

SophiaConf 2012

ShinKen

The word 'ShinKen' is written in a stylized, black, serif font. The letter 'K' is highlighted in red. A graphic of a sword is integrated into the text, with the blade passing through the letters 'i', 'n', 'K', and 'e'. The hilt of the sword is visible on the left side.

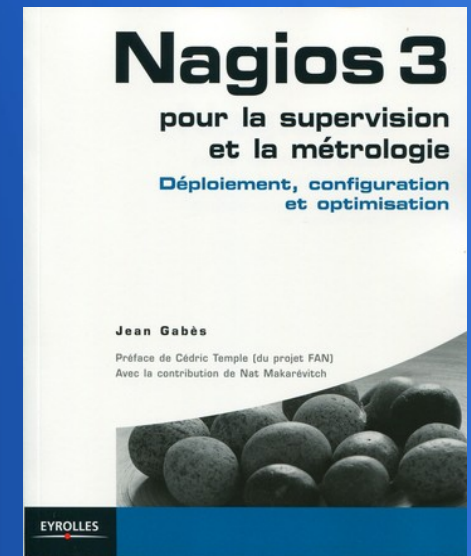
Jean Gabès

SophiaConf 
2012 Du 2 au 4 juillet

Qui suis-je ?

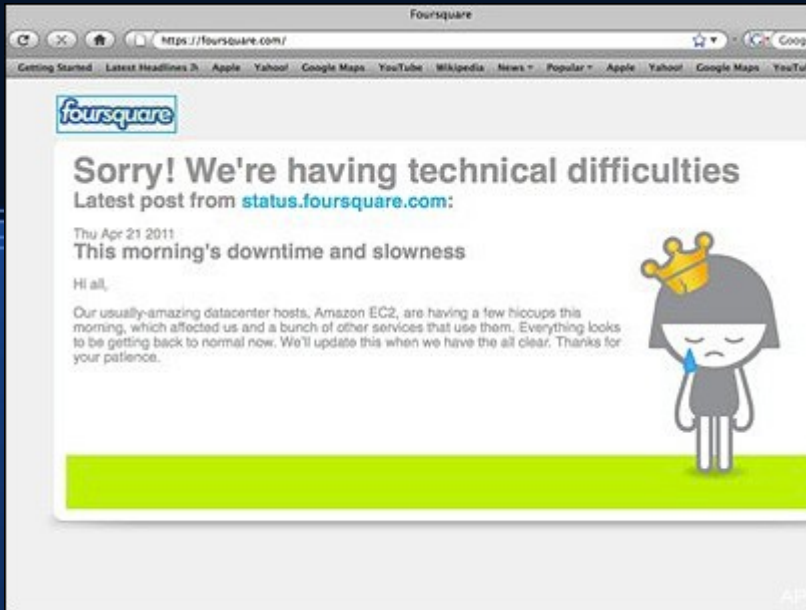
Jean Gabès

Administrateur système sur Bordeaux,
auteur du livre Nagios3 aux éditions Eyrolles
et de Shinken



Pourquoi superviser ?

Quand l'IT va mal, le business va mal...



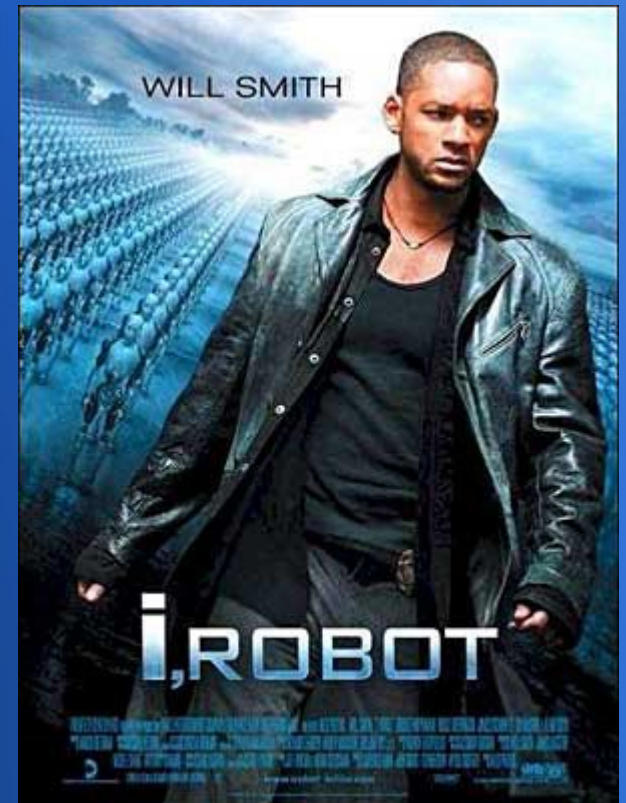
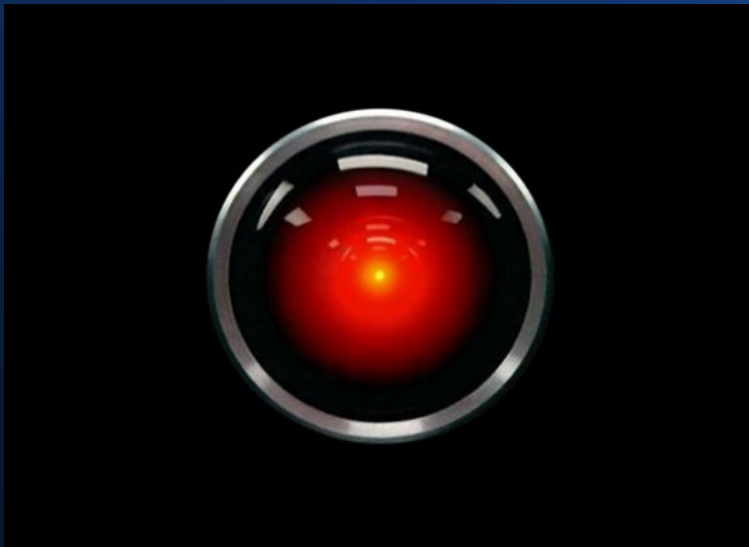
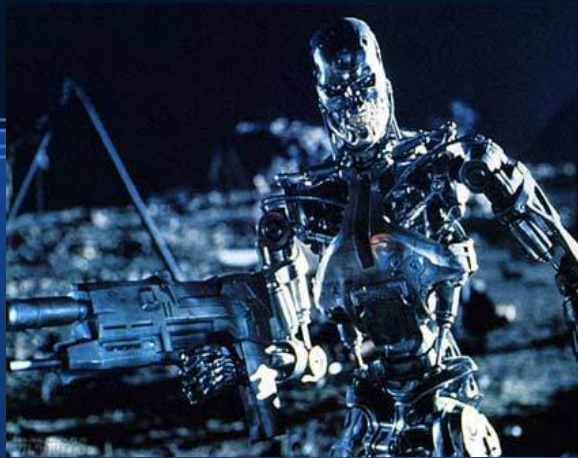
502. That's an error.

The server encountered a temporary error and could not complete your request.

Please try again in 30 seconds. That's all we know.



Ou voire pire....



Pour sauver le monde business :
Les outils de supervision !

Nagios[®]

 **MUNIN**



Bon il y en a pleins...

ZABBIX

Shinken



 **ICINGA**

openNMS[®]

Concernant la supervision pure IT, Nagios™® est
la référence de ces 10 dernières années ...

Concernant la supervision pure IT, Nagios™® est
la référence de ces 10 dernières années ...

... grâce à beaucoup de modules

- Mod_gearman : Distribution de la charge sur le LAN
- LiveStatus : accès aux données
- Thruk/Multisite/NagVis : vue temps-réel
- PNP, Graphite : graphiques

Et des plugins de supervisions

```
$ check_disks -w 90% -c 95%
```

```
Disks OK | /=50% /var=80% /data=35%
```

```
$ echo $?
```

```
0
```

Plugins & modularité sont bien !

Mais si ce n'était plus suffisant ?

L'IT grossit de jours en jours

IT

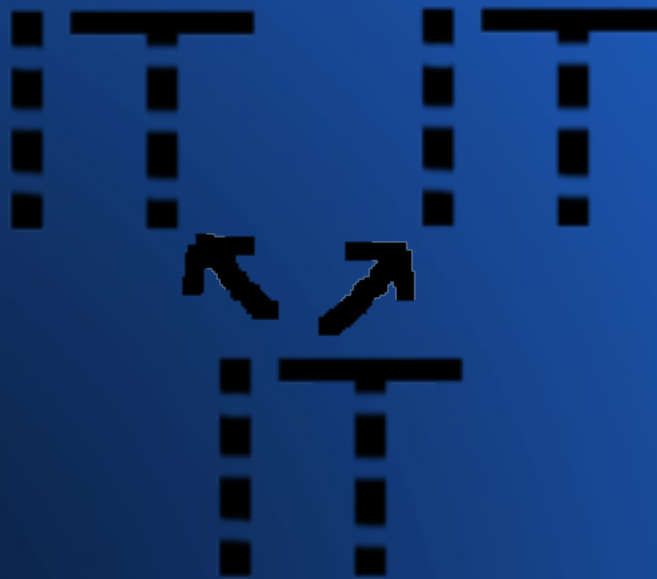
IT

IT

Avec plein de couches (physique, réseaux,
virtuel, ...)



Rempli de clusters



Et de sites distants



Difficultés classiques dans la supervision IT

- Trop de charge
- Gestion de la configuration
- Perte de site distant ?
- Haute disponibilité

Architecture idéale



Oui vous pouvez bricoler autour d'un Nagios™®
pour cela ...




... ou vous pouvez juste utiliser Shinken :)

Shinken est une réécriture complète de
Nagios™® (C) en Python

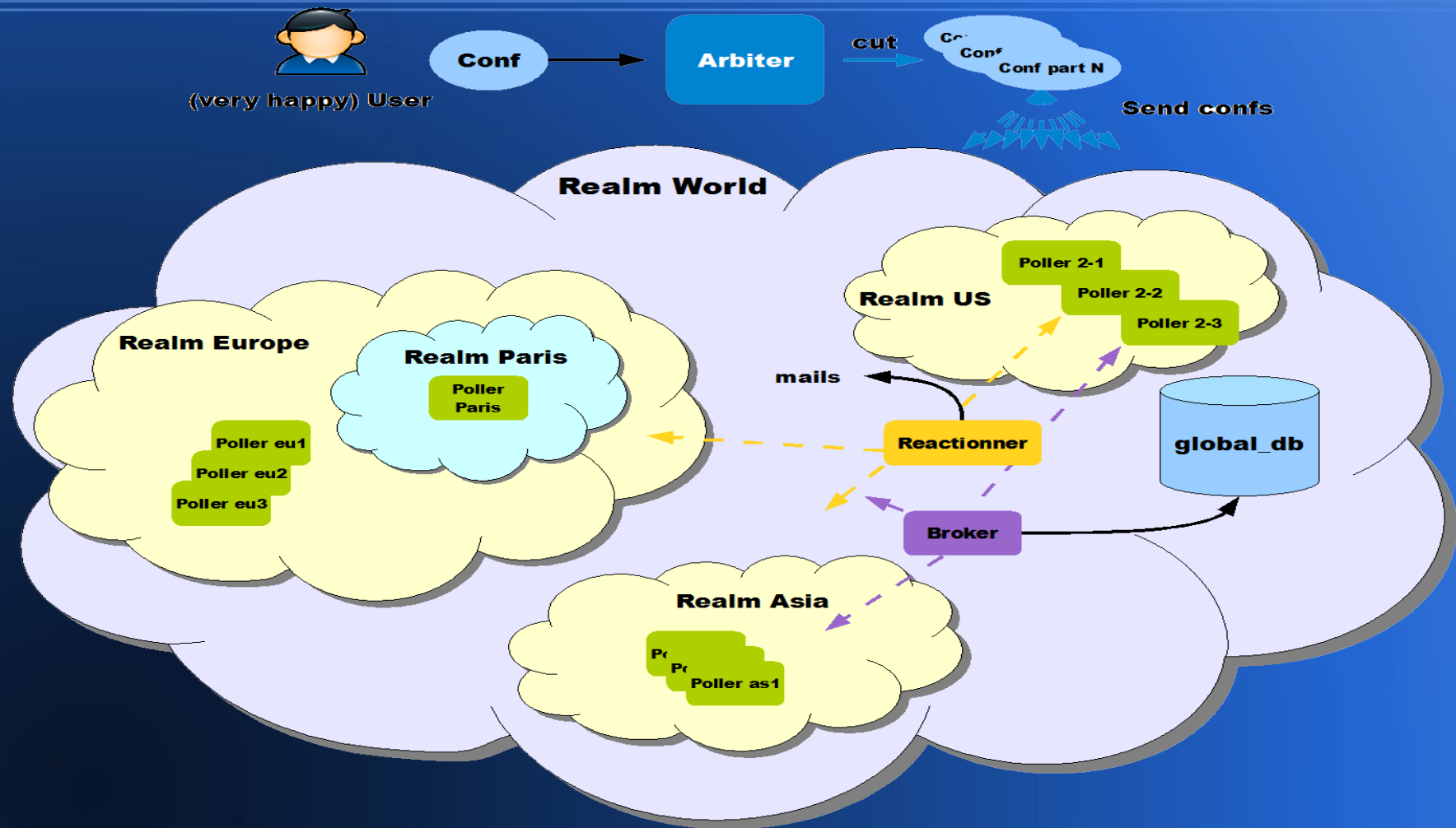
Attendez ! Python c'est lent !

Ok, on bench. Xeon 4cores@2.9ghz, 12Go ram,
dummy check

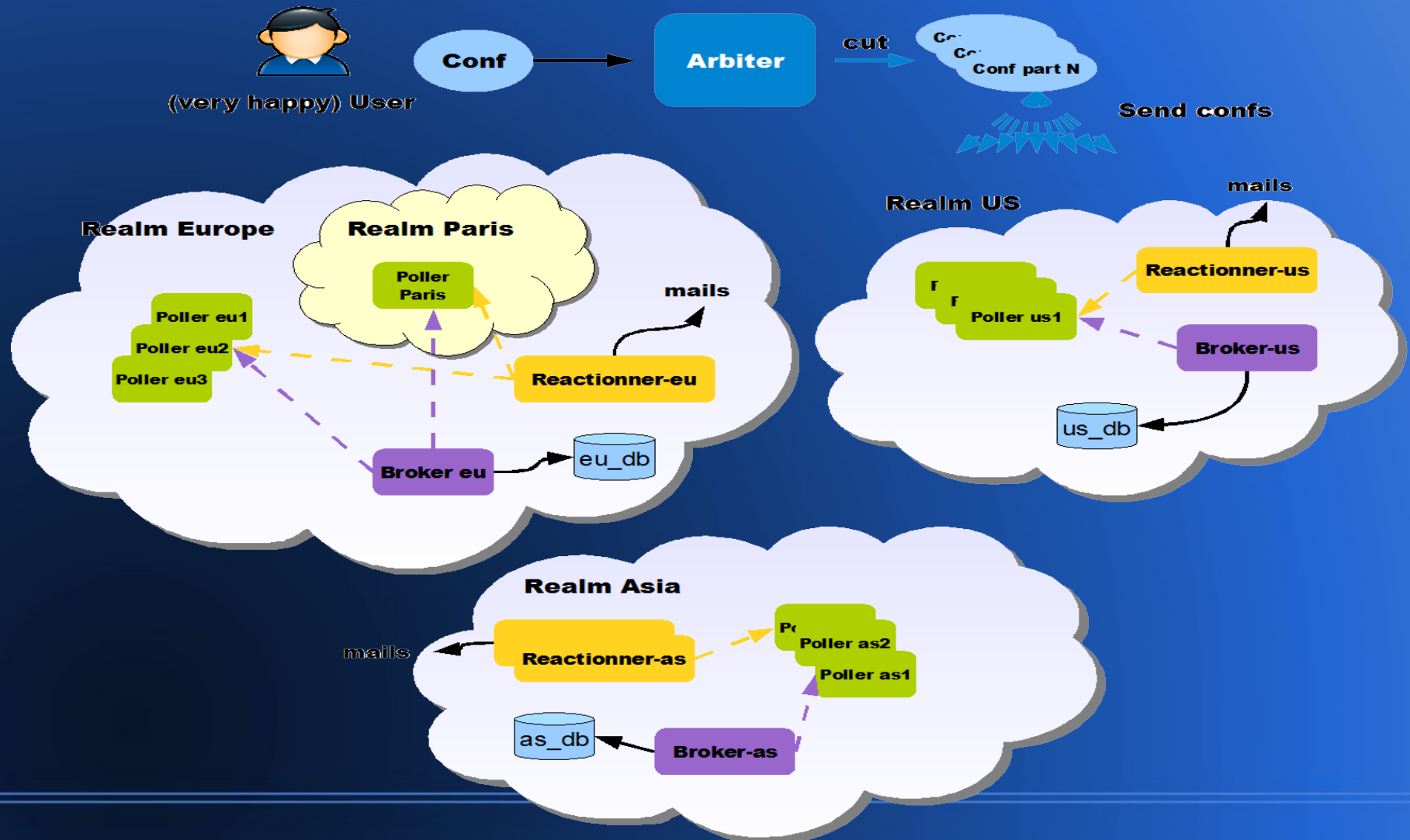
(en nombre max de checks en 5min)

- Nagios 3 (C) \Leftrightarrow icinga 1.6 (C) = 30K 
- Centreon-engine (C) = 25K 
- Shinken = 120K 

De grandes possibilités d'architecture



De grandes possibilités d'architecture



Les soucis de supervision IT sont réglés, mais
quid des problèmes des admins de 2012 ?

La virtualisation est partout



(OK peut être moins dans le futur avec la nouvelle politique de licence d'ESX5...)

Si un ESX crash, vous n'avez pas envie de recevoir 20+ alertes pour les VM dessus !

Que l'alerte de l'ESX. Simple : dépendance
d'hôte :)

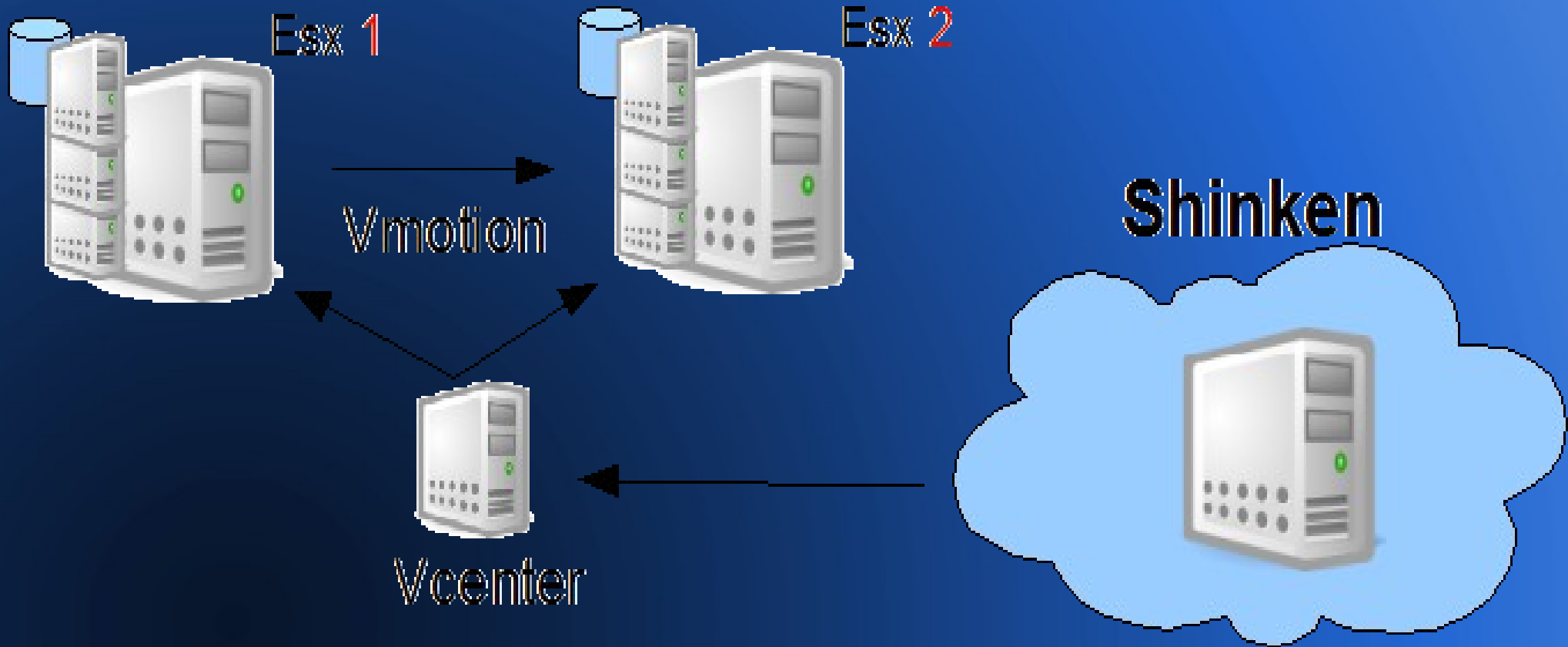


Mais les admins VMware sont des personnes étranges

Ils « VMotion » des VMs aussi souvent qu'un
codeur Perl tapes \$_

Donc oubliez la configuration en fichiers plats
manuels :)

Ils suffit d'utiliser le module Vmware™® pour
Shinken



OK, et si on s'attaquait à l'un des pires soucis
des admins ?

Pas la pénurie de café/bière...

Les fausses alertes !

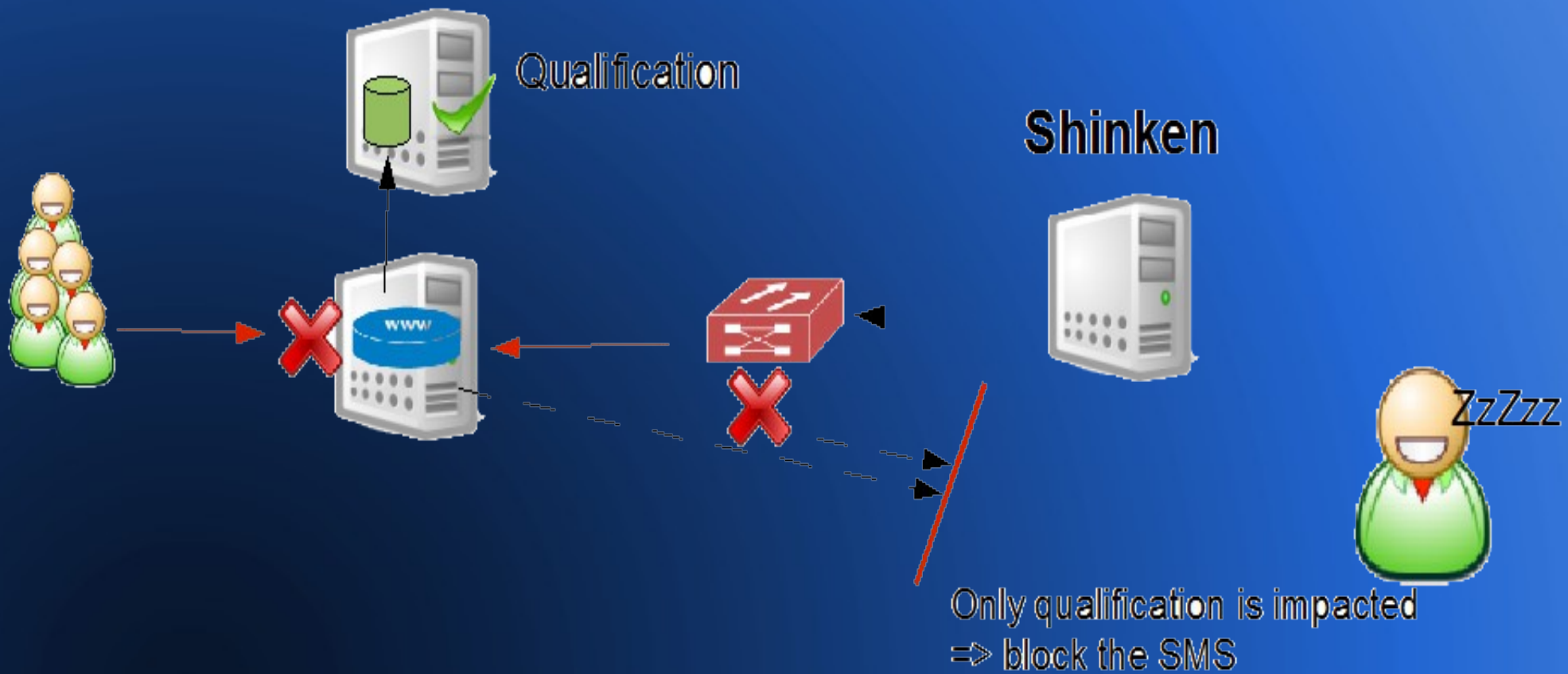


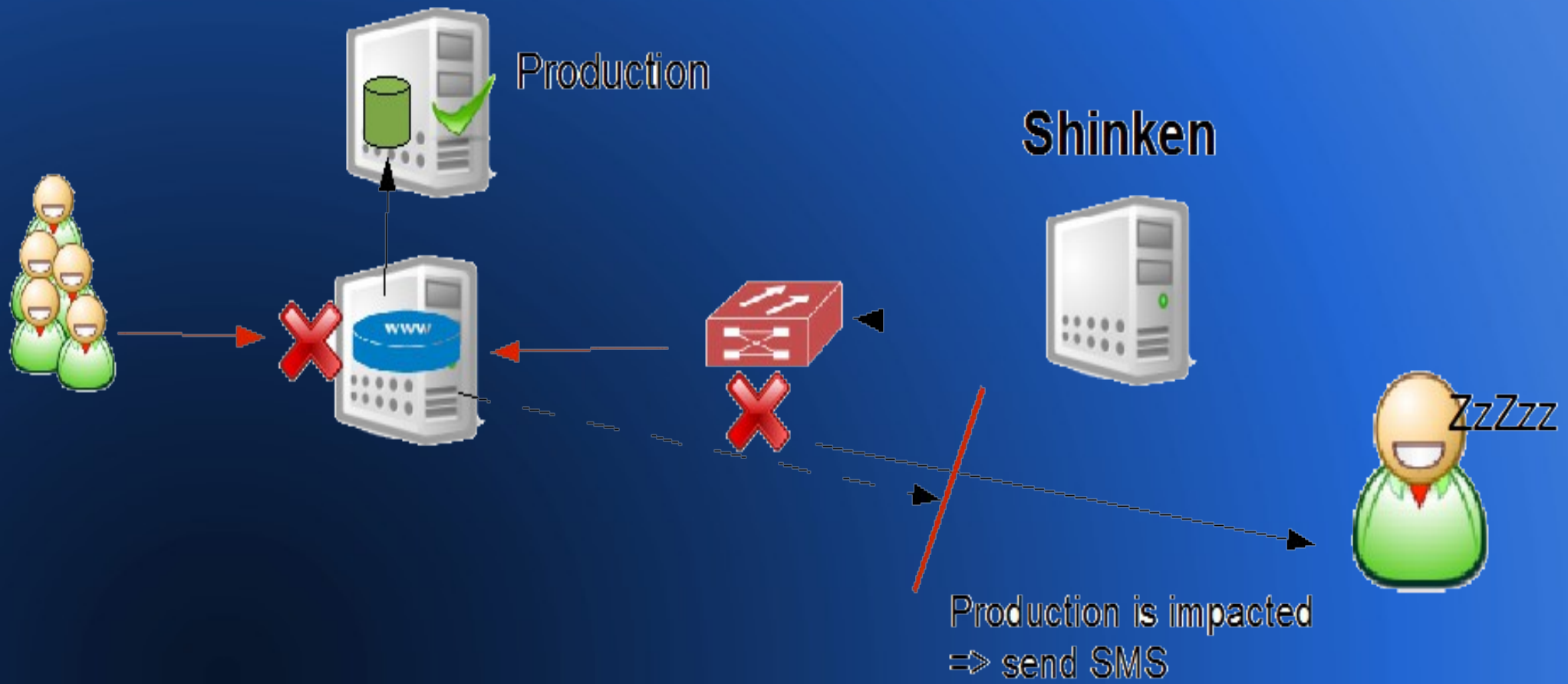
Exemple : une erreur critique sur de la qualification, est-ce vraiment si critique ?

Cas réel : un switch de production casse une application de qualification

Est-ce que l'on doit réveiller le pauvre admin à 3h
du mat pour ça ?? Non !

Se concentrer sur l'analyse des problèmes sources, et l'impact au niveau « business » des applications





La différence entre problèmes sources et impacts
est centrale dans Shinken

Et entre les niveaux d'importances business, plus
que juste warning/critical

Ok pour les alertes. Mais quid des interfaces graphiques ?

Shinken WebUI :

- Problèmes sources & impacts sur des vues différentes
- TOUT est trié suivant l'importance business
- Visualisation des dépendances sous forme d'arbres et de graphes
- HA et agrégation de données
- Pas de base de données !

- Très “visuelle”
- HTML5 (désolé pour IE6...)
- Limitation (volontaire...) des informations affichées
- Modulaire (PNP, graphite)
- Même votre boss va la comprendre...

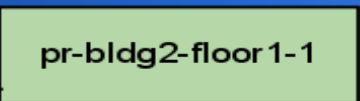
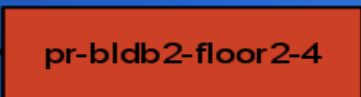
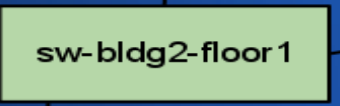
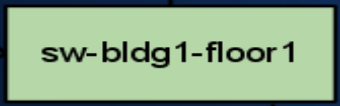
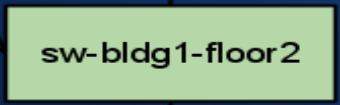
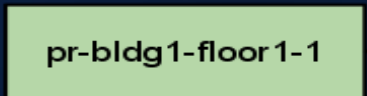
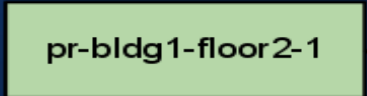
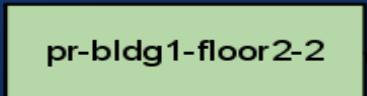
Deux types d'utilisateurs (incompatibles)

- Responsables : visualisation des impacts sur les applications end-users (et pourquoi elles sont tombées)
- Admins : visualisation des éléments IT qui sont les problèmes sources

- Vues Problèmes sources VS impacts
- Personne ne veut voir les deux
- Le tout trié suivant l'importance métier



&



Vue du responsable

Shinken Dashboard Impacts IT problems All Wall System Search

WWW is CRITICAL since 24s

CRITICAL: webserv1/WWW

Details Show impact map

Root problems unacknowledged :

sw-bldg2-floor2 is DOWN since 2m 8s
Try to fix it Acknowledge it!

Show dependency tree

- webserv1/app_web_apache_WWW_check_http is OK since 1m 37s
- dbsrv1/app_db_oracle_WWW_tbs_CMS_check_free is CRITICAL since 1m 58s
 - dbsrv1 is UNREACHABLE since 5s
 - sw-bldg2-floor2 is DOWN since 2m 8s **Root problem**
- dbsrv1/app_db_oracle_WWW_check_connect is CRITICAL since 1m 58s
 - dbsrv1 is UNREACHABLE since 5s
 - sw-bldg2-floor2 is DOWN since 2m 8s **Root problem**
- webserv1 is UP since 19s

Vue d'un administrateur

The screenshot displays the Shinken administrator interface. The top navigation bar includes 'Shinken', 'Dashboard', 'Impacts', 'IT problems', 'All', 'Wall', and 'System'. A search bar and user information 'Hi Admin' are also present. The main content area features a 'Select all' button and a '+ Add filters' button. The title 'Business impact : Top for business' is followed by three yellow stars. Below this, a table lists a single entry: 'sw-bldg2-floor2' with a red status indicator, a 'DOWN' label in a red box, '19s', and another 'DOWN' label. A 'No bookmarks' message is visible on the left side.

| Component | Status | Duration | Action |
|-----------------|--------|----------|--------|
| sw-bldg2-floor2 | DOWN | 19s | DOWN |

Et si l'admin veut voir pourquoi c'est si important...

The screenshot shows the Shinken monitoring interface. The top navigation bar includes 'Shinken', 'Dashboard', 'Impacts', 'IT problems', 'All', 'Wall', and 'System'. A search bar and user profile 'Hi Admin' are on the right. The main content area displays a 'Business impact : Top for business' section with three stars. Below this, a table shows the status of 'sw-bldg2-floor2' as 'DOWN' for 19s. A table below the status provides details for the host, realm, last check, next check, and actions. A list of impacted services follows, including 'UNKNOWN' for 'websrv1/WWW' and 'CRITICAL' for 'dbsrv1/app_db_oracle_WWW_tbs_SYSTEM_check_free'.

Select all

+ Add filters

No bookmarks

Business impact : Top for business ★★ ★

sw-bldg2-floor2 DOWN 19s DOWN

| Host | Realm | Last check | Next check | Actions |
|-----------------|-------|------------|------------|-------------------------|
| sw-bldg2-floor2 | All | 6s ago | in 1m 25s | Details |

Impacts:

- UNKNOWN for websrv1/WWW ★★ ★
- CRITICAL for dbsrv1/app_db_oracle_WWW_tbs_SYSTEM_check_free
- UNREACHABLE for dbsrv1
- UNKNOWN for dbsrv1/app_db_oracle_WWW_check_connect
- UNKNOWN for dbsrv1/app_db_oracle_WWW_dbcache
- UNKNOWN for dbsrv1/app_db_oracle_WWW_tbs\CMS_check_free
- UNKNOWN for dbsrv1/app_db_oracle_WWW_tbs_SYSAUX_check_free
- UNKNOWN for dbsrv1/app_db_oracle_WWW_tbs_USERS_check_free
- UNKNOWN for dbsrv1/os_linux_default_check_cron
- UNKNOWN for dbsrv1/os_linux_default_check_disks
- UNKNOWN for dbsrv1/os_linux_default_check_hardware
- UNKNOWN for dbsrv1/os_linux_default_check_inetd
- UNKNOWN for dbsrv1/os_linux_default_check_load
- UNKNOWN for dbsrv1/os_linux_default_check_ntp

Les deux vont comprendre un graphe

Shinken Dashboard: IT problems, All Wall, System

Search: Hi Admin

CRITICAL: webserv1/WWW
since 55s
Go to details

The graph displays a network topology with nodes and connections. Nodes include: prt-bldg1-floor2-1, prt-bldg1-floor2-2, prt-bldg1-floor2-3, sw-bldg1-floor2, webserv1, dbsrv1, and various checks like webserv1/WWW, web_apache_WWW_check_http, and app_db_oracle_WWW_tbs_CMS_check_free. Red 'X' markers indicate critical failures on several nodes and checks.

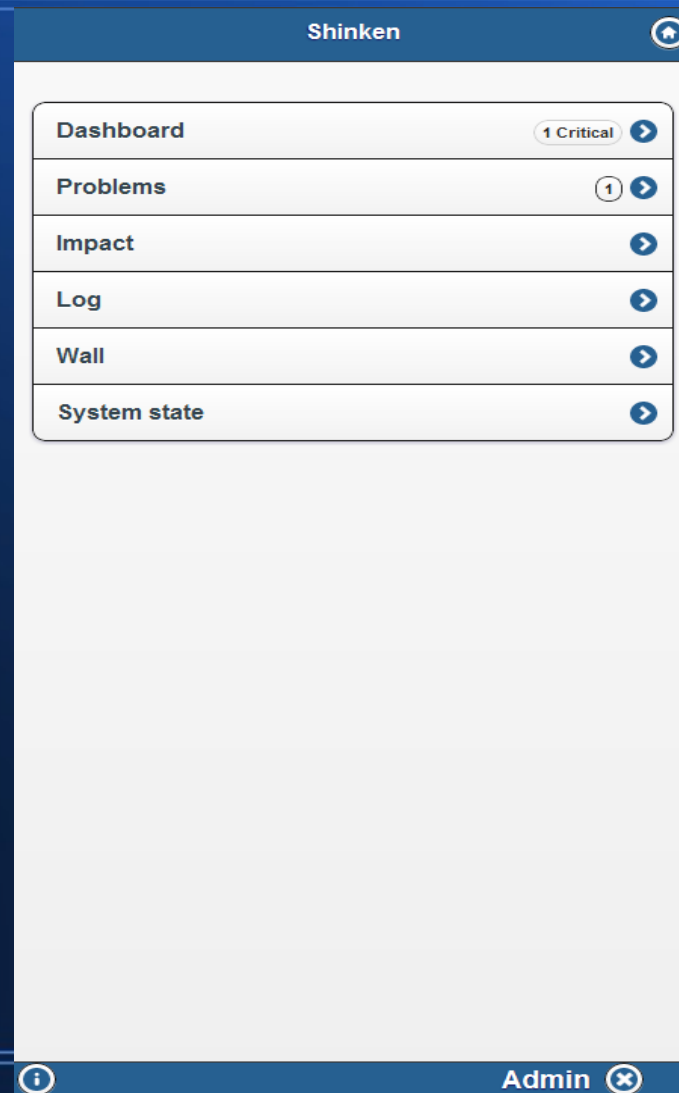
Et chacun peut avoir SON dashboard

The screenshot displays the Shinken dashboard interface. At the top, there is a navigation bar with 'Shinken', 'Dashboard', 'Impacts', 'IT problems', 'All', 'Wall', and 'System'. A search bar and user information 'Hi Admin' are also present. A green button '+ Add a new widget' is located in the top right corner.

The dashboard is divided into three main sections:

- IT problems:** A list of issues with status icons (DOWN or CRITICAL) and star ratings. The list includes:
 - DOWN for sw-bldg2-floor2 (3 stars)
 - DOWN for prt-bldg1-floor1-1 (3 stars)
 - DOWN for prt-bldg1-floor1-2 (3 stars)
 - DOWN for prt-bldg1-floor2-1 (3 stars)
 - DOWN for prt-bldg1-floor2-2 (3 stars)
 - DOWN for prt-bldg1-floor2-3 (3 stars)
 - CRITICAL for localhost/LocalCpu (3 stars)
 - CRITICAL for localhost/LocalMem (3 stars)
- Dependencies graph of webserv1:** A network diagram showing the status of 'webserv1' and its dependencies. The root node 'webserv1' is highlighted in a yellow box and is 'UP: webserv1 since 8m 10s'. It has a 'Go to details' button. The graph shows dependencies on 'sw-bldg1-floor2' (UP) and various OS and application checks. A red 'X' icon is placed over the 'webserv1' node in the graph, indicating a conflict or error.
- Impacts:** A section showing the impact of the selected widget. It displays a large red 'X' icon and the text 'CRITICAL for webserv1/WWW' (3 stars).

Et sa version « mobile »



Back Shinken

Dashboard Problems Impacts

☆☆☆🔴 DOWN: sw-bldg2-floor2 +

i Admin ✕

The image shows a mobile application interface for 'Shinken'. At the top, there is a navigation bar with a 'Back' button on the left and a home icon on the right. Below this is a tabbed interface with three tabs: 'Dashboard', 'Problems', and 'Impacts'. The 'Problems' tab is currently selected. The main content area displays a single alert: '☆☆☆🔴 DOWN: sw-bldg2-floor2', where the first three stars are yellow and the fourth is red. A plus sign icon is to the right of the alert. At the bottom of the screen, there is a footer bar with an information icon on the left and the text 'Admin' followed by a close icon on the right.

Demo : <http://demo-shinken.web4all.fr/>

OK, on voit seulement ce que l'on souhaite voir.
Bien.

Mais une lourde tâche reste : rajouter nos serveurs dans l'outil!

Les templates de configuration de Nagios™®
sont indispensables!

I'm your father



Mais pas suffisant. Il reste encore trop d'éléments à définir

Shinken permet d'accrocher des vérifications par des expressions complexes du genre « Linux&Prod »

Ceci permet de n'avoir qu'à « tagger » ses machines au lieu de multiplier les groupes et sous groupes de serveurs

Dans Nagios™®, on considère que 80% de la configuration consiste en l'écriture des services.

Shinken propose des solutions pour limiter
fortement ces 80%.

Exemple : clé `duplicate_foreach`
Génère un service par “propriété” d'un hôte.

```
Define host{  
  host_name  srv-lin-1  
  Use        linux  
  _disks     /, /var, /data  
}
```

```
Define service {  
  host_name  linux  
  Register   0  
  Description Disk $KEY$  
  check_command check_disk!$KEY$  
}
```

Fait prouvé : un bon informaticien est fainéant

Fait sûrement vrai : les admins sont de bons informaticiens!



Un admin préfère éviter de :

- Écrire un plugin de 0
- Tagger manuellement ses machines
- Écrire la configuration de nouveaux types de serveurs/applications

- Plugins : Merci Monitoring-exchange.org!
- Tagging : merci skonf discovery
- Nouvelle configuration : merci les packs Shinken

Pourquoi tagger manuellement ses serveurs quand on peut juste écrire des règles pour le faire?

Module de découverte de Shinken!

- Runners : scripts qui “scanne” et qui sort des données
- Rules : lit les données et génère de la configuration

Ex : nmap runner scanne un serveur et exporte des données

```
$ nmap_discovery_runner.py -t localhost  
localhost::isup=1  
localhost::os=linux  
localhost::osversion=2.6.x  
localhost::osvendor=linux  
localhost::macvendor=hp  
localhost::openports=22,80,3306  
localhost::fqdn=localhost  
localhost::ip=127.0.0.1
```


localhost : use ssh,mysql,http,linux

Découverte multi-niveaux :

- 1 Si on match une donnée
- 2 On lance un nouveau runner
- 3 On ré-applique les règles
- 4 GOTO 1

Ex : découverte des shares Windows

```
define discoveryrun {  
    discoveryrun_name      WindowsShares  
    discoveryrun_command  discovery_windows_share  
  
    # And scan only windows detected hosts!  
    os                    windows  
}
```

Résultat

```
define host {  
    host_name      win-srv  
    use            windows  
  
    _shares        Work,Public,Private  
}
```

Lancement en CLI :

```
shinken-discovery -c etc/discovery.cfg --db Mongoddb -m  
'NMAPTARGET=localhost'
```


Ou mieux : l'UI sKonf!

sKonf :

- UI pour la gestion facile de sa configuration
- Découverte ou configuration classique
- Gère les paramètres spécifiques de Shinken
- Stade Beta avancé

Discover your new hosts

Scan:

localhost oracleserver mailserver

▼ Show advanced options

Scan!

Here are the results :

| | | |
|--|----------|---|
| <input type="text" value="oracleserver"/> | Hostname | <input type="button" value="✕"/> |
| <input type="text" value="oracle x linux x ssh x generic-host x"/> | | Tags |
| | | <input type="button" value="✓ Validate"/> |

| | | |
|--|----------|---|
| <input type="text" value="mailserver"/> | Hostname | <input type="button" value="✕"/> |
| <input type="text" value="windows x windows2008 x http x https x smtp x imap x imaps x generic-host x"/> | | Tags |
| | | <input type="button" value="✓ Validate"/> |

| | | |
|--|----------|---|
| <input type="text" value="localhost"/> | Hostname | <input type="button" value="✕"/> |
| <input type="text" value="mysql x linux x http x ssh x generic-host x"/> | | Tags |
| | | <input type="button" value="✓ Validate"/> |

Generic

Macros

Notifications

Dependencies

Advanced

Hostname ?

Display name

Address

Tags

Maintenance Period

Check Period

Check Command Args

Max Check Attempts

Normal Check Interval*
60 seconds

Active Checks Enabled

Passive Checks Enabled

Generic

Macros

Notifications

Dependencies

Advanced

ORACLE

DATABASES TEST,PROD

LINUX

CPU_CRIT 90% Set ?

CPU_WARN 80% Set ?

LOAD_CRIT 3,3,3 ?

LOAD_WARN 2,2,2 ?

MEMORY_CRIT 95,50 ?

MEMORY_WARN 90,20 ?

SNMPCOMMUNITY \$SNMPCOMMUNITYREAD\$?

STORAGE_CRIT 95% Set ?

STORAGE_WARN 90% Set ?

SSH

SSHPORT 22

Packs ?

Packs = fichier zip avec tout ce dont vous avez besoin sur un sujet particulier (comme Linux, Windows ou EMC)

- Fichiers cfg (templates, commands, services, discovery, ...)
- Templates de graphiques (PNP ou Graphite)
- Images (pour que votre UI soit jolie :))
- Fichier .pack file (json, descriptif)
- Pas (encore) d'installation de plugin

Heu... pourquoi créer un .zip avec tout ça?

- A. Le déplacer dans /dev/null
- B. Le partager!
- C. Me l'envoyer pour que je lance un outil “open core” comme NagiosXI
- D. Obiwan Kenobi

Partager via community.shinken-monitoring.org
(démon hostd, disponible dans les sources
Shinken)

Créer un tel fichier zip est aussi facile que de
lancer :

```
$ shinken-packs -c -p /path/to/linux.pack
```

Et pour l'envoyer :

```
$ shinken-packs -u -k APIKEY -z /tmp/linux.zip
```

(une clé api est générée dès que vous êtes enregistrés sur le site)

Et pour les récupérer?

Sur le site :



Pack linux

Publisher: naparuba

Description: Standard linux checks, like CPU, RAM and disk space. Checks are done by SNMP.

Documentation: [Link](#)

 Download it!

Host tags

-  LINUX

Services linked

- Load
- Disks
- Memory
- Cpu
- NetworkUsage

Ou directement depuis l'UI sKonf :

Get new packs

Tags

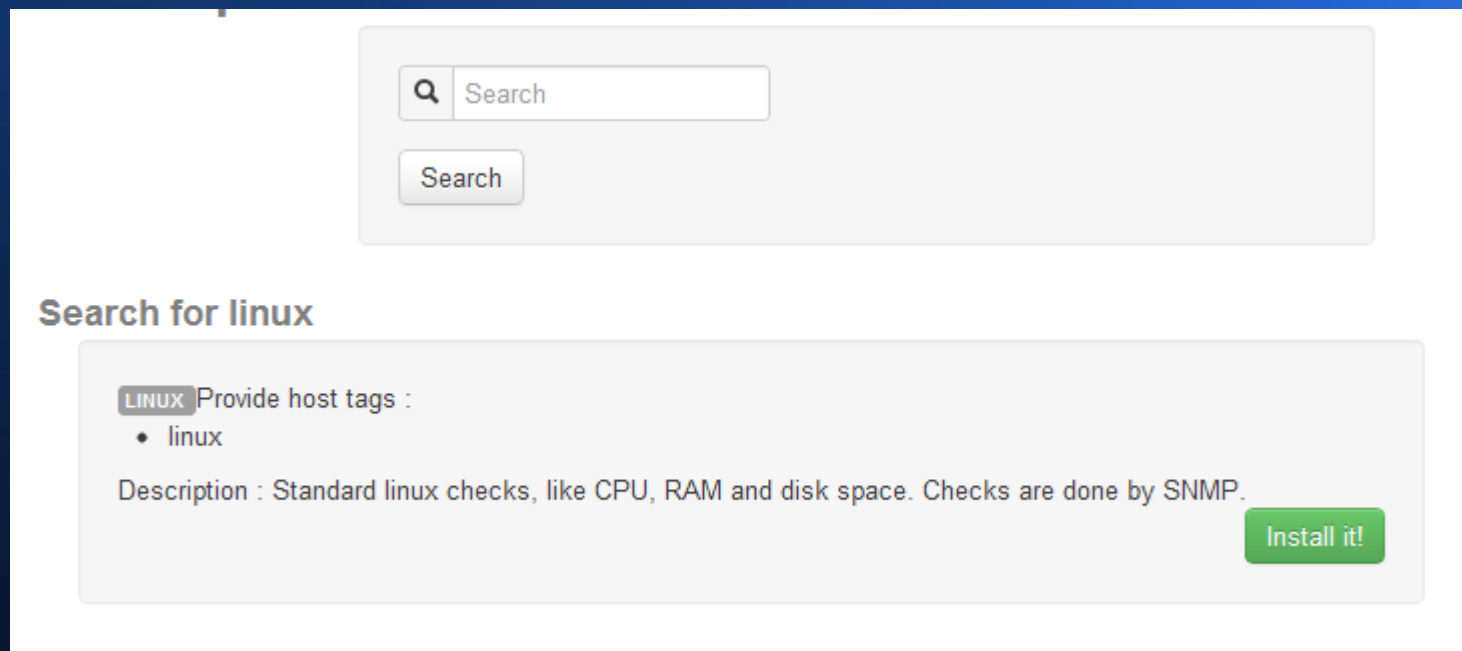
[aix \(1\)](#) [akcp \(1\)](#) [databases \(4\)](#) [dc \(1\)](#) [emc \(1\)](#) [environmental \(1\)](#) [exchange \(1\)](#) [hp \(2\)](#) [hpux \(1\)](#) [iis \(1\)](#) [linux \(1\)](#) [microsoft \(3\)](#) [mongodb \(1\)](#) [mssql \(1\)](#)
[mysql \(1\)](#) [netapp \(1\)](#) [oracle \(1\)](#) [os \(4\)](#) [printer-hp \(1\)](#) [printers \(1\)](#) [sample \(1\)](#) [sandbox \(1\)](#) [servers \(1\)](#) [storage \(2\)](#) [virtualization \(1\)](#) [vmware \(1\)](#) [windows \(1\)](#)

All categories

(0)

- [databases \(4\)](#)
- [storage \(2\)](#)
- [servers \(1\)](#)
- [environmental \(1\)](#)
- [sandbox \(1\)](#)
- [virtualization \(1\)](#)
- [printers \(1\)](#)
 - [printers/hp \(1\)](#)
- [os \(4\)](#)
- [microsoft \(3\)](#)

Depuis sKonf :



The screenshot displays the sKonf search interface. At the top, there is a search bar with a magnifying glass icon and the text "Search". Below the search bar is a "Search" button. The search results are displayed under the heading "Search for linux". The first result is a card with a "LINUX" tag, the text "Provide host tags :", a bulleted list containing "linux", and a description: "Description : Standard linux checks, like CPU, RAM and disk space. Checks are done by SNMP." A green "Install it!" button is located at the bottom right of the result card.

Search

Search

Search for linux

LINUX Provide host tags :

- linux

Description : Standard linux checks, like CPU, RAM and disk space. Checks are done by SNMP.

Install it!

Au final ?

- L'architecture est adaptable aux grands environnements
- Beaucoup d'améliorations par rapport à Nagios™®
- La WebUI est géniale, sKonf le sera prochainement
- Des triggers à la Zabbix arrivent!
(corrélation&KPI)
- Lancement de services professionnels autour du projet :)

Merci

Des questions?