La situation de départ :
  On reçoit un jour un mail nous signalant que la site www.toto.com d'adresse ip xxx.xxx.xxx.xxx a subi des tentatives d'intrusion depuis l'adresse ip source publique de notre passerelle wifi. Le site nous informe qu'il réfléchit aux suites à donner. Afin d'être prêt à réagir, nous allons chercher à identifier la personne.

Accounting (traçabilité)

- La démarche d'identification de la personne :
  On va commencer par chercher dans les logs du nat l'adresse ip du site toto.com. Une fois cette adresse trouvée il va falloir identifier les différentes (si il y en a plusieurs) adresses privées ayant accédé à ce site. Un horodatage précis de l'attaque doit nous permettre facilement de retrouver la bonne adresse ip privée. A partir de là il suffit de rechercher dans notre base d'accounting radius mysql les identifiants liés à cette adresse privée pour l'heure qui nous intéresse. On n'aura plus qu'à vérifier que l'adresse mac que l'on trouve au niveau de l'accounting est bien la même que l'adresse mac de la machine de la personne que l'on soupçonne.

Accounting (traçabilité)

- La mise en place de la récupération de toutes ces traces permet de pouvoir facilement suivre les actions des utilisateurs du réseau, qu'ils soient « locaux » ou « distant », et garantit ainsi la responsabilité des administrateurs vis à vis de la loi. Il n'y a pas de difficultés majeures, hormis peut-être pour le script eduroam_monitor.pl qui souffre d'un manque de documentation.

Conclusion et projet

- Le monitoring dépend beaucoup du contexte, taille du réseau, moyens dont on dispose, degré de qualité de service que l'on souhaite.
- Pour l'accounting, la marge de manoeuvre réside surtout dans les moyens techniques, la loi obligeant les administrateurs à conserver des éléments très précis pour pouvoir « tracer » les utilisateurs.

Conclusion et projet

- Ce qu'on aimerait mettre au point : la possibilité de charger dans une base mysql l'ensemble des sources de logs et ce à des fins d'analyse qui peuvent être
  - la sécurité en étudiant le comportement moyen d'un utilisateur et en recherchant par la suite les comportements suspects.
  - Faire des recherches beaucoup plus rapidement en cas d'incident.
  - Générer des statistiques sur les temps de connexions et les débits à des fins de monitoring.