



L'hébergement cloud à MiNET HOSTING

Seaweedbrain
14.06.2023

Table of contents

01

Petit historique

02

Présentation de base

03

L'architecture
réseau

04

La plateforme web

05

Sécurité et dangers

06

Les projets futurs

01

Petit historique

Hosting, dans sa forme actuel

01.04.2021

par D.C.

2 ans

de bêta, après quelques mois de coupure complète
(raisons de sécurités)

03.04.2023

version 1.0

Depuis 2021 ...

Développement de
fonctionnalités

Lourd travail de
correction

02

Présentation basique

Hosting au fond c'est quoi ?

Hosting : il y en a pour
tout le monde 🥰

Réseau

Administration reseau de toutes
les VMs, enjeux de sécurité



DevOps

Application web pour les adherents et
les admins pour contrôler 100% des
VMs

Sys admin

Full CI/CD, 2 hyperviseurs en
charge de l'hébergement de toutes
les machines des adherents.
Déploiement automatique



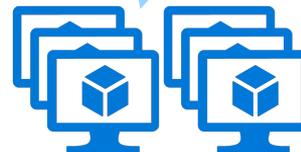
Hosting : Comment ça marche ?



Web Application



Accès Internet
SSH



API de proxmox



PROXMOX

Hosting : Ça marche avec quoi ?

hosting.minet.net



CI/CD



Flask

API



PROXMOX

Aomine - Kars - Wammu

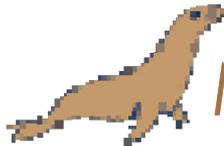
Hebergement



DNS



Frontend



MariaDB

BDD



HashiCorp

Packer

Génération des templates

Hosting

Bienvenue sur le panel d'administration Hosting
Ici vous pouvez gérer toutes les VM et entrées DNS

bg

Statistiques

VM créées

112

VM actives

85

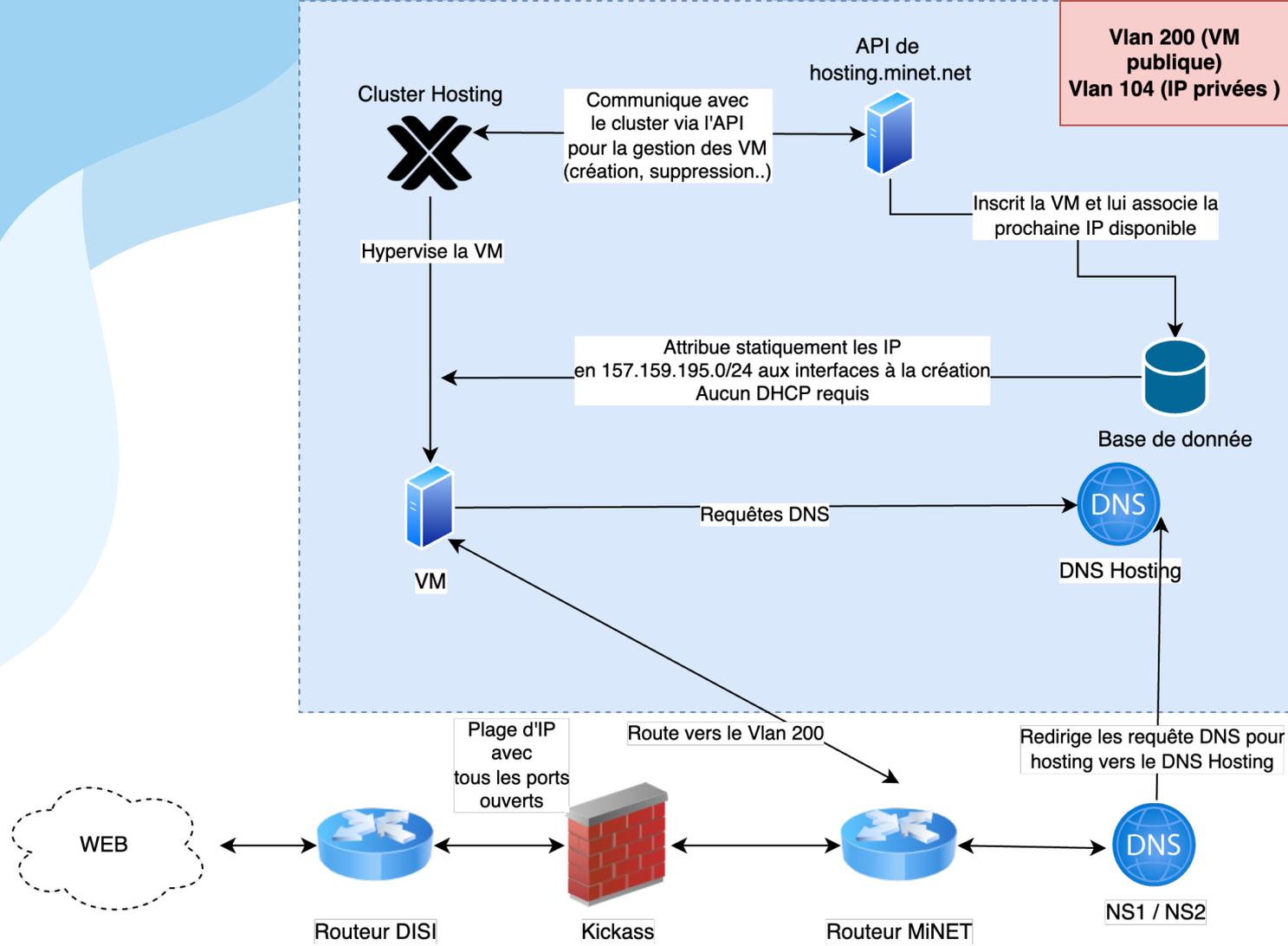
Entrées DNS

62

03

L'architecture réseau

Comment que c'est que ça communique
toussa ?



Les VMs



Debian 11 avec fail2ban
installé par défaut

qemu-agent installé et activé



Tous les soirs

Accès SSH par clé et
comptes gérés par Cloud-init

Clones de template proxmox
pré-défini

Cloud init

ou initialiseur informatique

The screenshot shows the Proxmox VE interface for a Virtual Machine (VM) named '234 (cyberhub-test) on node 'kars''. The interface includes a top navigation bar with 'PROXMOX Virtual Environment 7.2-4 dev', 'Documentation', 'Create VM', 'Create CT', and 'root@pam'. The left sidebar shows a 'Server View' of various VMs. The main panel displays the configuration for the selected VM, with the 'Cloud-Init' section highlighted. The configuration table is as follows:

Property	Value
User	tperel
Password	*****
DNS domain	minet.net
DNS servers	157.159.195.51
SSH public key	thomasperel@orange.fr
IP Config (net0)	ip=157.159.195.119/24,gw=157.159.195.1

Cloud init

ou initialiseur informatique

Virtual Environment 7.2-4 dev Documentation Create VM Create CT root@pam

Server View

- 100 (nathan-stenopinsky)
- 190 (ns)
- 191 (vm-test)
- 192 (horus)
- 197 (test-dns-hosting)
- 198 (papy)
- 199 (farmia2023)
- 200 (ykts-db)
- 204 (goofyserie-mc)
- 205 (goofyserie-mc)
- 208 (site-mission-sprint)
- 210 (test-debian)
- 211 (portfolio)
- 212 (hephaistos)
- 214 (draw2io-server)
- 218 (supervision2)
- 219 (pngate)
- 223 (livrablebda)
- 224 (the-forge)
- 226 (p2t)
- 227 (openthevote)

Virtual Machine 234 (cyberhub-test) on node 'kars'

Start Shutdown Migrate Console More Help

Summary Add Remove Edit Disk Action Revert

- Console
- Hardware
- Cloud-Init
- Options
- Task History
- Monitor
- Backup
- Replication
- Snapshots
- Firewall
- Permissions

Memory	3.00 GiB
Processors	1 (1 sockets, 1 cores) [kvm64]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CloudInit Drive (ide0)	replicated_3_times_hosting:vm-234-cloudinit,media=cdrom,size=4M
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (scsi0)	replicated_3_times_hosting:vm-234-disk-0,iotread=1,size=10G
Network Device (net0)	virtio=6A:76:4B:E1:78:10,bridge=vibr200,firewall=1

Cloud init

ou initialiseur informatique

```
1 manage_etc_hosts: true
2
3 users:
4   - default
5
6 disable_root: true
7
8 apt_update: true
9
10 # Upgrade the instance on first boot
11 apt_upgrade: true
12
13 # Reboot after package install/update if necessary
14 apt_reboot_if_required: true
15
16 # Install useful packages
17 packages:
18   - vim
19   - fail2ban
20
21 # Write out new SSH daemon configuration. Standard debian 11 configuration
22 # apart from forbidding root login and disabling password authentication
23 write_files:
24   - path: /etc/ssh/sshd_config
25     content: |
26       PermitRootLogin no
27       PubkeyAuthentication yes
28       PasswordAuthentication no
29       PermitEmptyPasswords no
30       ChallengeResponseAuthentication no
31       UsePAM yes
32       X11Forwarding yes
33       PrintMotd no
34       AcceptEnv LANG LC_*
35       Subsystem sftp /usr/lib/openssh/sftp-server
36
```

```
36
37 # The modules that run in the 'init' stage
38 cloud_init_modules:
39   - seed_random
40   - write_files
41   - set_hostname
42   - update_hostname
43   - update_etc_hosts
44   - ca-certs
45   - users-groups
46   - ssh
47
48 # The modules that run in the 'config' stage
49 cloud_config_modules:
50   - set-passwords
51   - ntp
52   - timezone
53   - disable-ec2-metadata
54
55 # The modules that run in the 'final' stage
56 cloud_final_modules:
57   - package-update-upgrade-install
58   - scripts-vendor
59   - scripts-per-once
60   - scripts-per-boot
61   - scripts-per-instance
62   - scripts-user
63   - ssh-authkey-fingerprints
64   - final-message
65
66 system_info:
67   # This will affect which distro class gets used
68   distro: debian
69   # Default user name + that default users groups (if added/used)
70   default_user:
71     name: debian
72     lock_passwd: true
73     gecos: Debian
74     groups: [adm, audio, cdrom, dialout, dip, floppy, netdev, plugdev, sudo, video]
75     sudo: ["ALL=(ALL:ALL) ALL"]
76     shell: /bin/bash
77   paths:
78     cloud_dir: /var/lib/cloud/
79     templates_dir: /etc/cloud/templates/
80     upstart_dir: /etc/init/
81   package_mirrors:
82     - arches: [default]
83     failsafe:
84       primary: http://deb.debian.org/debian
85       security: http://security.debian.org/
86   ssh_svcname: ssh
```

Processus de creation de VM



PROXMOX



HOSTING

hosting.minet.net

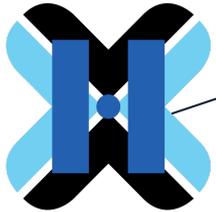


Processus de creation de VM

Clone le template de la
VM via l'API



PROXMOX



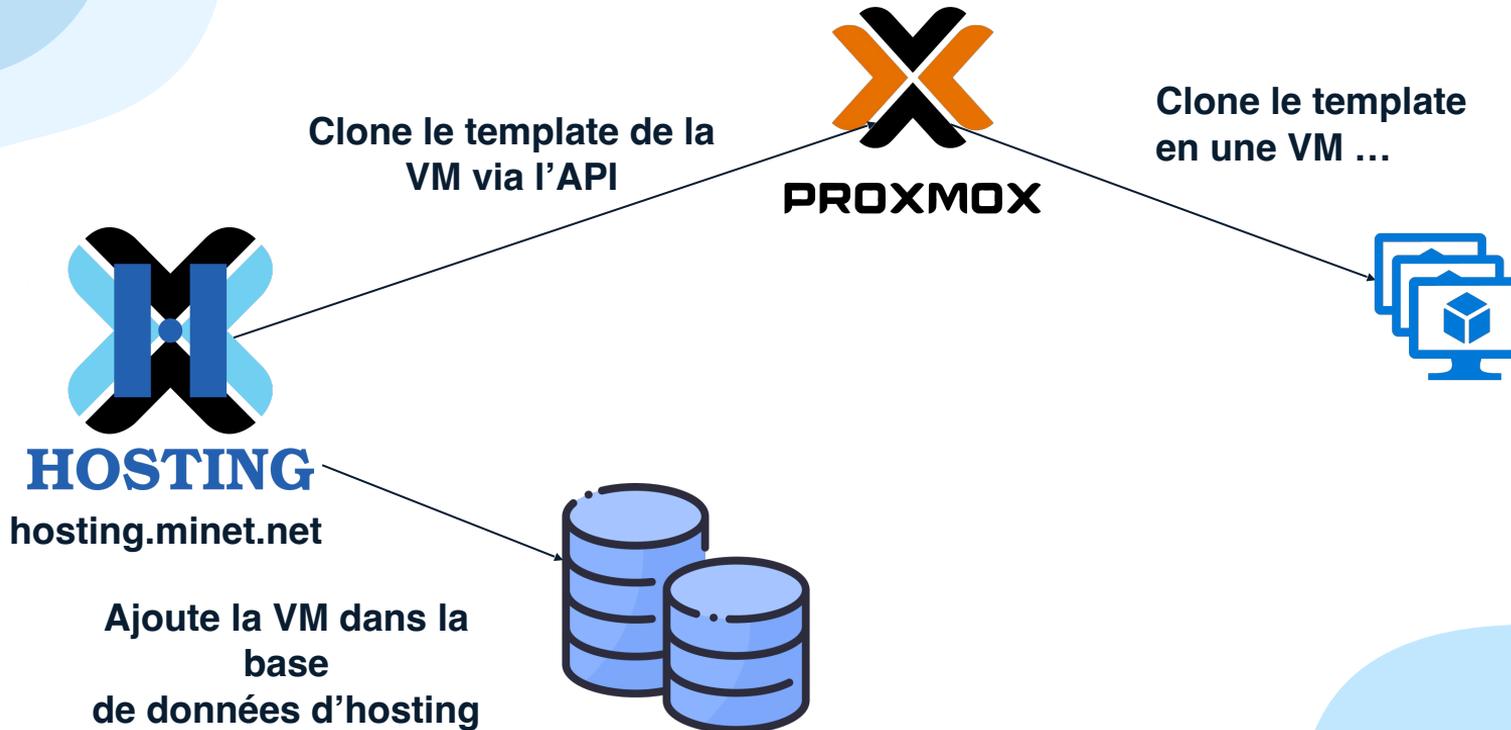
HOSTING

hosting.minet.net

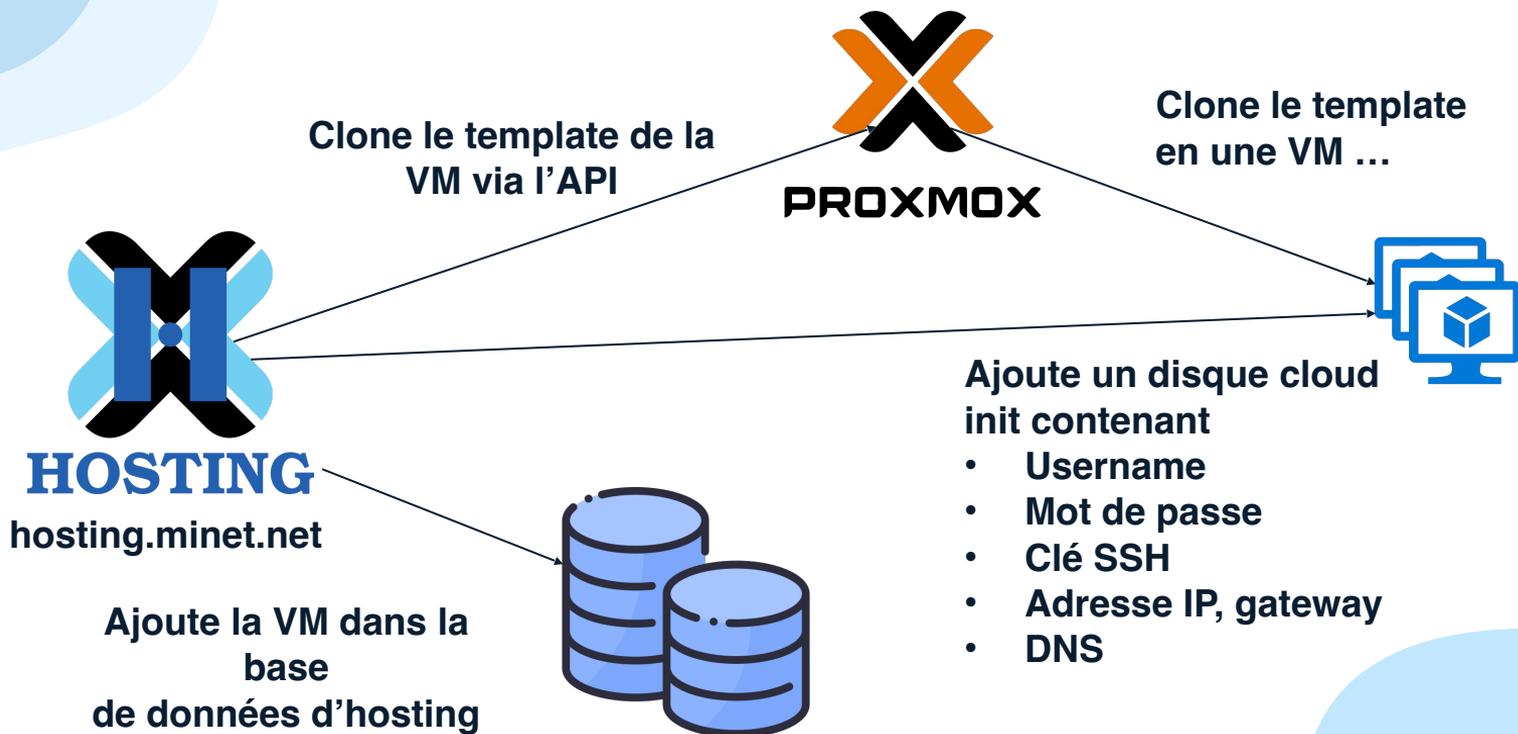
Ajoute la VM dans la
base
de données d'hosting



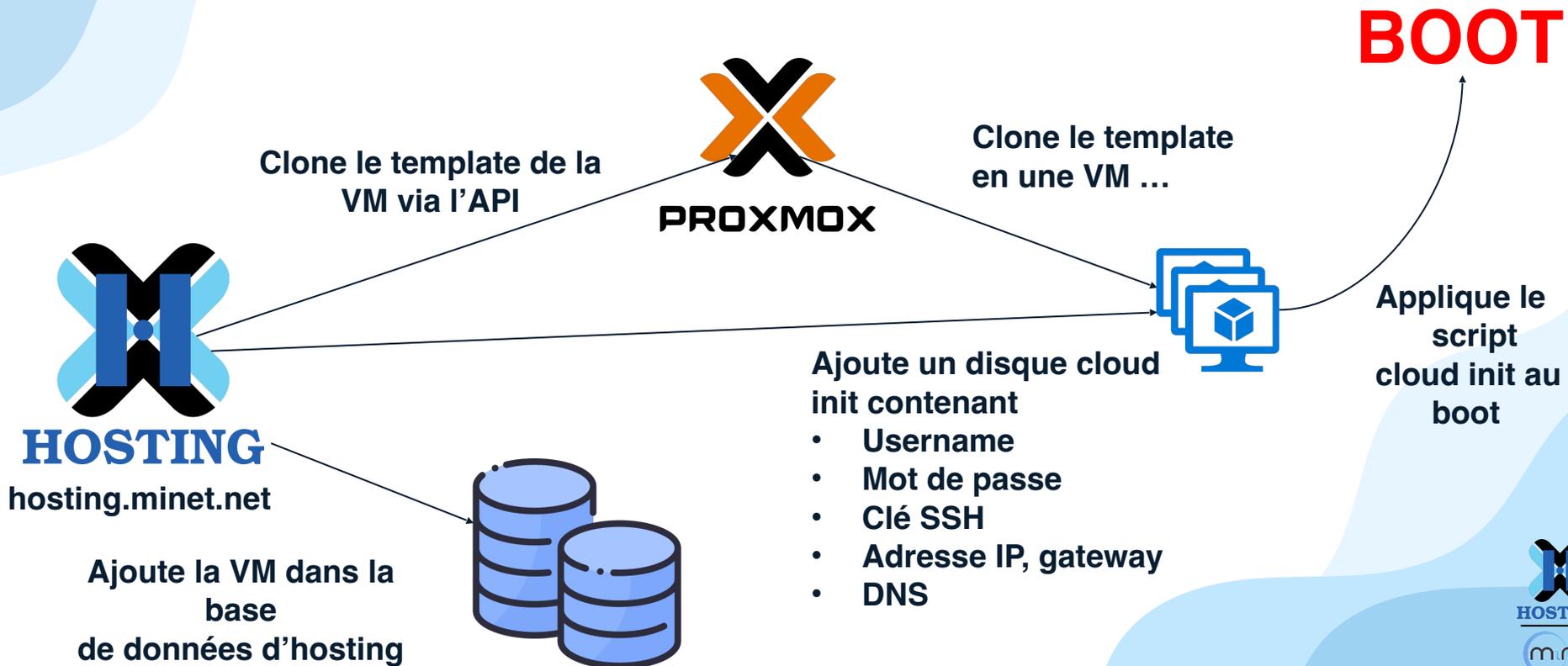
Processus de creation de VM



Processus de creation de VM



Processus de creation de VM



Processus d'ajout d'une entrée DNS

BIND 9



HOSTING

hosting.minet.net



DNS de MiNET

Processus d'ajout d'une entrée DNS

Ajouter l'entrée dans le
DNS d'hosting



HOSTING

hosting.minet.net

Ajouter la VM dans la
base
de données d'hosting



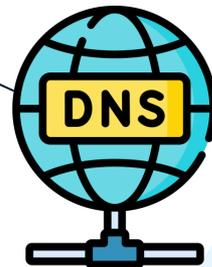
DNS de MiNET

Processus d'ajout d'une entrée DNS

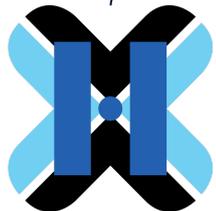
Ajouter l'entrée dans le
DNS d'hosting



Redirige toutes les
requêtes DNS pour
h.minet.net



DNS de MiNET



HOSTING

hosting.minet.net

Ajouter la VM dans la
base
de données d'hosting



D'un point de vue adressage

IPs appartenant à l'école

192.168.104.0/24

157.159.195.0/24

– **157.159.195.1-157.159.195.10**

– **157.159.195.11-157.159.195.255**

D'un point de vue adressage

157.159.0.0/16 IPs appartenant à l'école

192.168.104.0/24

157.159.195.0/24

– **157.159.195.1-157.159.195.10**

– **157.159.195.11-157.159.195.255**

D'un point de vue adressage

157.159.0.0/16 IPs appartenant à l'école

192.168.104.0/24 Réseau administration privé

157.159.195.0/24

– **157.159.195.1-157.159.195.10**

– **157.159.195.11-157.159.195.255**

D'un point de vue adressage

157.159.0.0/16 IPs appartenant à l'école

192.168.104.0/24 Réseau administration privé

157.159.195.0/24 Réseau public, VLAN 200

– **157.159.195.1-157.159.195.10**

– **157.159.195.11-157.159.195.255**

D'un point de vue adressage

157.159.0.0/16 IPs appartenant à l'école

192.168.104.0/24 Réseau administration privé

157.159.195.0/24 Réseau public, VLAN 200

– **157.159.195.1-157.159.195.10** IP réservée pour l'administration

– **157.159.195.11-157.159.195.255**

D'un point de vue adressage

157.159.0.0/16 IPs appartenant à l'école

192.168.104.0/24 Réseau administration privé

157.159.195.0/24 Réseau public, VLAN 200

– **157.159.195.1-157.159.195.10** IP réservée pour l'administration

– **157.159.195.11-157.159.195.255** IP attribuées aux VMs

04

La plateforme web

Objectif : dépasser les 25 000 contributions sur
le repo github

04

La plateforme web

Objectif : dépasser les 25 000 contributions sur
le repo github

Ouais je flex, mais c'est ma formation, donc
je
fais ce que je veux

04

La plateforme web

Objectif : dépasser les 25 000 contributions sur
le repo github

Ouais je flex, mais c'est ma formation, donc
je
fais ce que je veux

Comment que c'est que ça marche ?



hosting.minet.net

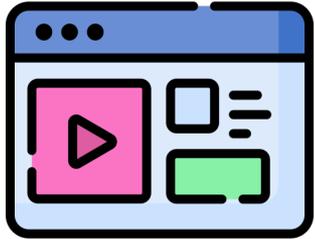
**2 SERVEURS
WEB
DIFFÉRENTS**



backprox.minet.net



Comment que c'est que ça marche ?



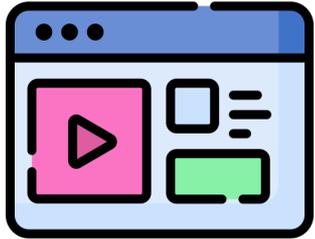
hosting.minet.net



backprox.minet.net



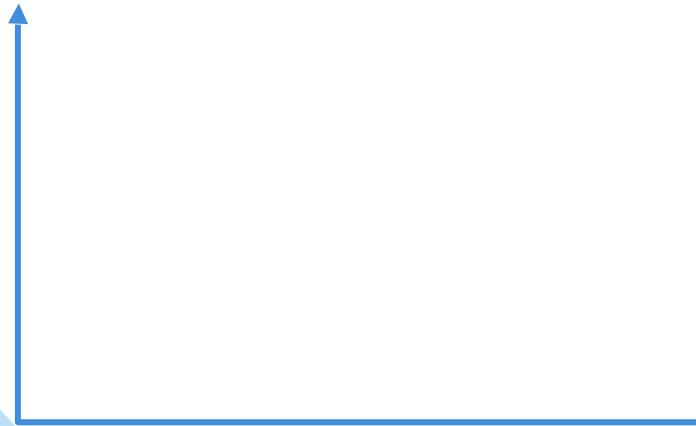
Comment que c'est que ça marche ?



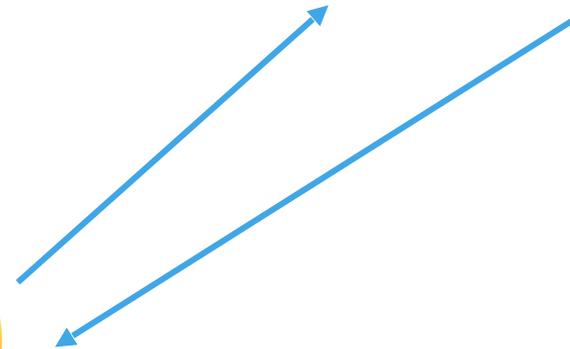
hosting.minet.net



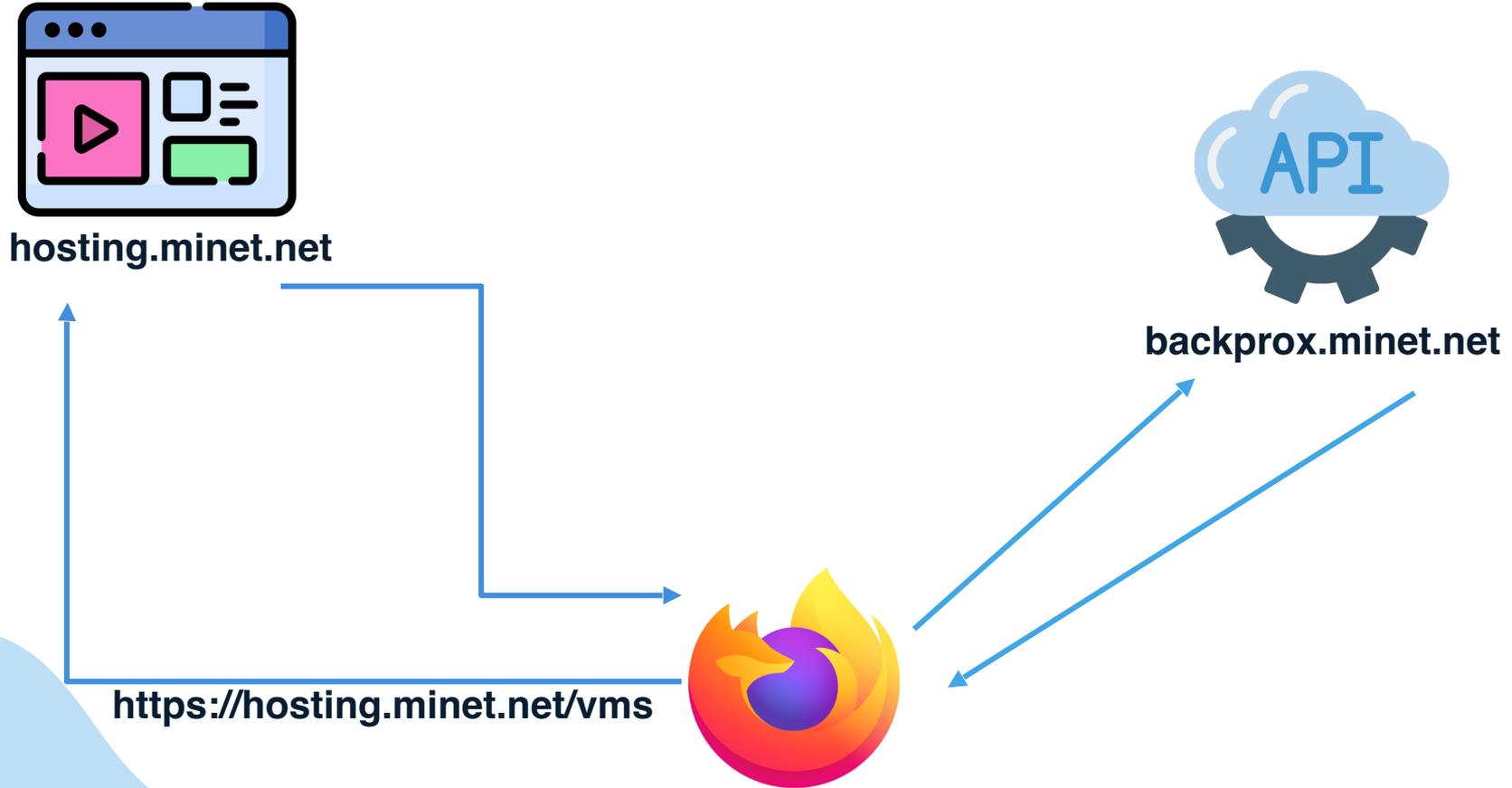
backprox.minet.net



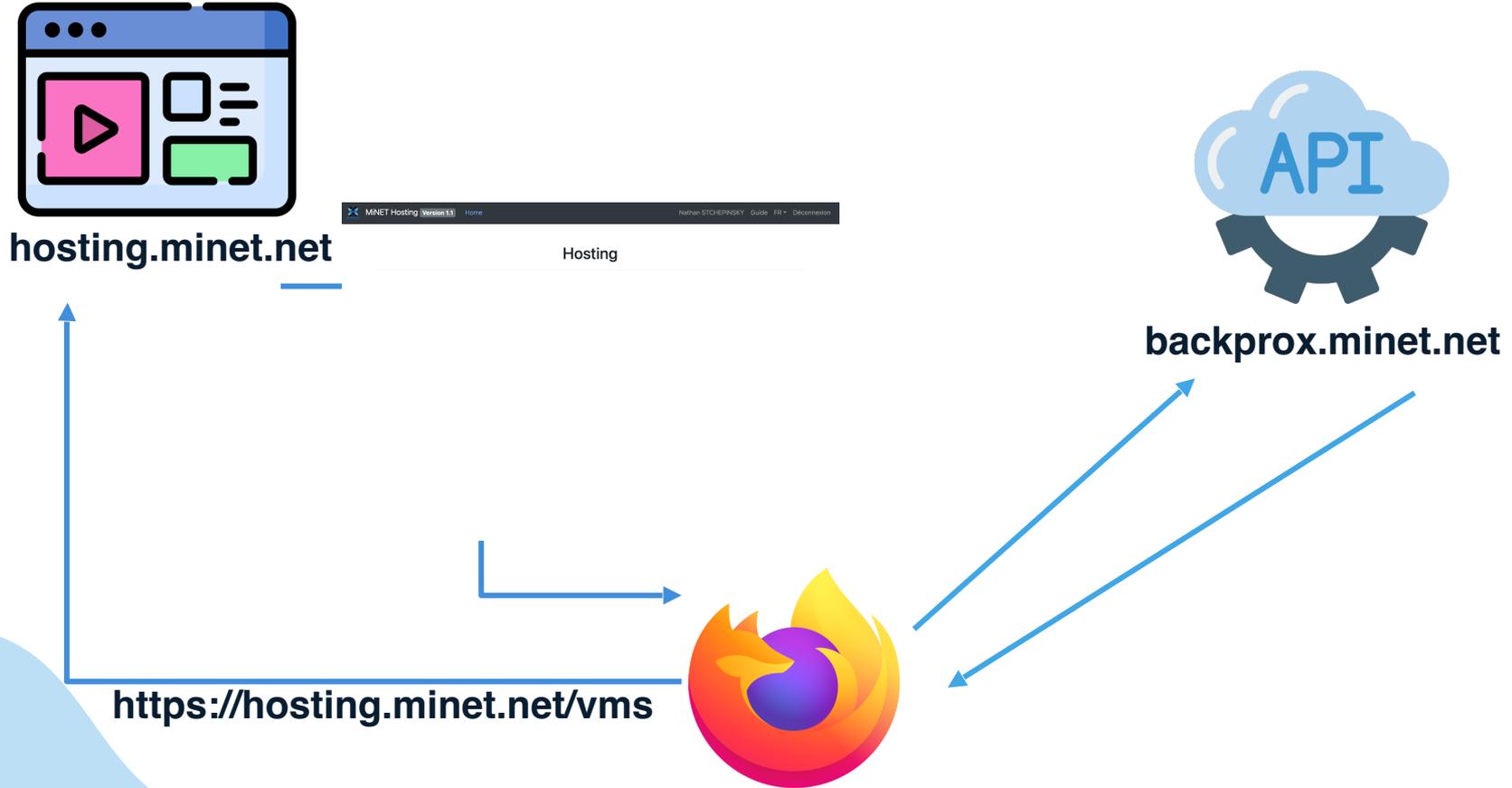
<https://hosting.minet.net/vms>



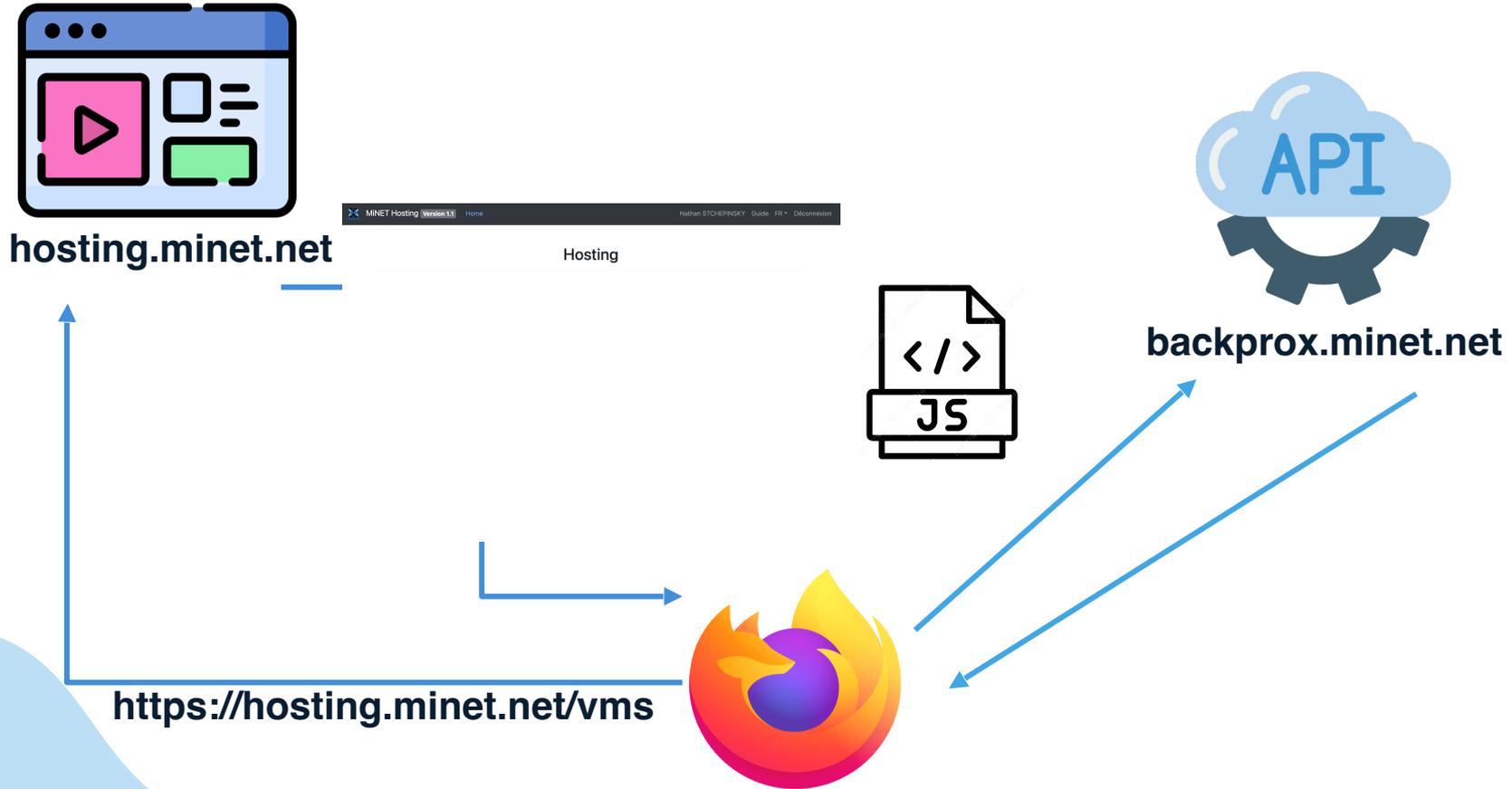
Comment que c'est que ça marche ?



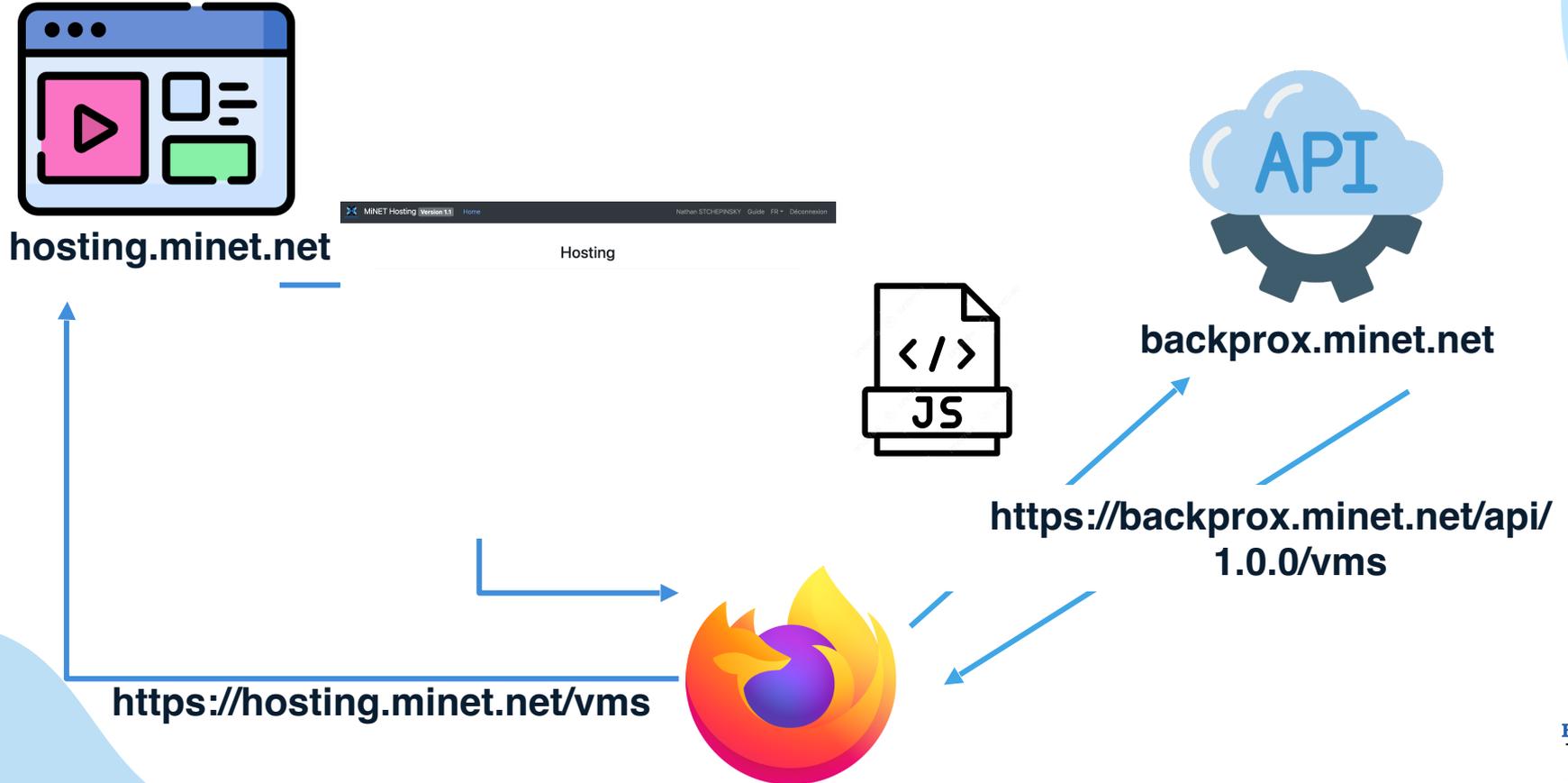
Comment que c'est que ça marche ?



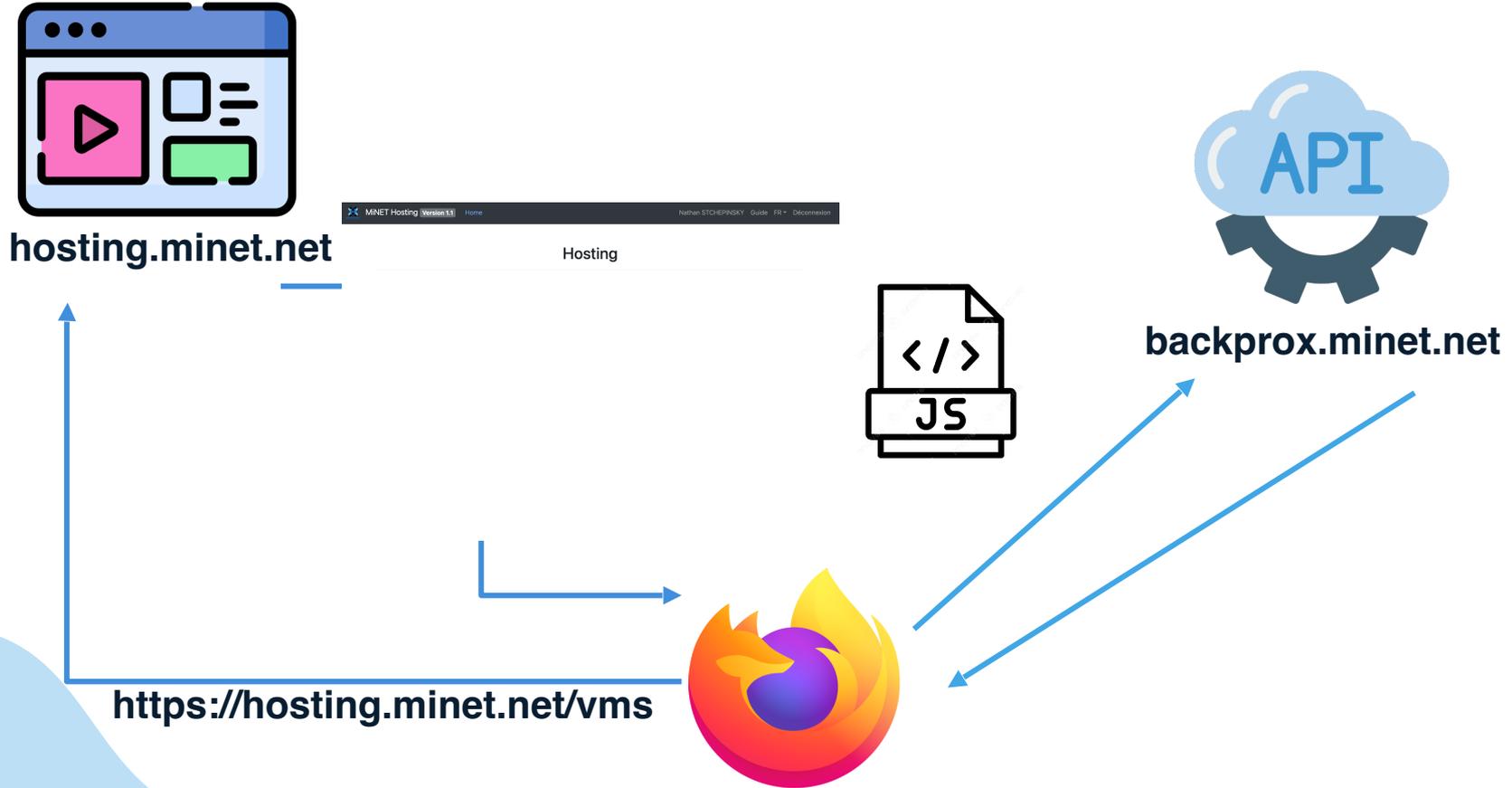
Comment que c'est que ça marche ?



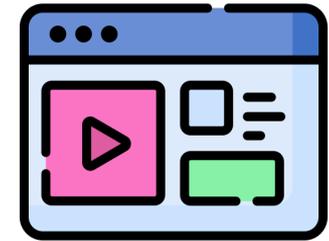
Comment que c'est que ça marche ?



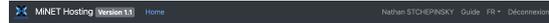
Comment que c'est que ça marche ?



Comment que c'est que ça marche ?



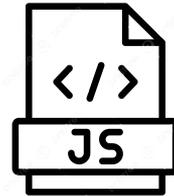
hosting.minet.net



Hosting



backprox.minet.net

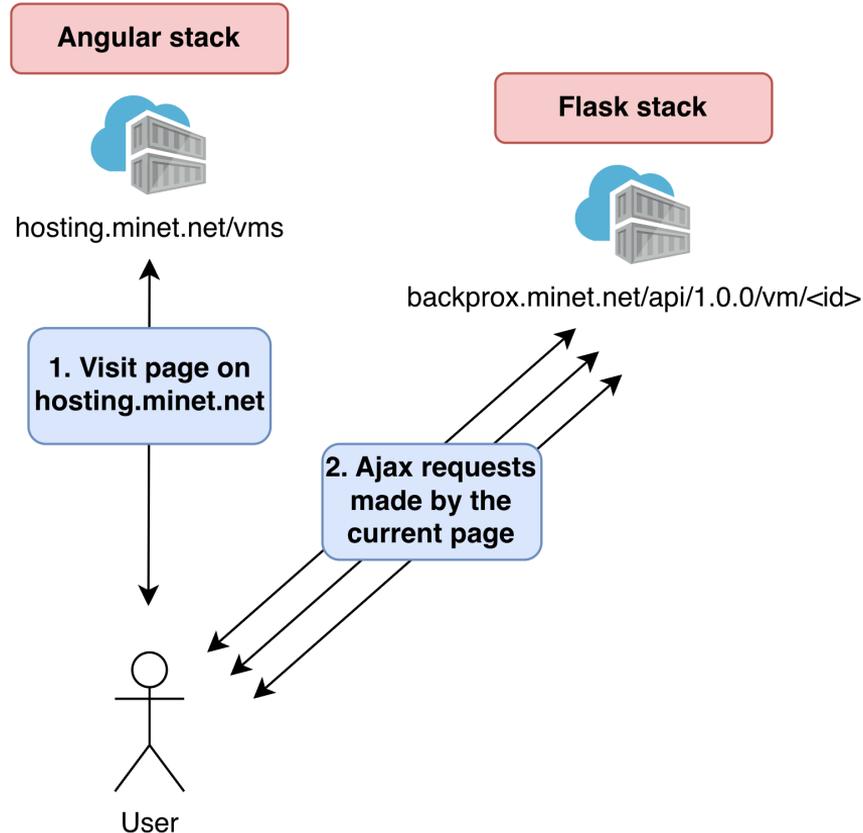


<https://hosting.minet.net/vms>



```
1 [132, 207, 231, 173, 218, 180, 225, 162, 163, 151, 200, 112, 139, 189,  
2 169, 203, 115, 117, 157, 177, 222, 229, 224, 135, 146, 215, 181, 214,  
3 123, 230, 170, 168, 147, 119, 150, 111, 120, 221, 178, 213, 216, 208,  
4 183, 220, 164, 129, 172, 126, 128, 140, 185, 136, 133, 116, 130, 141,  
5 145, 137, 138, 1010, 165, 158, 127, 121, 154, 174, 114, 159, 152, 199,  
6 210, 201, 233, 161, 211, 235, 193, 194, 131, 182, 219, 236, 184, 192,  
7 206, 226, 232, 118, 167, 186, 176, 202, 144, 217, 227, 205, 198, 234,  
8 195, 166, 143, 148, 187, 223, 149, 175, 125, 212, 209, 228, 191, 204]
```

Comment que c'est que ça marche ?



P'tit quizz

Allez sur hosting.minet.net et connectez vous en tant qu'adhérent.

Combien de requêtes votre navigateur fait-il à l'API ?

0

8

9

10

P'tit quizz

Allez sur hosting.minet.net et connectez vous en tant qu'adhérent.

Combien de requêtes votre navigateur fait-il à l'API ?

0

8

9

10

P'tit quizz

Allez sur hosting.minet.net et connectez vous en tant qu'adhérent.

Combien de requêtes votre navigateur fait-il à l'API ?

0

8

Oui je sais trou du cul, tu as plus de requêtes parce que tu as déjà des VMs, mais qui l'a demandé ?

9

10

P'tit quizz

Allez sur hosting.minet.net et connectez vous en tant qu'adhérent.

Combien de requêtes votre navigateur fait-il à l'API ?

0

8

Oui je sais trou du cul, tu as plus de requêtes parce que tu as déjà des VMs, mais qui l'a demandé ?

9

10

On regarde ensemble ?

Partie I Le frontend

app-routing.module.ts : les routes

```
1 const routes: Routes = [  
2   {path: '', component: HomeComponent},  
3   {path: 'vms', component: VmsComponent},  
4   {path: 'vms/:vmid', component: VmComponent},  
5   {path: 'dns', component: DnsComponent},  
6   {path: 'legal', component: LegalComponent},  
7   {path: 'manual', component: ManualComponent},  
8   {path: 'history', component: HistoryComponent},  
9   {path: '**', redirectTo: ''},  
10 ];
```



Partie I
Le frontend

Les composants

Contient tout le code HTML
d'un
composant
*(le corps la page des VMs,
home, etc ...)*

Est intégré directement dans
l'`index.html`, en fonction de
la route



Partie I
Le frontend

index.html : la base

```
1 <!doctype html>
2 <html>
3   <head></head>
4
5   <body>
6     <app-root></app-root>
7   </body>
8 </html>
```

<app-root>

app.component.html

```
1 <app-navbar></app-navbar>
2
3 <ng-template></ng-template>
4
5 <app-footer></app-footer>
6
```



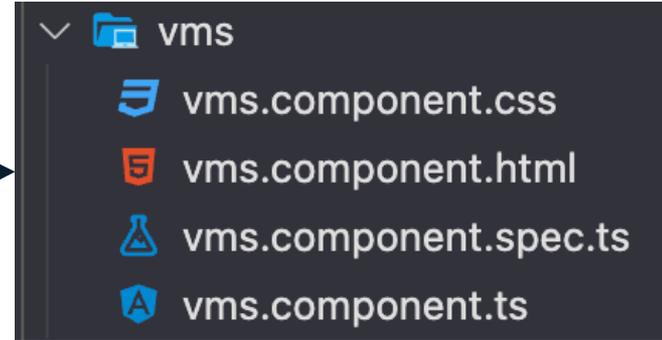
Partie I
Le frontend

app.component.html

```
1 <app-navbar></app-navbar>
2
3 <ng-template></ng-template>
4
5 <app-footer></app-footer>
6
```

<ng-template>

component



Partie I
Le frontend

app.component.html

```
1 <app-navbar></app-navbar>
2
3 <ng-template></ng-template>
4
5 <app-footer></app-footer>
6
```

<ng-template>

component

```
vms
├── vms.component.css
├── vms.component.html
├── vms.component.spec.ts
└── vms.component.ts
```



Partie I
Le frontend

app.component.html

```
1 <app-navbar></app-navbar>
2
3 <ng-template></ng-template>
4
5 <app-footer></app-footer>
6
```

<ng-template>

component

```
└─ vms
   ├── vms.component.css
   ├── vms.component.html
   ├── vms.component.spec.ts
   └── vms.component.ts
```



Partie I Le frontend

component.ts Typescript TABASSE javascript

Bon, écoute-moi bien. TypeScript déchire carrément la gueule de JavaScript, et je vais te dire pourquoi.

D'abord, TypeScript est comme le grand frère badass de JavaScript. Il lui met une bonne claque avec son système de typage statique. Tu vois, JavaScript est un langage permissif, il te laisse te fourrer dans n'importe quelle galère sans te prévenir. Mais TypeScript, lui, il te dit "Hé, attention ! Tu essaies de mélanger des types comme un idiot !". Il t'oblige à déclarer les types de tes variables, tes paramètres de fonction et tes retours de valeurs. Ça veut dire moins de bugs stupides qui se produisent lors de l'exécution, parce que TypeScript les repère avant même que tu lances ton code de merde.

Ensuite, TypeScript, c'est le mec qui sait comment bien gérer la programmation orientée objet. Il sait comment utiliser les classes, l'héritage, les interfaces et tout le bordel. Ça rend ton code beaucoup plus organisé et compréhensible. Fini le bordel incompréhensible de JavaScript où tu ne sais pas qui fait quoi. TypeScript te permet de structurer ton code de façon claire et de définir des contrats entre les différentes parties de ton programme. C'est comme mettre de l'ordre dans la putain de jungle de JavaScript.

Et attends, y'a encore mieux ! TypeScript a un système de compilation qui transforme ton code TypeScript en JavaScript utilisable par les navigateurs et les moteurs JavaScript. Tu peux donc utiliser les dernières fonctionnalités de JavaScript tout en profitant des améliorations de TypeScript. En plus, ça optimise ton code pour qu'il soit plus court et plus rapide. Ça donne des performances de ouf, mec.

Pour couronner le tout, TypeScript a une putain de communauté qui déchire tout. Tous les grands frameworks comme Angular, React et Vue.js le supportent à fond. Ça veut dire que tu peux utiliser les meilleures technologies tout en bénéficiant des avantages de TypeScript. C'est comme si tu rejoignais une bande de mecs badass qui savent ce qu'ils font.

Donc voilà, en gros, TypeScript met une sacrée raclée à JavaScript. Son système de typage statique, sa programmation orientée objet, sa compilation et sa communauté de malades font de lui le choix ultime. Si tu veux coder comme un vrai pro et mettre JavaScript à genoux, choisis TypeScript.



ChatGPT



Partie I Le frontend

component.html

Intègre utilise et est utilisé par typescript

```
1 <div class="container text-center" *ngIf="!loading && (user.chartevalidated || user.admin)">
2   <h1 class="text-center mb-2">VM: {{ user.vms[0].name }}</h1>
3
4   <div class="alert"
5     [ngClass]="{
6       'alert-danger': deletionStatus == 'deleting' || vm_has_error,
7       'alert-secondary': user.vms[0].status === 'stopped',
8       'alert-info': user.vms[0].status === 'creating',
9       'alert-warning': user.vms[0].status === 'booting',
10      'alert-success': user.vms[0].status === 'running' || deletionStatus == 'deleted'
11    }">
12   </div>
13 </div>
```



Partie I

Le frontend

Les pages

- **/ : Home** - Création de VMs
- **/vms : Listes des VMs** – Liste de toutes les VMs pour les admins
- **/vms/<vmid> : Vue particulière d'une**
- **/dns : Liste des entrées DNS** – Liste de toutes les entrées DNS pour les admins

Partie I

Le frontend

Les fonctionnalités

- **/ : Home** - Création de VMs
- **/vms : Listes des VMs** – Liste de toutes les VMs pour les admins
- **/vms/<vmid> : Vue particulière d'une**
- **/dns : Liste des entrées DNS** – Liste de toutes les entrées DNS pour les admins

Partie I

Le frontend

Les fonctionnalités

Historique des IPs

Historique des attributions d'IP

Cet historique technique permet de retracer les éventuels changements d'IP d'une VM via le DHCP.

« 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 »

Rechercher une IP / nom d'utilisateur

IP	Date	ID de la VM	ID Utilisateur
157.159.195.106	2021-04-15T19:44:36Z	cin	106
157.159.195.106	2021-04-15T22:13:52Z	cin	106
157.159.195.109	2021-04-15T23:38:33Z	cin	109
157.159.195.110	2021-04-15T23:43:37Z	cin	110
157.159.195.112	2021-04-16T02:54:46Z	cin	112
157.159.195.106	2021-04-16T09:12:05Z	jgo	106
157.159.195.109	2021-04-16T20:25:07Z	cin	109
157.159.195.110	2021-04-18T23:09:37Z	cin	110
157.159.195.110	2021-04-19T01:04:17Z	cin	110
157.159.195.109	2021-04-20T19:04:11Z	jgo	109

Transfert de propriété

ID : 143

Type : bare vm

Statut : running

Nom : asgard

Adresse IPv4 : 157.159.195.33

Démarrage automatique : Décochez cette option si vous ne souhaitez pas que votre VM soit automatiquement démarrée dans le cas d'un redémarrage de notre serveur

Propriétaire : trustody

Créé le : 2023-03-23

Optime : 81d 13h 55min 50s

CPU : 2

RAM (GB) : 4

Espace disque (GB) : 10

0.88 / 4 GB

4%

Changer mes identifiants

Supprimer Eteindre

Compte actuel : trustody

Login adhérent Transférer la propriété

Partie I

Le frontend

Les fonctionnalités

Différents niveau de freeze de compte :
le freeze_state



Hosting



Votre compte est gelé !

Votre cotisation a expiré ! Vous pourrez toujours gérer vos VMs pendant plusieurs jours. Après 30 jours d'expiration, vos VMs seront éteintes. Après 60 jours, elles seront définitivement détruites. **ATTENTION : vous avez seulement 30 jours pour renouveler votre cotisation, avant l'extinction de vos VMs**

Votre cotisation a expiré

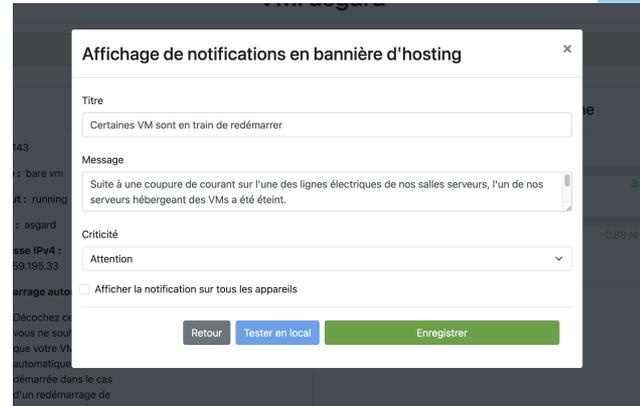
Votre cotisation a expiré. Vous ne pouvez pas créer de VMs

Partie I

Le frontend

Les fonctionnalités

Les notifications par bannières :



MiNET Hosting **Version 1.1**

[Home](#) [VMs](#) [DNS](#) [Notification](#)

Nathan STCSTEPINSKY [Guide](#) [FR](#) [Déconnexion](#)

Cette formation est vraiment incroyable
Tg Nicolas nonobstant



Hosting



Partie I

Le frontend

Les fonctionnalités

Update des credentials d'une VM

VM: horus

Statut : allumée et en fonctionnement

Mettre à jour vos identifiants

Nom d'utilisateur de la VM :

Mot de passe :

Clé SSH publique :

En mettant à jours vos identifiants, vous supprimez les anciens credentials. Pour ajouter de nouveaux comptes ou moyen de connexion, ajoutez les directement sur la VM.

[Retour](#) [Mettre à jour et redémarrer](#)

Partie I

Le frontend

La fonctionnalité principale :

Les ✨ ressources dynamiques ✨

6 CPUs restant

9 GO de RAM restant

30 GO de stockage restant

Créez votre Machine Virtuelle

Vous disposez de ressources gratuite que vous pouvez attribuer à 1, 2 ou 3 machines virtuelles

6 CPUs
8 GO de RAM
30 GO de stockage

Configurer votre VM

Nombre de CPU : **0 CPUs**



RAM : **0 GO**



Stockage : **0 GO**

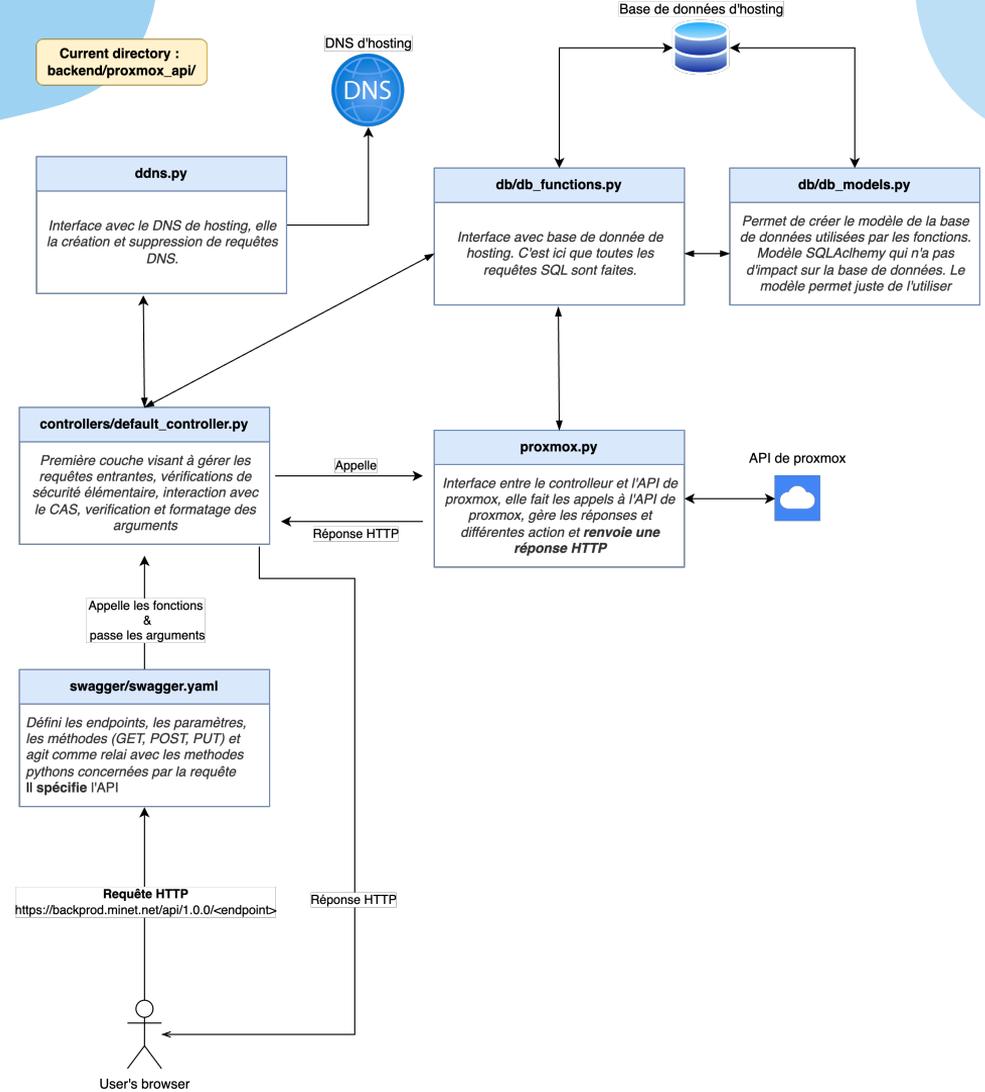


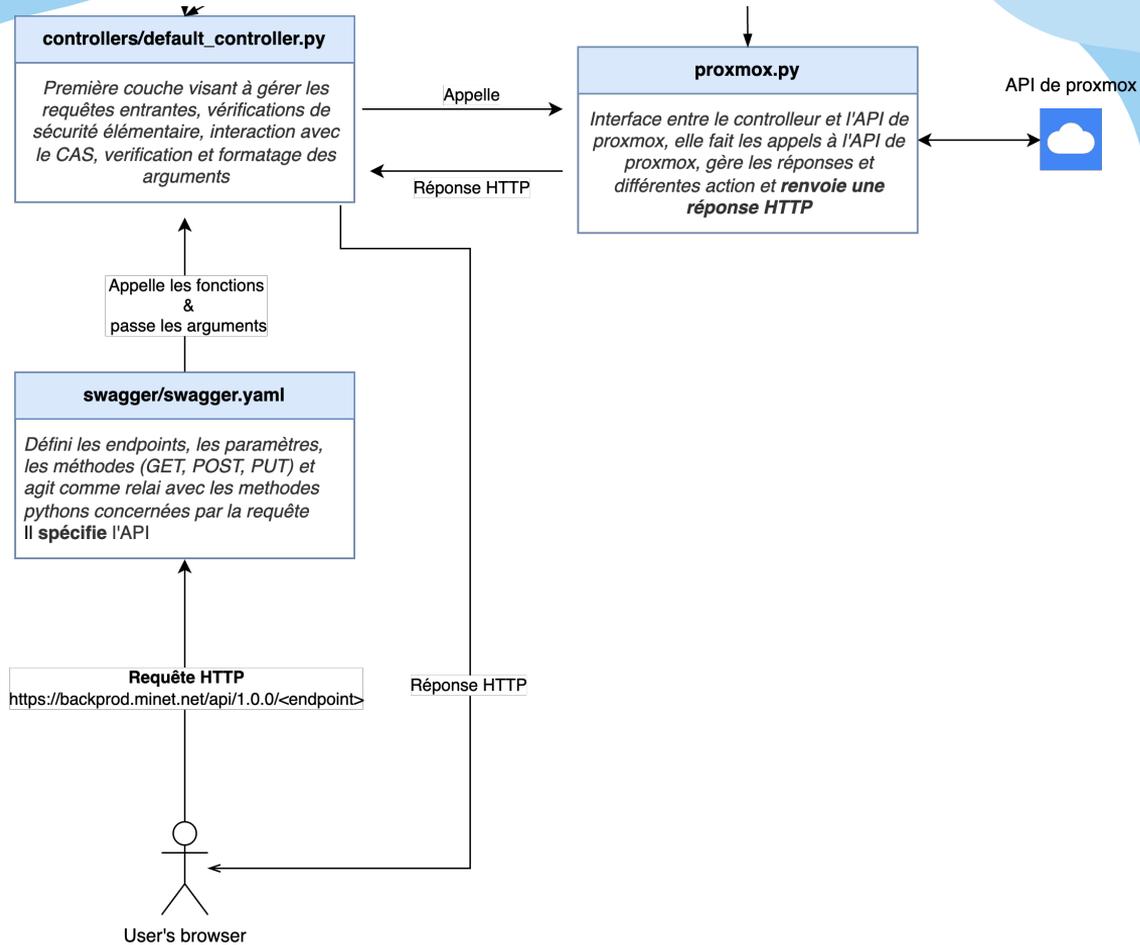
Attention, une fois créée, il n'est plus possible de ré-allouer les ressources !
Il faudra supprimer les machines pour les rendre accessible de nouveau

Partie II

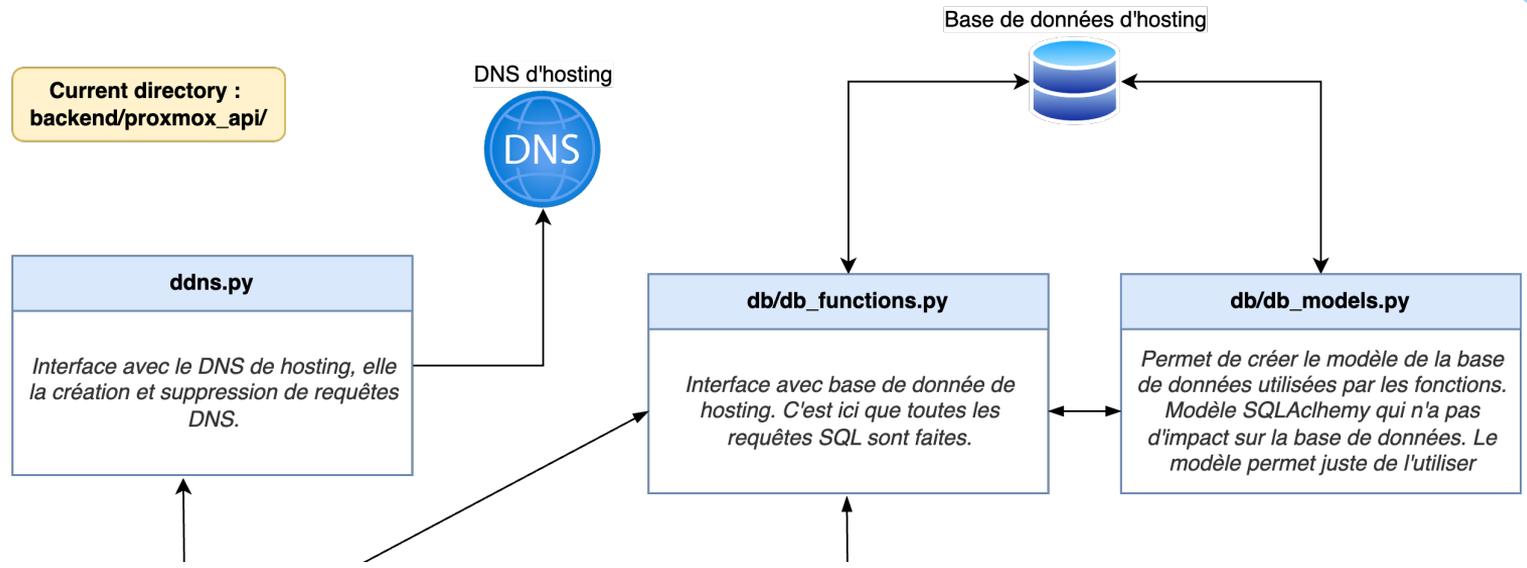
L'API

<https://backprox.minet.net/api/1.0.0/ui>



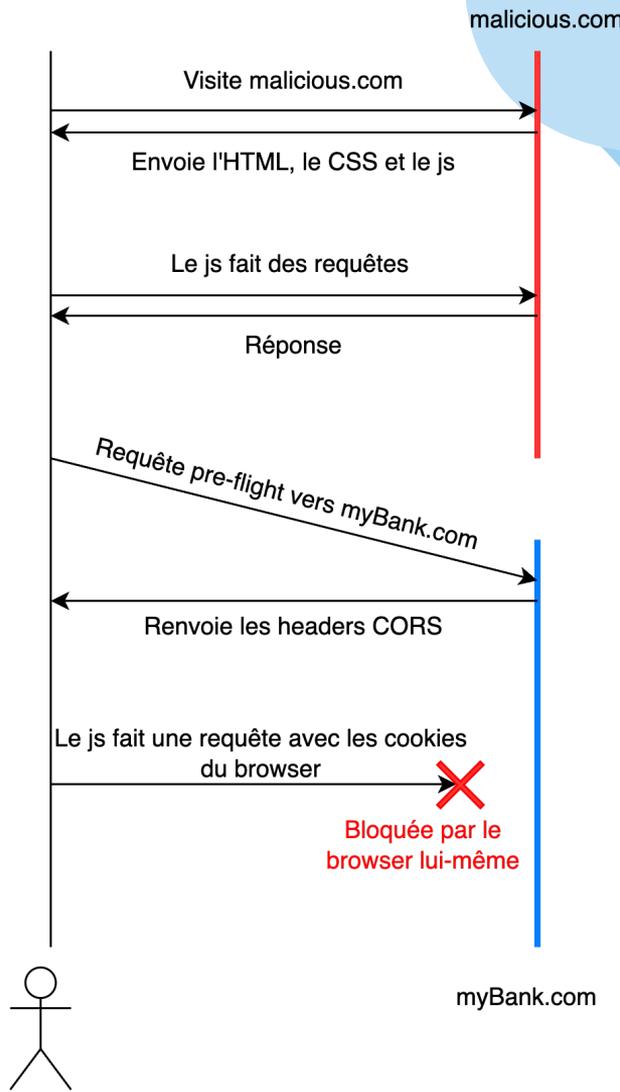


Current directory :
backend/proxmox_api/



Partie II L'API

Petit digression,
les **CORS**



Partie II

L'API

Les tests de code



Partie II

L'API

Les tests de code



< test_backend

69 tests

0 failures

0 errors

100% success rate

352.03s

Tests

Suite	Name	Filename	Status	Duration	Details
test.integration.test_vm_life_10G	test_valid_vm_creation		✓	61.45s	View details
test.integration.test_vm_life_30G	test_valid_vm_creation		✓	56.14s	View details
test.integration.test_vm_life_20G	test_valid_vm_creation		✓	50.28s	View details
test.integration.test_vm_life_20G	test_vm_start		✓	37.72s	View details
test.integration.test_vm_life_30G	test_vm_start		✓	34.95s	View details

Partie II

L'API

Les tests de code



< test_backend

69 tests

0 failures

0 errors

100% success rate

352.03s

Tests

Suite	Name	Filename	Status	Duration	Details
test.integration.test_vm_life_10G	test_valid_vm_creation		✓	61.45s	View details
test.integration.test_vm_life_30G	test_valid_vm_creation		✓	56.14s	View details
test.integration.test_vm_life_20G	test_valid_vm_creation		✓	50.28s	View details
test.integration.test_vm_life_20G	test_vm_start		✓	37.72s	View details
test.integration.test_vm_life_30G	test_vm_start		✓	34.95s	View details

69 tests

Partie II L'API

Les tests de code



< test_backend

69 tests

0 failures

0 errors

100% success rate

352.03s

Tests

Suite	Name	Filename	Status	Duration	Details
test.integration.test_vm_life_10G	test_valid_vm_creation		✓	61.45s	View details
test.integration.test_vm_life_30G	test_valid_vm_creation		✓	56.14s	View details
test.integration.test_vm_life_20G	test_valid_vm_creation		✓	50.28s	View details
test.integration.test_vm_life_20G	test_vm_start		✓	37.72s	View details
test.integration.test_vm_life_30G	test_vm_start		✓	34.95s	View details

69 tests

46% de
coverage

05

Sécurité et dangers

L'un des points le plus important

Le risque ...

 Status	running
 HA State	none
 Node	wammu
 CPU usage	100.05% of 16 CPU(s)
 Memory usage	57.66% (9.22 GiB of 16.00 GiB)
 Bootdisk size	30.00 GiB
 IPs	No Guest Agent configured

Sécurité anti-spoofing : le firewall de proxmox

Virtual Machine 192 (horus) on node 'kars'

▶ Start ⏻ Shutdown ▼ ↻ Migrate >_ Console ▼ More ▼ ? Help

- Summary
- >_ Console
- Hardware
- Cloud-Init
- Options
- Task History
- Monitor
- Backup
- Replication
- Snapshots
- Firewall**
- Options
- Alias
- IPSet
- Log

Buttons: Add Copy Insert: Security Group Remove Edit

	On	Type	Action	Macro	Interface	Protocol	Source	S.Port	Destination	D.Port	Log level	Co
☰ 0	<input checked="" type="checkbox"/>	out	ACCEPT				+hosting				nolog	
☰ 1	<input checked="" type="checkbox"/>	in	ACCEPT						+hosting		nolog	
☰ 2	<input checked="" type="checkbox"/>	out	DROP								nolog	
☰ 3	<input checked="" type="checkbox"/>	in	DROP								nolog	

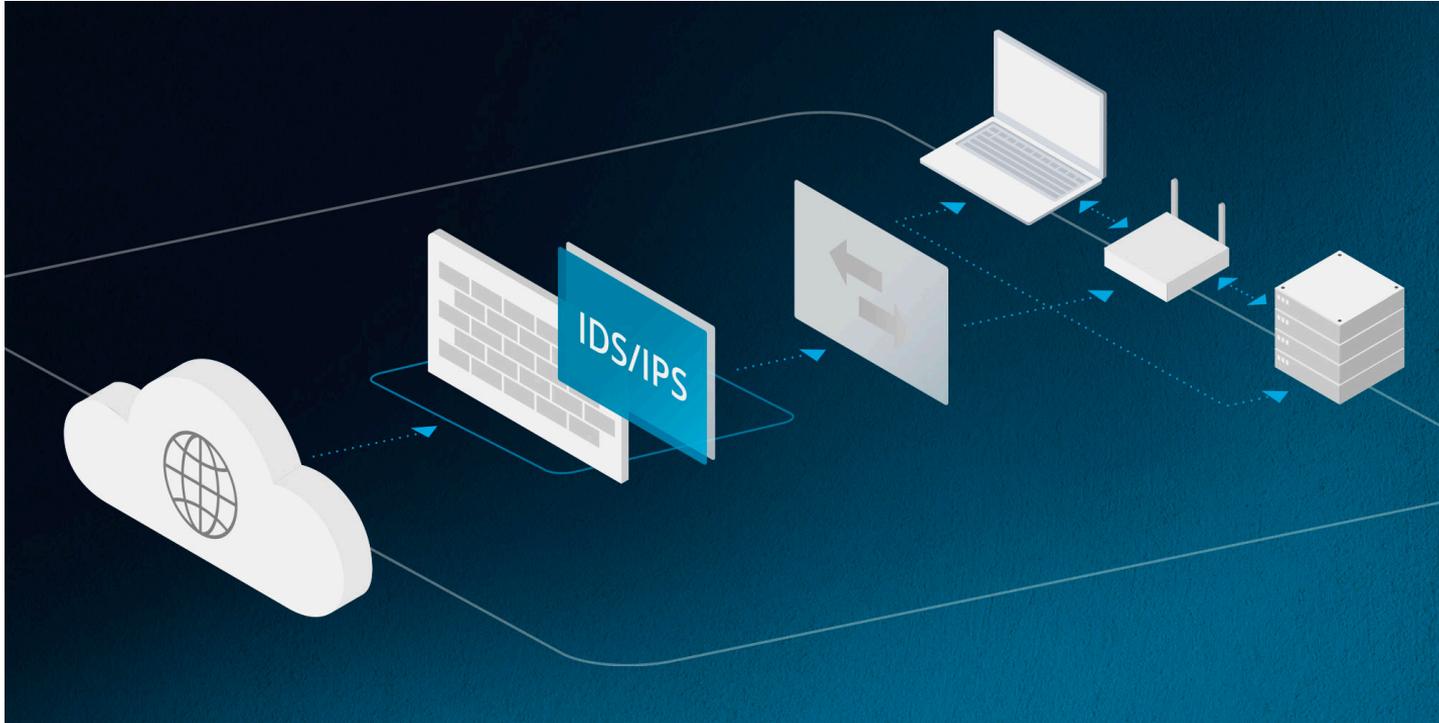
Sécurité anti-spoofing : ... depuis le code directement

```
350 # order matters
351 proxmox.nodes(node).qemu(vmid).firewall.options.put(enable=1)
352 proxmox.nodes(node).qemu(vmid).firewall.options.put(ipfilter=0) "ipfilter": Unknown word.
353 proxmox.nodes(node).qemu(vmid).firewall.options.put(policy_in="ACCEPT")
354 proxmox.nodes(node).qemu(vmid).firewall.rules.post(action="DROP", type="out", log="nolog", enable=1) # OUT DROP -log
nolog
355 proxmox.nodes(node).qemu(vmid).firewall.rules.post(action="DROP", type="in", log="nolog", enable=1) # IN DROP -log nolog
356 proxmox.nodes(node).qemu(vmid).firewall.rules.post(action="ACCEPT", type="in", dest="+hosting", log="nolog", enable=1)
# IN ACCEPT -dest +hosting -log nolog
357 proxmox.nodes(node).qemu(vmid).firewall.rules.post(action="ACCEPT", type="out", source="+hosting", log="nolog",
enable=1) # OUT ACCEPT -source +hosting -log nolog
358
```

Brute force : le nmap

```
Jun 14 16:52:21 horus sshd[17180]: Invalid user rancher from 82.180.162.185 port 43438
Jun 14 16:52:21 horus sshd[17180]: Received disconnect from 82.180.162.185 port 43438:11: Bye Bye [preauth]
Jun 14 16:52:21 horus sshd[17180]: Disconnected from invalid user rancher 82.180.162.185 port 43438 [preauth]
Jun 14 16:52:25 horus sshd[17182]: Received disconnect from 182.16.179.214 port 56378:11: Bye Bye [preauth]
Jun 14 16:52:25 horus sshd[17182]: Disconnected from authenticating user root 182.16.179.214 port 56378 [preauth]
Jun 14 16:53:08 horus sshd[17189]: Invalid user ale from 103.82.145.161 port 53536
Jun 14 16:53:08 horus sshd[17189]: Received disconnect from 103.82.145.161 port 53536:11: Bye Bye [preauth]
Jun 14 16:53:08 horus sshd[17189]: Disconnected from invalid user ale 103.82.145.161 port 53536 [preauth]
Jun 14 16:54:08 horus sshd[17192]: Received disconnect from 82.180.162.185 port 49922:11: Bye Bye [preauth]
Jun 14 16:54:08 horus sshd[17192]: Disconnected from authenticating user root 82.180.162.185 port 49922 [preauth]
Jun 14 16:54:30 horus sshd[17195]: Invalid user boo from 182.16.179.214 port 46816
Jun 14 16:54:30 horus sshd[17195]: Received disconnect from 182.16.179.214 port 46816:11: Bye Bye [preauth]
Jun 14 16:54:30 horus sshd[17195]: Disconnected from invalid user boo 182.16.179.214 port 46816 [preauth]
Jun 14 16:54:50 horus sshd[17198]: Received disconnect from 103.82.145.161 port 45676:11: Bye Bye [preauth]
Jun 14 16:54:50 horus sshd[17198]: Disconnected from authenticating user root 103.82.145.161 port 45676 [preauth]
Jun 14 16:56:29 horus sshd[17202]: Received disconnect from 182.16.179.214 port 36360:11: Bye Bye [preauth]
Jun 14 16:56:29 horus sshd[17202]: Disconnected from authenticating user root 182.16.179.214 port 36360 [preauth]
Jun 14 16:57:38 horus sshd[17206]: Invalid user test from 83.97.73.83 port 53128
Jun 14 16:57:54 horus sshd[17206]: Connected to user by invalid user test 83.97.73.83 port 53128 [preauth]
Jun 14 16:58:22 horus sshd[17209]: Invalid user hudson from 103.82.145.161 port 41621
Jun 14 16:58:23 horus sshd[17209]: Received disconnect from 103.82.145.161 port 41621:11: Bye Bye [preauth]
Jun 14 16:58:23 horus sshd[17209]: Disconnected from invalid user hudson 103.82.145.161 port 41621 [preauth]
Jun 14 16:58:26 horus sshd[17211]: Invalid user cdsmgr from 182.16.179.214 port 54592
Jun 14 16:58:27 horus sshd[17211]: Received disconnect from 182.16.179.214 port 54592:11: Bye Bye [preauth]
Jun 14 16:58:27 horus sshd[17211]: Disconnected from invalid user cdsmgr 182.16.179.214 port 54592 [preauth]
Jun 14 17:00:09 horus sshd[17216]: Invalid user wordpress from 103.82.145.161 port 60016
Jun 14 17:00:09 horus sshd[17216]: Received disconnect from 103.82.145.161 port 60016:11: Bye Bye [preauth]
Jun 14 17:00:09 horus sshd[17216]: Disconnected from invalid user wordpress 103.82.145.161 port 60016 [preauth]
Jun 14 17:00:26 horus sshd[17219]: Received disconnect from 182.16.179.214 port 44580:11: Bye Bye [preauth]
Jun 14 17:00:26 horus sshd[17219]: Disconnected from authenticating user root 182.16.179.214 port 44580 [preauth]
Jun 14 17:01:53 horus sshd[17223]: Invalid user dev from 103.82.145.161 port 36082
Jun 14 17:01:53 horus sshd[17223]: Received disconnect from 103.82.145.161 port 36082:11: Bye Bye [preauth]
Jun 14 17:01:53 horus sshd[17223]: Disconnected from invalid user dev 103.82.145.161 port 36082 [preauth]
```

Intrusion Detection & Prevention System



Piste de projet : Déployer *suricata* uniquement sur la hosting ?

Security by design

La particularité du design frontend/API

06

Les projets futurs

C'est CADEAU

Attention aux alternatives

Des milliards de projets encore à faire !

<https://gitlabint.priv.minet.net/hosting/api/-/issues>

Hosting > API > Issues

Open 19 Closed 49 All 68 Bulk edit New issue

🕒 Search or filter results... Q Created date ⌵

- Ajouter la date de la dernière backup effectuée sur les vue des VMs**
#68 - created 1 week ago by Nathan STCHEPINSKY
feature frontend proxmox 🔖 0
- Mieux segmenter l'utilisation des proxys**
#67 - created 2 weeks ago by Nathan STCHEPINSKY
bug gitlab 🔖 0
- Définir les quota maximum des ressources dans la db**
#65 - created 1 month ago by Nathan STCHEPINSKY
critical database dev fixed feature 👤 0 updated 5 days ago
- Upgrade to flaks 2.3**
#63 - created 1 month ago by Nathan STCHEPINSKY
feature frontend Non-prioritaire 🔖 0 updated 1 month ago
- Il faut vérifier le freeze state des comptes pas encore dans la db**
#60 - created 2 months ago by Nathan STCHEPINSKY
API bug frontend 👤 1 updated 1 month ago
- Il faut instaurer un timeout sur la recherche des ressources actuellement consommées**
#59 - created 2 months ago by Nathan STCHEPINSKY
API bug frontend proxmox 🔖 0
- Supprimer tous les disques cloud init liés à 0 VM**
#58 - created 2 months ago by Nathan STCHEPINSKY
bug proxmox 🔖 0
- Ajouter la possibilité de bloquer des comptes sur hosting**
#56 - created 2 months ago by Nathan STCHEPINSKY
API database feature frontend working on 👤 1 🔖 0 updated 2 months ago
- Certains IP de machines ne sont pas selectionnables dans l'ajout des entrées DNS**
#54 - created 3 months ago by Nathan STCHEPINSKY 🔖 0
- Après le changement de creds, la pop up est réouverte avec la clé publique à la place de tous les champs**
#53 - created 3 months ago by Nathan STCHEPINSKY
bug frontend 🔖 0

