**Objets utilisés par syslog-ng :**

* Source driver : TCP/IP, file…
* Source : collection de source driver
* Destination driver
* Destination
* Filtres
* Macro : $HOST par exemple spécifie une partie du log
* Parser
* Rewriter rule : réécrire, ajouter ou supprimer des parties du log.
* Log path : combinaison de sources, destinations, filtres, parsers, rewriters… = log statement
* Template : restructuration du format du log
* Option : interne à syslog-ng

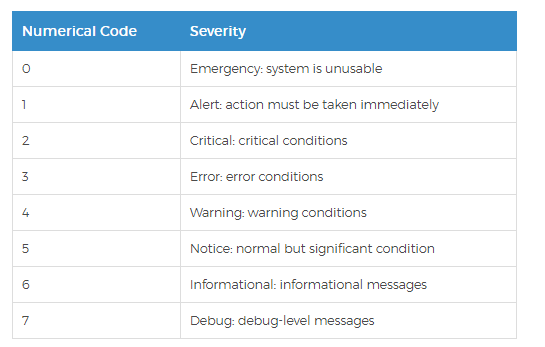
**Arrivé d’un message :**

* Si aucun timezone, on ajoute le timezone local ou le timezone spécifié.

**s**

* RFC 3164 : syslog legacy : 1 K maxi, message contenant PRI, HEADER, MSG.
* RFC 5424 : IETF : nouveaux syslog. Message contient : HEADER (PRI+…), STRUCTURED-DATA, MSG
* Header : Priorité basé sur facility et severity , version (1), ISOTIMESTAMP, HOSTNAME, APP, PID, MSGID
* Structured-Data : [métas informations]





**Syntaxe :**

source s\_local {

foo() ;

foo2() ;

} ;

Possibilité d’inline définition : comme les classes anonymes en java qui ne fonctionnent qu’une fois.

@define name "value" //accès à la variable avec `name`

@include file //idem qu’en C

Block : sorte de fonctions pouvant être réutilisées (réutilisation de code dans la conf)

Syslog-ng –syntax-only //checker la validité du fichier de conf.

**Modules :**

Syslog-ng –version : liste des modules available

Syslog-ng –module-registry : description des modules available

@module moduleName pour inclure un module.

**Dans le fichier de conf :**

Source { } pour spécifier une source

Destination {}

Log {} : relié une source à une destination en utilisant des filtres…

**Fonctions de source :**

Source s\_name {

Unix-stream("path to socket" max-connections(10) group(log)) ; //écoute sur une socket SOCK\_STREAM

Network(ip(X.X.X.X) port(X)) ; //TCP

Network(ip(X.X.X.X) port(X) transport("udp")) ; //UDP

File(path) follow-freq(1) flags(no-parse) ; //check toutes les 1 secondes

//ne parse pas en format syslog

Internal() ; //messages syslog-ng

Snmptrap() ;

System() ; //messages systems

Stdin() ;

…

} ;

**Fonctions de destination :**

Destination d\_name{

Graylog2( //syslog-ng >=3.14

host ("X.X.X.X")

) ;

} ;

**Fonctions de correspondance source/filtre/dest :**

Log{

Source1(s1) ;

Filter(filtre) ;

Destination(dest) ;

Flags(flags) ;

} ;