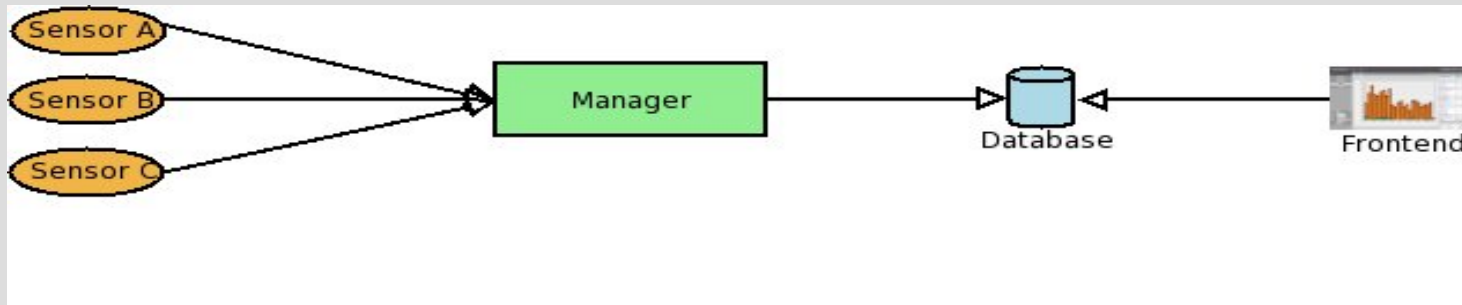


Prelude IDS

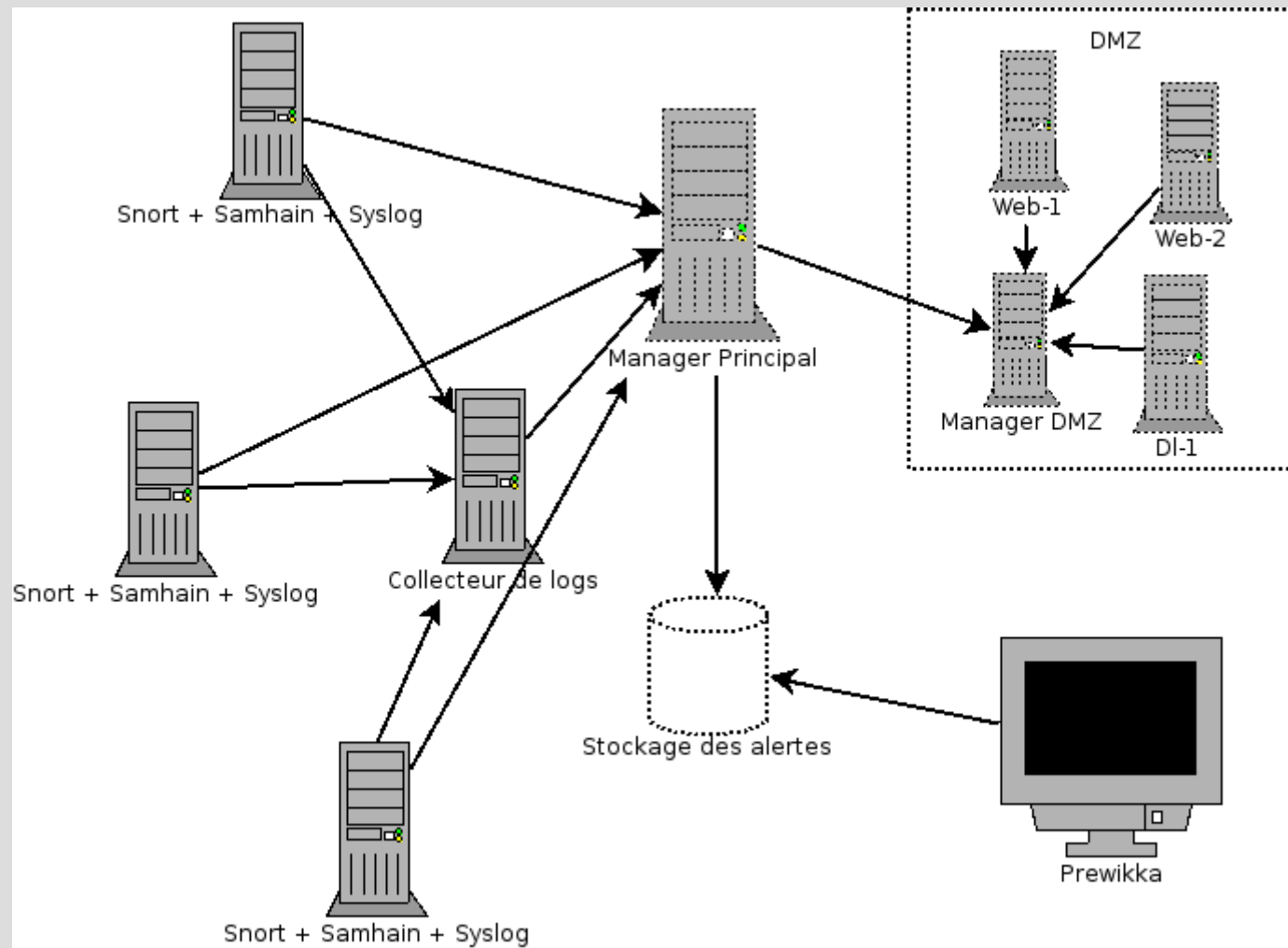
“You will have it up in the ass anyhow, but with prelude that will hurt less”

Basics



- Sensors :
 - Snort
 - Prelude LML
 - Samhain
 - Linux PAM
 -

Some architecture



IDMEF 1/2

alert:

analyzer(0):

analyzerid: 579774451772381

name: PAM

manufacturer: Sebastien Tricaud <http://www.kernel.org/pub/linux/libs/pam/>

model: PAM

version: CVS 0.79

class: pam

ostype: Linux

osversion: 2.6.11-1-686-smp

process:

name:

pid: 22906

create_time: 00:44:10 23/03/2005 (1111535050.50461)

classification:

text: Authentication Failure

source(0):

spoofed: unknown (0)

node:

category: hosts (6)

name: evil.cracker.org

user:

category: application (1)

user_id(0):

type: original-user (0)

tty: ssh

process:

name: ssh

pid: 22906

target(0):

IDMEF 2/2

```
decoy: unknown (0)
interface:
user:
  category: application (1)
  user_id(0):
    type: target-user (2)
    name: GROSNAINDESBOIS
assessment:
  impact:
    type: other (0)
    description: User not known to the underlying authentication module
```

Thanks...

“The beer appeal was enough to make me talk about
it :-)”