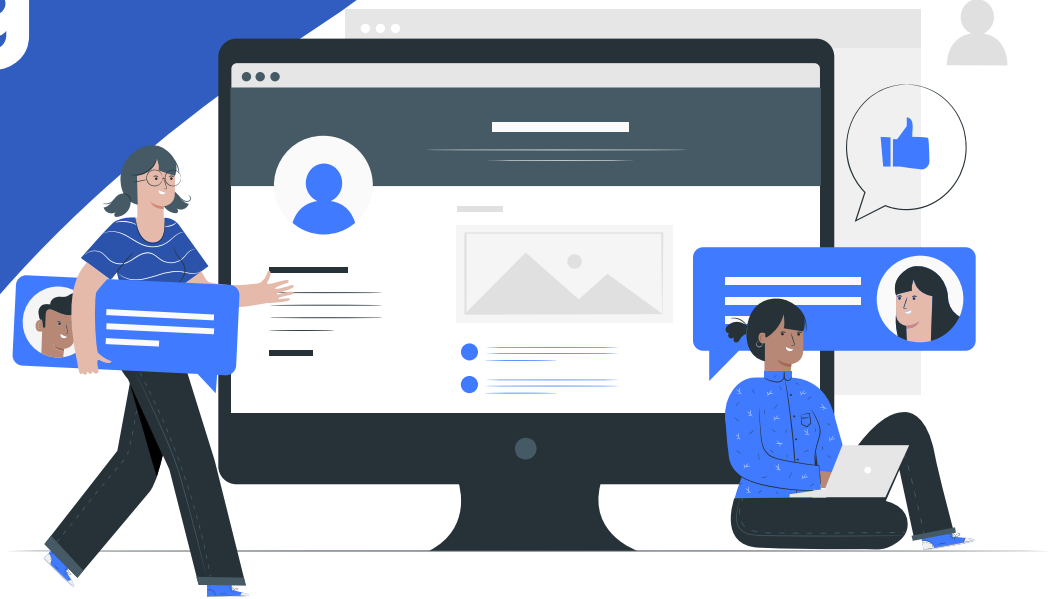


Formation Monitoring

Seaweedbrain
Rustacé



De quoi va-t-on parler ?

01

Le monitoring
c koi ?

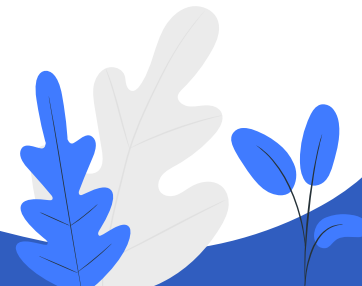
02

Zabbix c ki ?

03

Cluster ELK
c koi ?

01 Le Monitoring





is watching you



Température Trafic réseau
État des disques Processus
Processus CPU RAM Espace
Activité Intrusion
suspecte physique



Sirius



is watching you

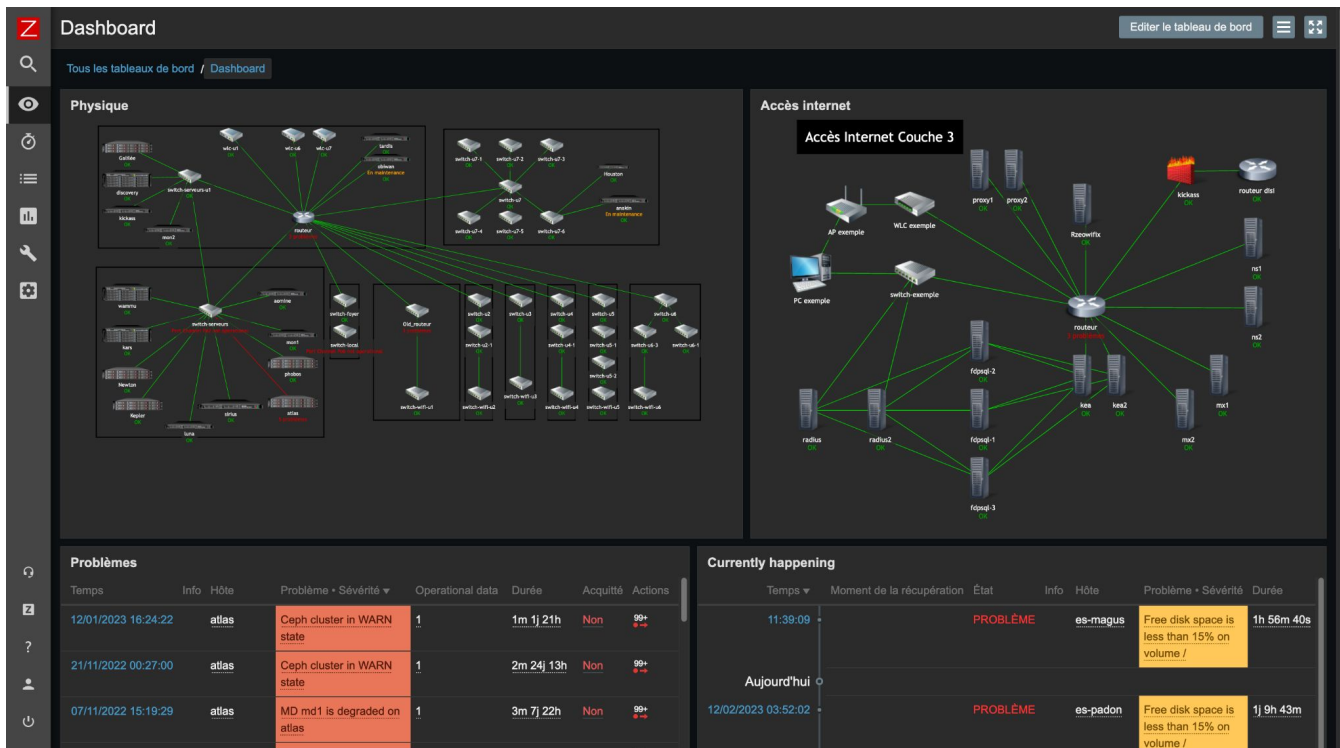


ZABBIX

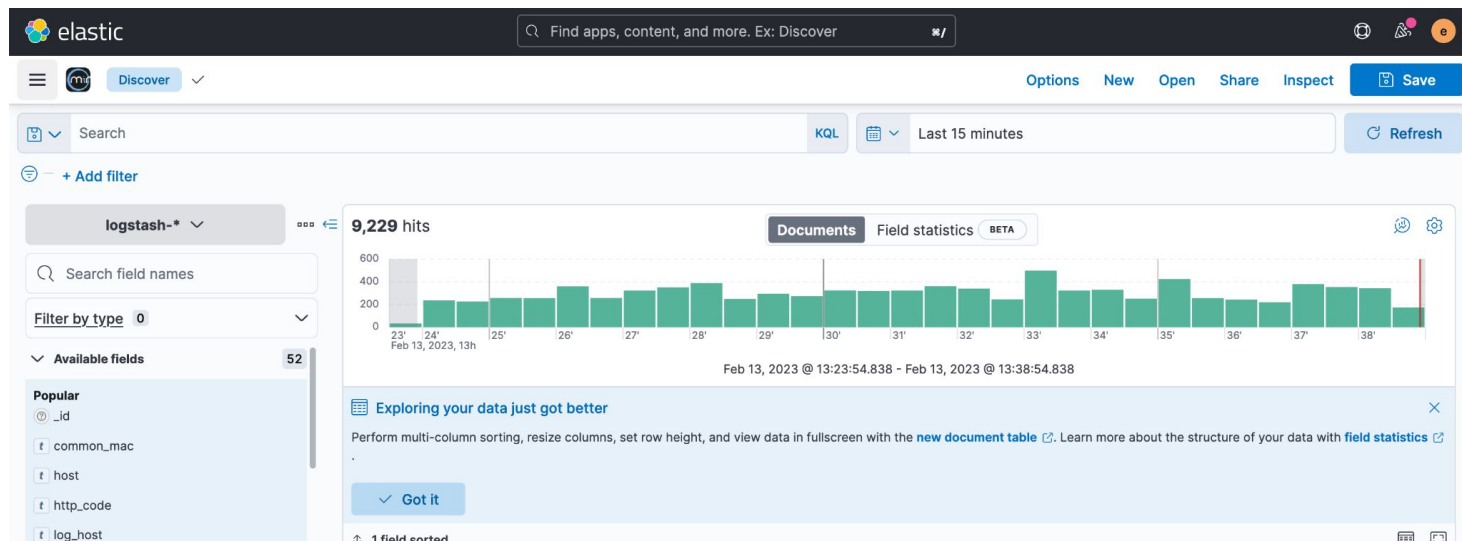


Monitoring général :

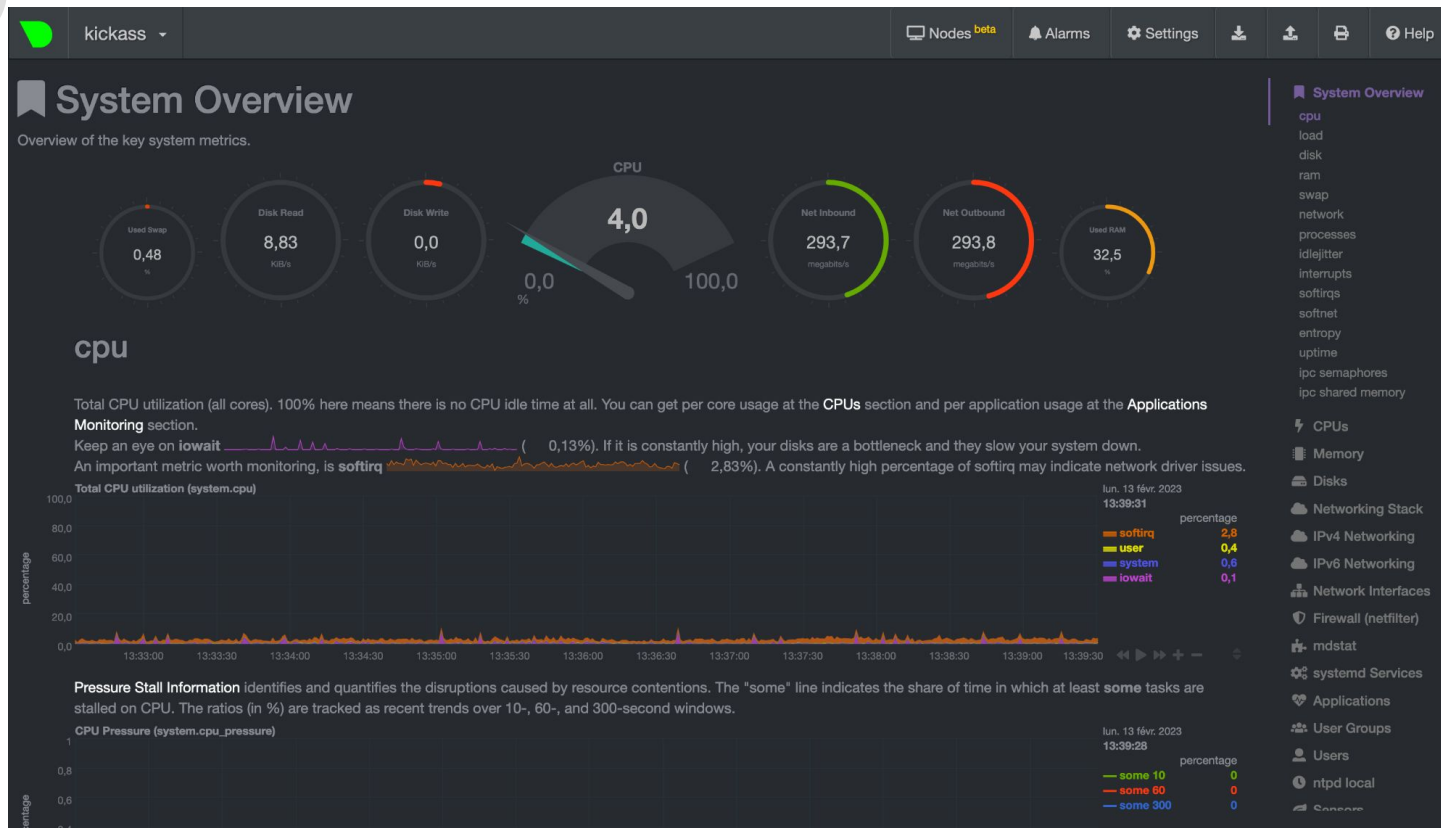
ZABBIX



Monitoring log :



Monitoring kickass :



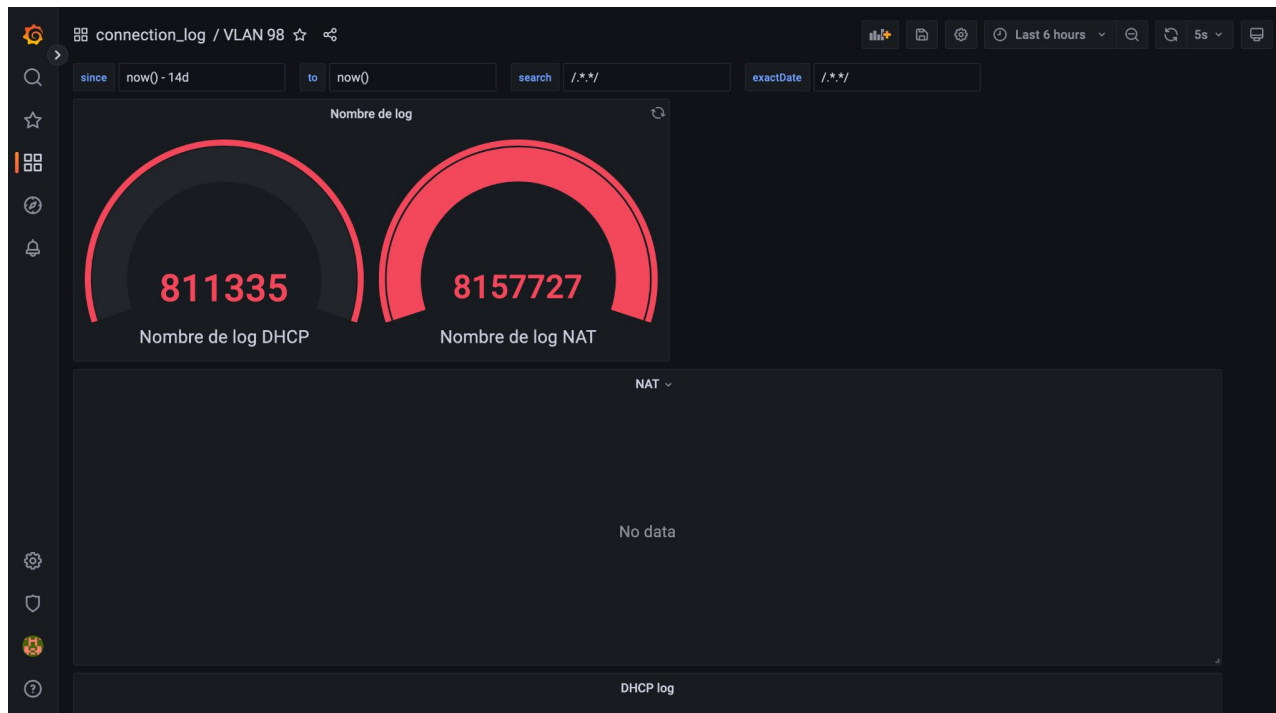
Monitoring logs de connexions :

 **influxdb**

 **chronograf**

 **telegraf**

 **Grafana**

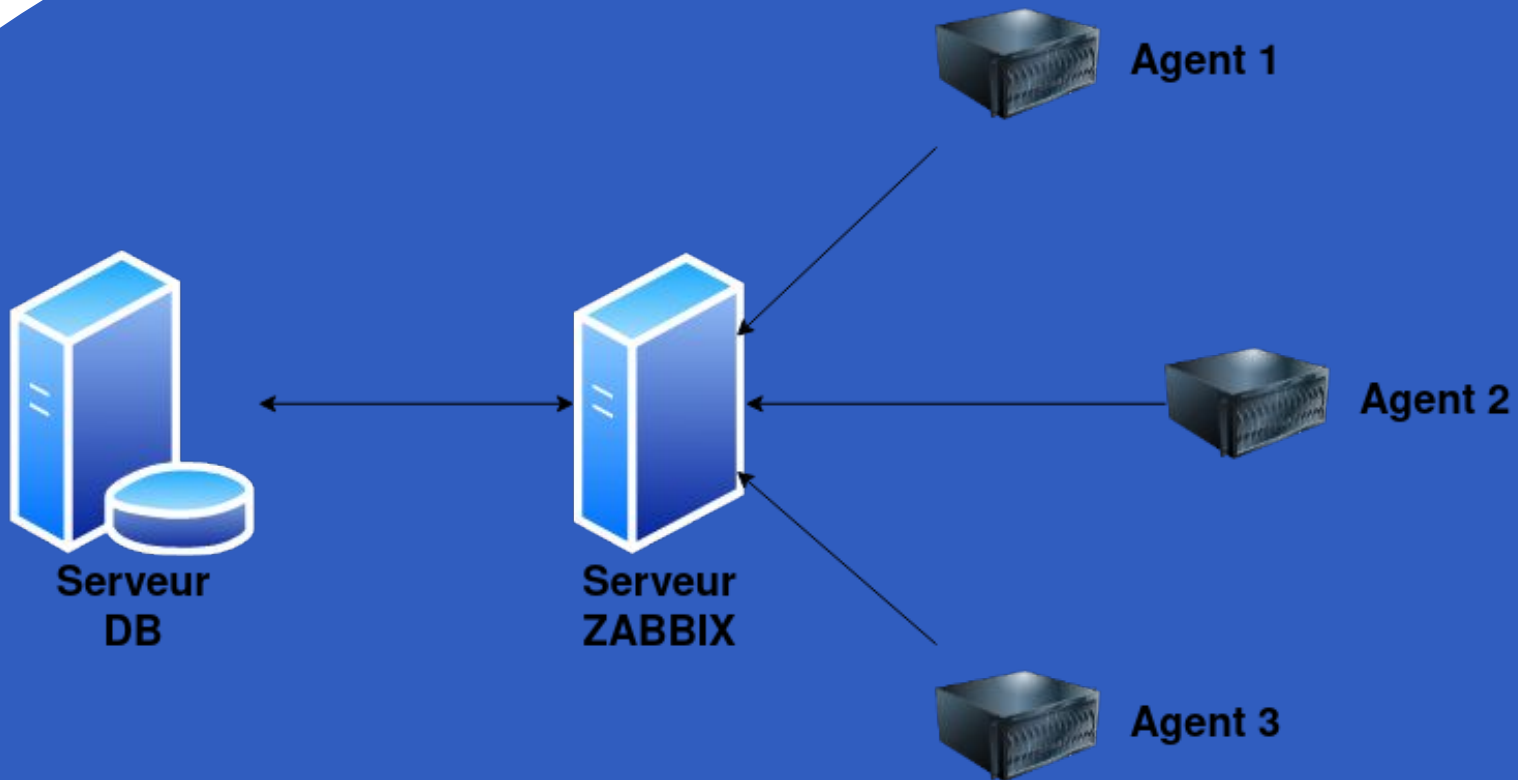


 **minet**

02

ZABBIX







**Serveur
ZABBIX**



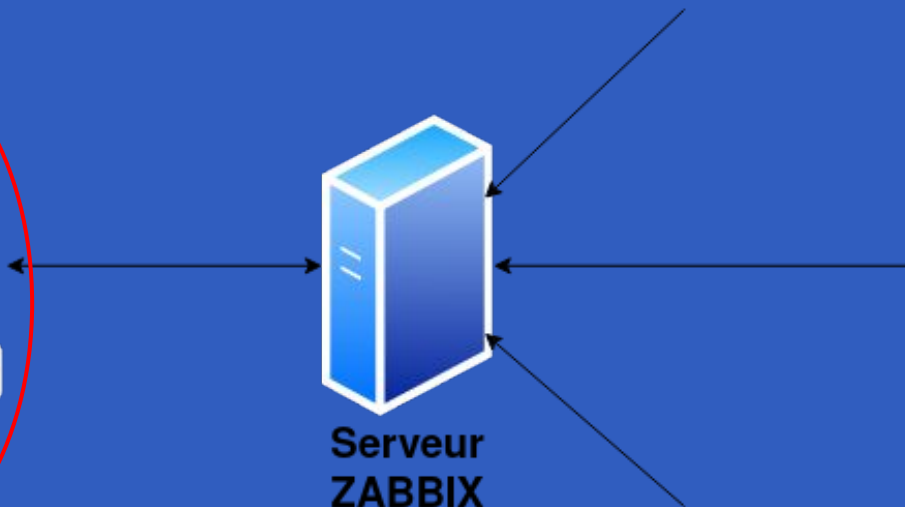
Agent 1



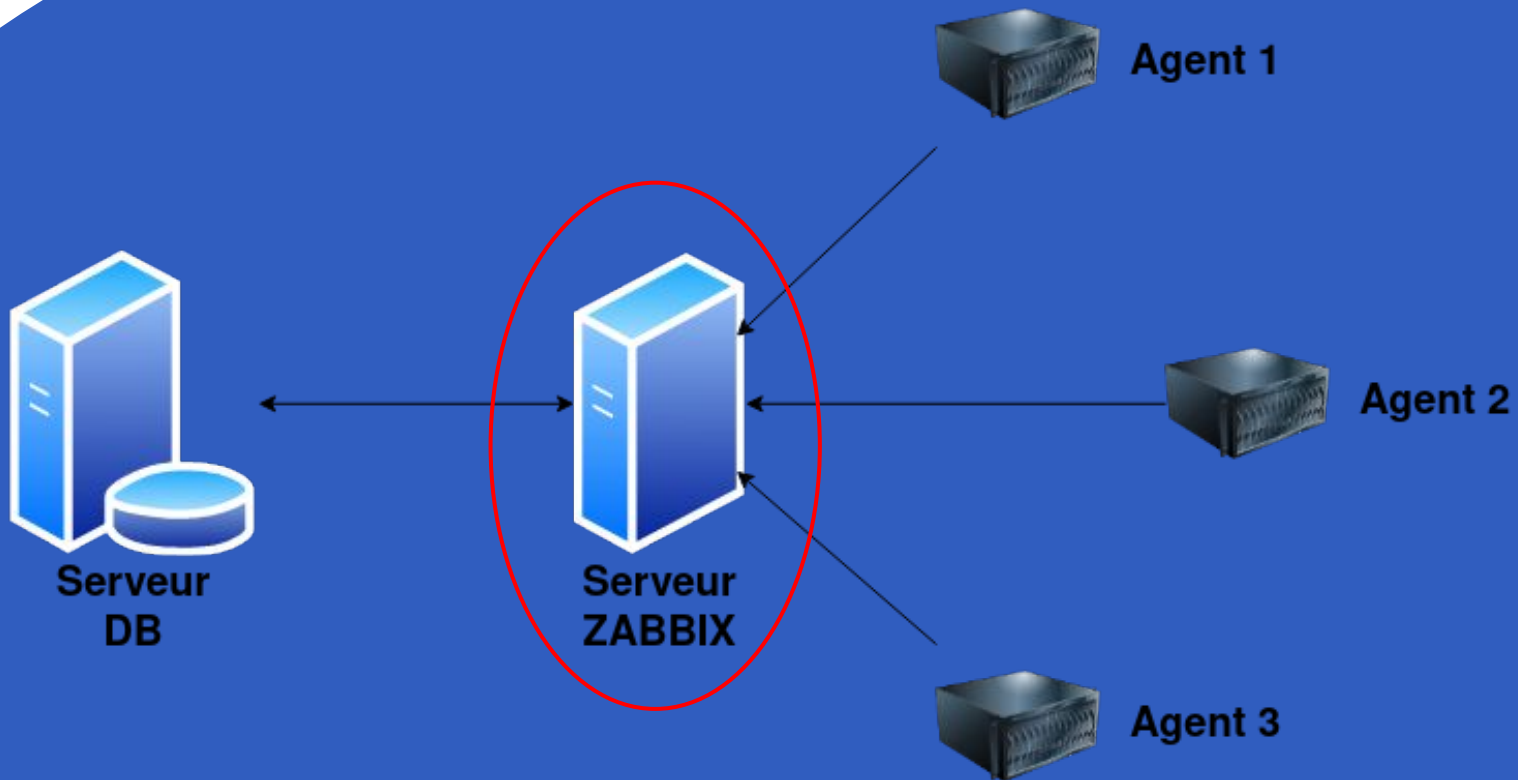
Agent 2



Agent 3









Le serveur ZABBIX

Centralise le traitement des données

- + Peut détecter les problèmes (paramétrable)
 - + Peut faire des alertes (mails, SMS)
 - + Interface web
 - + Ratio
- 

Le serveur ZABBIX :: Les problèmes

Temps ▼	Sevérité	Moment de la récupération	Etat	Info	Hôte	Problème	Durée	Acquitte	Actions	Tags
11:39:09	Avertissement		PROBLÈME		es-magus	Free disk space is less than 15% on volume /	6h 34m 49s	Non		Application: Filesystems
Aujourd'hui										
12/02/2023 03:52:02	Avertissement		PROBLÈME		es-padon	Free disk space is less than 15% on volume /	1j 14h 21m	Non		Application: Filesystems
Hier										
11/02/2023 12:52:24	Avertissement		PROBLÈME		miniroutix	Free disk space is less than 15% on volume /	2j 5h 21m	Non		Application: Filesystems
09/02/2023 20:24:50	Avertissement		PROBLÈME		Old_routeur	Port Channel Po7 not operational ?	3j 21h 49m	Non		Application: Interface(s)
09/02/2023 20:24:50	Avertissement		PROBLÈME		Old_routeur	Port Channel Po4 not operational ?	3j 21h 49m	Non		Application: Interface(s)
08/02/2023 18:10:55	Avertissement		PROBLÈME		es-dhalsim	Free disk space is less than 15% on volume /	5j 3m	Non		Application: Filesystems
08/02/2023 01:06:48	Avertissement		PROBLÈME		routeur	Port Channel Po3 not operational ?	5j 17h 7m	Non		Application: Interface(s)
08/02/2023 01:06:48	Avertissement		PROBLÈME		routeur	Port Channel Po2 not operational ?	5j 17h 7m	Non		Application: Interface(s)
07/02/2023 22:32:48	Avertissement		PROBLÈME		routeur	Port Channel Po4 not operational ?	5j 19h 41m	Non		Application: Interface(s)
07/02/2023 13:36:19	Avertissement		PROBLÈME		es-magus	Lack of free swap space on es-magus ?	6j 4h 37m	Non		Application: Memory
Février										
21/01/2023 22:49:53	Moyen		PROBLÈME		limesurvey	Zabbix agent on limesurvey is unreachable for 5 minutes	22j 19h 24m	Non		Application: Zabbix ag...
21/01/2023 22:47:10	Moyen		PROBLÈME		limesurvey	Service not publicly available ?	22j 19h 26m	Non		Application: Web
21/01/2023 22:21:50	Avertissement		PROBLÈME		limesurvey	Processor load is too high on limesurvey	22j 19h 52m	Non		Application: CPU Application: Performa...
15/01/2023 06:06:04	Avertissement		PROBLÈME		U1-1318	AP U1-1318 is unavailable by ICMP	29j 12h 7m	Non		

Le serveur ZABBIX :: Les triggers

Trigger

Tags

Dependencies

* Name

CPU load too high on 'New host' for 3 minutes

Event name

CPU load too high on 'New host' for 3 minutes

Operational data

Severity

Not classified

Information

Warning

Average

High

Dis

* Expression

avg(/New host/system.cpu.load,3m)>2

Add

[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

Allow manual close

☐

URL

Description

Enabled

☒

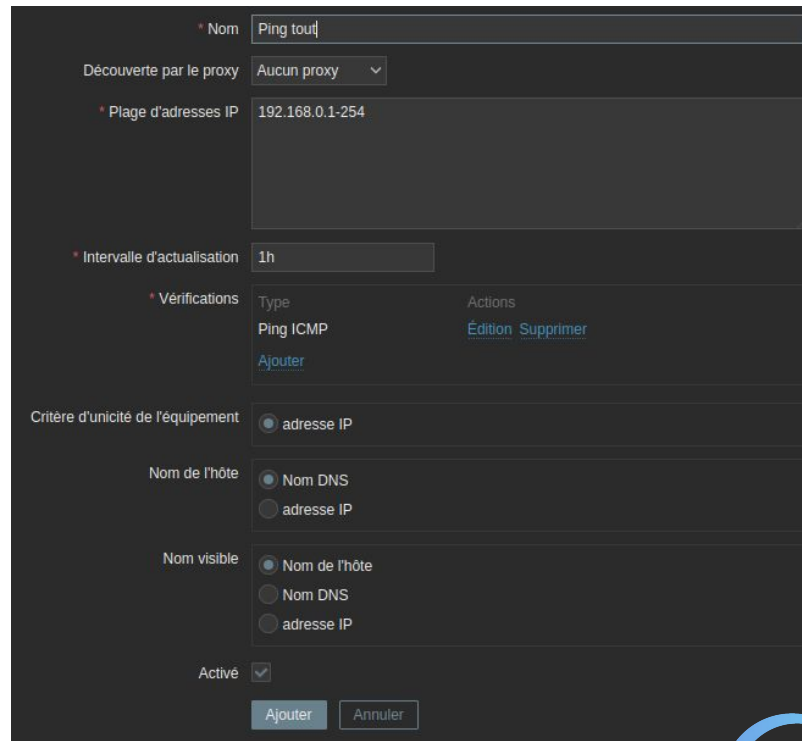
Add

Cancel

Le network discovery

Paramètre automatiquement
des triggers

S'update tout seul pour les
nouvelles machines



The screenshot shows a configuration form for network discovery. The fields are as follows:

- * Nom:** Ping tout
- Découverte par le proxy:** Aucun proxy (dropdown)
- * Plage d'adresses IP:** 192.168.0.1-254
- * Intervalle d'actualisation:** 1h
- * Verifications:**

Type	Actions
Ping ICMP	Édition Supprimer
Ajouter	
- Critère d'unicité de l'équipement:** ☒ adresse IP
- Nom de l'hôte:** ☒ Nom DNS, ☐ adresse IP
- Nom visible:** ☒ Nom de l'hôte, ☐ Nom DNS, ☐ adresse IP
- Activé:** ☒

Buttons at the bottom: [Ajouter](#) and [Annuler](#).





Les agents ZABBIX

S'installent sur les machine du réseau

Permettent de récupérer les infos sur la machine



Agent 1



Codé en C

C un bon langage

Portable

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

But

Remonter les données au serveur
ZABBIX

Passive/Active check

Agent 2



Codé en Go

Go utiliser un autre langage en fait

Portable

RHEL/CentOS 6, 7, 8, SLES 15 SP1+,
Debian, Ubuntu, Windows Server
2008 R2 et +, Windows 7 et +

But

Remonter un ou des éléments au
serveur ZABBIX

Nouveautés

Optimisations et plugins

03





Elasticsearch

Elasticsearch, c'est quoi ?



Stockage

Stockage distribué sur différents noeud



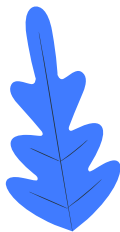
Indexation

Indexation des **mots**

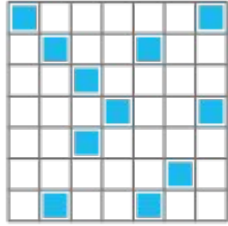


Recherche

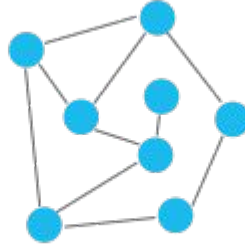
Rend du texte
recherchable
**efficacement et
facilement**



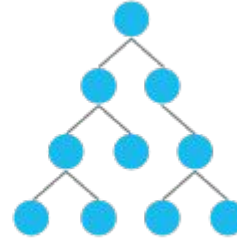
Not Only
SQL



Column-Family



Graph



Document



Key-Value

Apache
Lucene

Lucene



**Comment que
c'est que Elastic
search il stocke
les données, là ?**



**Les
index**

Les indices, c'est quoi ?

Quelle question incroyable !

Index1 : logs du 14.02

Document JSON

log1

Document JSON

log2

Document JSON

log3

Index2 : logs du 15.02

Document JSON

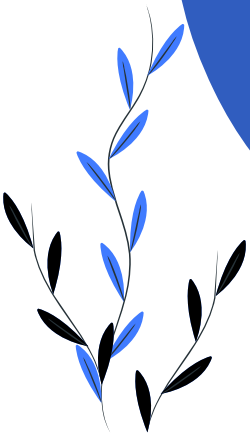
log4

Document JSON

log5

Document JSON

log6



**On complique les
choses ? 🧐**

Les index, c'est quoi ?

Quelle question incroyable !

Index1 : logs du 14.02

Document JSON

log1

Document JSON

log2

Document JSON

log3

Index2 : logs du 15.02

Document JSON

log4

Document JSON

log5

Document JSON

log6

Les indices, c'est quoi ?

Indice1 : logs du 14.02

Shard 1

Document JSON

Document JSON

Shard 2

Document JSON

Document JSON

Indice2 : logs du 15.02

Shard 3

Document JSON

Document JSON

Shard 4

Document JSON

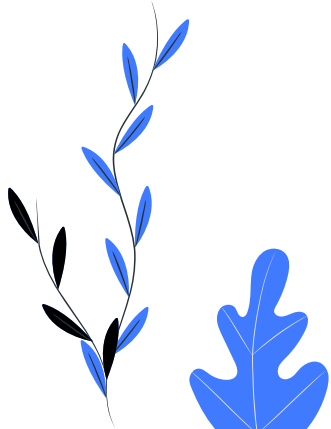
Document JSON

Shard 1

Shard 4

Shard 2

Shard 3



Perte d'information
L'index est dégradé,
des documents sont
perdus



Shard 1



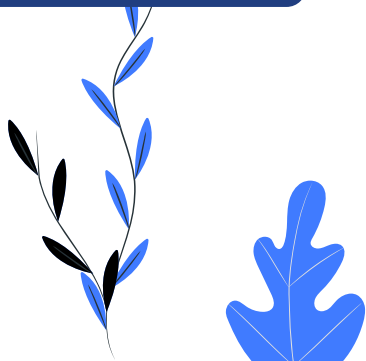
Shard 2

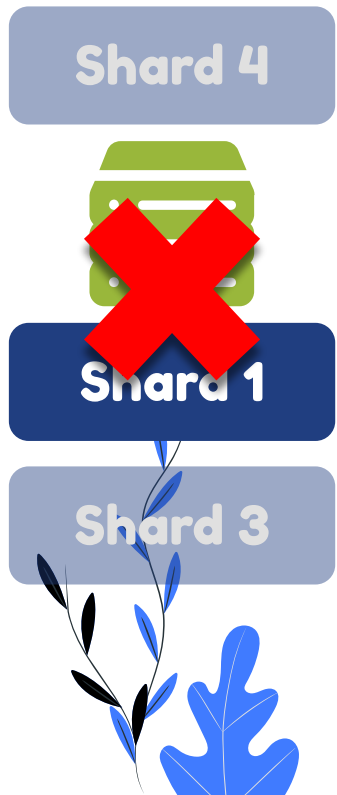


Shard 3



Shard 4

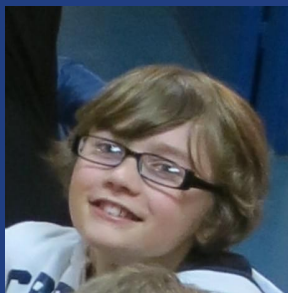




On récapitule

1A avec un avenir

Shard 1

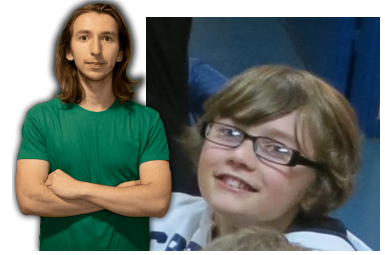
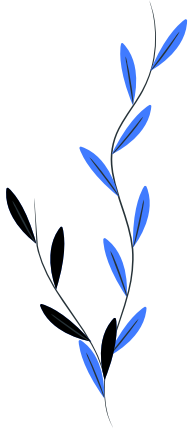


Les Nicolas

Shard 2

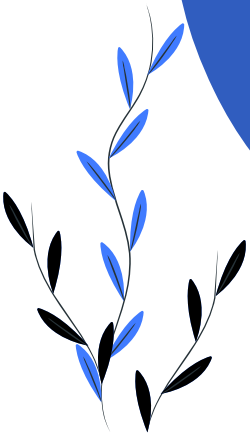


On récapitule





**Ok Nathan t'es
mignon mais
comment on indexe
des logs ?**



Indexation des mots

Salut! Je suis en Suède pour mon échange et j'ai ramené mon routeur MiNET avec moi.

Le problème c'est que lorsque je le reset (pour pouvoir me co en wifi avec le routeur branché depuis la prise ethernet) il apparaît toujours en tant que MiNET dans ma liste de réseaux wifi dispo (au lieu d'être appelé par le réseau de base GL). Du coup je voulais savoir si vous sauriez comment palier au problème.



Indexation des mots

Étape 1 : Normalisation

Salut! Je suis en Suède pour mon échange et j'ai ramené mon routeur MiNET avec moi.

Le problème c'est que lorsque je le reset (pour pouvoir me co en wifi avec le routeur branché depuis la prise ethernet) il apparaît toujours en tant que MiNET dans ma liste de réseaux wifi dispo (au lieu d'être appelé par le réseau de base GL). Du coup je voulais savoir si vous sauriez comment palier au problème.

Indexation des mots

Étape 1 : Normalisation

salut je suis en suede pour mon echange et j'ai ramene mon
routeur minet

avec moi

le problème c'est que lorsque je le reset pour pouvoir me co
en wifi avec le routeur branché depuis la prise ethernet il
apparaît toujours en tant que minet dans ma liste de réseaux
wifi dispo au lieu d'être appelé par le réseau de base gl du
coup je voulais savoir si vous sauriez comment palier au
problème



Indexation des mots

Étape 2 : Division en token

salut, je, suis, en, suede, pour, mon, echange, et, j'ai, ram
ene, mon, routeur, minet, avec, moi, le, problème, c'est, qu
e, lorsque, je, le, reset, pour, pouvoir, me, co, en, wifi, av
ec, le, routeur, branché, depuis, la, prise, ethernet, il, a
pparait, toujours, en, tant, que, minet, dans, ma, liste, de
, réseaux, wifi, dispo, au, lieu, d'être, appelé, par, le, ré
seau, de, base, gl, du, coup, je, voulais, savoir, si, vous, s
auriez, comment, palier, au, problème



Indexation des mots

Étape 3 : Filtrage

salut, je, suis, en, suede, pour, mon, echange, et, j'ai, ram
ene, mon, routeur, minet, avec, moi, le, problème, c'est, qu
e, lorsque, je, le, reset, pour, pouvoir, me, co, en, wifi, av
ec, le, routeur, branché, depuis, la, prise, ethernet, il, a
pparait, toujours, en, tant, que, minet, dans, ma, liste, de
, réseaux, wifi, dispo, au, lieu, d'être, appelé, par, le, ré
seau, de, base, gl, du, coup, je, voulais, savoir, si, vous, s
auriez, comment, palier, au, problème

Indexation des mots

Étape 3 : Filtrage

salut, suis, suede, echange, ai, ramene, routeur, minet, av
ec, moi, le, problème, est, reset, pouvoir, co, wifi, avec, r
outeur, branché, prise, ethernet, apparait, minet, liste,
réseaux, wifi, dispo, lieu, d'être, appelé, réseau, base, g
l, voulais, savoir, sauriez, comment, palier, problème



Indexation des mots

Étape 4 : Stemming

salut, suis, suede, echange, ai, re, s, routeur, minet, av
ec, moi, le, problème, est, re, pouvoir, co, wifi, avec, r
outeur, branché, prise, t, apparait, minet, liste,
réseaux, wifi, di, e, etre, appelé, réseau, base, g
l, voulais, s, sauriez, comment, palier, problème

**j'ai la flemme mais vous avez
compris**

Indexation des mots

Étape 5 : Indexation

salut, suis, suède, échange, ai, ramène, routeur, minet, avec, moi, le, problème, est, reset, pouvoir, co, wifi, avec, routeur, branché, prise, ethernet, apparaît, minet, liste, réseaux, wifi, dispose, lieu, d'être, appelé, réseau, base, gl, voulais, savoir, sauriez, comment, palier, problème

Une partie de
l'indice

Segments

Token	Nb occurrence ds document	Position dans le document
Suède	1	L.209 des perles adhérents MiNET
Mini-routeur	19	L.23 de la page MR, L.209 de la page miniroutix...
Nicolas	56 768 902	Chaque ligne des perles MiNET

Comment qu'on communique ?



Comment qu'on communique ?

Avant tout avec HTTP

Lister les indexs

https://node/_cat/indices

État du cluster

https://node/_cluster/health

Structure d'un index

<https://node/<nomindice>>

Lecture des
données d'un index

https://node/nomindice/_search?q=<champ>:<condition>

On peut utiliser n'importe quel noeud elasticsearch !



Et avec du JSON ?

```
curl -XGET -H 'Content-Type: application/json'  
https://node/<index>/_search -d <json>
```

```
1 {  
2   "query": {  
3     "match": {  
4       "prenom": "Thomas"  
5     }  
6   },  
7   "fields": [  
8     "prenom",  
9     "nom"  
10  ],  
11   "_source": false  
12 }
```

```

1 {
2   "query": {
3     "bool": {
4       "must":
5         [
6           "match" :
7             {
8               //condition
9             },
10          "range" :
11            {
12              "fields.note_hyperfrquence":
13                {
14                  "gt" : 7
15                }
16            }
17          ],
18          "should" :
19            [
20              //match or range
21            ],
22          "must not":
23            [
24              //match or range
25            ],
26        ]
27      },
28      "fields": [
29        "fields.prenom",
30        "fields.nom"
31      ],
32      "_source": false
33    }

```

must Condition obligatoire

should Ajoute du poids à une condition

must not Condition obligatoirement fausse

range Condition mathématique



Logstash

Logstash c'est un tube **raciste**



J'ai chaud
En vrai ça va mieux
Didier s'est trompé de mdp
J'ai reboot, oups
Nishogi m'a éteint



logstash

{ user : 'nishogi',
Event : 'shutdown' }

{ user : 'didier',
Event : 'password
failure' }



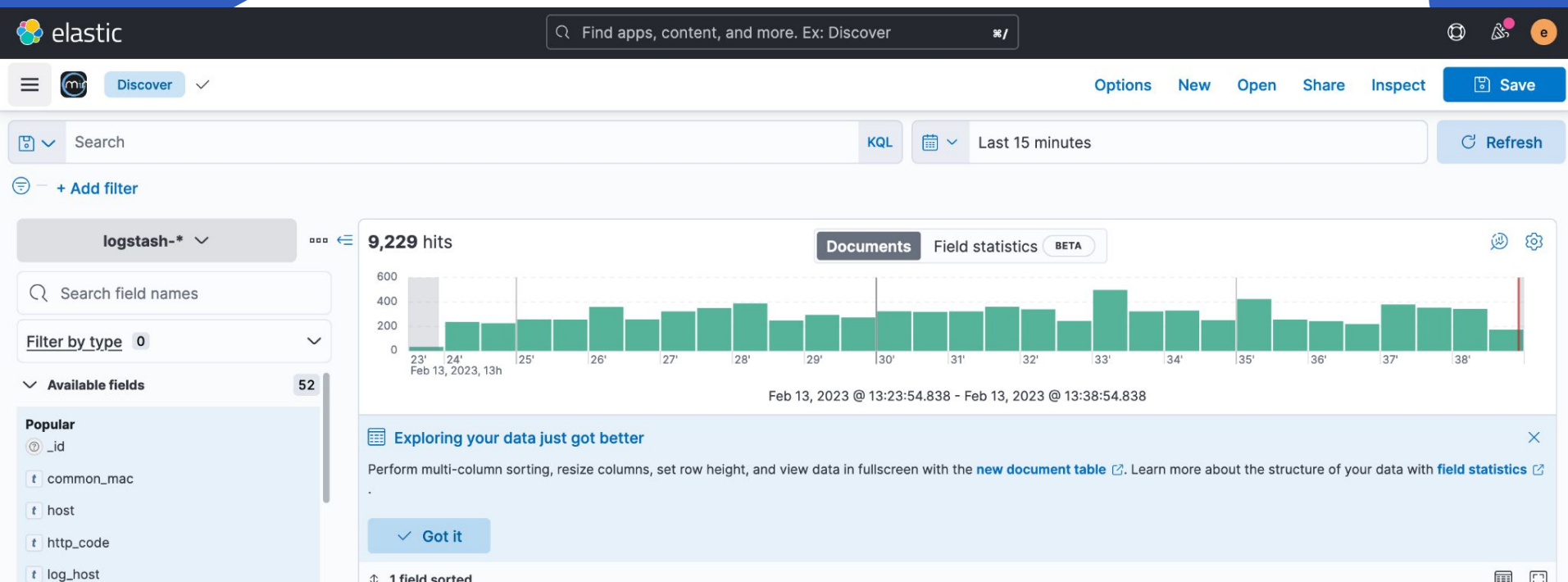
elasticsearch





Kibana

C bo et pratique



La syntaxe KIBANA

Value1 AND value2

field:value

Recherche la valeur dans le champ spécifié

value

Recherche la valeur dans tous les champs

Ratio rapport

Recherche Ratio ou rapport dans les champs

"double_ratio"

Recherche "double ratio" dans les champs

value~

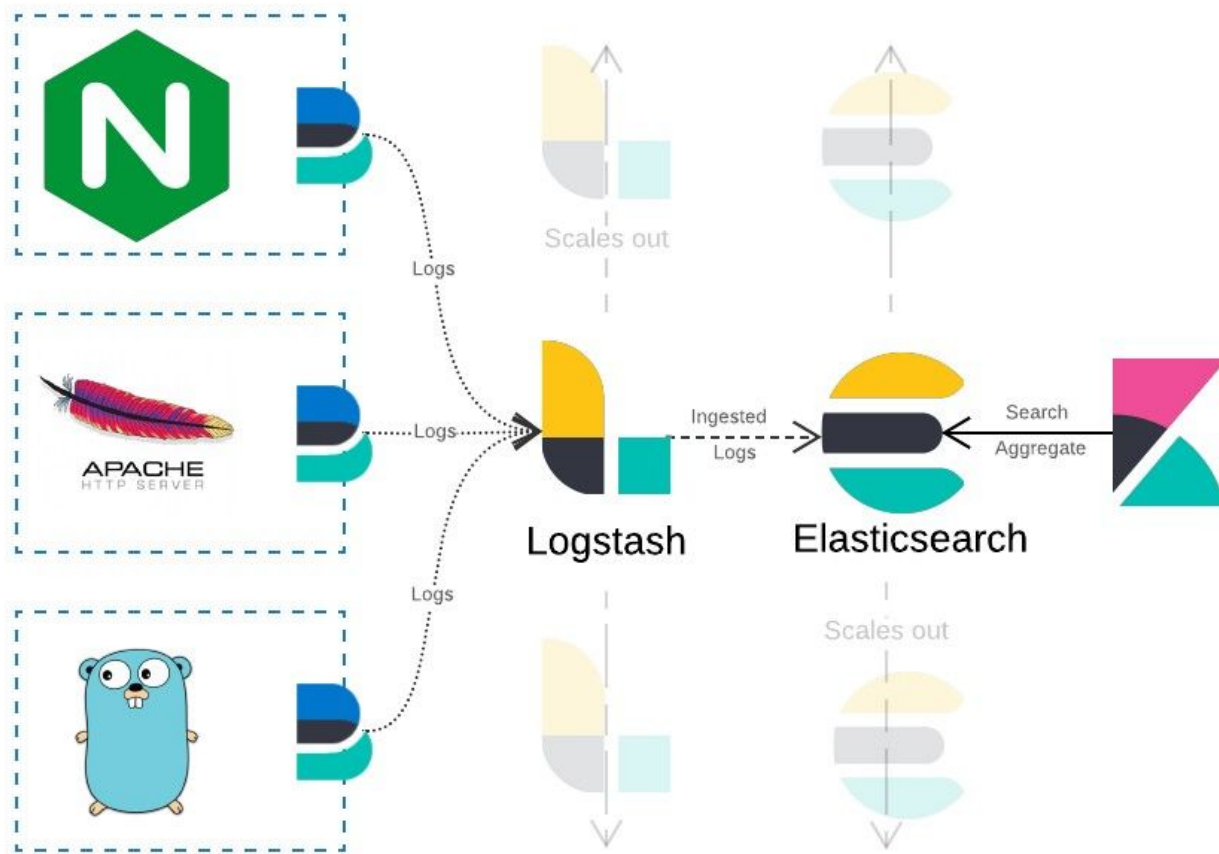
Valeur ressemblant à la valeur spécifiée

Date:[from:to]

Valeur comprise dans la plage temporelle spécifiée

Value1 OR value2

En résumé



Appréciez la diapo de qualité, c'est pas moi qui l'ai faite





Kahoot!



...and our sets of editable icons

You can resize these icons without losing quality.

You can change the stroke and fill color; just select the icon and click on the paint bucket/pen.

In Google Slides, you can also use Flaticon's extension, allowing you to customize and add even more icons.



Educational Icons



Medical Icons



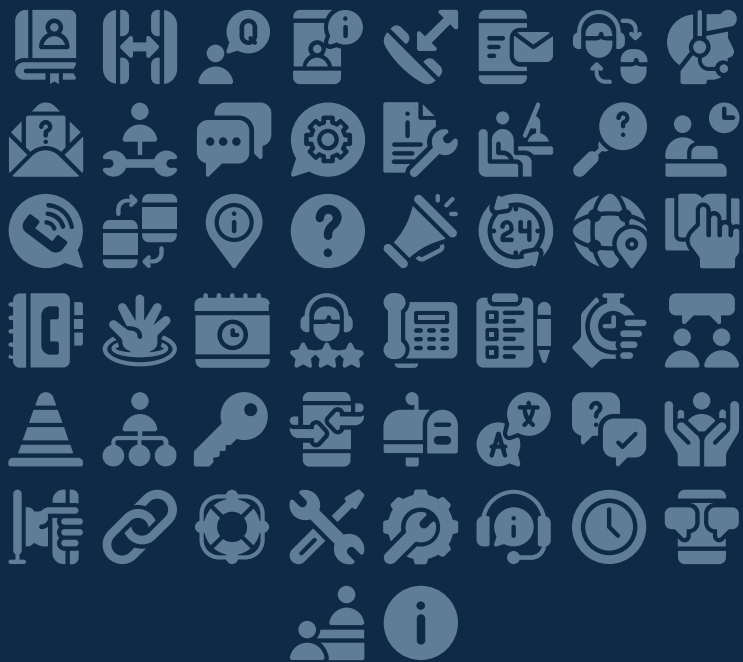
Business Icons



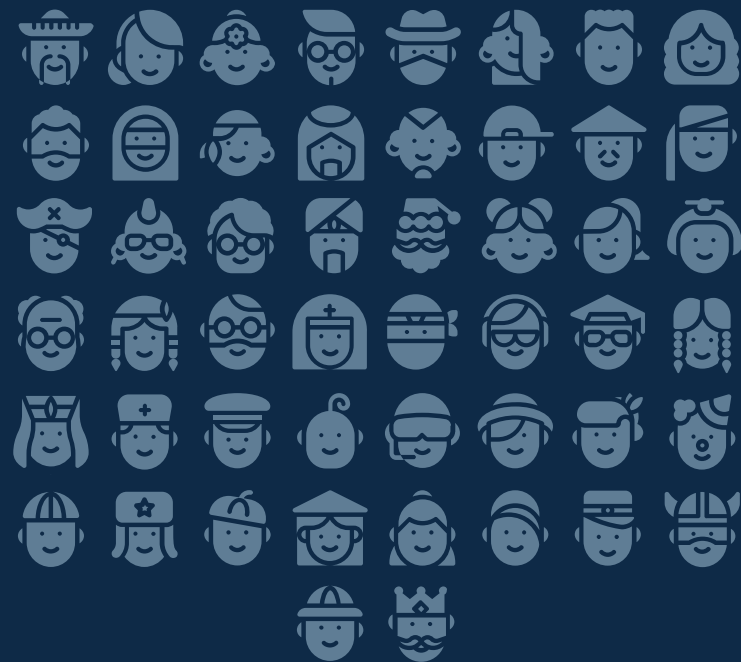
Teamwork Icons



Help & Support Icons



Avatar Icons



[illegible][illegible]

Nature Icons



SEO & Marketing Icons



