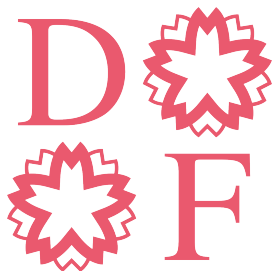


De l'auto-hébergement à l'entre-hébergement : Garage, pour conserver ses données ensemble

Vincent Giraud

Capitole du Libre 2022

Samedi 19 novembre 2022



<https://deuxfleurs.fr>

Deuxfleurs est une association militant en faveur d'un internet plus convivial, avec une organisation et des rapports de force repensés.

Nous faisons partie du CHATONS¹ depuis avril 2022.



1. Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires

Une partie substantielle des contenus en ligne est aujourd'hui hébergée sur le cloud, à savoir, des énormes centres de données.



Cette délégation de responsabilité (et de pouvoir) est particulièrement prisée dans le monde professionnel.

Cette approche recèle de nombreux inconvénients :

- une gestion, des environnements et des logiciels opaques

Cette approche recèle de nombreux inconvénients :

- une gestion, des environnements et des logiciels opaques
- des prix pas faciles à contrôler

Cette approche recèle de nombreux inconvénients :

- une gestion, des environnements et des logiciels opaques
- des prix pas faciles à contrôler
- une dépendance envers l'opérateur dangereuse et intéressée

Cette approche recèle de nombreux inconvénients :

- une gestion, des environnements et des logiciels opaques
- des prix pas faciles à contrôler
- une dépendance envers l'opérateur dangereuse et intéressée
- une confusion volontairement entretenue chez les non-spécialistes en informatique

Cette approche recèle de nombreux inconvénients :

- une gestion, des environnements et des logiciels opaques
- des prix pas faciles à contrôler
- une dépendance envers l'opérateur dangereuse et intéressée
- une confusion volontairement entretenue chez les non-spécialistes en informatique
- des choix écologiquement nocifs

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
- On gagne en vie privée

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
- On gagne en vie privée
- On gagne en libertés

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
- On gagne en vie privée
- On gagne en libertés
- On est responsabilisé face à ses besoins

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
 - On gagne en vie privée
 - On gagne en libertés
 - On est responsabilisé face à ses besoins
- On repose sur une connexion internet pour particulier

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
 - On gagne en vie privée
 - On gagne en libertés
 - On est responsabilisé face à ses besoins
- On repose sur une connexion internet pour particulier
 - Un certain savoir-faire et moult compétences sont requis

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
 - On gagne en vie privée
 - On gagne en libertés
 - On est responsabilisé face à ses besoins
- On repose sur une connexion internet pour particulier
 - Un certain savoir-faire et moult compétences sont requis
 - Assurer la résilience de ses services est difficile

Une alternative : héberger ses données à la maison !

- On récupère la souveraineté sur ses données
 - On gagne en vie privée
 - On gagne en libertés
 - On est responsabilisé face à ses besoins
- On repose sur une connexion internet pour particulier
 - Un certain savoir-faire et moult compétences sont requis
 - Assurer la résilience de ses services est difficile
 - Bien sauvegarder ses données, et ceci au-delà de son site géographique, n'est pas évident

Opérer des systèmes de fichiers pour des services en ligne implique certaines délicatesses pour l'administrateur : leur hiérarchie, leurs noms, la gestion du verrouillage et d'autres complications dues à la spécification POSIX...

schéma tikz ici ?

Le standard S3 apporte des facilités ; on réduit le stockage à un paradigme de clé-valeur basé essentiellement sur deux opérations seulement : lire ou écrire une clé.

Sauvegarder pour se parer contre les pannes matérielles est une chose...
Sauvegarder pour se parer contre les cambriolages et les incendies en est une autre !

Sauvegarder pour se parer contre les pannes matérielles est une chose...
Sauvegarder pour se parer contre les cambriolages et les incendies en est une autre !

Répartir géographiquement ses données devient alors nécessaire.

On a vu récemment se développer au sein du CHATONS la notion d'entre-hébergement : les sauvegardes étant compliquées à assurer, on peut se partager celles-ci pour diminuer la charge sur chaque administrateur.

schéma tikz ici ?

Pour assurer la confidentialité, on peut chiffrer les données au niveau applicatif.

Garage essaye de répondre à l'ensemble de ces contraintes.

Il s'agit d'un logiciel libre permettant de distribuer un service S3 sur diverses machines éloignées.

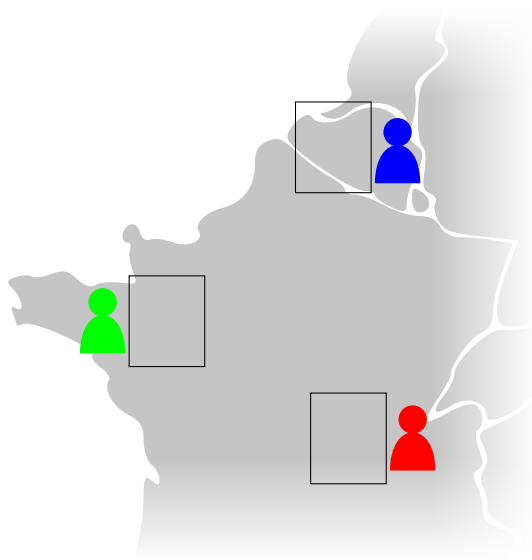


Garage

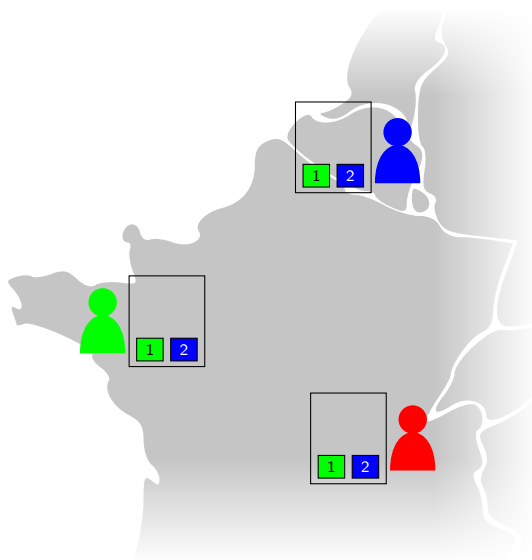
<https://garagehq.deuxfleurs.fr/>

Garage va donc prendre en compte les zones au moment de répliquer les données.

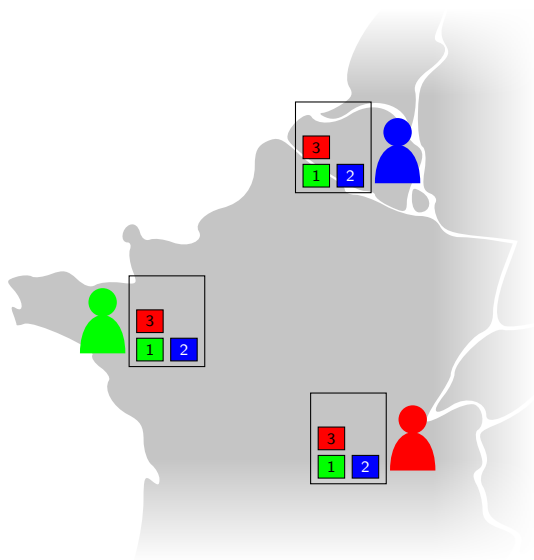
```
alex@io:~$ docker exec -ti garage /garage status
==== HEALTHY NODES ====
ID                Hostname  Address                               Tags                               Zone    Capacity
d9b5959e58a3ab8c... drosera   [2a01:e0a:260:b5b0::4]:3901       [drosera,atuin]                   atuin   20
156d0f7a88b1e328... digitale [2a01:e0a:260:b5b0::3]:3901       [digitale,atuin]                   atuin   10
966dfc7ed8049744... datura   [2a01:e0a:260:b5b0::2]:3901       [datura,atuin]                     atuin   10
7d50f042280fea98... io       [2a01:e0a:5e4:1d0::57]:3901       [io,jupiter]                       jupiter 20
alex@io:~$
```



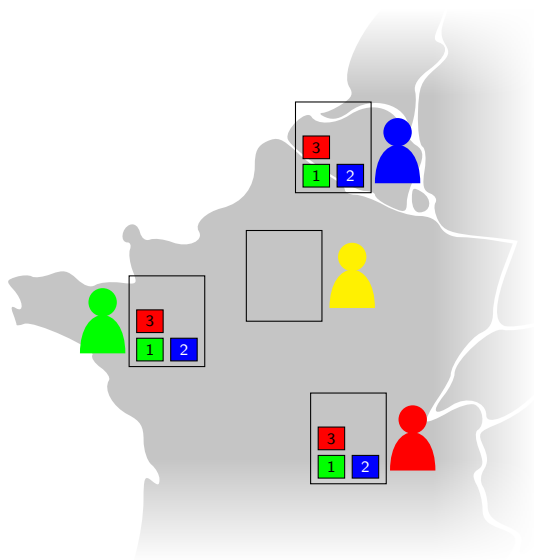
Chaque objet est dupliqué sur plusieurs zones différentes.



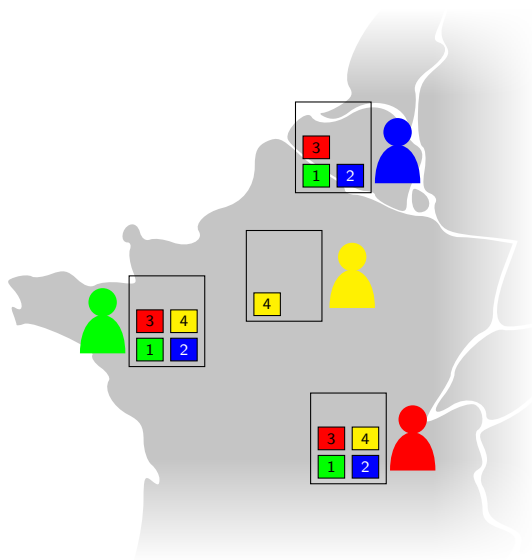
Chaque objet est dupliqué sur plusieurs zones différentes.



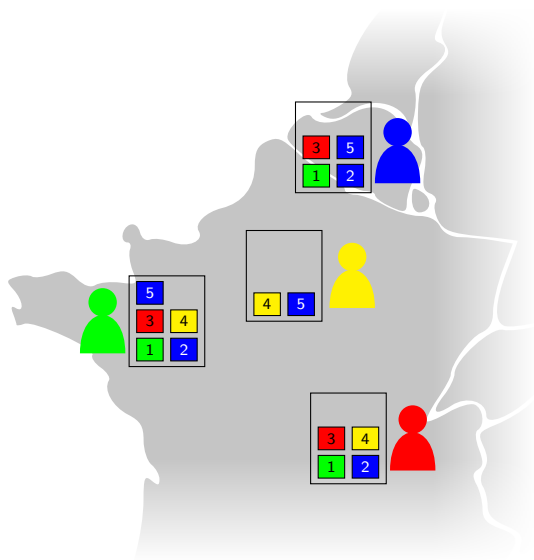
Chaque objet est dupliqué sur plusieurs zones différentes.



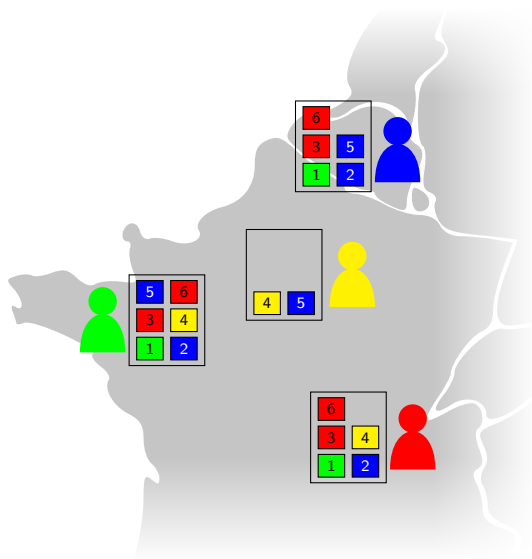
Chaque objet est dupliqué sur plusieurs zones différentes.



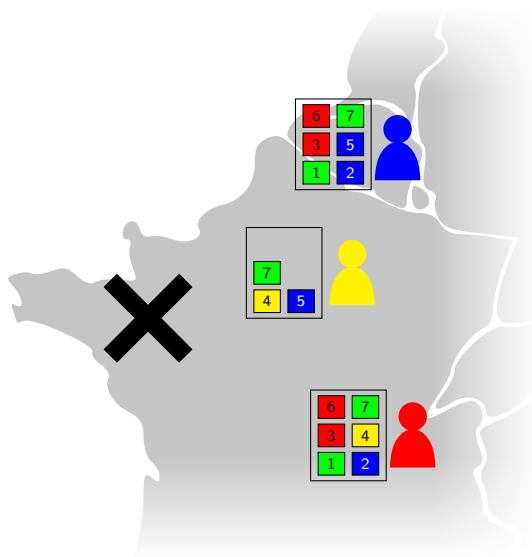
Chaque objet est dupliqué sur plusieurs zones différentes.



Chaque objet est dupliqué sur plusieurs zones différentes.



Chaque objet est dupliqué sur plusieurs zones différentes.



Chaque objet est dupliqué sur plusieurs zones différentes.

Si une zone devient indisponible, les autres continuent d'assurer le service.

Cette redondance allège grandement la charge qui repose sur les administrateurs face aux incidents ou tracas du quotidien.

Dans le cadre du programme *Horizon 2021* de l'Union Européenne, nous avons reçu une subvention de la part de l'initiative NGI Pointer².



Nous avons ainsi pu financer le développement de Garage pendant 2 années.

2. Next Generation Internet Program for Open Internet Renovation

De par nos valeurs, nous avons attribué la licence AGPL version 3 à Garage, notamment afin qu'il reste parmi les biens communs.



Nous avons décidé d'écrire Garage à l'aide du langage Rust, afin d'obtenir une compilation vers des binaires natifs et efficaces.



Ce choix permet également de bénéficier des avantages reconnus de Rust en termes de sécurité.

Garage peut ainsi être performant sur des machines limitées. Les prérequis sont minimales : n'importe quelle machine avec un processeur qui a moins d'une décennie, 1 gigaoctet de mémoire vive, et 16 gigaoctets de stockage suffit.

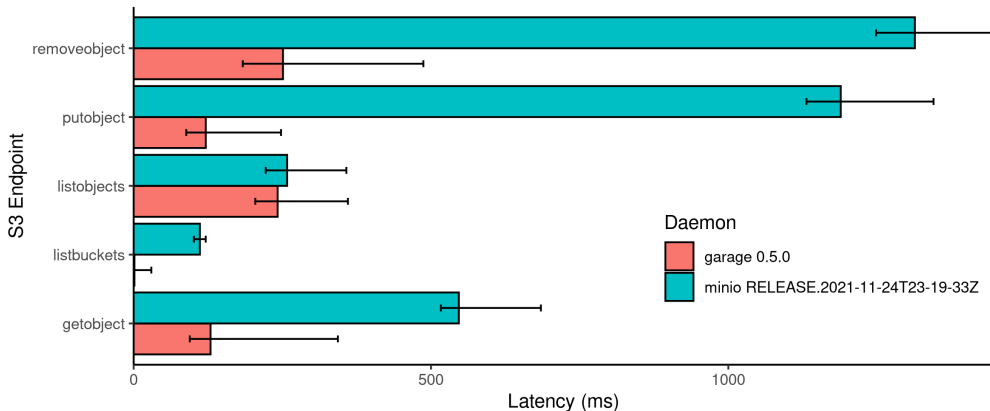
Cet aspect est déterminant : il permet en effet d'héberger sur du matériel acheté d'occasion, pour réduire l'impact écologique de nos infrastructures.

S3 endpoint latency in a simulated geo-distributed cluster

100 measurements, 5 nodes, 100ms RTT + 20ms jitter between nodes

no contention: latency is due to intra-cluster communications

colored bar = mean latency, error bar = min and max

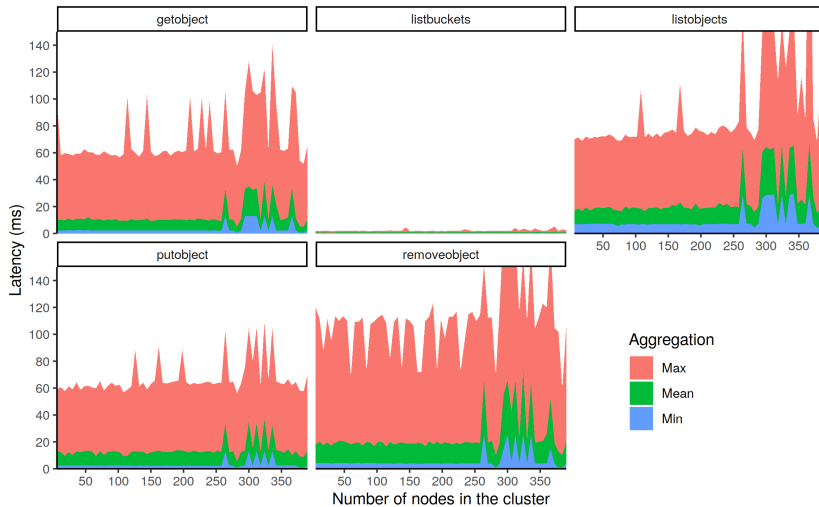


Get the code to reproduce this graph at <https://git.deuxfleurs.fr/quentin/benchmarks>

Garage response time on common S3 endpoints with various cluster size

ran on 6 physical nodes on Grid5000 with multiple instances on each node
spread on 3 zones: Lyon (nova), Rennes (paravance) and Nantes (economie)

few contention, latency is mainly due to RPC communications except on biggest values



Get the code to reproduce this graph at <https://git.deuxfleurs.fr/quentin/benchmarks>