

La gestion des journaux Informatiques

TutoJRES – 19 Juin 2008

- Julien Charpin -

Centre d'Océanologie de Marseille - CNRS



# CENTRALISATION DES LOGS AVEC SYSLOG-NG

# SOMMAIRE



- **INTRODUCTION**
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - Principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG (Monitoring graphique)**
  - Installation & configuration
  - Utilisation
- **CONCLUSION**

# SOMMAIRE



- **INTRODUCTION**
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - Principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG (Monitoring graphique)**
  - Installation & configuration
  - Utilisation
- **CONCLUSIONS**

# INTRODUCTION



- POURQUOI TRACER ?
  - > Contexte Juridique
- POURQUOI CENTRALISER ?
  - > Contexte technique

# INTRODUCTION



- CONTEXTE JURIDIQUE

- **Août 2004** -> Publication de la LCEN
- **Octobre 2004** -> Publication par le CNRS de la décision fixant un cadre réglementaire,
- **Février 2005** -> courrier adressé aux Directeurs d'Unité explicitant le dispositif.
  - Texte officiel sur la politique de gestion des traces ->  
[https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po\\_gest\\_traces.pdf](https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po_gest_traces.pdf)

# INTRODUCTION



- CONTEXTE JURIDIQUE
  - Texte décrivant le cadre réglementaire relatif à l'utilisation et à la conservation des "fichiers de journalisation" **en fonction du type de service audité** (*postes de travail, serveurs HTTP, serveurs SMTP, équipements réseaux, applications spécifiques ...*)
  - Entre autres choses définit une durée de **conservation maximale d'1 an.**

# INTRODUCTION



- CONTEXTE TECHNIQUE

- Situation existante :

- Plusieurs serveurs
    - Plusieurs services
    - => **beaucoup** de fichiers de logs

- Solution -> **Centraliser** car :

- Rationalisation
    - Élévation du niveau de sécurité
    - Simplification de la tâche de l'administrateur
    - Répondre plus facilement à une requête judiciaire ...

# INTRODUCTION



- Problématique locale au COM
  - **Plusieurs** serveurs (Samba/LDAP, HTTP, DNS, DHCP, SSH, FTP ...)
  - **2** sites distants/600 utilisateurs
- Solution retenue :
  - **Syslog-ng** car possibilité de trier avec plus de finesse les différents logs reçus sur un serveur



# SOMMAIRE



- INTRODUCTION
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, installation)
  - Principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG**
  - Installation & configuration
  - Utilisation
- CONCLUSION

# SYSLOG-NG : Présentation



Gestionnaire de journaux systèmes de nouvelle génération (**ng = new generation**), capable (entre autres) :

- de **filtrer** les messages en utilisant les expressions régulières
- d'envoyer/recevoir les logs sur le réseau via **UDP** ou **TCP**
- Compatible **IPV6**

# SYSLOG-NG : Disponibilité



- Sur la plupart des distributions sous forme de paquet (Debian, Red Hat, Mandriva ...)
- En téléchargement (format **tar.gz**) sur SOURCEFORGE (<http://sourceforge.net/projects/syslog-ng/>) ou chez BALABIT (<http://www.balabit.com/downloads/files/syslog-ng/sources/stable/>)

# SYSLOG-NG : Installation



- **Debian** : apt-get install syslog-ng
- **Red Hat** : yum install syslog-ng
- ...
- **Sources** : ./configure, make, make install  
pour la version tar.gz

# SOMMAIRE



- INTRODUCTION
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - Principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG**
  - Installation & configuration
  - Utilisation
- **CONCLUSION**

# SYSLOG-NG : Principes de base



## ***/etc/syslog-ng/syslog-ng.conf***

- Ce fichier de configuration est divisé en 5 parties qui sont :
  - options
  - sources
  - destinations
  - filtres
  - logs

# SYSLOG-NG : Principes de base



la configuration repose sur la définition, le nommage et le paramétrage d'**objets globaux**, définis dans le fichier de conf `syslog-ng.conf` et qui sont :

- **source** -> Définition de la provenance des messages de logs reçus par syslog-ng.
- **destination** -> Où et comment le message de log est-il envoyé (local ou distant) ?
- **filter** -> les messages ne seront envoyés vers la destination définie que s'ils "matchent" les règles de filtrage définies.
- **log** -> définit le traitement de chaque message de log reçu, en fonction des items **source**, **destination** et **filter**.

# SYSLOG-NG : Principes de base



- Rappel de la structure d'un message de logs :
  - 2 types d'information sont utilisés pour caractériser un message de log :
    - **priorité** (level) : *none, debug, info, notice, warning, error, crit, alert, emerg*
    - **type** (facilities) : *authpriv, cron, daemon, kern, local0 -> local7, lpr, mail, news, syslog, user, uucp, ftp,mark*



# SYSLOG-NG : Principes de base



- Architecture générale de la configuration syslog-ng :

Log = Source + filtre + destination

# SYSLOG-NG : Principes de base



```
<type> <identifiant> { <parameters> };
```

- 1er champ : **type** d'objet (*source, destination, filter, log*)
- 2ème champ : **identifiant** de l'objet (*s\_source1, d\_network, f\_filterdemo1, ...*)
- 3ème champ : liste de **paramètres** propres à chaque type d'objet.

# SYSLOG-NG : Principes de base



- Liste des champs paramètres :
  - les **drivers**
  - les **expressions**
  - les **flags**
  - les **Macros**

# SYSLOG-NG : Principes de base



- paramètres des objets : les **drivers**
  - propres au type d'objet **source** et **destination** permettant de spécifier des canaux de communication pour envoyer et recevoir des logs :
    - **source** : *internal()*, *unix-stream()*, *udp()*, *tcp()*, *udp6()*, *tcp6()* ...
    - **destination** : *file()*, *unix-stream()*, *tcp()*, *udp()*, *tcp6()*, *fifo()*, *pipe()*, *program()* ...



# SYSLOG-NG : Principes de base



- paramètres des objets : les **expressions**
  - propres au type **filter**, s'appliquent aux messages de logs reçus. Elles sont construites à partir de :
    - **fonctions** pré-définies : *host(regex)*, *match(regex)*, *program(regex)*, *facility*, *level(emerg, alert, err ...)*, ...
    - **parenthèses**
    - **des opérateurs booléens** : *and*, *or*, *not*

# SYSLOG-NG : Principes de base



- paramètres des objets : les **expressions**
  - exemple d'utilisation des expressions dans la construction des filtres :

```
filter f_demofilter1 {  
    host("host1") and match("deny"); };
```

```
filter f_demoregexp {  
    host("system.*1") and match("deny"); };
```

# SYSLOG-NG : Principes de base



- paramètres des objets : les **flags**
  - propres à l'objet **log**, permettent de modifier le fonctionnement type d'écriture des logs :
    - **final** : ne pas envoyer le message à une autre destination
    - **flow-control** : arrêter de lire le message provenant de cette source si la destination ne peut pas les accepter
    - ...



# SYSLOG-NG : Principes de base



- paramètres des objets : les **flags**
  - Exemple d'utilisation des flags :

```
log {  
    source(s_demo);  
    destination(d_tcp);  
    flags(flow-control); };
```

( = les logs provenant de la source "s\_demo" et envoyés vers la destination "d\_tcp" sont ignorés si la machine définie dans "d\_tcp" ne répond plus)

# SYSLOG-NG : Principes de base



- paramètres des objets : les **Macros**
  - fonctions internes de syslog-ng qui peuvent être utilisées pour construire des noms de fichiers de destination de logs.
    - **HOST , MONTH, DAY ...**

# SOMMAIRE



- INTRODUCTION
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - Principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG**
  - Installation & configuration
  - Utilisation
- **CONCLUSION**

# SYSLOG-NG : Config.Serveur (Options)



- Syslog-ng a un certain nombre d'**options** permettant de définir le comportement vis à vis du DNS, des droits et des permissions sur les fichiers et répertoires créés ...

Pour tout savoir :

- `man syslog-ng.conf`

# SYSLOG-NG : Config.Serveur (Options)



- Principales **options** :
  - **use\_dns** -> demande la résolution des noms DNS pour les machines qui envoient leurs logs,
  - **owner(...), group(...), perm(...), dir\_perm(...)** -> fixe la propriété et les permissions sur les fichiers et répertoires créés,
  - **sync(...)** -> permet de spécifier une taille du buffer pour diminuer l'activité du disque,
  - ...

# SYSLOG-NG : Config.Serveur (Options)



## • Exemple de déclaration d'**options** :

```
options {  
    sync(0);#Définir le nombre de lignes à "bufferiser"  
    create_dirs(yes);#Autoriser syslog-ng à créer des répertoires  
    group(adm);#les fichiers et répertoires appartiendront au  
        groupe adm  
    perm(0640);#définition des droits sur les fichiers  
    dir_perm(0755);#définition des droits sur les répertoires  
    use_dns(no);#Ne pas chercher à résoudre les noms DNS  
};
```

# SYSLOG-NG : Config.Serveur (Sources)



- Après les options, commence la configuration des objets globaux de syslog-ng avec la définition des **sources**
  - > Définit la provenance des logs reçus par syslog-ng
    - Interne (messages du kernel ...),
    - Réseau (udp ou tcp).

# SYSLOG-NG : Config.Serveur (Sources)



```
source s_all {  
    internal(); #messages internes syslog-ng  
    unix-stream("/dev/log");#Écouter le socket /dev/log  
    file("proc_kmsg" log_prefix("kernel: "));#Lire le  
        fichier proc_kmsg  
};  
  
source s_network { udp(); };#Écouter le port 514/UDP  
  
source s_network1 { udp(10.2.3.4); };#Écouter le port  
    514/UDP pour les messages de la machine 10.2.3.4  
  
source s_network2 { tcp(port(54230)); };#Écouter le port  
    54230/TCP  
  
source s_network3 { tcp(ip(10.2.3.4) port(54230)); };  
    #Écouter le port 54230/TCP pour la machine 10.2.3.4
```



# SYSLOG-NG : Config.Serveur (Destinations)



- les **destinations** permettent de définir les fichiers ou les cibles réseaux vers lesquelles on veut écrire les logs reçus. Pour cela, on dispose de drivers :
  - **file()** -> permet d'écrire dans un fichier,
  - **program()** -> permet d'appeler un programme externe (usr/bin/mysql ....),
  - **tcp(),udp()** -> on envoie les logs vers une destination réseau en TCP ou en UDP,
  - **tcp6(),udp6()** -> la même chose mais IPV6.

# SYSLOG-NG : Config.Serveur (Destinations)



- quelques **destinations** classiques

```
destination d_auth { file("/var/log/auth.log"); }  
;#Écrire dans le fichier spécifié
```

```
destination d_syslog { file("/var/log/syslog"); }  
;#Écrire dans le fichier spécifié
```

```
destination d_udp { udp("192.168.0.2"); };#Écrire vers  
la machine spécifié sur port 514/UDP
```

```
destination d_tcp { tcp("192.168.0.2") port(1999); }  
;#Écrire vers la machine spécifiée sur le port  
1999/TCP
```

# SYSLOG-NG : Config.Serveur (Destinations)



- exemple de définition de **destination** vers une base MySQL :

```
destination d_mysql {  
    program("/usr/bin/mysql -usyslogadmin -psyslogadmin syslog"  
    template("INSERT INTO logs (host, facility, priority, level, tag,  
        datetime, program, msg)  
    VALUES ( '$HOST', $FACILITY, '$PRIORITY', '$LEVEL', '$TAG',  
        '$YEAR-MONTH-$DAY' $HOUR:$MIN:$SEC', '$PROGRAM',  
        '$MSG');\n")  
    template-escape(yes)); }
```

# SYSLOG-NG : Config.Serveur (Macros)



Syslog-ng dispose d'un mécanisme de **Macros** qui sont substituées par leur valeur lorsqu'un message de log est traité :

- **HOST** : donne le nom de la machine source
- **YEAR, MONTH, DAY** : donnent les informations de date
- **STAMP** : timestamp formaté
- **PRIORITY** : niveau de gravité du message,
- **FACILITY** : Facilité du message
- **PROGRAM** : le nom du programme qui envoie le message
- **PID** : le PID du programme qui envoie le message
- ...

# SYSLOG-NG : Config.Serveur (Macros)



- Utilisation dans la construction des noms de fichiers de destination :

**destination** d\_archivage {

```
file("/var/log/syslog-  
ng/$YEAR.$MONTH.$DAY/$HOST/messages")
```

```
}; #Écrire dans `date`/`hostname`/messages
```

**destination** df\_facility\_dot\_info

```
{ file("/var/log/$FACILITY.info"); }; #Écrire dans un fichier  
nom_de_la_facilité.info
```

```
pcsic6:/var/log/syslog-ng# ls
2007.11.28 2008.01.08 2008.02.06 2008.03.06 2008.04.04 2008.05.03
2007.11.29 2008.01.09 2008.02.07 2008.03.07 2008.04.05 2008.05.04
2007.11.30 2008.01.10 2008.02.08 2008.03.08 2008.04.06 2008.05.05
2007.12.01 2008.01.11 2008.02.09 2008.03.09 2008.04.07 2008.05.06
2007.12.02 2008.01.12 2008.02.10 2008.03.10 2008.04.08 2008.05.07
2007.12.03 2008.01.13 2008.02.11 2008.03.11 2008.04.09 2008.05.08
2007.12.04 2008.01.14 2008.02.12 2008.03.12 2008.04.10 2008.05.09
2007.12.05 2008.01.15 2008.02.13 2008.03.13 2008.04.11 2008.05.10
2007.12.06 2008.01.16 2008.02.14 2008.03.14 2008.04.12 2008.05.11
2007.12.07 2008.01.17 2008.02.15 2008.03.15 2008.04.13 2008.05.12
2007.12.08 2008.01.18 2008.02.16 2008.03.16 2008.04.14 2008.05.13
2007.12.09 2008.01.19 2008.02.17 2008.03.17 2008.04.15 2008.05.14
2007.12.10 2008.01.20 2008.02.18 2008.03.18 2008.04.16 2008.05.15
2007.12.11 2008.01.21 2008.02.19 2008.03.19 2008.04.17 2008.05.16
2007.12.12 2008.01.22 2008.02.20 2008.03.20 2008.04.18 2008.05.17
2007.12.13 2008.01.23 2008.02.21 2008.03.21 2008.04.19 2008.05.18
2007.12.14 2008.01.24 2008.02.22 2008.03.22 2008.04.20 2008.05.19
2007.12.15 2008.01.25 2008.02.23 2008.03.23 2008.04.21 2008.05.20
2007.12.16 2008.01.26 2008.02.24 2008.03.24 2008.04.22 2008.05.21
2007.12.17 2008.01.27 2008.02.25 2008.03.25 2008.04.23 2008.05.22
2007.12.18 2008.01.28 2008.02.26 2008.03.26 2008.04.24 2008.05.23
2007.12.19 2008.01.29 2008.02.27 2008.03.27 2008.04.25 2008.05.24
2007.12.20 2008.01.30 2008.02.28 2008.03.28 2008.04.26 2008.05.25
2007.12.21 2008.01.31 2008.02.29 2008.03.29 2008.04.27 2008.05.26
2008.01.03 2008.02.01 2008.03.01 2008.03.30 2008.04.28 2008.05.27
2008.01.04 2008.02.02 2008.03.02 2008.03.31 2008.04.29 2008.05.28
2008.01.05 2008.02.03 2008.03.03 2008.04.01 2008.04.30
2008.01.06 2008.02.04 2008.03.04 2008.04.02 2008.05.01
2008.01.07 2008.02.05 2008.03.05 2008.04.03 2008.05.02
pcsic6:/var/log/syslog-ng# ll 2008.04.03
total 20
drwxr-xr-x 2 root root 4096 2008-04-03 00:08 139.124.2.103
drwxr-xr-x 2 root root 4096 2008-04-03 00:10 139.124.2.105
drwxr-xr-x 2 root root 4096 2008-04-03 00:07 139.124.2.107
drwxr-xr-x 2 root root 4096 2008-04-03 00:02 139.124.2.2
drwxr-xr-x 2 root root 4096 2008-04-03 11:46 139.124.2.9
pcsic6:/var/log/syslog-ng# ll 2008.04.03/139.124.2.107/
total 184
-rw-r----- 1 root adm 180528 2008-04-03 23:58 reseau.log
pcsic6:/var/log/syslog-ng#
```

# SYSLOG-NG : Config.Serveur (Filtres)



Permettent de créer des règles de filtrage : un message de log donné ne sera dirigé vers une destination donnée que s'il "matche" la règle de filtrage :

```
filter f_auth { facility(auth, authpriv); }; #On ne
garde que si la facilité est "auth" ou "authpriv"

filter f_syslog { not facility(auth, authpriv); };#Le
conraire ...

filter f_messages {
    level(info, notice, warn)
    and not facility(cron);
};#On garde si le niveau est 'info', 'notice' ou
'warn' et si la facilité n'est pas 'cron'
```

# SYSLOG-NG : Config.Serveur (Log)



- On peut maintenant construire les directives **log**. Chaque message est susceptible d'être traité par toutes les directives **log** présente dans le fichier :

```
log {  
    source(s_all);#messages provenant de cette source,  
    filter(f_auth);#si correspondent à ce filtre,  
    destination(d_auth);#sont envoyés vers cette dest  
};
```

```
log {  
    source(s_all);#messages provenant de cette source,  
    filter(f_messages);#si correspondent à ce filtre,  
    destination(df_messages);#sont envoyés vers cette  
    dest
```

```
};
```



# SYSLOG-NG : Config.Serveur (Log)



- Dans cet exemple on logge 2 fois le même message de log vers 2 destinations différentes.

```
log {  
    source(s_network);#logs provenant du réseau,  
    destination(d_archivage);#sont envoyés vers cette  
        destination  
};  
  
log {  
    source(s_network);#logs provenant du réseau,  
    destination(d_mysql);#sont écrits vers cette base  
        MySQL  
};
```

# SOMMAIRE



- **INTRODUCTION**
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG**
  - Installation & configuration
  - Utilisation
- **CONCLUSION**

# SYSLOG-NG : Config.Client

## Linux



### Syslog :

Configurer pour la redirection des logs (**514/UDP**)  
avec par exemple la ligne suivante dans  
**/etc/syslog.conf** :

```
...  
#Redirection vers loghost  
*. * @10.1.2.3  
auth,authpriv.* -/var/log/syslog  
*.*;auth,authpriv.none -/var/log/syslog  
...
```

On peut envoyer les logs vers une machine  
distante **et** continuer à tracer dans des fichiers  
locaux.

# SYSLOG-NG : Config.Client

## Linux



- **Syslog-ng :**

- 1) Définir les sources

```
source s_local { unix-stream("/dev/log"); };
```

- 2) Définir une destination

```
destination d_network { udp("@loghost"); };
```

- 3) Définir (éventuellement) un filtre

- 4) Définir le traitement du message de log

```
log {
```

```
source(s_local);#les logs de cette machine,
```

```
destination(d_network);#seront envoyés vers un  
serveur syslog
```

```
};
```

# SYSLOG-NG : Config.Client

## Windows



- Observateur d'évènements -> *Pas prévu par défaut*
- **Snare** (Open Source) d'Interselect Alliance -> Redirection vers Syslog ou Syslog-ng
  - Clients NT/2000/XP/2003
  - Spécification du **serveur** et du **port** via l'interface web d'administration sur port 6161



**Latest Events**

- Network Configuration
- Remote Control Configuration
- Objectives Configuration
- View Audit Service Status
- Apply the Latest Audit Configuration**

Local Users  
Domain Users  
Local Group Members  
Domain Group Members  
Registry Dump

# SNARE Network Configuration

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	<input type="text"/>
Destination Snare Server address	10.1.2.3
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input checked="" type="checkbox"/>
Export Snare Log data to a file?	<input type="checkbox"/>
Enable active USB auditing? (This option requires the service to be fully restarted)	<input type="checkbox"/>
Enable SYSLOG Header?	<input checked="" type="checkbox"/>
SYSLOG Facility	User
SYSLOG Priority	Notice

Change Configuration Reset Form

- Gestion de l'ordinateur (local)
  - Outils système
    - Observateur d'événements
    - Dossiers partagés
    - Utilisateurs et groupes locaux
    - Journaux et alertes de performance
    - Gestionnaire de périphériques
  - Stockage
    - Stockage amovible
    - Défragmenteur de disque
    - Gestion des disques
  - Services et applications
    - Services
    - Contrôle WMI
    - Service d'indexation

### Services

#### SNARE

[Arrêter le service](#)  
[Redémarrer le service](#)

Description :  
 Snare is a program that facilitates the central collection and processing of Windows NT/2000/XP/2003 Event Log information. All three primary event logs (Application, System and Security) are monitored, and the secondary logs (DNS, Active Directory, and File Replication) are monitored if available. Event information is converted to tab delimited text format, then delivered to a remote server.

Nom	Description	État	Type de démarrage	Ouvrir une session en tant que
Onduleur	Gère un on...		Manuel	Service local
Ouverture de sessi...	Prend en c...	Déma...	Automatique	Système local
Pare-feu Windows ...	Assure la t...	Déma...	Automatique	Système local
Partage de Bureau ...	Permet à u...		Manuel	Système local
Planificateur de tâc...	Permet à u...	Déma...	Automatique	Système local
Plug-and-Play	Permet à l'...	Déma...	Automatique	Système local
QoS RSVP	Fournit la s...		Manuel	Système local
Routage et accès d...	Offre aux ...		Désactivé	Système local
SavRoam	Symantec ...		Manuel	Système local
Serveur	Prend en c...	Déma...	Automatique	Système local
Serveur d'impressio...	Fournit un ...		Manuel	Système local
Service COM de gr...	Gère le gra...		Manuel	Système local
Service d'administr...	Configure l...	Déma...	Manuel	Système local
Service d'approvisi...	Gère les fic...		Manuel	Système local
Service de découve...	Active la d...	Déma...	Manuel	Service local
Service de la passe...	Offre la pri...	Déma...	Manuel	Service local
Service de numéro ...	Extrait le n...		Manuel	Système local
Service de rapport ...	Active le ra...	Déma...	Automatique	Système local
Service de restaura...	Effectue d...	Déma...	Automatique	Système local
Service de transfer...	Transfère ...		Manuel	Système local
Service d'indexation	Construit u...		Manuel	Système local
Service Gestion des ...	Gère les ce...		Manuel	Système local
Service Protocole E...	Fournit au...		Manuel	Système local
Services de crypto...	Fournit troi...	Déma...	Automatique	Système local
Services IPSEC	Gère la str...	Déma...	Automatique	Système local
Services Terminal S...	Permet à pl...	Déma...	Manuel	Système local
SNARE	Snare is a ...	Déma...	Automatique	Système local
Spouleur d'impression	Charge de...	Déma...	Automatique	Système local
Station de travail	Crée et ma...	Déma...	Automatique	Système local
Stockage amovible			Manuel	Système local
Symantec AntiVirus	Fournit des...	Déma...	Automatique	Système local
Symantec AntiVirus...	Contrôle et...	Déma...	Automatique	Système local
Symantec Event M...	Event prop...	Déma...	Automatique	Système local
Symantec Network ...	Symantec ...		Manuel	Système local
Symantec Settings ...	Settings st...	Déma...	Automatique	Système local
Symantec SPBBCSvc	Symantec ...	Déma...	Automatique	Système local
Système d'événem...	Prend en c...	Déma...	Manuel	Système local
Téléphonie	Fournit la p...	Déma...	Manuel	Système local

**Network Configuration**

**Remote Control Configuration**

**Objectives Configuration**

**View Audit Service Status**

**Apply the Latest Audit Configuration**

Local Users  
 Domain Users  
 Local Group Members  
 Domain Group Members  
 Registry Dump

# SNARE Filtering Objectives Configuration

The following filtering objectives of the SNARE unit are active:

Action Required	Criticality	Event ID Include/Exclude	Event ID Match	User Include/Exclude	User Match	General Match	Return	Event Src
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Information	Include	Logon_Logoff	Include	*	*	Success Failure Error Information Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Clear	Include	Process_Events	Include	*	cmd.exe	Success Failure Error Information Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Warning	Include	User_Group_Management_Events	Include	*	*	Success Failure Error Information Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Information	Include	Reboot_Events	Include	*		Success Failure	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Priority	Include	Security_Policy_Events	Include	*		Success Failure Error Information Warning	Security
<input type="button" value="Delete"/> <input type="button" value="Modify"/>	Information	Include	*	Include	*		Success Failure Error Information Warning	System Application

Select this button to add a new objective.



# SYSLOG-NG : Config.Client

## Windows



### Windows (Sortie Snare) :

```
Wed Jan 30 15:10:33 2008      593  Security      charpin.j
  User Success Audit PORT-JULIEN  Suivi détaillé      Un
  processus est terminé :  Id. du processus : 864  Nom du fichier
  image : C:\WINDOWS\system32\cmd.exe  Utilisateur : charpin.j
  Domaine : PORT-JULIEN  Id. d'ouv. de session :
  (0x0,0x21AEDA)      0

Jan 30 15:10:39 139.124.2.9 MSWinEventLog      1      Application
  2      Wed Jan 30 15:10:31 2008      108    SNARE  Unknown
  User N/A Information PORT-JULIEN  None      The
  service was stopped.      0
```

# PHP-SYSLOG-NG



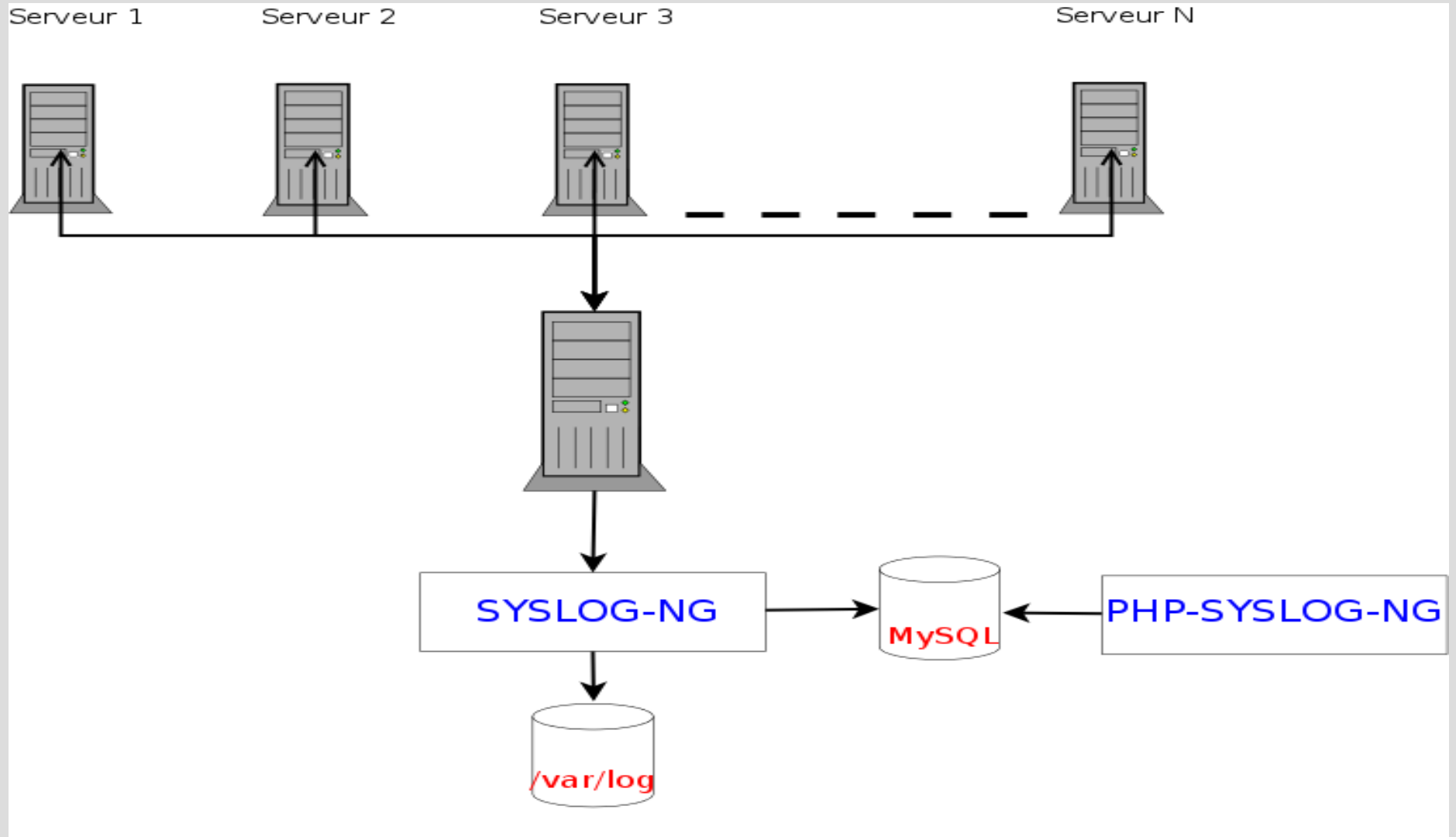
Outil Graphique de  
surveillance des LOGS

# SOMMAIRE



- **INTRODUCTION**
- **SYSLOG-NG**
  - Présentation (possibilités, téléchargement, install)
  - principes généraux
  - Configuration serveur
  - Configuration client
- **PHP-SYSLOG-NG**
  - Installation & configuration
  - Utilisation
- **CONCLUSION**

# PHP-SYSLOG-NG : Principe de fonctionnement



# PHP-SYSLOG-NG



- GÉNÉRALITÉS
  - GNU Général Public Licence V2
- TÉLÉCHARGEMENT
  - <http://code.google.com/p/php-syslog-ng/downloads/list>
  - Version (Mai 2008) : **php-syslog-ng-2.9.8**

# PHP-SYSLOG-NG



- PREREQUIS
  - MySQL 5.x
  - PHP 5 :
    - php5
    - php5-cli (fournit l'interpréteur /usr/bin/php5)
    - php5-gd (module de manipulation des images)
    - php5-mysql (module de connexion avec MySQL)
  - PERL

# PHP-SYSLOG-NG



- PREREQUIS

- Modifier Configuration de PHP -> /etc/php5/apache2/php.ini (sous Debian) :
  - memory\_limit = 128M
  - max\_execution\_time = 300

# PHP-SYSLOG-NG :

## Installation



- Le fichier tar.gz téléchargé est à décompresser et décompacter dans le répertoire contenant les documents du site web (/var/www par exemple).
- Pas de paquetage Red Hat ou Debian à ce jour
- Configurer Apache pour :
  - Créer un site virtuelou
  - configurer Apache pour avoir accès à <http://localhost/php-syslog-ng/>



# PHP-SYSLOG-NG :

## Installation



- Un fichier placé dans **\$INSTALL/scripts/logrotate.d** est à copier dans **/etc/logrotate.d/php-syslog-ng/** (rotation des fichiers de logs des opérations de php-syslog-ng dans le répertoire **/var/log/php-syslog-ng**)

# PHP-SYSLOG-NG :

## Installation



le fichier **\$INSTALL/scripts/crontab** contient des lignes à rajouter dans la crontab de root pour maintenir à jour la base MySQL créée.

- logrotate.php
- reloadcache.php
- squeezeedb.php

# PHP-SYSLOG-NG :

## Configuration



- Se connecter sur <http://localhost/php-syslog-ng/> pour :
  - **Créer** une base de données "**syslog**" avec les comptes utilisateurs adéquats
  - **paramétrer** le site (mot de passe admin, adresse ...)

pre-installation check

license

step 1

step 2

step 3

step 4



## pre-installation check

Next >>

### Pre-installation check for: Php-Syslog-NG 2.9.8 Stable [ cdukes ] 10-May-2008 15:53 EST

If any of these items are highlighted in red then please take actions to correct them. Failure to do so could lead to your PHP-Syslog-NG installation not functioning correctly.

PHP version >= 4.1.0	Yes
- zlib compression support	Available
- XML support	Available
- GD support	Available
- MySQL support	Available
config.php	Writeable
Session save path	/var/lib/php5, Writeable

### Recommended settings:

These settings are recommended for PHP in order to ensure full compatibility with PHP-Syslog-NG. However, PHP-Syslog-NG will still operate if your settings do not quite match the recommended

Directive	Recommended	Actual
Safe Mode:	OFF:	OFF
Display Errors:	ON:	ON
File Uploads:	ON:	ON
Magic Quotes GPC:	ON:	ON
Magic Quotes Runtime:	OFF:	OFF
Register Globals:	OFF:	OFF
Output Buffering:	OFF:	OFF
Session auto start:	OFF:	OFF
Memory Limit:	>= 128MB:	128
Max Execution Time:	>= 60 sec:	300

### Directory and File Permissions:

In order for PHP-Syslog-NG to function correctly it needs to be able to access or write to certain files or directories. If you see "Unwriteable" you need to change the permissions on the file or directory to allow PHP-Syslog-NG to write to it.

config/	Writeable
jpgcache/	Writeable

PHP-Syslog-NG installation

pre-installation check

license

**step 1**

step 2

step 3

step 4



# step 1

Next >>

## MySQL database configuration:

Setting up Php-Syslog-NG to run on your server involves 4 simple steps...

Please enter the hostname of the server Php-Syslog-NG is to be installed on.

Enter the MySQL username, password and database name you wish to use with Php-Syslog-NG.

Enter the table name prefix (if any) to be used by this Php-Syslog-NG instance and select what to do in case there are existing tables from former installations.

Install the samples unless you want to start with a completely empty site.

Host Name *This is usually 'localhost'*  
localhost

MySQL User Name *Enter a valid username such as 'root' or a username given by your server administrator.*  
root

MySQL Password *For site security using a password for the mysql account is mandatory*  
\*\*\*\*\*

Verify MySQL Password *Retype password for verification*  
\*\*\*\*\*

MySQL Database Name *Some hosts only allow a certain DB name per site. If this is the case, set that name here and use the Prefix option below.*  
syslog

MySQL Port *Specify the port which MySQL is running on (Default is 3306)*  
3306

MySQL Table Prefix *Do NOT use 'old\_' since this is used for backup tables*

Syslog User Name *This user is used to access the SQL (read) data on the backend, there's probably no need to change it from the default (sysloguser)*  
sysloguser

Syslog User Password *For site security using a password for the mysql account is mandatory*  
\*\*\*\*\*

Verify Password *Retype password for verification*  
\*\*\*\*\*

Syslog Admin Name *This user is used to access the SQL (write) data on the backend, there's probably no need to change it from the default (syslogadmin)*  
syslogadmin

Syslog Admin Password *For site security using a password for the mysql account is mandatory*  
\*\*\*\*\*

Verify Password *Retype password for verification*  
\*\*\*\*\*

Drop Existing Tables

Backup Old Tables *Any existing backup tables from former installations will be replaced*

Install Sample Data *Checking this option will install sample data*

Install CEMDB Data *Checking this option will install data for the Cisco Error Message Database*



pre-installation check

license

step 1

**step 2**

step 3

step 4



## step 2

Next >>

**Enter the name of your Php-Syslog-NG site:**

---

**SUCCESS!**

Type in the name for your Php-Syslog-NG site. This name is used in email messages so make it something meaningful.

Site name

e.g. The Home of Php-Syslog-NG



pre-installation check

license

step 1

step 2

**step 3**

step 4



### step 3

Next >>

#### Confirm the site URL, path, admin e-mail and file/directory chmods

If URL and Path looks correct then please do not change. If you are not sure then please contact your ISP or administrator. Usually the values displayed will work for your site.

SITEURL is used to indicate that this server is installed in a subdirectory such as <http://server/syslog/>. Be sure to include a trailing slash on SITEURL

Enter your e-mail address, this will be the e-mail address of the site SuperAdministrator.

The permission settings will be used while installing Php-Syslog-NG itself, by the Php-Syslog-NG addon-installers and by the media manager. If you are unsure what flags should be set, leave the default settings at the moment. You can still change these flags later in the site global configuration.

URL

Install Path

Site URL

Your E-mail

Admin password

File Permissions

Dont CHMOD files (use server defaults)


CHMOD files to:

Directory Permissions

Dont CHMOD directories (use server defaults)

CHMOD directories to:

- pre-installation check
- license
- step 1
- step 2
- step 3
- step 4



## step 4

**Final Step: CEMDB Install**

Next: Be sure to click the "Install CEMDB" button to start CEMDB import!

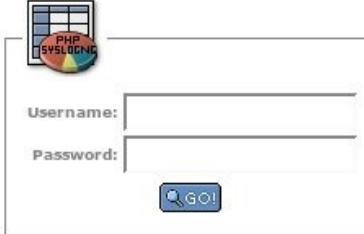
PLEASE REMEMBER TO COMPLETELY REMOVE THE INSTALLATION DIRECTORY

Administration Login Details

Username : admin

Password : nErvKFmZ





A login form box containing a PHP logo, a 'Username:' label with an input field, a 'Password:' label with an input field, and a 'GO!' button with a magnifying glass icon.

This System is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. This warning has been provided by the United States Department of Justice and is intended to ensure that monitoring of user activity is not in violation of the Communications Privacy Act of 1986.

# PHP-SYSLOG-NG :

## Configuration



```
source s_network {udp()};
```

...

```
destination d_mysql {
```

```
    program("/usr/bin/mysql -usyslogadmin -psyslogadmin syslog"
```

```
    template("INSERT INTO logs (host, facility, priority, level, tag,  
            datetime, program, msg)
```

```
    VALUES ( '$HOST', $FACILITY, '$PRIORITY', '$LEVEL', '$TAG',  
            '$YEAR-MONTH-$DAY' $HOUR:$MIN:$SEC', '$PROGRAM',  
            '$MSG');\n")
```

```
    template-escape(yes)); }
```

```
log {source(s_network); destination(d_archivage); }; #Ces 2  
    destinations,
```

```
log {source(s_network); destination(d_mysql); }; #sont utilisées  
    pour les messages de log provenant du réseau.
```

## USING TABLE: logs

## USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.

Cache last updated on 2008-06-09 09:27:46.

HOSTS: 7		PROGRAMS: 41		SYSLOG FACILITY:		SYSLOG PRIORITY:	
Include	<input type="radio"/>	Include	<input type="radio"/>	Include	<input type="radio"/>	Include	<input type="radio"/>
Exclude	<input checked="" type="radio"/>	Exclude	<input checked="" type="radio"/>	Exclude	<input checked="" type="radio"/>	Exclude	<input checked="" type="radio"/>
RegExp Matching?	<input type="checkbox"/>	RegExp Matching?	<input type="checkbox"/>				
Hostname match	<input type="text"/>	Program match	<input type="text"/>				
-----AND-----	<ul style="list-style-type: none"> <li>139.124.2.103</li> <li>139.124.2.105</li> <li>139.124.2.107</li> <li>139.124.2.12</li> <li>139.124.2.2</li> <li>139.124.2.9</li> </ul>	-----AND-----	<ul style="list-style-type: none"> <li>CRON</li> <li>KERN</li> <li>MSWinEventLog 1</li> <li>NONE</li> <li>anacron</li> <li>arpwatch</li> </ul>	<ul style="list-style-type: none"> <li>auth</li> <li>authpriv</li> <li>cron</li> <li>daemon</li> <li>kern</li> <li>local0</li> <li>local2</li> <li>local4</li> </ul>	<ul style="list-style-type: none"> <li>debug</li> <li>info</li> <li>notice</li> <li>warning</li> <li>err</li> <li>crit</li> <li>alert</li> <li>emerg</li> </ul>		

	DATE	TIME
From:	<input type="text"/>	<input type="text"/>
To:	<input type="text"/>	<input type="text"/>

RECORDS PER PAGE	50
TopX	10
ORDER BY	datetime
SEARCH ORDER	DESC

## SEARCH MESSAGE:

Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	

Search Tail Graph Reset

## Common Graphs:

Select a Graph Type

Executed in 0.0196092128754 seconds

[Donate](#)

The code you support today may turn out to be **SkyNet** tomorrow...

**CHANGE YOUR PASSWORD:**

Old password:

New password:

Retype new password:

**ADD USER:**

New username:

New user password:

Retype new user password:

**CHANGE USER'S PASSWORD:**

Username:

New password:

Retype new password:

**DELETE USER:**

**SET USER ACCESS:**



The code you support today may turn out to be SkyNet tomorrow...

USING TABLE: logs

USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.

Cache last updated on 2008-06-09 09:27:46.

<b>HOSTS: 7</b> Include <input checked="" type="radio"/> Exclude <input type="radio"/> RegExp Matching? <input type="checkbox"/> Hostname match <input type="text"/> -----AND----- 139.124.2.103 139.124.2.105 139.124.2.107 139.124.2.12 139.124.2.2 139.124.2.9		<b>PROGRAMS: 41</b> Include <input type="radio"/> Exclude <input checked="" type="radio"/> RegExp Matching? <input type="checkbox"/> Program match <input type="text"/> -----AND----- CRON KERN MSWinEventLog 1 NONE anacron arpwatch		<b>SYSLOG FACILITY:</b> Include <input type="radio"/> Exclude <input checked="" type="radio"/> auth authpriv cron daemon kern local0 local2 local4	<b>SYSLOG PRIORITY:</b> Include <input type="radio"/> Exclude <input checked="" type="radio"/> debug info notice warning err crit alert emerg
--	--	--	--	--	---

DATE <b>From:</b> <input type="text"/> <input type="text"/> <b>To:</b> <input type="text"/> <input type="text"/>	TIME <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	<b>RECORDS PER PAGE</b> 50 <b>TopX</b> 10 <b>ORDER BY</b> datetime <b>SEARCH ORDER</b> DESC
--	--	--

**SEARCH MESSAGE:**

Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/> RegExp <input type="checkbox"/>	<input type="text"/>	

Search Tail Graph Reset

**Common Graphs:**  
 Select a Graph Type

## BACK TO SEARCH

Number of Entries Found: 27,427

 SEVERITY LEGEND  
 DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG

SEQ	HOST	FACILITY	FO	LO	COUNT	DATE TIME	PROGRAM	MESSAGE
126709	139.124.2.2	cron				16:50:45		/USR/SBIN/CRON[15321]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126711	139.124.2.2	cron				16:50:45		/USR/SBIN/CRON[15323]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126703	139.124.2.2	cron				16:49:45		/USR/SBIN/CRON[15310]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126705	139.124.2.2	cron				16:49:45		/USR/SBIN/CRON[15312]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126689	139.124.2.2	cron				16:48:45		/USR/SBIN/CRON[15299]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126691	139.124.2.2	cron				16:48:45		/USR/SBIN/CRON[15301]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126684	139.124.2.2	cron				16:47:45		/USR/SBIN/CRON[15288]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126685	139.124.2.2	cron				16:47:45		/USR/SBIN/CRON[15290]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126667	139.124.2.2	cron				16:46:45		/USR/SBIN/CRON[15250]: (root) CMD (if [ -x /usr/bin/mrtg ] && [ -r /etc/mrtg.cfg ]; then env LANG=C /usr/bin/mrtg /etc/mrtg.cfg >> /var/log/mrtg/mrtg.log 2>&1; fi)
126670	139.124.2.2	cron				16:46:45		/USR/SBIN/CRON[15252]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126671	139.124.2.2	cron				16:46:45		/USR/SBIN/CRON[15254]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126661	139.124.2.2	cron				16:45:45		/USR/SBIN/CRON[15239]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126663	139.124.2.2	cron				16:45:45		/USR/SBIN/CRON[15240]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126655	139.124.2.2	cron				16:44:45		/USR/SBIN/CRON[15227]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126657	139.124.2.2	cron				16:44:45		/USR/SBIN/CRON[15229]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126649	139.124.2.2	cron				16:43:45		/USR/SBIN/CRON[15209]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126651	139.124.2.2	cron				16:43:45		/USR/SBIN/CRON[15211]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126634	139.124.2.2	cron				16:42:45		/USR/SBIN/CRON[15195]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126635	139.124.2.2	cron				16:42:45		/USR/SBIN/CRON[15197]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126620	139.124.2.2	cron				16:41:45		/USR/SBIN/CRON[15159]: (root) CMD (if [ -x /usr/bin/mrtg ] && [ -r /etc/mrtg.cfg ]; then env LANG=C /usr/bin/mrtg /etc/mrtg.cfg >> /var/log/mrtg/mrtg.log 2>&1; fi)
126622	139.124.2.2	cron				16:41:45		/USR/SBIN/CRON[15162]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126623	139.124.2.2	cron				16:41:45		/USR/SBIN/CRON[15163]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126613	139.124.2.2	cron				16:40:45		/USR/SBIN/CRON[15149]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126615	139.124.2.2	cron				16:40:45		/USR/SBIN/CRON[15151]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126606	139.124.2.2	cron				16:39:45		/USR/SBIN/CRON[15137]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126608	139.124.2.2	cron				16:39:45		/USR/SBIN/CRON[15139]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126598	139.124.2.2	cron				16:38:45		/USR/SBIN/CRON[15113]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126600	139.124.2.2	cron				16:38:45		/USR/SBIN/CRON[15115]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126590	139.124.2.2	cron				16:37:45		/USR/SBIN/CRON[15099]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)
126592	139.124.2.2	cron				16:37:45		/USR/SBIN/CRON[15101]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126574	139.124.2.2	cron				16:36:45		/USR/SBIN/CRON[15063]: (root) CMD (if [ -x /usr/bin/mrtg ] && [ -r /etc/mrtg.cfg ]; then env LANG=C /usr/bin/mrtg /etc/mrtg.cfg >> /var/log/mrtg/mrtg.log 2>&1; fi)
126576	139.124.2.2	cron				16:36:45		/USR/SBIN/CRON[15066]: (root) CMD (/usr/local/sbin/modif_prop_meteo.sh >/var/tmp/modif_prop_meteo.out 2>&1)
126578	139.124.2.2	cron				16:36:45		/USR/SBIN/CRON[15067]: (root) CMD (/usr/local/sbin/modif_prop_cytometrie.sh >/var/tmp/modif_prop_precym.out 2>&1)


[Donate](#)
[Logout](#) [Search](#) [Config](#) [Help](#) [About](#)

 The code you support today may turn out to be **SkyNet** tomorrow...

**USING TABLE: logs**
**USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.**

Cache last updated on 2008-06-09 09:27:46.

**HOSTS: 7**

 Include 

 Exclude 

 RegExp Matching? 

Hostname match

=====AND=====






**PROGRAMS: 41**

 Include 

 Exclude 

 RegExp Matching? 

Program match

=====AND=====






**SYSLOG FACILITY:**

 Include 

 Exclude 








**SYSLOG PRIORITY:**

 Include 

 Exclude 









DATE

TIME

From:



To:



RECORDS PER PAGE

TopX

ORDER BY

SEARCH ORDER

**SEARCH MESSAGE:**

 Exclude  RegExp 


AND

 Exclude  RegExp 


AND

 Exclude  RegExp 





**Common Graphs:**

[Donate](#)The code you support today may turn out to be **SkyNet** tomorrow...**BACK TO SEARCH**Number of Entries Found: **7**
 SEVERITY LEGEND  
 DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG

SEQ	HOST	FACILITY	FO	LO	COUNT	DATE TIME	PROGRAM	MESSAGE
125919	139.124.2.103	daemon				15:39:22	dhcpcd	dhcpcd: DHCPOFFER on 139.124.2.247 to 00:0a:57:11:2a:00 via 139.124.17.126
125918	139.124.2.103	daemon				15:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125917	139.124.2.103	daemon				15:39:16	dhcpcd	dhcpcd: DHCPACK on 139.124.16.138 to 00:03:93:da:c6:80 via 139.124.16.250
125916	139.124.2.103	daemon				15:39:16	dhcpcd	dhcpcd: DHCPREQUEST for 139.124.16.138 from 00:03:93:da:c6:80 via 139.124.16.250
125902	139.124.2.103	daemon				15:36:58	named	named[9667]: zone 18.124.139.in-addr.arpa/IN: refresh: retry limit for master 139.124.67.229#53 exceeded
125901	139.124.2.103	daemon				15:36:58	last	last message repeated 3 times
125889	139.124.2.103	daemon				15:36:13	named	named[9667]: zone 18.124.139.in-addr.arpa/IN: refresh: failure trying master 139.124.67.229#53: timed out

Result Page: [1]

Executed in **0.0145289897919 seconds**





## USING TABLE: logs

## USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.

Cache last updated on 2008-06-09 09:27:46.

## HOSTS: 7

Include Exclude RegExp Matching? 

Hostname match

=====AND=====

  
 139.124.2.103  
 139.124.2.105  
 139.124.2.107  
 139.124.2.12  
 139.124.2.2  
 139.124.2.9

## PROGRAMS: 41

Include Exclude RegExp Matching? 

Program match

=====AND=====

  
 CRON  
 KERN  
 MSWinEventLog 1  
 NONE  
 anacron  
 arpswatch

## SYSLOG FACILITY:

Include Exclude 
  
 auth  
 authpriv  
 cron  
 daemon  
 kern  
 local0  
 local2  
 local4

## SYSLOG PRIORITY:

Include Exclude 
  
 debug  
 info  
 notice  
 warning  
 err  
 crit  
 alert  
 emerg

	DATE	TIME
From:	<input type="text"/>	<input type="text"/>
To:	<input type="text"/>	<input type="text"/>

RECORDS PER PAGE 50

TopX 10

ORDER BY datetime

SEARCH ORDER DESC

## SEARCH MESSAGE:

Exclude <input type="checkbox"/>	RegExp <input checked="" type="checkbox"/>	<input type="text" value="00:0a:57:11:2a:00"/>	AND
Exclude <input type="checkbox"/>	RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/>	RegExp <input type="checkbox"/>	<input type="text"/>	





## Common Graphs:

[Donate](#)
[Logout](#)    [Search](#)    [Config](#)    [Help](#)    [About](#)

 The code you support today may turn out to be **SkyNet** tomorrow...

## BACK TO SEARCH

Number of Entries Found: 3,448

DEBUG    INFO    NOTICE    WARNING    ERROR    CRIT    ALERT    EMERG

## SEVERITY LEGEND

SEQ	HOST	FACILITY	FO	LO	COUNT	DATE TIME	PROGRAM	MESSAGE
126922	139.124.2.103	daemon				17:09:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126923	139.124.2.103	daemon				17:09:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126815	139.124.2.103	daemon				16:59:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126816	139.124.2.103	daemon				16:59:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126694	139.124.2.103	daemon				16:49:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126695	139.124.2.103	daemon				16:49:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126603	139.124.2.103	daemon				16:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126604	139.124.2.103	daemon				16:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126507	139.124.2.103	daemon				16:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126508	139.124.2.103	daemon				16:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126398	139.124.2.103	daemon				16:19:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126399	139.124.2.103	daemon				16:19:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126279	139.124.2.103	daemon				16:09:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126280	139.124.2.103	daemon				16:09:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126153	139.124.2.103	daemon				15:59:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126154	139.124.2.103	daemon				15:59:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126033	139.124.2.103	daemon				15:49:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
126034	139.124.2.103	daemon				15:49:21	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125918	139.124.2.103	daemon				15:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125919	139.124.2.103	daemon				15:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125821	139.124.2.103	daemon				15:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125822	139.124.2.103	daemon				15:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125695	139.124.2.103	daemon				15:19:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125696	139.124.2.103	daemon				15:19:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125350	139.124.2.103	daemon				15:09:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
125351	139.124.2.103	daemon				15:09:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124950	139.124.2.103	daemon				14:59:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124951	139.124.2.103	daemon				14:59:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124821	139.124.2.103	daemon				14:49:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124822	139.124.2.103	daemon				14:49:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124683	139.124.2.103	daemon				14:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124684	139.124.2.103	daemon				14:39:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124542	139.124.2.103	daemon				14:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124543	139.124.2.103	daemon				14:29:22	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124434	139.124.2.103	daemon				14:19:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126
124435	139.124.2.103	daemon				14:19:23	dhcpcd	dhcpcd: DHCPDISCOVER from 00:0a:57:11:2a:00 via 139.124.17.126

[Donate](#)

The code you support today may turn out to be **SkyNet** tomorrow...

## USING TABLE: logs

## USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.

Cache last updated on 2008-06-09 09:27:46.

## HOSTS: 7

Include Exclude RegExp Matching? 

Hostname match

=====AND=====

## PROGRAMS: 41

Include Exclude RegExp Matching? 

Program match

=====AND=====

## SYSLOG FACILITY:

Include Exclude 

## SYSLOG PRIORITY:

Include Exclude 

DATE TIME  
**From:**     
**To:**

RECORDS PER PAGE TopX ORDER BY SEARCH ORDER 

## SEARCH MESSAGE:

Exclude  RegExp   AND  
 Exclude  RegExp   AND  
 Exclude  RegExp

## Common Graphs:

## BACK TO SEARCH

Number of Entries Found: **56,199**
 SEVERITY LEGEND  
 DEBUG   INFO   NOTICE   WARNING   ERROR   CRIT   ALERT   EMERG

SEQ	HOST	FACILITY	FO	LO	COUNT	DATE TIME	PROGRAM	MESSAGE
126850	139.124.2.2	auth				17:03:23	CRON	CRON[15646]: (pam_unix) session closed for user root
126845	139.124.2.2	auth				17:02:45	CRON	CRON[15646]: (pam_unix) session opened for user root by (uid=0)
126846	139.124.2.2	auth				17:02:45	CRON	CRON[15648]: (pam_unix) session opened for user root by (uid=0)
126849	139.124.2.2	auth				17:02:45	CRON	CRON[15648]: (pam_unix) session closed for user root
126844	139.124.2.2	auth				17:02:19	CRON	CRON[15613]: (pam_unix) session closed for user root
126843	139.124.2.2	auth				17:01:46	CRON	CRON[15611]: (pam_unix) session closed for user root
126842	139.124.2.2	auth				17:01:45	CRON	CRON[15614]: (pam_unix) session closed for user root
126835	139.124.2.2	auth				17:01:44	CRON	CRON[15611]: (pam_unix) session opened for user root by (uid=0)
126836	139.124.2.2	auth				17:01:44	CRON	CRON[15613]: (pam_unix) session opened for user root by (uid=0)
126838	139.124.2.2	auth				17:01:44	CRON	CRON[15614]: (pam_unix) session opened for user root by (uid=0)
126834	139.124.2.2	auth				17:01:20	CRON	CRON[15586]: (pam_unix) session closed for user root
126833	139.124.2.2	auth				17:00:46	CRON	CRON[15587]: (pam_unix) session closed for user root
126823	139.124.2.2	auth				17:00:45	CRON	CRON[15582]: (pam_unix) session opened for user root by (uid=0)
126824	139.124.2.2	auth				17:00:45	CRON	CRON[15584]: (pam_unix) session opened for user root by (uid=0)
126827	139.124.2.2	auth				17:00:45	CRON	CRON[15587]: (pam_unix) session opened for user root by (uid=0)
126829	139.124.2.2	auth				17:00:45	CRON	CRON[15586]: (pam_unix) session opened for user root by (uid=0)
126831	139.124.2.2	auth				17:00:45	CRON	CRON[15582]: (pam_unix) session closed for user root
126832	139.124.2.2	auth				17:00:45	CRON	CRON[15584]: (pam_unix) session closed for user root
126822	139.124.2.2	auth				17:00:20	CRON	CRON[15508]: (pam_unix) session closed for user root
126817	139.124.2.2	auth				16:59:45	CRON	CRON[15508]: (pam_unix) session opened for user root by (uid=0)
126819	139.124.2.2	auth				16:59:45	CRON	CRON[15510]: (pam_unix) session opened for user root by (uid=0)
126821	139.124.2.2	auth				16:59:45	CRON	CRON[15510]: (pam_unix) session closed for user root
126814	139.124.2.2	auth				16:59:22	CRON	CRON[15464]: (pam_unix) session closed for user root
126797	139.124.2.2	auth				16:58:45	CRON	CRON[15464]: (pam_unix) session opened for user root by (uid=0)
126799	139.124.2.2	auth				16:58:45	CRON	CRON[15466]: (pam_unix) session opened for user root by (uid=0)
126801	139.124.2.2	auth				16:58:45	CRON	CRON[15466]: (pam_unix) session closed for user root
126795	139.124.2.2	auth				16:58:21	CRON	CRON[15454]: (pam_unix) session closed for user root
126790	139.124.2.2	auth				16:57:45	CRON	CRON[15454]: (pam_unix) session opened for user root by (uid=0)
126792	139.124.2.2	auth				16:57:45	CRON	CRON[15456]: (pam_unix) session opened for user root by (uid=0)
126794	139.124.2.2	auth				16:57:45	CRON	CRON[15456]: (pam_unix) session closed for user root
126789	139.124.2.2	auth				16:57:23	CRON	CRON[15418]: (pam_unix) session closed for user root
126788	139.124.2.105	auth				16:57:02	CRON	CRON[1342]: (pam_unix) session closed for user root
126786	139.124.2.105	auth				16:56:56	CRON	CRON[1342]: (pam_unix) session opened for user root by (uid=0)
126785	139.124.2.2	auth				16:56:46	CRON	CRON[15416]: (pam_unix) session closed for user root
126775	139.124.2.2	auth				16:56:45	CRON	CRON[15416]: (pam_unix) session opened for user root by (uid=0)
126777	139.124.2.2	auth				16:56:45	CRON	CRON[15419]: (pam_unix) session opened for user root by (uid=0)
126778	139.124.2.2	auth				16:56:45	CRON	CRON[15421]: (pam_unix) session opened for user root by (uid=0)

## USING TABLE: logs

## USING CACHE TO POPULATE HOST, FACILITY, AND PROGRAM FIELDS.

Cache last updated on 2008-06-09 09:27:46.

HOSTS: 7		PROGRAMS: 41		SYSLOG FACILITY:		SYSLOG PRIORITY:	
Include	<input type="radio"/>	Include	<input type="radio"/>	Include	<input type="radio"/>	Include	<input type="radio"/>
Exclude	<input checked="" type="radio"/>	Exclude	<input checked="" type="radio"/>	Exclude	<input checked="" type="radio"/>	Exclude	<input type="radio"/>
RegExp Matching?	<input type="checkbox"/>	RegExp Matching?	<input type="checkbox"/>				
Hostname match	<input type="text"/>	Program match	<input type="text"/>				
====AND====	<ul style="list-style-type: none"> <li>139.124.2.103</li> <li>139.124.2.105</li> <li>139.124.2.107</li> <li>139.124.2.12</li> <li>139.124.2.2</li> <li>139.124.2.9</li> </ul>	====AND====	<ul style="list-style-type: none"> <li>CRON</li> <li>KERN</li> <li>MSWinEventLog 1</li> <li>NONE</li> <li>anacron</li> <li>arpwatch</li> </ul>	<ul style="list-style-type: none"> <li>auth</li> <li>authpriv</li> <li>cron</li> <li>daemon</li> <li>kern</li> <li>local0</li> <li>local2</li> <li>local4</li> </ul>	<ul style="list-style-type: none"> <li>debug</li> <li>info</li> <li>notice</li> <li>warning</li> <li>err</li> <li>crit</li> <li>alert</li> <li>emerg</li> </ul>		

DATE	TIME	RECORDS PER PAGE	50
From:	<input type="text"/>	TopX	10
To:	<input type="text"/>	ORDER BY	datetime
		SEARCH ORDER	DESC

## SEARCH MESSAGE:

Exclude <input type="checkbox"/>	RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/>	RegExp <input type="checkbox"/>	<input type="text"/>	AND
Exclude <input type="checkbox"/>	RegExp <input type="checkbox"/>	<input type="text"/>	





## Common Graphs:



Fichier Édition Affichage Aller à Signets Outils Onglets Aide

<http://pcsic24/php-syslog-ng/index.php?table=logs&excludeHost=1&host2=&excludeProgram=1&program2=&excludeFacility=1&excludePriority=0&priority%5B%5D=waming&date=&time=&> Aller à[Donate](#)[Logout](#) [Search](#) [Config](#) [Help](#) [About](#)The code you support today may turn out to be **SkyNet** tomorrow...**BACK TO SEARCH**Number of Entries Found: **186**

DEBUG INFO NOTICE WARNING ERROR CRIT ALERT EMERG

SEVERITY LEGEND

SEQ	HOST	FACILITY	FO	LO	COUNT	DATE TIME	PROGRAM	MESSAGE
125548	139.124.2.105	kern				15:11:02	kernel	kernel: usb-uhci.c: Detected 2 ports
125389	139.124.2.105	kern				15:11:01	kernel	kernel: Linux version 2.4.27-2-386 (horms@tabatha.lab.ultramonkey.org) (gcc version 3.3.5 (Debian 1:3.3.5-13)) #1 Wed Aug 17 09:33:35 UTC 2005
125391	139.124.2.105	kern				15:11:01	kernel	kernel: BIOS-e820: 0000000000000000 - 0000000000009fc00 (usable)
125392	139.124.2.105	kern				15:11:01	kernel	kernel: BIOS-e820: 0000000000009fc00 - 00000000000a0000 (reserved)
125393	139.124.2.105	kern				15:11:01	kernel	kernel: BIOS-e820: 00000000000f0000 - 000000000100000 (reserved)
125394	139.124.2.105	kern				15:11:01	kernel	kernel: BIOS-e820: 000000000100000 - 0000000020000000 (usable)
125395	139.124.2.105	kern				15:11:01	kernel	kernel: BIOS-e820: 00000000ffff0000 - 0000000100000000 (reserved)
125397	139.124.2.105	kern				15:11:01	kernel	kernel: On node 0 totalpages: 131072
125398	139.124.2.105	kern				15:11:01	kernel	kernel: zone(0): 4096 pages.
125399	139.124.2.105	kern				15:11:01	kernel	kernel: zone(1): 126976 pages.
125400	139.124.2.105	kern				15:11:01	kernel	kernel: zone(2): 0 pages.
125403	139.124.2.105	kern				15:11:01	kernel	kernel: Kernel command line: root=/dev/sdb1 ro
125404	139.124.2.105	kern				15:11:01	kernel	kernel: Local APIC disabled by BIOS -- reenabling.
125405	139.124.2.105	kern				15:11:01	kernel	kernel: Found and enabled local APIC!
125407	139.124.2.105	kern				15:11:01	kernel	kernel: Detected 668.192 MHz processor.
125408	139.124.2.105	kern				15:11:01	kernel	kernel: Console: colour VGA+ 80x25
125409	139.124.2.105	kern				15:11:01	kernel	kernel: Calibrating delay loop... 1333.65 BogoMIPS
125415	139.124.2.105	kern				15:11:01	kernel	kernel: Page-cache hash table entries: 131072 (order: 7, 524288 bytes)
125420	139.124.2.105	kern				15:11:01	kernel	kernel: CPU: Intel Pentium III (Coppermine) stepping 01
125425	139.124.2.105	kern				15:11:01	kernel	kernel: POSIX conformance testing by UNIFIX
125426	139.124.2.105	kern				15:11:01	kernel	kernel: enabled ExtINT on CPU#0
125427	139.124.2.105	kern				15:11:01	kernel	kernel: ESR value before enabling vector: 00000000
125428	139.124.2.105	kern				15:11:01	kernel	kernel: ESR value after enabling vector: 00000000
125429	139.124.2.105	kern				15:11:01	kernel	kernel: Using local APIC timer interrupts.
125430	139.124.2.105	kern				15:11:01	kernel	kernel: calibrating APIC timer ...
125431	139.124.2.105	kern				15:11:01	kernel	kernel: ..... CPU clock speed is 668.1940 MHz.
125432	139.124.2.105	kern				15:11:01	kernel	kernel: ..... host bus clock speed is 133.6385 MHz.
125433	139.124.2.105	kern				15:11:01	kernel	kernel: cpu: 0, clocks: 1336385, slice: 668192
125434	139.124.2.105	kern				15:11:01	kernel	kernel: CPU0<T0:1336384,T1:668192,D:0,S:668192,C:1336385>
125440	139.124.2.105	kern				15:11:01	kernel	kernel: PCI: Probing PCI hardware (bus 00)
125445	139.124.2.105	kern				15:11:01	kernel	kernel: Initializing RT netlink socket
125446	139.124.2.105	kern				15:11:01	kernel	kernel: Starting kswapd
125450	139.124.2.105	kern				15:11:01	kernel	kernel: pty: 256 Unix98 ptys configured
125455	139.124.2.105	kern				15:11:01	kernel	kernel: RAMDISK driver initialized: 16 RAM disks of 8192K size 1024 blocksize
125464	139.124.2.105	kern				15:11:01	kernel	kernel: VFS: Mounted root (cramfs filesystem).



# CONCLUSION

- Avantages :
  - Compatibilité avec le syslog classique
  - Plus grande souplesse de configuration
  - notion de filtre permet de trier plus en détail ses messages de logs
  - Avec PHP-Syslog-ng, peuvent être très utiles pour l'analyse d'incidents à posteriori
- Inconvénients
  - Prise en mains
  - Attention à ne pas trop "éclater" les traces