GESTION DES MESSAGES ET JOURNALISATION

ECOLE INFORMATIQUE 2015

Fabien Wernli

PARTIE I
PRODUCTION DE "LOGS"

SONDAGE

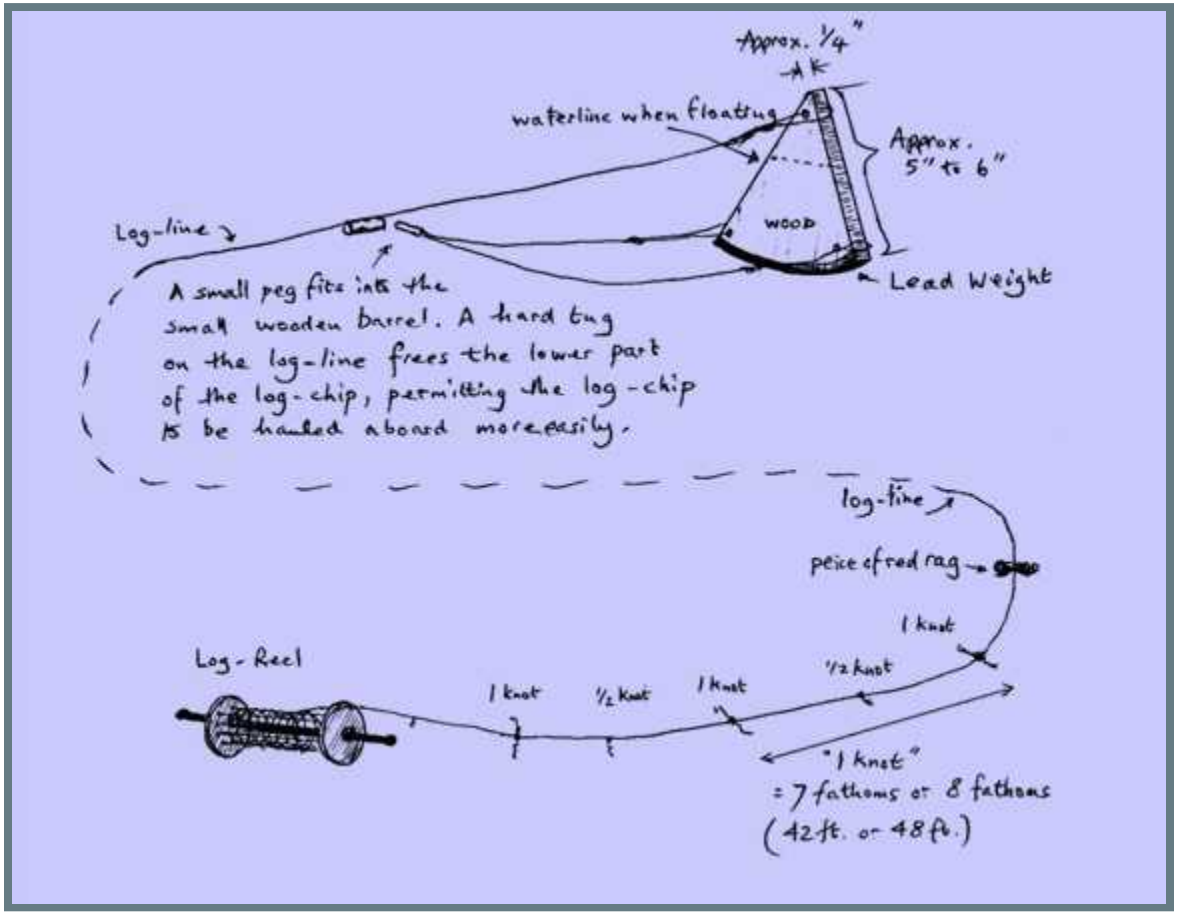
POUR LOGGER, QUI UTILISE...

- `printf/print/puts/say/…?`
- `ma_fonction_qui_reinvente_le_logging()?`
- `Logger -> new()?`
- un traitement automatisé?

HISTORIQUE

ETYMOLOGIE

- De l'anglais "bûche"
- Journal d'un bateau où l'on note la vitesse (~1670)



INFORMATIQUE

- Journal horodaté d'événements relatant le fonctionnement du SI
- Emission, transport et journalisation

LA SOURCE PRIMAIRE D'INFORMATIONS POUR L'EXPLOITANT

LE MOYEN DE COMMUNIQUER L'ÉTAT DE VOTRE BOÎTE NOIRE AU MONDE EXTÉRIEUR

SYSLOG

- Début de standard (années 1980) développé pour *Sendmail* (BSD): *syslog*

“In computing, syslog is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them.”

Wikipedia

SYSLOG

- Protocol de transport de messages
- Années 1980 pour *sendmail*
- RFC3164 (*status quo*) RFC5424 (standard)
- Contient plusieurs champs
  - `DATE`
  - `HOST`
  - `APPNAME`
  - `PRIORITY` (sévérité)
  - `FACILITY` (catégorie)
  - `MESSAGE`

LES LOGS DES SI

QUELS COMPOSANTS *LOGGENT*?

- les OS
- les applications
- le matériel embarqué
- les appareillages électriques et climatiques
- les équipements réseau
- …

DE MANIÈRE STANDARD?

WELCOME TO THE JUNGLE

- OS: GNU/Linux: syslog→fichiers

```
/var/log/messages
```

- OS: osx: ASL→fichiers

```
/Library/Logs/*
```

- OS: windows (depuis 2008): ???→???

```
%SystemRoot%\system32\winevt\logs
```

- App: apache: access (file), error (syslog)
- Equipements réseau: Cisco: "syslog" (non standard)
- BMC: IPMI
- Clims, électrique: APC, MGE: SNMP et/ou Modbus

WELCOME TO THE SYSLOG JUNGLE

- certains ne respectent pas le format
- certains mettent n'importe quoi dans `SEVERITY`, `FACILITY`
- la plupart n'implémentent pas la RFC (même 14 ans après la standardisation)

CONTENU NON STRUCTURÉ

```
named      FORMERR resolving 'ccpuppet.lb.in2p3.fr/AAAA/IN': 134.158.69.1

sshd       pam_unix(sshd:session): session closed for user atlas046

kernel     martian source 134.158.111.255 from 134.158.106.158, on dev et

nscd       5649 monitoring directory `/etc` (2)

dhcpd      DHCPDISCOVER from a0:36:9f:6f:87:74 via 134.158.208.254: unkno

xinetd     START: nrpe pid=7456 from=::ffff:134.158.108.120

hpss_logc Record type=DEBUG, Event time=2015/09/24 20:49:38 CEST, Severi
```

L'EXPLOITANT N'EST PAS MAÎTRE DE SES JOURNAUX

OU ALORS IL DOIT ÊTRE UN EXPERT...

...ÊTRE INVENTIF

Recourir à des logiciels combattant ce genre de pratiques

- Logstash
- syslog-ng
- sequencer
- …

Parsent les logs, extraient de l'information structurée, demandent beaucoup de temps

I, DEVELOPER

DÉJÀ, JE METS QUOI DANS LES LOGS?

Réponse: tout

- Debug
- Informations
- Erreurs
- Exceptions
- *Bref, tout ce que je peux, le plus que je peux*

DEBUG

```
~~printf "plop"~~
logger.log(DEBUG, "plop")
```

- Léger
- Permanent
- Structuré

INFO

```
logger.log(INFO, "user session started")
```

- Que fait mon programme actuellement?
- Accounting
- Statistiques
- Feedback

ERREURS

```
logger.log(WARN, "user failed to fulfill request")
```

- Nécessite l'attention de l'utilisateur
- Déroulement normal du flot du programme
- +/- même canal que INFO mais plus important

EXCEPTIONS

```
Program received signal SIGSEGV, Segmentation fault.
```

```
Died at main.pl line 42.
```

```
org.elasticsearch.index.mapper.MapperParsingException: failed to parse [timestamp]
        at org.elasticsearch.index.mapper.core.AbstractFieldMapper.parse(AbstractFieldMappe
        at org.elasticsearch.index.mapper.object.ObjectMapper.serializeValue(ObjectMapper.j
        at org.elasticsearch.index.mapper.object.ObjectMapper.parse(ObjectMapper.java:500)
        at org.elasticsearch.index.mapper.DocumentMapper.parse(DocumentMapper.java:541)
        at org.elasticsearch.index.mapper.DocumentMapper.parse(DocumentMapper.java:490)
        at org.elasticsearch.index.shard.service.InternalIndexShard.prepareCreate(InternalI
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardIndexOperation(Trans
        at org.elasticsearch.action.bulk.TransportShardBulkAction.shardOperationOnPrimary(T
        at org.elasticsearch.action.support.replication.TransportShardReplicationOperationA
        at org.elasticsearch.action.support.replication.TransportShardReplicationOperationA
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)
        at java.lang.Thread.run(Thread.java:745)
Caused by: org.elasticsearch.index.mapper.MapperParsingException: failed to parse date fiel
EEE MMM dd HH:mm:ss yyyyZZ], and timestamp number with locale []
        at org.elasticsearch.index.mapper.core.DateFieldMapper.parseStringValue(DateFieldMa
        at org.elasticsearch.index.mapper.core.DateFieldMapper.innerParseCreateField(DateFi
        at org.elasticsearch.index.mapper.core.NumberFieldMapper.parseCreateField(NumberFie
        at org.elasticsearch.index.mapper.core.AbstractFieldMapper.parse(AbstractFieldMappe
        ... 12 more
```

- Déroulement anormal du flot d'éxécution
- Peuvent être capturées ou non

ENCORE PLUS!

- Informations à la demande (signaux)
  - changement de niveau
  - métriques
  - statistiques

*“J'utilise le **Logger** pour suivre le flux d'exécution de mon application”*

LES 10 COMMANDEMANTS DU LOGGING

1. Tu utiliseras une librairie de log
2. Tu utiliseras le niveau de sévérité adapté
3. Tu ne pollueras pas les logs des autres
4. Tu ne configureras pas ton logger dans le code
5. Tu créeras des messages intelligibles
6. Tu créeras des messages humains et polis
7. Tu ajouteras du contexte
8. Tu ajouteras une référence unique à chaque message
9. A l'exploitant tu laisseras le contrôle
10. Tes logs seront multi-usages: homme et machine

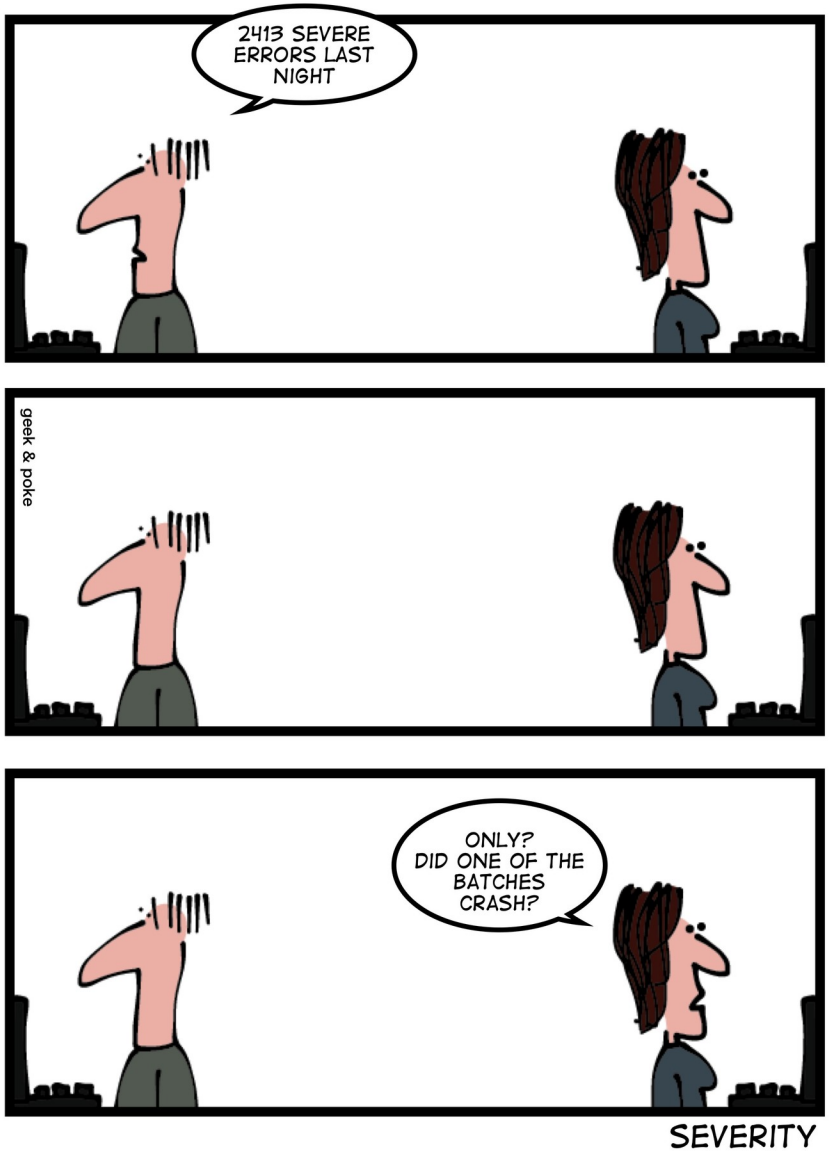
PROBLÈMES COURANTS

PROBLÈMES COURANTS

- "Alarm fatigue"
- Manque de contexte
- Manque de hiérarchie
- Manque de clarté
- Manque de référence
- Mise en page/style
- Localisation

"ALARM FATIGUE"

SIMPLY EXPLAINED



SEVERITY

"ALARM FATIGUE"

- Quand on crie au loup
- Salle d'Op: De 1983 à 2011 6 fois plus d'alarmes sonores différentes

SOLUTIONS

- Bien choisir `SEVERITY`
- Lier les messages connexes avec le plus de contexte possible!

Permettre au consommateur de nos logs de trier

CONTEXTE

- Quel est le composant affecté?
- A quel moment est-ce arrivé?
- Depuis combien de temps?

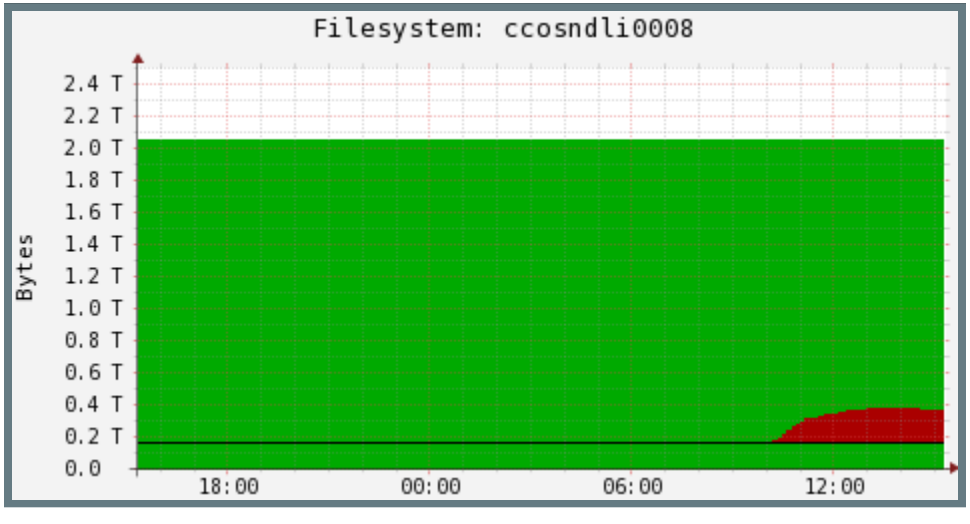
SOLUTIONS

- Ajouter le plus de contexte possible…
- … pour que le consommateur fasse le lien

```
################################
NAGIOS SERVICE NOTIFICATION
Sat Sept 12 22:12:37 CEST 2015
################################
Notification Type: RECOVERY
Host: ccosndli0008 (ccosndli0008)
Current Service State: OK

DISK OK - free space: /novatemp 99918 MB
/var 2749 MB (75% inode=96%): /instances

(Monitored by ccsvli28)
```



OUI MAIS EN TANT QUE DEV

- Stocker le contexte
- Structurer les messages
- MDC, NDC, Thread Context…
- *Java*: slf4j, log4j, logback
- *Python*: LoggerAdapter
- *Perl*: Log::Log4Perl
- *Ruby*: Log4R, cabin
- *Go*: Logrus
- Au pire: sérializer des clés/valeurs

NE PAS FIXER L'IMPLÉMENTATION

- Enrichit la fonctionalité du logiciel
- Favorise l'interopérabilité
- Donne le contrôle total à l'utilisateur
- Rend le logiciel indépendant aux changements et améliorations du framework de logging

COMMENT?

- Utiliser un framework d'abstraction
- L'exploitant configure ce dont il a l'habitude
- Perl: `Log::Contextual`
- Python: *N/A* `logging.getLogger(__name__)`
- ruby: polylog
- Au pire: écrire le sien

SOLUTION (JAVA): SLF4J

- Supporte java.util.logging, logback, log4j, …
- Logger simple par défaut
- S'intègre facilement au projet

`pom.xml`:

```
<dependency>
  <groupId>org.slf4j</groupId>
  <artifactId>slf4j-log4j12</artifactId>
  <version>1.7.12</version>
</dependency>
```

RÉFÉRENCE

CODE D'ERREUR OU UUID!

- Référencer l'événement sur le web, dans un bug report
- Caractériser une alerte
- Ne change jamais
- Est indépendant du message sous forme humaine et résiste au changement:
  - Faute de frappe
  - Localisation (internationalisation)
  - le parsing de messages est compliqué et coûteux

COMMENT?

Selon le langage:

- NDC
- MDC
- Thread context
- …

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import org.slf4j.MDC;
/* ... */
private static final Logger LOGGER = LoggerFactory.getLogger(DataParser.
/* ... */
MDC.put ("uuid", "5293e909-1720-4894-9f80-146ae76957c4");
LOGGER.warn("Erreur lors de la cnoversion de " + dataStr[i]
  + ". Cette valeur sera rmeplacée par 0", e);
MDC.remove("uuid");
```

LE LOG PARFAIT

UN LOG "IDÉAL"

```
---
datetim: 2015-10-21T16:29:00.0+0200
uniqid:  0b618bd0-7738-4abc-9e96-abe742d313e3
class:   fr.in2p3.cc.sshd
method:  sshd.connection.handler
ip:
  addr:  2001:660:5009:1:134:158:109:160
  type:  ipv6
auth:
  user:
    name: john
  group:
    name: doe
program: sshd
message: Connection refused to john from 2001:660:5009:1:134:158:109:160
```

À RETENIR

- Utiliser un logger
- De préférence, un logger abstrait
  - Exploitabilité (Sqale!)
  - Maintenabilité (Sqale!)
- Utiliser des *UUID*
- Logger le plus possible avec la bonne sévérité

DIVERS

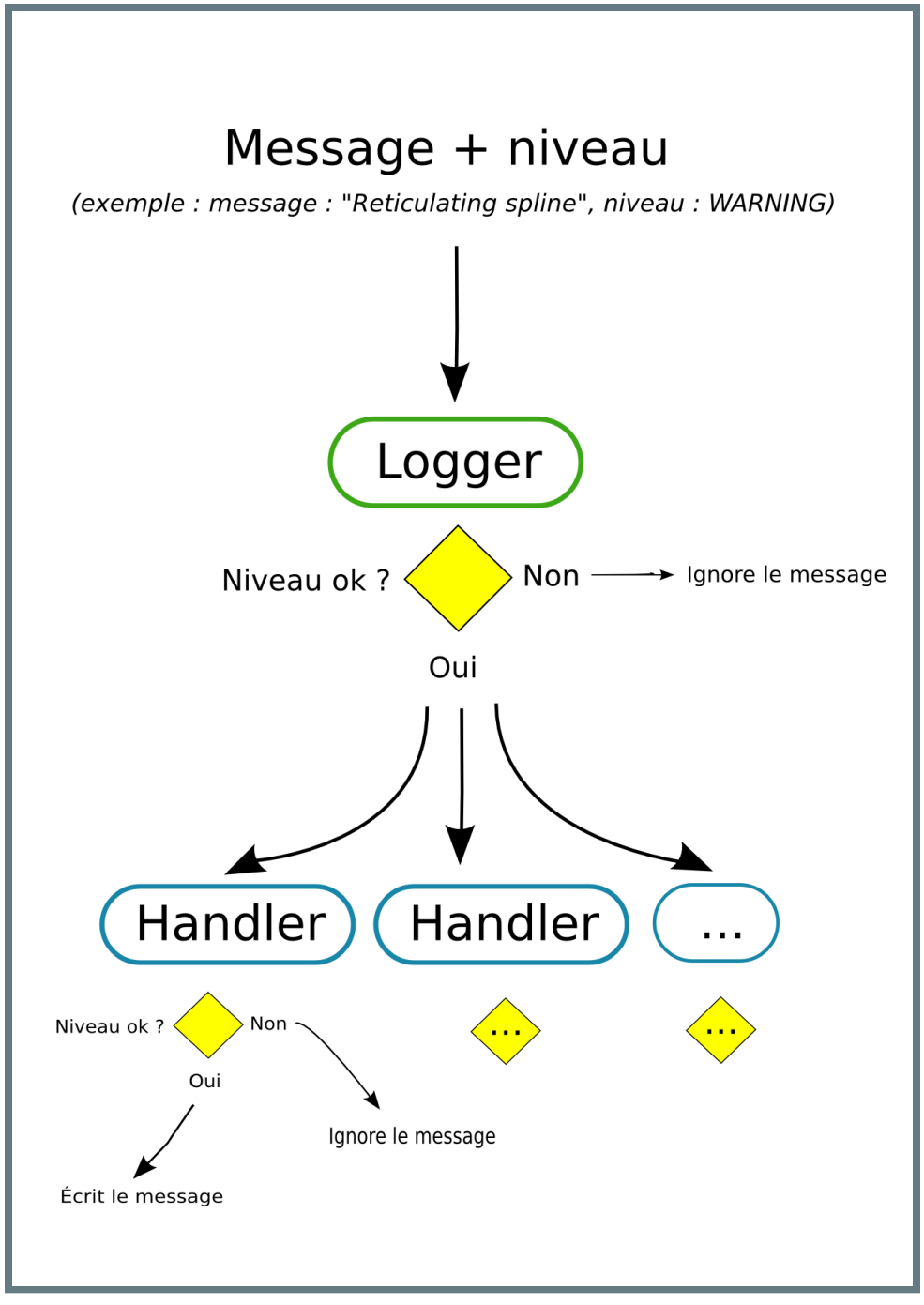
- Visibilité
  - Technique
  - Design
- Explication
  - Vulgarisation
  - Information
- Aide
  - Préanalyse
  - Exemples
- Référence
  - Localisation?
  - UUID!

RÉFÉRENCES

- Applying cardiac alarm management techniques to your on-call
- How to write a great error message, Thomas Fuchs
- The 4 H's of Writing Error Messages, Ben Rowe
- Alarm Fatigue, wikipedia
- The 5 Worst Error Messages in the History of Technology, Chris Bucholz
- S 164: Fall 2011 - Introduction to Computer Science HCI: Bad Examples: Error Messages
- Alarm management at AACN
- The 10 Commandments of Logging, Brice Figureau
- Loggly best practices
- 4 reasons a python logging library (…)
- Écrire des logs en Python, Sam & Max

ANNEXES

FONCTIONNEMENT D'UN LOGGER


Message + niveau
(exemple : message : "Reticulating spline", niveau : WARNING)
Logger
Niveau ok ?
Non
Ignore le message
Oui
Handler
Handler
...
Niveau ok ?
Non
Oui
Ignore le message
Écrit le message
...
...