UNIVERSITÉ CAEN NORMANDIE

.... Gestion d'erreurs et manipulation de journaux d'évènements 23.02.2023

Les logs sont suivis à la trace ☹

Smart network administrators know that logging of servers is important...

Don't let your log data slip through your fingers [1] ***...***

Auteur : Pascal Fougeray

Préambule : la loi !

Voici ce que dit la loi française

Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne

1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :

- a) L'identifiant de la connexion ;
- b) L'identifiant attribué par ces personnes à l'abonné ;
- c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
- d) Les dates et heure de début et de fin de la connexion ;
- e) Les caractéristiques de la ligne de l'abonné ;

Plus d'informations :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&categorieLien=id

La durée de conservation des données mentionnées à l'article 1er est d'un an

1. ***http://www.balabit.com/***

1 Introduction

Tout ne se passe pas pour le mieux dans le monde de l'Internet, des serveurs, des services et ça bug.

Il faut avoir une **trace** de ce qui se passe en bien comme en mal[2], afin de pouvoir analyser ce qui s'est passé quand cela s'est mal passé.

Et des fois cela se passe pas comme on voudrait...

Dans ce cours, je vais surtout me concentrer sur **Syslog qui est au monde du log, ce que Cisco est au monde du réseau.**

2 Définition de log

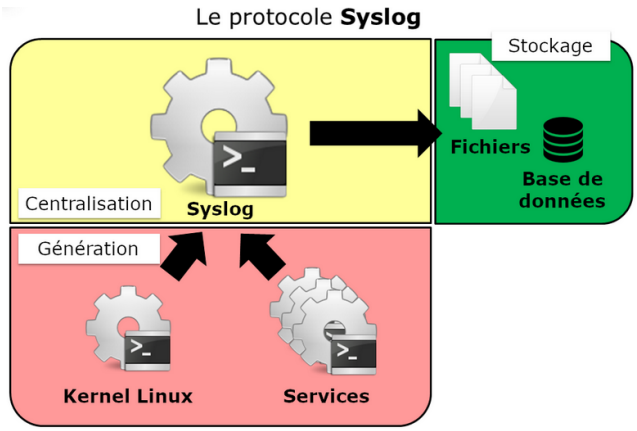
Un message journal de bord, ***logbook*** en anglais, est une **information générée** de manière **asynchrone** par une entité logique tel un processus ou physique tels les éléments actifs du réseau, routeurs et *switchs*, suite à un **évènement *erreur***, ***warning***, survenu.

L'évènement peut être :

— la suppression d'un fichier et/ou d'un répertoire,
— le ***login*** en local ou via telnet ou ssh d'un utilisateur sur un serveur, un routeur, un switch etc...,
— le ***shutdown*** ou ***updown*** d'une interface sur un élément actif du réseau : ***interface went Down : ge-3/0/0.0 (TRAP)***
— une alerte d'un élément actif du réseau : ***SNMP Trap : linkUp up/up ge-3/0/0.0***
— une session **BGP** Up depuis temps : ***BGP Session Up : 2a02 :70c0 : :2 (AS1664), time 4m 21s ago***
— l'adjacence **OSPF**, **LDP** etc... entre 2 routeurs sur un backbone MPLS,
— En fonction des types de programmes, les messages journaux sont stockés dans des fichiers spéciaux destinés à contenir ceux ci.

3 Le protocole et les messages Syslog

Syslog c'est en même temps un protocole et un ensemble de messages envoyés à l'aide de ce protocole.



3.1 Le protocole Syslog

Il est défini par les **RFC** :

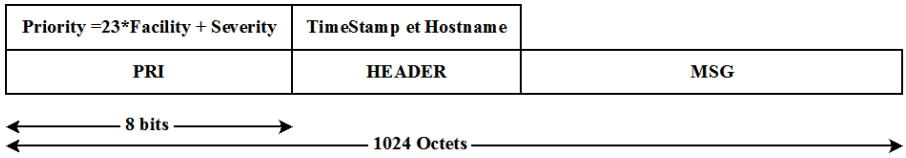
— **3164** : ***The BSD syslog Protocol*** datant de 2001http://www.faqs.org/rfcs/rfc3164.html et remplacé en 2009 par **5424** : ***The Syslog Protocol*** http://tools.ietf.org/html/rfc5424
— **3195** : ***Reliable Delivery for syslog*** datant de 2001 ***http://www.faqs.org/rfcs/rfc3195.html***
— **5425** : ***Transport Layer Security (TLS) Transport Mapping for Syslog*** datant de 2009 http://tools.ietf.org/ht
— **5426** : ***Transmission of Syslog Messages over UDP*** datant de 2009 http://tools.ietf.org/html/rfc5426
— **6587** : ***Transmission of Syslog Messages over TCP*** datant de 2012 https://tools.ietf.org/html/rfc6587

C'est un protocole en mode **texte** utilisant uniquement les caractères ASCII.

Par défaut, il s'appuie sur le protocole **UDP** et le **port 514** mais peut aussi s'appuyer sur **TCP** sur le port **6514** et même en **TLS** via **SSL**

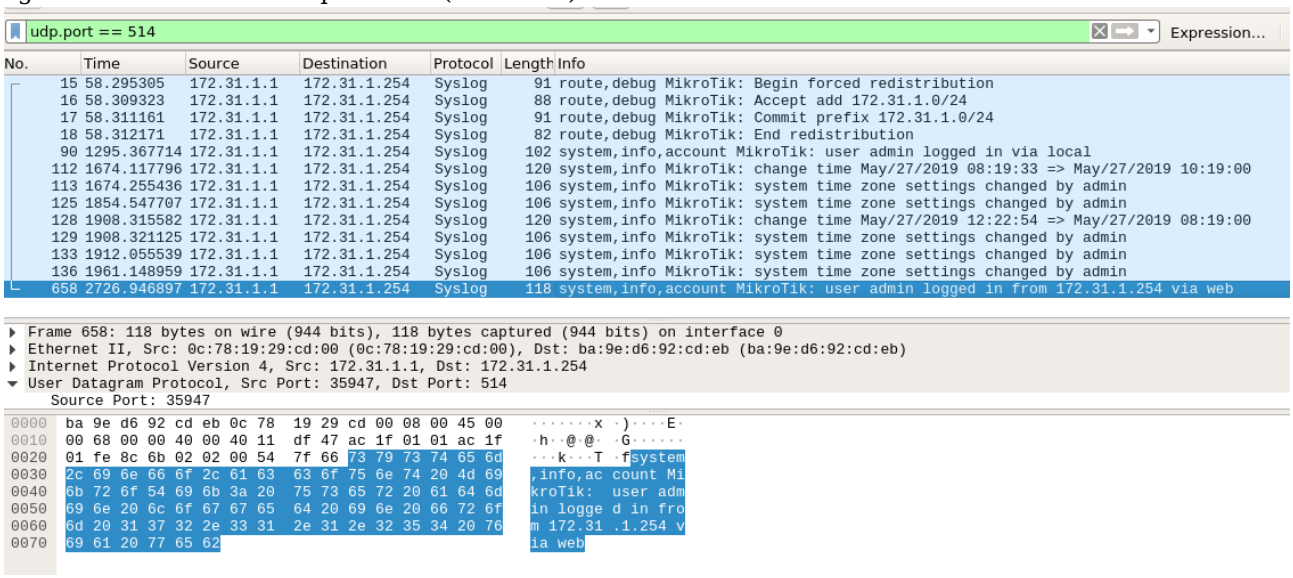
2. Non non, nous n'allons pas mettre des caméras de surveillance sur chaque lien, chaque matériel et chaque utilisateur !

La longueur totale d'une trame Syslog ne doit pas dépasser 1024 octets.
Une trame de protocole Syslog est composée de 3 parties :

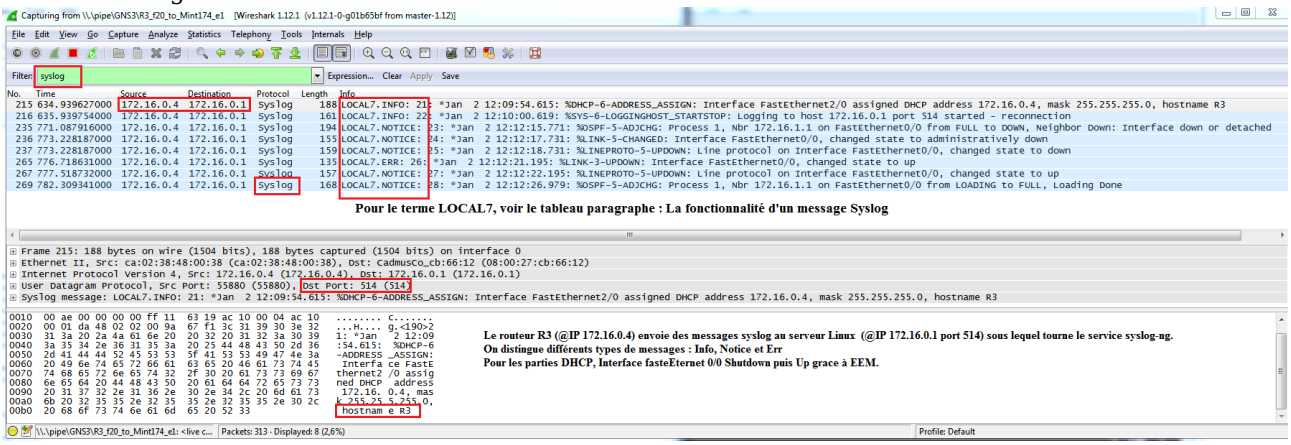


1. La partie **PRI**, composée obligatoirement de 3, 4 ou 5 caractères, contient un nombre représentant la **priorité**, codée en base 10, du message
2. La partie **HEADER**, contient 2 champs :
   (a) **HOSTNAME** peut contenir un nom de machine, une @ IPv4 ou IPv6 ou rien
   (b) **TIMESTAMP Mmm dd hh :mm :ss** pour *Month, Day Hour :Minute :Second*
3. La partie **MSG** contient le message texte à transférer.

La figure suivante illustre ce protocole (voir le TP)



Même image mais avec un routeur Cisco !



3.2 Le message Syslog

Le message Syslog définit des notions de **fonctionnalité** (***facility***), de **sévérité** (***severity***) et de **priorité** (***priority***) dans la RFC 3164.

3.2.1 La fonctionnalité d'un message Syslog

Elle correspond au type d'applications générant le message Syslog.
Il y a 24 fonctionnalités définies par la RFC 3164, tel que le montre le tableau suivant

N°	Usage	N°	Usage
0	***kernel messages***	9	***clock daemon***
1	***user-level messages***	10	***security/authorization messages***
2	***mail system***	11	***FTP daemon***
3	***system daemons***	12	***NTP subsystem***
4	***security/authorization messages***	13	***log audit***
5	***messages generated internally by syslogd***	14	***log alert***
6	***line printer subsystem***	15	***clock daemon***
7	***network news subsystem***	16 à 23	***local use 0*** jusqu'à ***local use 7***
8	***UUCP subsystem***		

3.2.2 La sévérité d'un message Syslog

Elle correspond au degré d'urgence ou d'importance du message Syslog. Elle est décidée par l'application qui envoie le message Syslog.

Il y a 8 niveaux de priorité, tel que le montre le tableau suivant

Niveau	Alias système	Signification	Meaning : pour Cisco ! ! !
0	**EMERG**	Le système est inutilisable.	***System is unusable.***
1	**ALERT**	Une action doit être prise immédiatement.	***Immediate action needed.***
2	**CRIT**	Problème critique.	***Critical conditions.***
3	**ERR**	Erreur	***Error conditions.***
4	**WARNING**	Avertissement.	***Warning conditions.***
5	**NOTICE**	Normal mais nécessite une attention particulière	***Normal but significant conditions.***
6	**INFO**	Information standard.	***Informational messages.***
7	**DEBUG**	Trace de débogage du noyau.	***Debugging messages.***

3.2.3 La priorité d'un message Syslog

Elle est définie par la fonctionnalité et la sévérité vues précédemment.

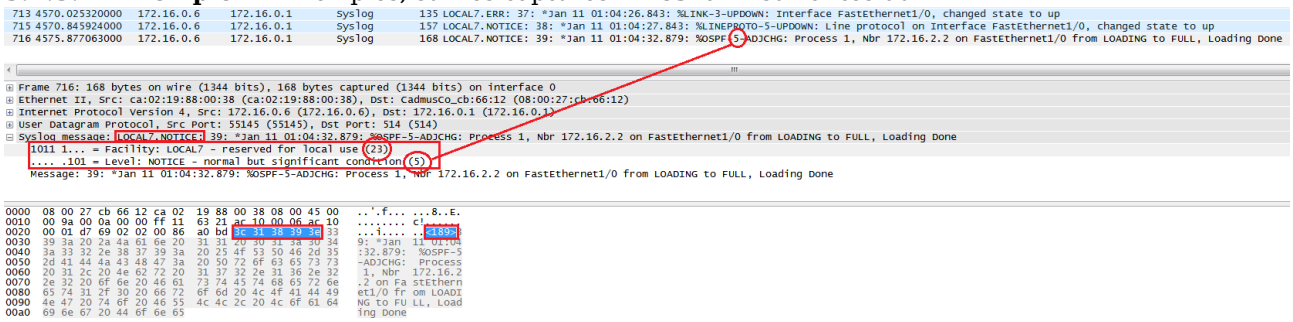
C'est est un nombre dont la valeur est le résultat d'une équation mathématique pas trop compliquée[3]

$$priorité = 8 * fonctionnalité + sévérité$$

Comment retrouver la fonctionnalité et la sévérité quand on connait la priorité.

Et bien il faut résoudre une équation à 2 inconnues[4]

3.2.3.1 Exemple 1 Exemples, sur les captures *wireshark* suivantes du TP-EEM



Ici la priorité, codée **31 38 39** en code ASCII, 3c et 3e étant les codes ASCII des signes < et >, a pour valeur189

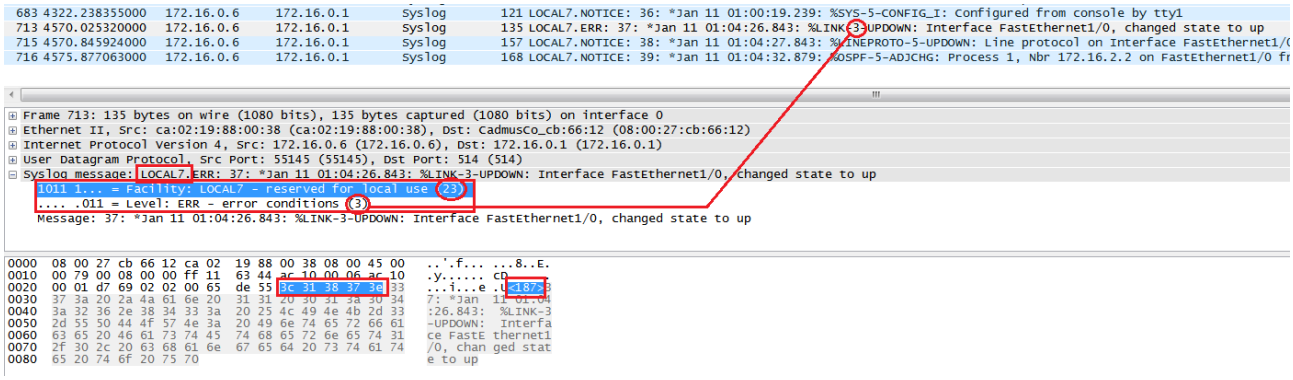
$$189\, mod\, 8 = 23\, reste\, 5$$

— la fonctionnalité vaut 23 : **local Use 7**

— la sévérité vaut **5** : **NOTICE** *Normal but significant conditions,* ici juste une information d'adjacence OSPF

3. Syslog a été définie par et pour des personnes pragmatiques ☺
4. Dans le monde des maths, c'est infaisable ou indéterminé, dans le monde des pragmatiques, on cherche et on trouve ☺

3.2.3.2 Exemple 2



Ici la priorité, codée **31 38 37** en code ASCII, 3c et 3e étant les codes ASCII des signes < et >, a pour valeur **187**

$$187\, mod\, 8 = 23\, reste\, 3$$

— la fonctionnalité vaut 23 : **local Use 7**

— la sévérité vaut **3** : **ERROR**, ici juste une interface ***Up***

Remarque : La priorité maximale est de 191, car la fonctionnalité la plus grande définie est 23 et la sévérité la plus grande est 7 : (23 * 8) + 7 = 191.

$$191 = 23 * 8 + 7$$

Le terme priorité porte à confusion, en effet, un message de priorité importante ne sera pas traité ou acheminé plus rapidement qu'un message de moindre priorité.

3.3 Lire les fichiers log

Voir le chapitre ? ? ? un peu plus loin

4 UDP vs TCP ?

Il est possible de ne pas s'appuyer sur le protocole UDP pour Syslog, mais de prendre le protocole TCP et de choisir son port spécifique

— Tout comme Syslog, UDP est un protocole orienté messages.
Un envoi sur le réseau correspond à une et une seule réception réseau, ce qui veut dire qu'une trame Syslog sur UDP est envoyée en un seul paquet IP et que ce paquet sera reçu en un seul bloc
Donc nul besoin d'un quelconque mécanisme de synchronisation entre l'Agent et le Manager, UDP ne suit pas l'état des paquets ou des échanges entre 2 éléments actifs.

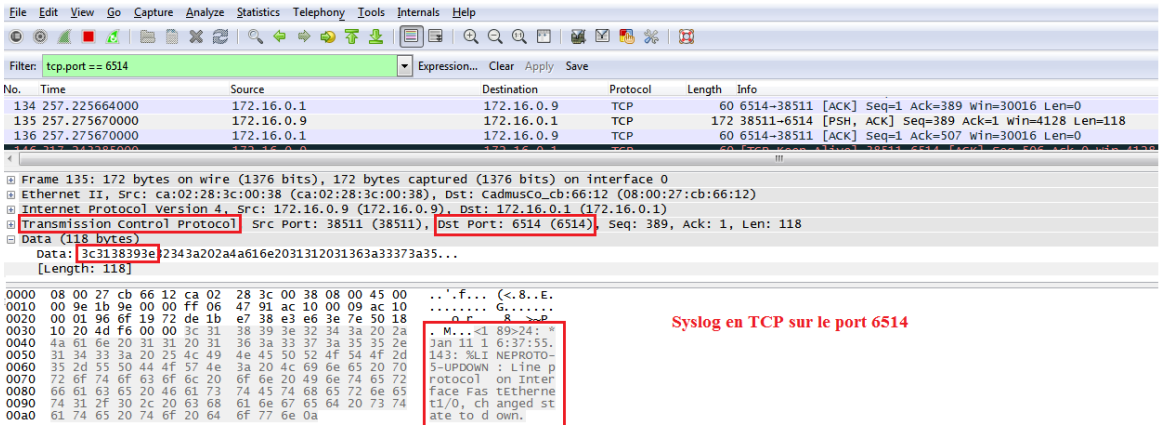
— TCP est un protocole orienté flux. Syslog étant orienté messages, la difficulté est d'extraire du flux TCP les différents messages Syslog. En TCP, la mécanique mise en place est totalement différente.
Un envoi peut correspondre à plusieurs réceptions et à plusieurs envois peut correspondre à une seule réception.
En TCP, il n'y a aucun lien entre le nombre d'envois et le nombre de réceptions.
Donc il y a nécessité d'avoir un mécanisme de synchronisation entre l'Agent et le Manager est nécessaire. TCP va chercher à savoir pour chaque paquet si celui-ci a bien été reçu tout cela engendrant des paquets supplémentaires par rapport à UDP.

Alors lequel choisir ?

Tout dépend des ressources disponibles, du nombre de clients et d'informations à gérer par le Manager et de l'importance que vous apporter aux logs par rapport au trafic.

Attention, la priorité doit être donné au trafic ! ! !

Voici ce que cela donne en capture wireshark, ici on a le lien *FastEthernet* 1/0 du routeur R3 qui est *Down*



Syslog en TCP sur le port 6514

Dans le fichier **/var/log/cisco.log**, on récupère :

monserveur log # tail cisco.log

Jan 11 16 :37 :52 172.16.0.9 : %OSPF-5-ADJCHG : Process 1, Nbr 172.16.2.2 on FastEthernet1/0 from FULL to DOWN, Neighbor Down : Interface down or detached

Jan 11 16 :37 :53 172.16.0.9 : %SYS-6-LOGGINGHOST_STARTSTOP : ***Logging to host 172.16.0.1 port 6514 started - reconnection***

Jan 11 16 :37 :54 172.16.0.9 : %LINK-5-CHANGED : ***Interface FastEthernet1/0, changed state to administratively down***

Jan 11 16 :37 :55 172.16.0.9 : %LINEPROTO-5-UPDOWN : Line protocol on Interface FastEthernet1/0, changed state to down

monserveur log #

5 La synchronisation des logs

Le champ TIMESTAMP est très important pour savoir quand a eu lieu l'évènement !

Pour cela Cisco préconise l'installation d'un serveur **NTP** et la synchronisation des horloges des routeurs et *switchs*.

It is recommended that you enable NTP throughout the network and system architecture to ensure proper timestamps are reported. This ensures that all incoming Syslog messages are synchronized so that you can effectively determine the correct time and correlation of incoming events.

En effet, si on désire savoir précisément à quel moment l'évènement, ayant donné naissance à un log, a eu lieu, il faut que tous les systèmes qui communiquent leurs logs au manager soient tous synchronisés.

Pour cela on utilise le protocole **NTP** *Network Time Protocol* qui donne l'heure, un peu comme le téléphone portable pour un étudiant...

5.1 Sous Linux

Pas difficile..., attention à ne pas confondre avec **ntpdate** ! ! !

1. ***monserveur CA # apt-get install ntp***
2. Fichier conf ***/etc/ntp.conf*** etc...
3. La suite ici : http://doc.ubuntu-fr.org/ntp

Ainsi, notre serveur Linux pourra servir de serveur temps au routeur.

Il est possible de modifier la date sous GNU/Linux, mais cela peut engendrer un dysfonctionnement au niveau des services et rendre le système instable !

Les ordinateurs actuelles possèdent une horloge interne qui conserve la date et l'heure, quand la machine est hors-tension. Elle est appelée, horloge BIOS, horloge CMOS, ou RTC (*Real Time Clock*).

Lors du démarrage, Linux initialise sa propre horloge système avec l'heure stockée dans le RTC. Une interruption "timer", mise en place au démarrage, incrémente régulièrement l'horloge système, qui n'est rien d'autre qu'une adresse mémoire. Le contenu de celle-ci peut être affiché avec la commande date.

Pour modifier la date, c'est la commande date...

Exemple : date 091516482345 donne 16h48 15 septembre 2345 [5]

Attention, avec VirtualBox, c'est l'horloge du Host qui est prise en compte ! ! !

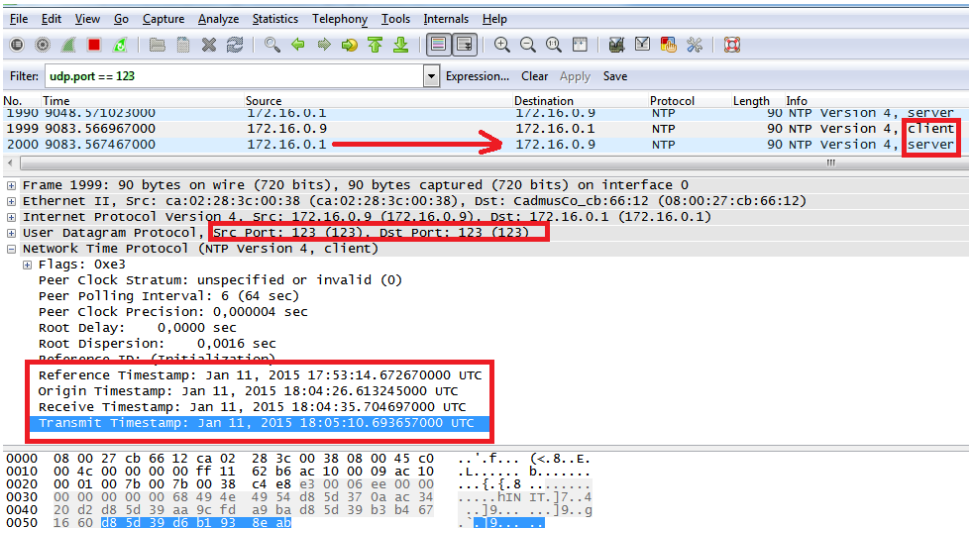
5. Je sais, j'ai un peu d'avance...

5.2 Cisco

Une commande facile à comprendre

— Rx(config) ***ntp server source @IP du serveur***

Et voici ce que cela donne



6 Syslog vs SNMP [6]

One of the most common questions about Syslog is : "Can't I just turn on SNMP traps and forget about Syslog ?"

The simple answer is : ***no****.*

In general, there are significantly more Syslog messages available within IOS as compared to SNMP Trap messages.

For example, a Cisco Catalyst 6500 switch running Cisco IOS Software Release 12.2(18)SXF contains about

— ***90 SNMP trap*** *notification messages,*

— *but has* ***more than 6000 Syslog event messages****.*

If there is a choice to be made between using SNMP traps or Syslog, ***the logical answer is Syslog****.*

However, it's also important to recognize that messaging support varies by hardware platform, technology, and specific software release ; consequently, a truly robust and full-featured event management solution would take advantage of all event indicators. Where there are redundancies between SNMP traps and Syslog messages, de-duplication to eliminate excessive notices is necessarily part of the Syslog analysis process.

*Additionally, you may opt to send Syslog messages in a trap to your SNMP manager by using the "****snmp-server enable traps syslog****" command.*

http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-557812.html#wp9000

7 La pratique

Il faut bien, non ?

7.1 Mikrotik

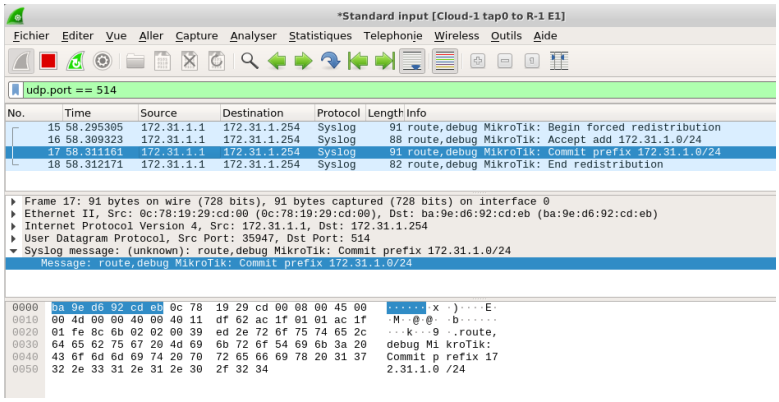
Les routeurs Mikrotik comme tous les autres routeurs des autres fabricants savent envoyer des logs !

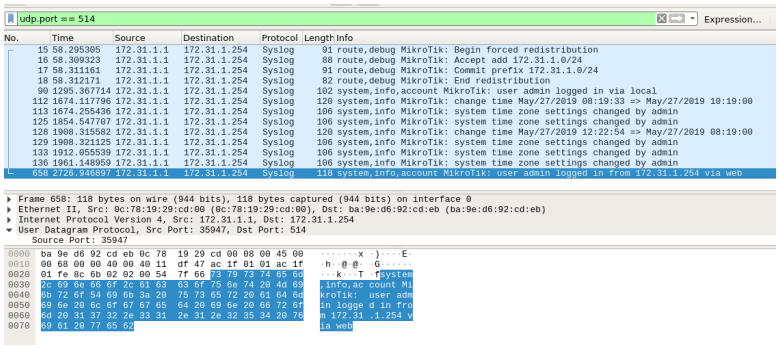
La coffiguration est très simple et vous ne devriez pas avoir de problème au TP

6. Je suis ni pour ni contre bien au contraire, puisque j'enseigne les 2 ☺


```
/interface bridge
add comment="La loopback L0" mtu=65535 name=l0
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no disabled=yes
set [ find default-name=ether2 ] disable-running-check=no
/system logging action
add name=ServeurLog remote=172.31.1.254 target=remote
/ip address
add address=1.1.1.1 interface=l0 network=1.1.1.1
add address=172.31.1.1/24 interface=ether2 network=172.31.1.0
/system clock
set time-zone-name=Europe/Paris
/system identity
set name=R1
/system logging
add action=ServeurLog prefix=R1 topics=event
```

Une Capture Wireshark doit vous donner cela !





Voici rapidement la conf d’un routeur pour les logs, facile à comprendre !

```
/system logging action
add name=ServeurLog remot
/ip address
add address=172.31.1.1/24
add address=1.1.1.1 inter
/snmp
set contact=pascal.fouger
    Campus2 src-address=1
    trap-interfaces=all t
/system clock
set time-zone-name=Europe
/system identity
set name=R1
/system logging
add action=ServeurLog pre
[admin@R1] >
```

Vous aurez à l'expliquer en TP !
Lors du TP sur les logs avec un routeur de type Mikrotik que nous ferons !
Patience ☺

7.2 Sous Linux

Lorsque le système démarre, fonctionne et effectue tout type d'action, ses actions et celles de la plupart de ses services sont **tracées** dans divers fichiers.

Deux services sont spécialisés dans la réception des messages à écrire dans ces fichiers :

1. **klogd** : ***kernel log daemon***, chargé de la gestion des informations émises par le noyau.
2. **syslogd** (remplacé par **syslogd**-ng) : ***system log daemon***, chargé de la gestion des informations émises par tout type de service et éventuellement le noyau.

7.2.1 klogd

Le service **klogd** gère les messages émis par le noyau. Il dispose de 2 sources d'accès aux messages :

1. le système de fichiers virtuel ***/proc***, utilisé par défaut s'il est présent, et notamment ***/proc/kmsg*** ;
2. les appels systèmes via l'API du noyau, notamment **sys_syslog**, si /proc est absent ou si le paramètre -s a été passé à ***klogd***.

Les messages du noyau ont 8 niveaux de priorité étagés de 0 (haute priorité) à 7 (message de débogage), voici leurs définitions.

Niveau	Alias système	Signification	Meaning : pour Cisco ! ! !
0	**EMERG**	Le système est inutilisable.	*System is unusable.*
1	**ALERT**	Une action doit être prise immédiatement.	*Immediate action needed.*
2	**CRIT**	Problème critique.	*Critical conditions.*
3	**ERR**	Erreur	*Error conditions.*
4	**WARNING**	Avertissement.	*Warning conditions.*
5	**NOTICE**	Normal mais nécessite une attention particulière	*Normal but significant conditions.*
6	**INFO**	Information standard.	*Informational messages.*
7	**DEBUG**	Trace de débogage du noyau.	*Debugging messages.*

— Le service **klogd** renvoie les messages de niveau 0 à 6 à **syslogd** qui redirigera ceux-ci dans les fichiers de logs se trouvant dans le répertoire ***/var/log*** et éventuellement sur les consoles concernées. Les informations de débogage de niveau 7 ne sont pas tracées par défaut.
— Le service **syslogd** (ou **syslog-ng**) reçoit les messages issus des services mais aussi de **klogd**. Il les dispatche ensuite selon l'émetteur, la sévérité, dans des fichiers, des consoles, sous forme de mails aux utilisateurs du système, ***root*** par exemple.
— Les actions les plus courantes sont l'écriture des logs dans des fichiers et la redirection de messages sur une console ou l'envoi de messages à ***root***.

Remarques

Avec les distributions actuelles, le service **klogd** n'est pas installé par défaut. En effet, il est en conflit avec **syslog-ng** et les 2 ne peuvent pas être installés parallèlement.

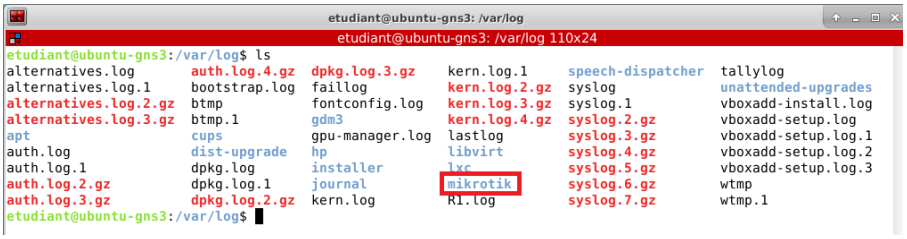
Pour installer **klogd** : ***apt-get install busybox-syslogd***
renvoie
monserveur CA # apt-get install busybox-syslogd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants seront ENLEVES :
syslog-ng syslog-ng-core syslog-ng-mod-json syslog-ng-mod-mongodb
syslog-ng-mod-sql
Si syslog-ng est déjà installé ! ! !
Je vous conseille d'utiliser syslog-ng ! ! !

7.2.2 Les fichiers de traces (log)

Les logs systèmes sont situés par convention dans le répertoire ***/var/log***. Tous les logs de ce répertoire ne proviennent pas obligatoirement de **syslogd**. C'est le cas par exemple des informations de connexion. Voici un exemple du contenu de ce répertoire. Il contient plusieurs fichiers textes et des répertoires.

Des **services** peuvent concentrer et écrire leurs messages dans cette arborescence, sans passer par **syslogd** !

L'image suivante représente une liste non exhaustive des fichiers de log d'une distribution Mint 17.4 fonctionnant en machine virtuelle sous VirtualBox.

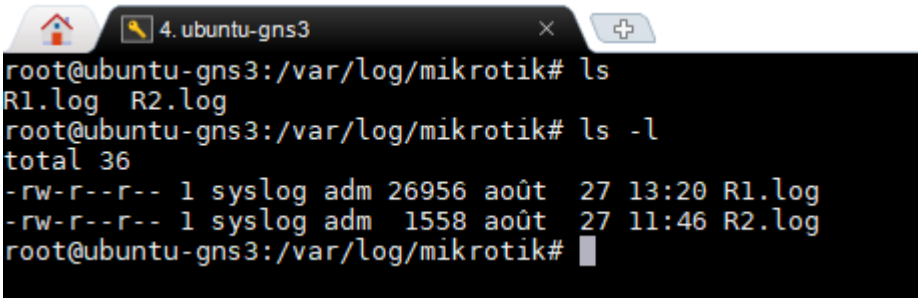


On peut y voir quelques fichiers et répertoires facilement identifiables :

auth.log : le journal des authentifications.

bootstrap.log : le journal de ce qui s'est passé au ***boot*** (démarrage)

Mikrotik : le répertoire journal des routeurs Mikrotik (voir le TP)



kern.log : le journal du noyau

mail.log : le journal du du système de messagerie, mails

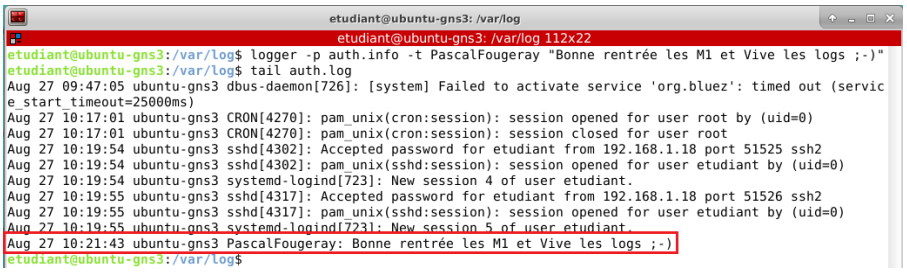
syslog : le journal du service syslog lui-même

user.log : le journal des processus des utilisateurs

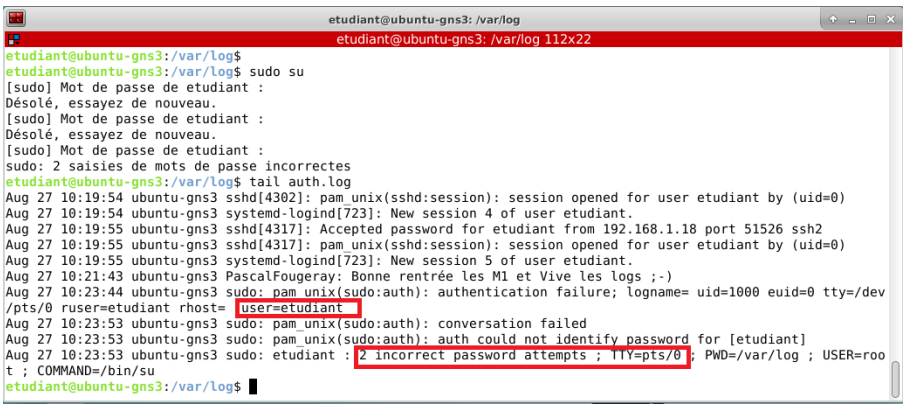
7.2.3 logger

La commande **logger** permet d'envoyer un message à ***syslog*** même connecté en tant que simple utilisateur

exemple : ***logger -p auth.info -t PascalFougeray "Bonne rentrée les M1 et Vive les logs ;-)"***
le résultat se trouve dans le fichier ***/var/log/auth.log*** que l'on peut lire à l'aide de la commande tail :
tail /var/log/auth.log donne :



Si on essaie de se loguer avec un mauvais mot de passe on peut le voir



7.2.4 Le format d'un message de log

Un journal au format syslog comporte dans l'ordre les informations suivantes :

— la date à laquelle a été émis le log,
— le nom de l'équipement ayant généré le log, ***hostname***,
— une information sur le processus qui a déclenché cette émission,
— le niveau de priorité du log,
— un identifiant du processus ayant généré le log
— un corps de message indiquant ce qui s'est passé.

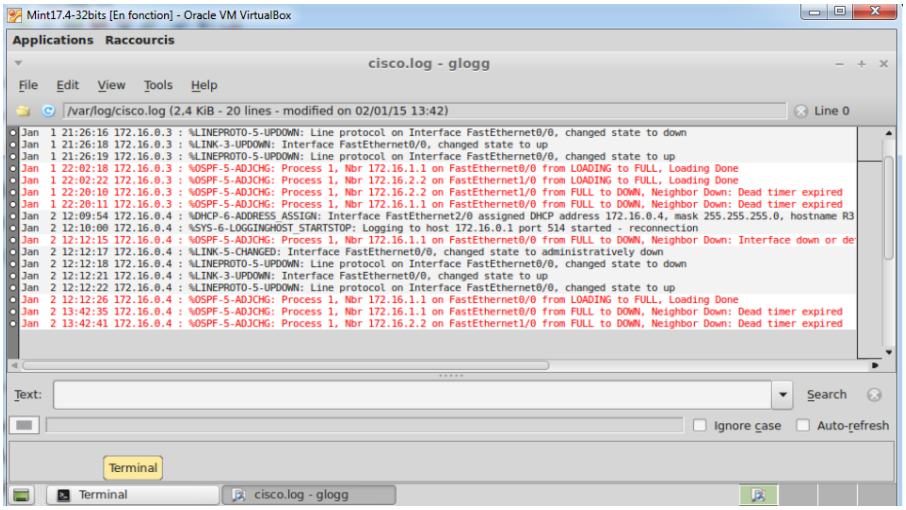
Exemple de message Syslog :

Message : 21 : *Jan 2 12 :09 :54.615 : %DHCP-6-ADDRESS_ASSIGN : Interface FastEthernet2/0 assigned DHCP address 172.16.0.4, mask 255.255.255.0, hostname R3

7.2.5 Lire un fichier log

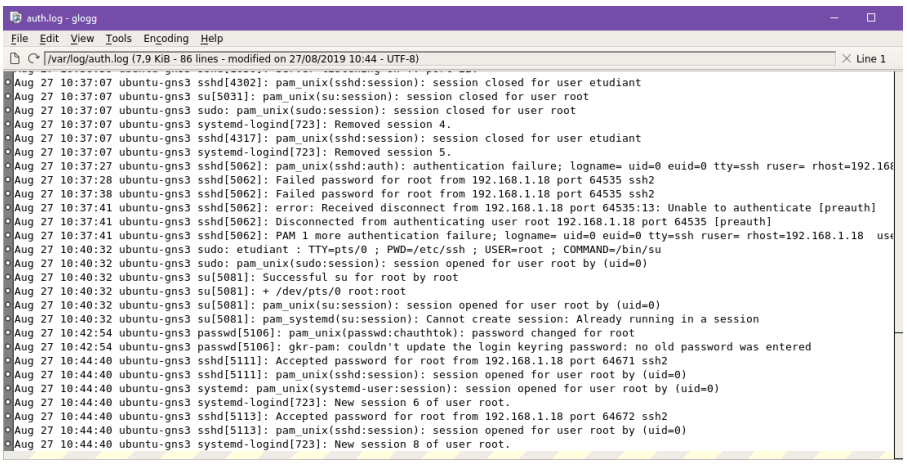
Il existe de nombreuse commandes sous Linux pour lire un fichier de logs.

— ***cat*** : pas terrible si le fichier est conséquent, tout défile...
— ***more*** & ***less*** pour le lire page par page
— ***head*** et ***tail***[7] : pour lire le début et la fin, commandes très pratiques et très utilisées, l'option ***-n*** permet d'indiquer le nombre de lignes à lire
  — ***head -n 5 /var/log/syslog*** : lit les 5 premières lignes,
  — ***tail -n 5 /var/log/syslog*** : lit les 5 dernières lignes,
  — ***tail -f -s 3 /var/log/syslog*** : (*f, follow* et *s, second*) recherche les changements toutes les 3 secondes.
— utilitaire ***glogg*** : **http://glogg.bonnefon.org/** fonctionne sous Windows & Linux.
  Ici la visualisation du journal ***/var/log/cisco.log*** avec coloration en rouge des traces contenant le ***tag OSPF***.



plus récent, **glogg** ouvert avec ***mobaxterm*** sous windows

7. tiens tiens, cela me rappel MPLS-TE ☺



7.2.6 Syslog-ng

Si vous voulez des informations !
En TP nous verrons **Rsyslog** !
Il n'y a aucune difficulté pour le configurer et l'installer, tout est sur le Net et vous savez lire... Mais voici qu'en même quelques explications

1. **Installer** : *monserveur CA # **apt-get install busybox-syslogd***
2. **Configurer** :
   (a) **Éditer** le fichier ***/etc/syslog-ng/syslog.conf***
   Exemple dans notre cas :
      i. Si en UDP : ajouter les lignes suivantes à la fin du fichier
      *source s_cisco { udp(ip(0.0.0.0) port(**514**)); };*
      *destination d_cisco { file("**/var/log/cisco.log**"); };*
      log { source(s_cisco); destination(d_cisco); };
      ii. si en TCP : ajouter les lignes suivantes à la fin du fichier
      *source s_cisco { tcp(ip(0.0.0.0) port(**6514**)); };*
      *destination d_cisco { file("**/var/log/cisco.log**"); };*
      log { source(s_cisco); destination(d_cisco); };
   (b) **Tester** la syntaxe en lançant la commande ***syslog-ng***, si tout est bon, elle ne renvoie rien sinon vous obtenez un message comme celui là

```
monserveur log # syslog-ng
Error parsing source, source plugin ppp not found in /etc/syslog-ng/syslog-ng.conf at line 165, column 18:

source s_cisco { ppp(ip(0.0.0.0) port(6514)); };
                 ^^^

syslog-ng documentation: http://www.balabit.com/support/documentation/?product=syslog-ng
mailing list: https://lists.balabit.hu/mailman/listinfo/syslog-ng
```

   ppp n'importe quoi c'est tcp bien sur ☺
3. Créer le fichier */var/log/**cisco.log***
4. **Lancer** le serveur : ***/etc/init.d/syslog-ng start***
5. **Vérifier** qu'il tourne en tâche de fond à l'aide de la commande de notre Président de la république

7.2.6.1 Syslog-ng VS syslog

Syslog-ng à remplacé syslog pour les raisons suivantes :

- Il offre en plus des fonctionnalités déjà offertes par syslog :
- La possibilité d'envoi et de réception des messages via le protocole TCP donc une meilleure fiabilité,
- Le filtrage et la répartition des messages avec des expressions régulières donc une plus grande flexibilité,
- Le chiffrement des échanges de messages entre les ressources via le protocole TLS donc une meilleure sécurité,
- La compatibilité avec IPv6, donc l'avenir est assuré,
- La compatibilité avec les bases de données de type SQL telles Mysql, PostgreSQL, Oracle, etc...

7.2.6.2 L'architecture de Syslog-ng

Syslog - NG peut fonctionner
- comme client par l'envoi des logs,
- comme serveur avec la réception des logs,
- comme ***relay*** en relayant des messages,
- ou à la fois comme client et serveur.

Si l'on désire centraliser et exploiter les logs dans un contexte sécurité, il faut modifier l'architecture en intégrant des modules tels :
- une base de données pour le stockage des logs,
- une interface Web pour l'exploitation facilitée des logs,
- une PKI (Public Key Infrastructure) pour la gestion des certificats et clefs,
- un ou plusieurs serveurs, d'où la notion de ***relay***
- un ou plusieurs clients.

Exemples de solutions :
- ***logzilla*** http://www.logzilla.net/index.php/download

7.2.7 Rsyslog

Voir le TP ou bien lire la doc ☺

7.3 Sous Windows

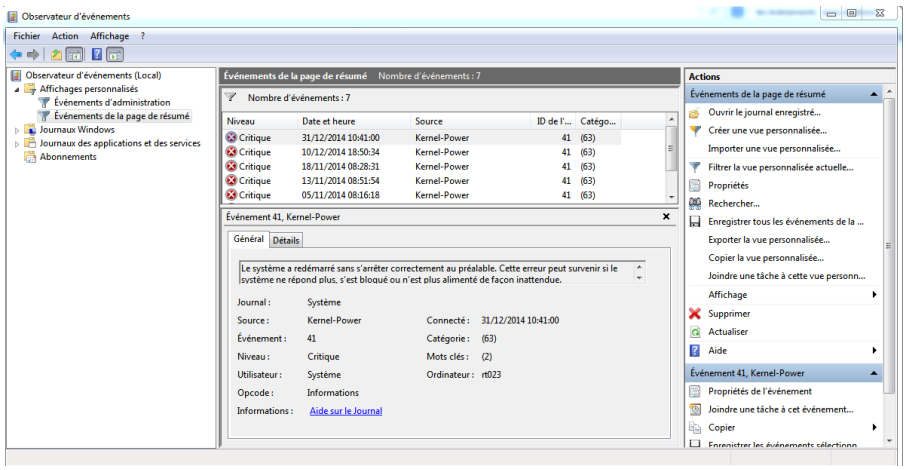
Windows client a 3 types de logs, un serveur tel Windows 2022 en a plus...
Mais pas le temps de traiter cette partie...
Si vous voulez l'insatller chez vous :
https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2022

1. Le log **Application** qui contient les évènements rapportés par les différentes applications installées.
   Se situe dans : ***%SystemRoot%\System32\Config\AppEvent.evt***
2. Le log **Sécurité** qui contient les évènements audités ainsi que ceux concernant la sécurité.
   Se situe dans : ***%SystemRoot%\System32\Config\SecEvent.evt***
3. Le log **Système** qui contient les évènements rapportés par les composants système tels les processus, le *kernel*, les *drivers*.
   Se situe dans : ***%SystemRoot%\System32\Config\SysEvent.evt***

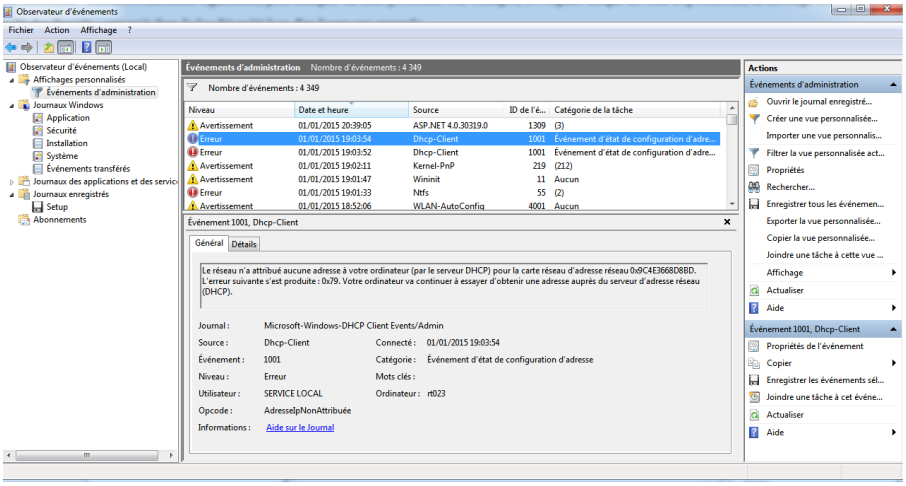
Chaque log peut contenir 5 types d'évènements :

1. ***Information*** - indique, par exemple, qu'une application, un driver, ou un service a démarré correctement. Un évènement de type information sera écrit dans la log.
2. ***Erreur*** - indique un problème, une perte de fonctionnalité ou une erreur pendant le démarrage. Par exemple, si un service ne démarre pas au démarrage, un évènement de type erreur sera écrit dans la log.
3. ***Avertissement*** - non nécessairement significatif, peut indiquer un futur problème. Par exemple, si l'espace disque devient trop restreint, un message d'avertissement apparaitra dans la log.
4. ***Audit des Succès*** - apparait dans la log Sécurité lors d'un *logon* par exemple.
5. ***Audit des Échecs*** - apparait dans la log Sécurité lors d'un *logon* par exemple, si un mauvais mot de passe a été saisi.

S'ouvre avec la commande : ***eventvwr.msc***



Les différents journaux



La liste complète des évènements est accessible par le menu de gauche

— **Journal des applications** : Il contient les évènements enregistrés par les applications ou les programmes. C'est le concepteur du programme qui décide quels évènement seront enregistrés ou non.
— **Journal de sécurité** : Garde en mémoire l'historique des ouvertures de sessions, l'ouverture et la suppression de certains fichiers et tout ce que l'administrateur de l'ordinateur
— **Journal du programme d'installation (configuration)** : Il contient les évènements relatifs à l'installation des applications.
— **Journal système** : Il contient les évènements enregistrés par les composants système de Windows comme par exemple l'échec du chargement d'un pilote ou d'un autre composant du système lors du démarrage.
— **Journal Évènements Transférés (Transmis)** : Il est utilisé pour stocker les évènements collectés depuis des ordinateurs distants.
— **Journaux des applications et des services** : Ils stockent des évènements provenant d'une application ou d'un composant isolé, plutôt que des évènements qui peuvent avoir un impact sur l'ensemble du système.

8 Conclusion

Les logs sont à l'administrateur système ce que SNMP est à l'administrateur réseau.
Dans certaines situations les 2 technologies/techniques servent pour la même architecture.

Donc que vous deveniez administrateur système, administrateur réseau ou bien les deux, ce qui est souvent le cas dans les "petites" infrastructures, vous devez connaitre ce domaine. ☺