



Formation Monitoring

Jules GONZALES
Bence KOLONICS

30 Mars 2022



Menu du jour. ... bah non t'as cru ahah

- Par contre vu le tacos qu'on s'est tapé avant..... Ce ratio il te donne faim ?

- **Qu'est-ce que le monitoring ?**
- **Cluster ELK**
- **Zabbix**

- **Qu'est-ce que le monitoring ?**
- **Cluster ELK**
- **Zabbix**

Qu'est-ce que le monitoring ?



Qu'est-ce que le monitoring ?



« Le savoir c'est le pouvoir » - *Dan ABNETT*

- Art de savoir en temps réel ce qu'il se passe
- Anticiper les problèmes
- Consulter un historique de problèmes
- Centraliser des informations
- Retrouver des bribes d'informations facilement

Qu'est-ce que le monitoring ? - Komenkonfait



Qu'est-ce que le monitoring ? – Et à MiNET ?



Monitoring général



NETDATA

Pare-feu



kibana



logstash



elasticsearch

Logs

- **Qu'est-ce que le monitoring ?**
- **Cluster ELK**
- **Zabbix**



- Moteur de recherche et d'analyse RESTful distribué
- NoSQL (indexation documents orientés texte)
- Moteur de recherche adaptable et puissant
- Utilisation de Lucene : 

Chaque requête -> Poids des mots -> Score.

Un mot = une colonne par document

Cluster ELK – Elasticsearch



TEXTE A - En été dans les près les oiseaux
transpirent des pieds **et** l'odeur **de** leurs chaussettes
fait pousser les paquerettes...

TEXTE B - Un régiment **de** fromages
blancs, partait en guerre contre les
camemberts...

Recueil de textes cultivants...

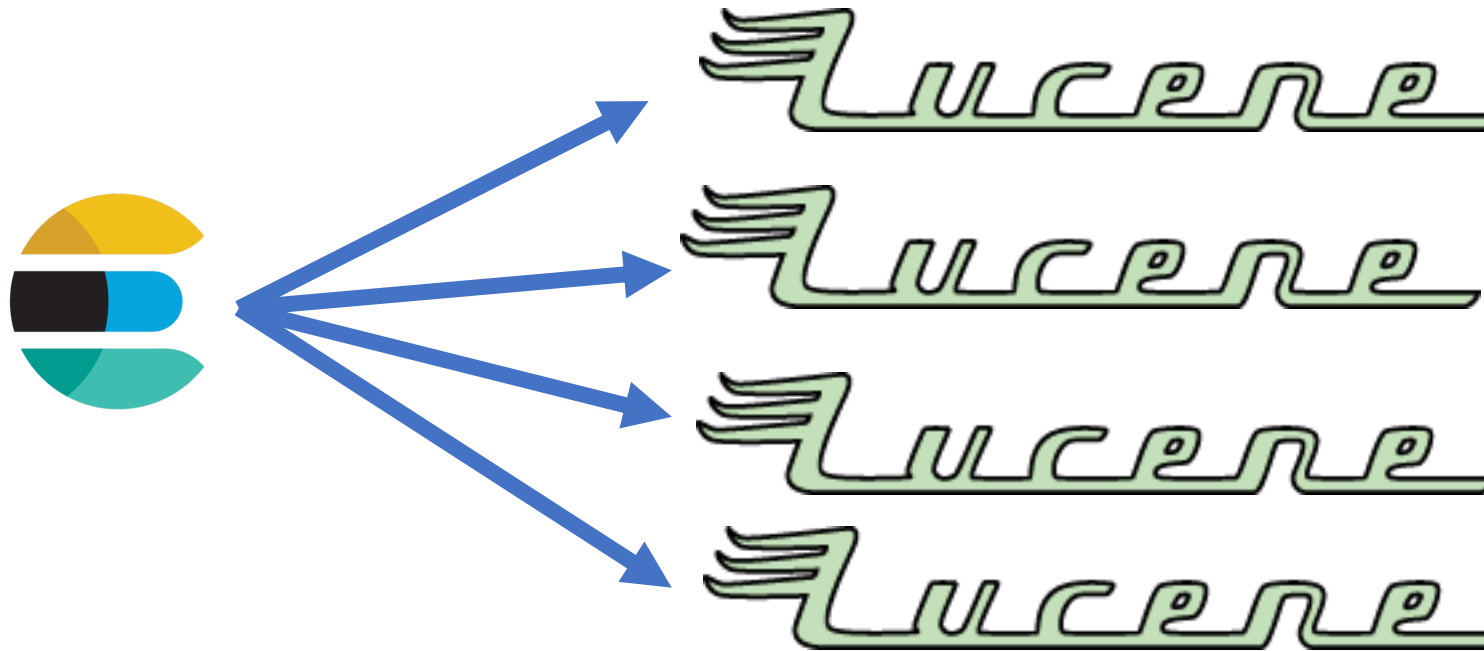
TEXTE C - Qui **peut** faire **de** la voile sans vent ?
Qui **peut** ramer sans rames ? **Et** qui **peut** quitter
son ~~mandat~~ **ami**, sans verser de larmes ?

TEXTE D - **Je** suis un pantin, qu'on a
maltraité, qu'on a accroché au fond
d'une vitrine. **Je** vous en supplie, il
faut m'acheter, **je** serai votre **ami**, on
peut tout me dire !

	Texte A	Texte B	Texte C	Texte D
de	1	1	1	0
je	0	0	0	3
peut	0	0	3	1
ami	0	0	1	1



Distribution des données



ROUTAGE, TRAITEMENT SIMULTANE, REPLICATION



Sharding

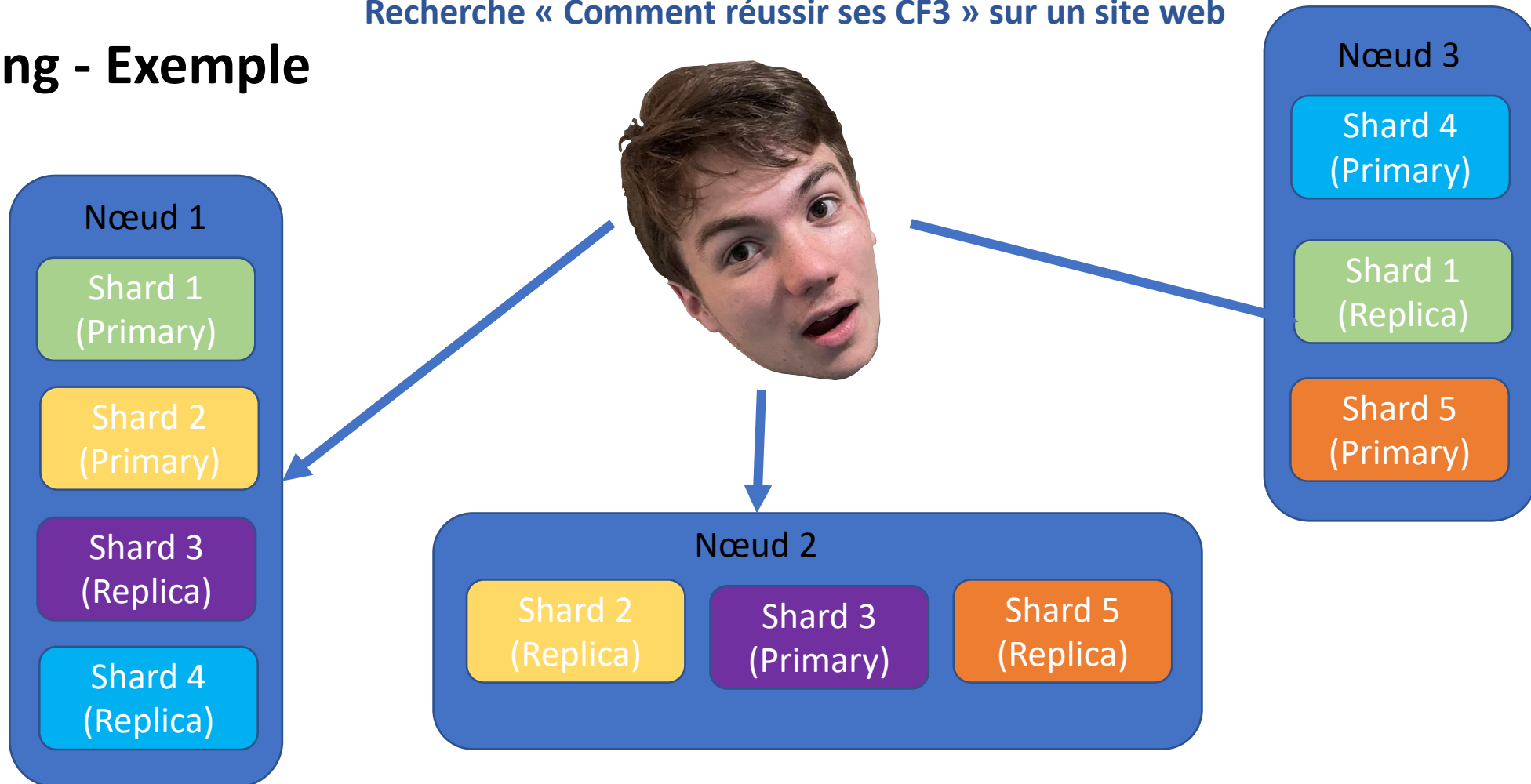
Index : collecte de documents en lien les uns avec les autres.
Décomposé en shards

Shard : Morceau d'index, contient les documents. (peut être **Primaire** ou **Repliqué**)



Recherche « Comment réussir ses CF3 » sur un site web

Sharding - Exemple





Exploitation des données

Liste des index : *https://cluster/_cat/indices*

Structure d'un index (mapping) : *<https://cluster/nomindice/>*

Lecture des données d'un index: *https://cluster/nomindice/_search*

Exemple :

```
curl -XGET -H "Content-Type: application/json" https://formation-monitoring.minet.net/_search?q=title: Star Wars | json_pp
```

A vous !

- **Donnez les noms des index présents sur la machine de TP disponible à l'adresse <https://formation-monitoring.minet.net/>**
- **Trouvez la structure des données puis affichez celles-ci**



Exploitation des données

Requêtes JSON

`curl -XGET -H 'Content-Type: application/json' https://formation-monitoring.minet.net/ -d @nomfichier`

```
{
  "query": {
    "match": {
      "fields.title": "Star Wars"
    }
  },
  "fields": [
    "fields.title"
  ],
  "_source": false
}
```



Exploitation des données

Requêtes JSON

Must : le résultat DOIT résoudre les conditions citées

Should : le résultat a un score ++ si la condition est remplie

Must not : le résultat ne DOIT PAS résoudre les conditions citées

Range : Permet de vérifier des inégalités mathématiques

A vous !

- Affichez la liste des films dont un acteur est Nathalie Portman et le directeur est Alan Taylor et dont le score est **OBLIGATOIREMENT** inférieur à 500. Faire apparaître les champs étudiés.

```
{
  "query": {
    "bool": {
      "must": [
        {
          "match": {
            "fields.actors": "Harrison Ford"
          }
        },
        {
          "range": {
            "fields.rank": {
              "lt": 1000
            }
          }
        }
      ]
    }
  },
  "_source": false,
  "fields": [
    "fields.title"
  ]
}
```



- Pipeline destiné au traitement des données
- Ingère des documents
- Filtre
- Transforme -> Uniformisation
- Renvoi

Cluster ELK – Kibana



- Interface graphique utilisateur
- Visualisation
- Navigation





Syntaxe des recherches

field:value : Recherche la valeur dans le champ spécifié

value : Recherche la valeur dans tous les champs

Value : toto tata : Recherche toto ou tata dans les champs

Value « toto tata » recherche « toto tata » dans les champs

Value1 AND Value2

Value 1 OR Value2

Value~ : valeur ressemblant à la valeur spécifiée

Date:[from:to] : Valeur comprise dans la plage temporelle spécifiée

A vous ! On recommence ! <https://formation-monitoring-kibana.minet.net/>

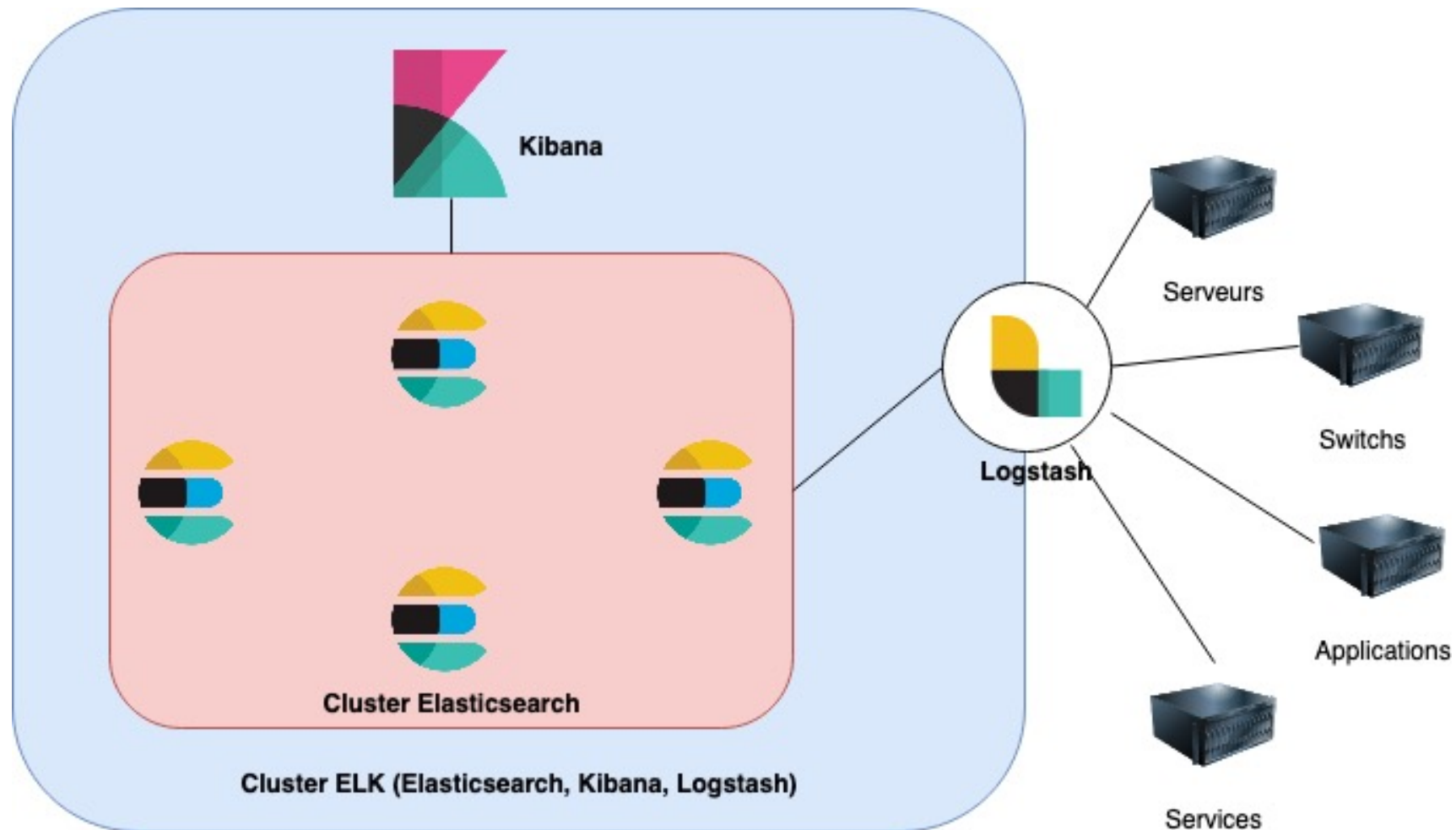
- Affichez la liste des films dont un acteur est Nathalie Portman et le directeur est Alan Taylor et dont le score est inférieur à 500. Ne faire apparaître que les champs étudiés.



Monitoring du cluster - Hearthbeat

Name ↑	Alerts	Status	Shards
 es-dhalsim http://localhost:9200	 Clear	 Online	84
 es-luffy http://localhost:9200	 Clear	 Online	83
 es-magus http://localhost:9200	 Clear	 Online	83
 es-padon http://localhost:9200	 Clear	 Online	84

Cluster ELK – Schéma général



- **Qu'est-ce que le monitoring ?**
- **Cluster ELK**
- **Zabbix**

- **Le serveur de traitement**
- **La base de données**
- **L'interface Web**
- **L'Agent***
- **Le Proxy***
- **Le SNMP***



Zabbix – Le serveur de traitement



- écrit en C
- Processus central
- Interrogations et les réceptions
- Utilisation d'items et de triggers
- Notifications

Zabbix – La base de données



ORACLE



Zabbix – L'interface graphique



Merci le shutdown sauvage de discovery !

Problèmes							
temps	Info	Note	Problème - Severité	Operational data	Duration	Acquired	Actions
17:56:22	kea2		kea-dhcp4 is not running	0	8m 46s	Non	84
17:56:10	kea30		kea-dhcp4 is not running	0	8m 58s	Non	84
17:34:52	Ldap-slave		LDAP service is down on Ldap-slave	Down (0)	30m 16s	Non	83
17:33:23	kea2		kea-dhcp6 is not running	0	31m 45s	Non	85
17:32:50	adh6-api		Service not publicly available	1	32m 18s	Non	83
17:32:43	kea		kea-dhcp6 is not running	0	32m 25s	Non	85
17:32:42	kea		kea-dhcp4 is not running	0	32m 27s	Non	85
28/03/2022 18:38:24	titania		Ceph cluster in WARN state	1	1j 23h 26m	Non	82
25/02/2022 02:14:32	obiwan		mumudvb is not running	0	1m 3j 14h	Non	82
17:56:22	...		...	...	...	...	...

Zabbix – L'interface graphique



Création d'un item

Item Tags Preprocessing

* Name CPU load

Type Zabbix agent

* Key system.cpu.load

Type of information Numeric (float)

* Host interface 127.0.0.1:10050

Units

* Update interval 1m

Custom intervals

Type	Interval	Period
Flexible	Scheduling	50s
		1-7,00:00-24:

Add

* History storage period Do not keep history Storage period 90d

* Trend storage period Do not keep trends Storage period 365d

Zabbix – L'interface graphique



Création d'un trigger

Trigger Tags Dependencies 1

* Name High CPU utilization (over {CPU.UTIL.CRIT}% for 5m)

Event name High CPU utilization (over {CPU.UTIL.CRIT}% for 5m)

Operational data Current utilization: {ITEM.LASTVALUE1}

Severity Not classified Information **Warning** Average High Dis

* Expression `min(/New host/system.cpu.util,5m)>{CPU.UTIL.CRIT}`

[Expression constructor](#)

OK event generation Expression Recovery expression None

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match

* Tag for matching

Allow manual close ☐

URL

Description CPU utilization is too high. The system might be slow to respond.

Enabled ☒

Zabbix – L'interface graphique



Exemple de visualisation de problème

<https://zabbix.minet.net/>

Zabbix – L'agent 1



Codé en C

Installé sur les machines surveillées
(hosts)

Supporté par :

Linux, IBM AIX, FreeBSD, NetBSD,
OpenBSD, HP-UX, Mac OS X, Solaris: 9,
10, 11, Windows (depuis XP)

Son but : remonter au serveur une ou
plusieurs valeurs spécifiques

Deux types de check :

- Passive check
- Active check

Zabbix – L'agent 2



Codé en Go (et un peu de C)

Installé sur les machines surveillées
(hosts)

Supporté par :

RHEL/CentOS 6, 7, 8, SLES 15 SP1+,
Debian 9, 10, Ubuntu 18.04, 20.04,
Windows Server 2008 R2 et plus,
Windows 7 et +

Son but : remonter des un ou des
éléments

Nouveautés :

- Optimisations
- Plugins

- Templates
- OID
- MIB
- Exemple : OID : 1.3.6.1.2.1.25.1.1

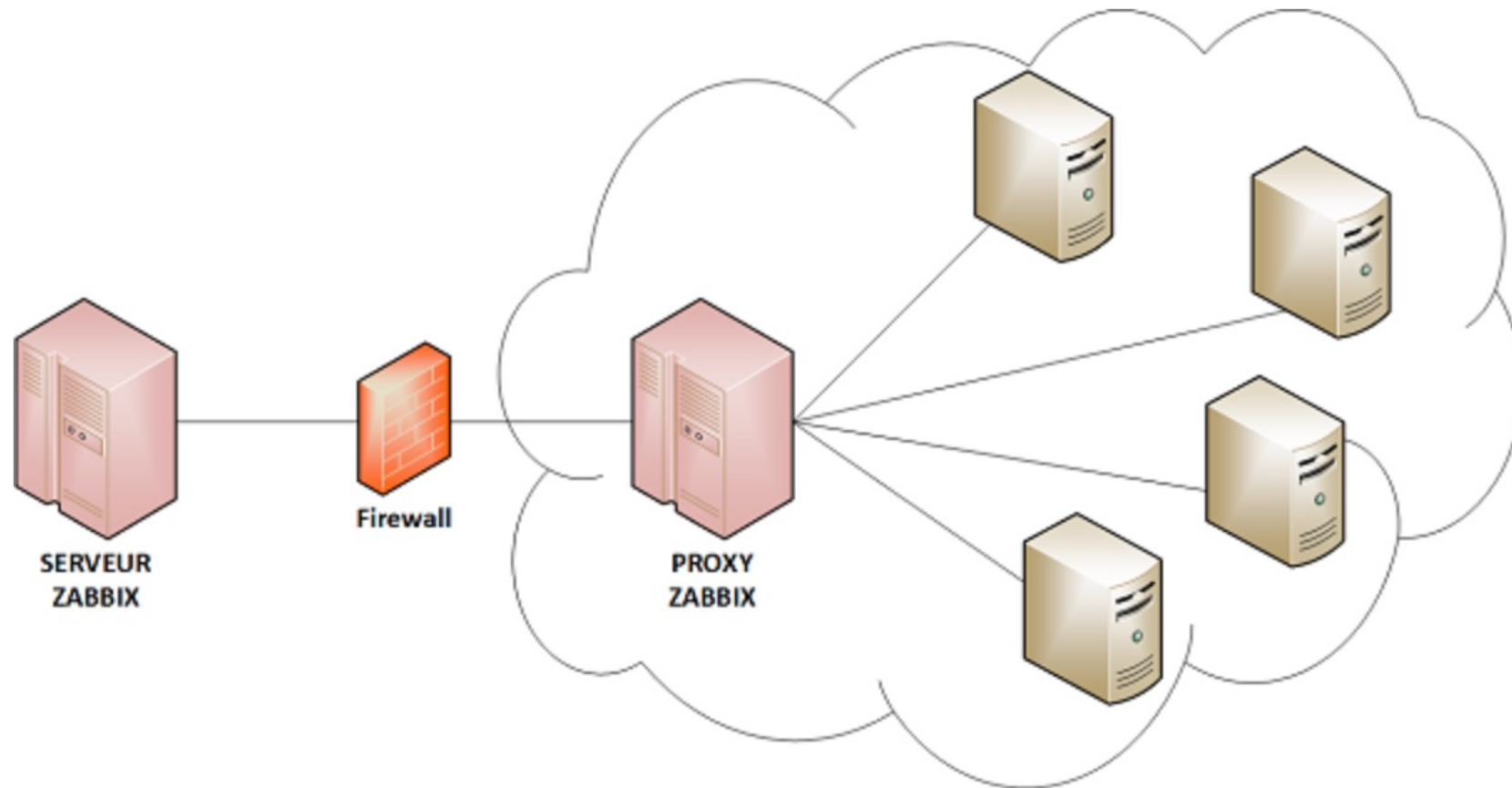
Zabbix – SNMP



Key
OID
Community
Type de donnée

Détails	
OID	1.3.6.1.2.1.25.1.1
Module	HOST-RESOURCES-MIB (CISCO)
Nom	hrSystemUptime
Acces	readonly
Status	current
Description	The amount of time since this host was last initialized. Note that this is different from sysUpTime in the SNMPv2-MIB [RFC1907] because sysUpTime is the uptime of the network management portion of the system.
Syntaxe	TimeTicks (SNMPv2-SMI)

Zabbix – Le proxy



Un emplacement distant est surveillé par un seul proxy Zabbix

Kahooooooooot ?

