Contexte

Booktic

Révision 0
04/12/25
Nombre de Pages :9

Antoine Pontier 2025

Introduction et Sommaire

Ce document est un compte rendu mis à jour du contexte, il concentre plusieurs autres compte rendu

Le contexte est un environnement de travail et un environnement de formation, il représente une entreprise fictive nommée Booktic qui est une boutique en ligne de livre. L'objectif est de mettre en place toutes les infrastructures nécessaire au fonctionnement de cette société fictive

Sommaire

1. Infrastructure

Cette catégorie documente les infrastructures utilisées pour équiper le contexte

1.1 Machines

Booktic doit s'équiper d'un réseau fonctionnel et compétent, le contexte doit répondre à un besoin d'équiper une société de tailles moyenne hébergeant des services Web.

Modèle	Quantité	Type	Utilisation
Cisco 2801	2	Routeur	Permettre interconnexion entre des VLAN
Cisco Catalyst 2960	1	Switch	
Aruba J9780A	1	Switch	
HP Z240	2	Workstation	Virtualiser des machines et services

Ce matériel est un peux obsolète, les Cisco datent d'avant 2010 et sont potentiellement concerné par des failles de sécurités mais ils sont parfaitement fonctionnel et convienne à notre utilisation

Les Workstations HP Z240 sont des ordinateurs qui serviront à héverger des machines virtuelles (voir chapitre 2.1)

1.2 Réseaux et VLAN

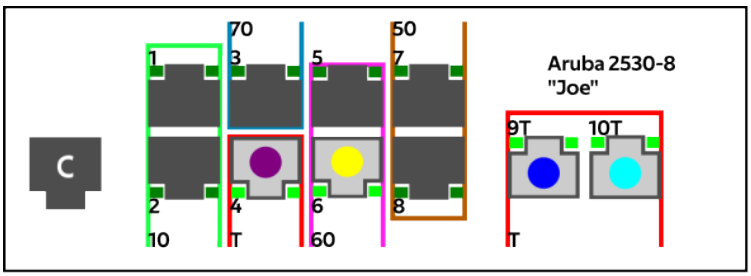
Il est recommandé d'isoler les différentes utilisation du réseau pour maintenir un niveau de sécurité et de cloisonnement, Le choix es été fait d'utiliser des VLAN pour économiser du matériel

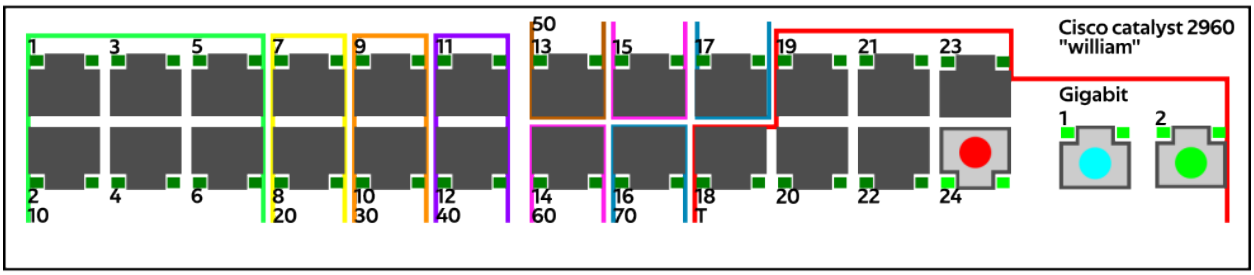
Réseau	VLAN
172.17.1.0/24	10 DATA
172.17.10.0/24	20 Users
172.18.0.240/28	30 Admin
172.18.0.0/27	40 DMZ
172.19.0.0/24	50 Wifi
?	60 Wan
10.0.0.0/24	70 ToIP

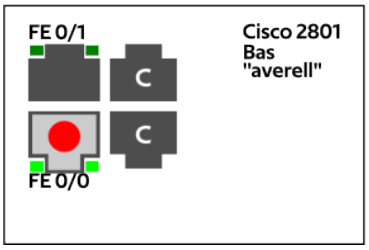
L'adressage du réseau WAN dépend du FAI (Fournisseur d'accès à internet)

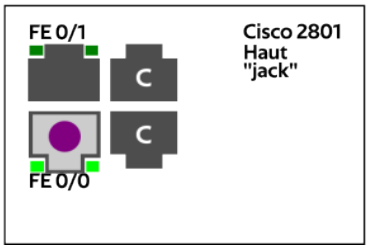
1.3 Câblage

Le contexte est composé de plusieurs équipements









Les VLAN sont indiqué par les zones de couleurs

Couleur	Extrémité 1	Extrémité 2
Rouge	Cisco 2801 FE0/0 Bas	Catalyst 2960 port 24
Bleu ciel	Catalyst 2960 Giga 1	Aruba port 10T
Bleu fonçé	Aruba port 9T	Station Z240 Axel
Vert clair	Catalyst 2960 Giga 2	Station Z240 Antoine
Violet	Cisco 2801 FE0/0 Haut	Aruba port 4
Jaune	Aruba port 5	FAI

Les tags et les câbles sont regroupé par couleurs. Les ports indiqué avec C dessus sont les ports consoles.

2. Virtualisation

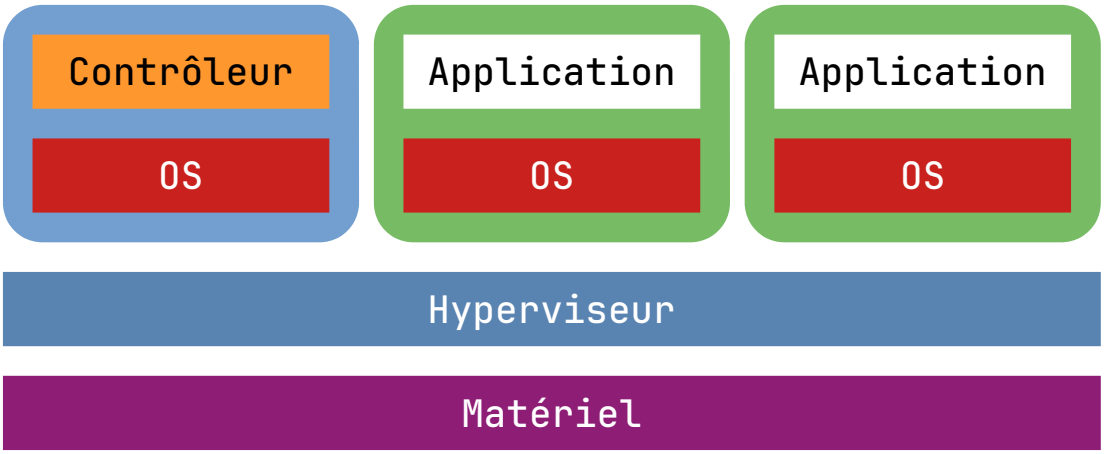
La virtualisation est une technologie qui permet la création de machines virtuelles. De pars leur nature virtuelle, les machines virtuelles peuvent être clonée et déployée rapidement et économiquement, il apportent aussi un niveau de sécurité et redondance plus grande qu'une machine classique

Elles sont le choix idéal pour pouvoir héberger un grand nombre de petit serveurs

2.1 Serveur

Les Serveurs de virtualisation sont des workstation Z240 de chez HP avec Windows serveur 2019 avec le service Hyper-V d'installé.

Hyper-V est un hyperviseur créé par Microsoft, il est fourni avec Windows Serveur et les éditions Windows Pro et permet de générer sous Windows des machines virtuelles avec une infrastructure plus ou moins complexe. Malheureusement, il n'est plus supporté par Microsoft et ses mises à jour prendront fin en même temps que Windows serveur 2022



Hyper-V est un hyperviseur de type 1, c'est à dire qu'il ne s'exécute pas par dessus un OS mais directement à la couche matérielle ce qui offre beaucoup plus de performance

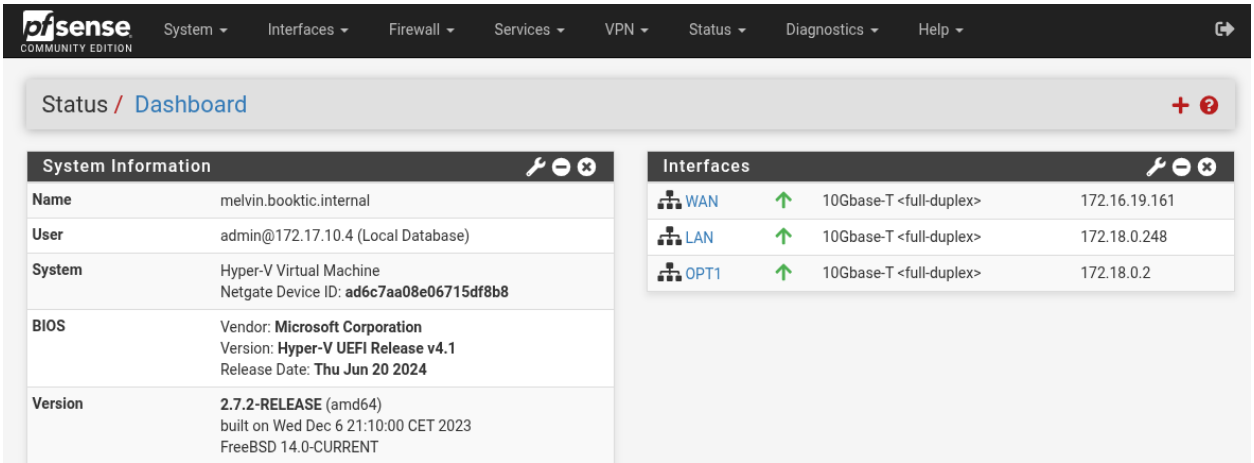
Le problème d'Hyper-V est que vu qu'il s'exécute à la couche matériel, il virtualise le système « hôte » à coté des autres machines virtuelles ce qui cause des instabilité en cas de désynchronisation entre l'hyperviseur et son service de contrôle sur le système « hôte »

2.2 Machines

Ne seront cité dans cette catégorie que les machines virtualisée qui sont essentielles au bon fonctionnement du contexte

2.2.a Pare-feu

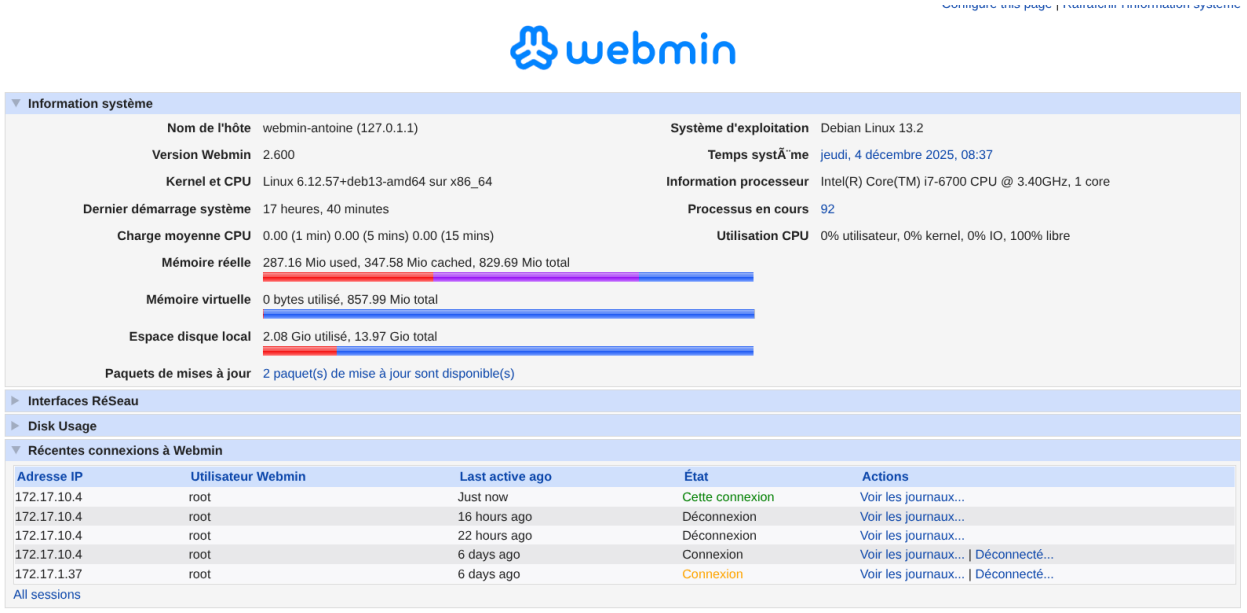
Pour remplir le rôle du pare-feu nous avons sélectionné le projet opensource Pfsense qui est une distribution Linux pour pare-feu avec de nombreuses fonctionnalités



Pfsense à néanmoins rencontré des problèmes de stabilité à cause de différents problème comme celui du protocole CARP cité au chapitre 3.2

2.2.b DHCP + DNS

Le DHCP et DNS sont hébergé sur une machine Debian 13 avec le service d'administration Webmin d'installé



Webmin est une interface web qui permet d'effectuer de nombreuses tâches avec une interface graphique au lieu d'un terminal, cet outil est déployable assez rapidement via le script

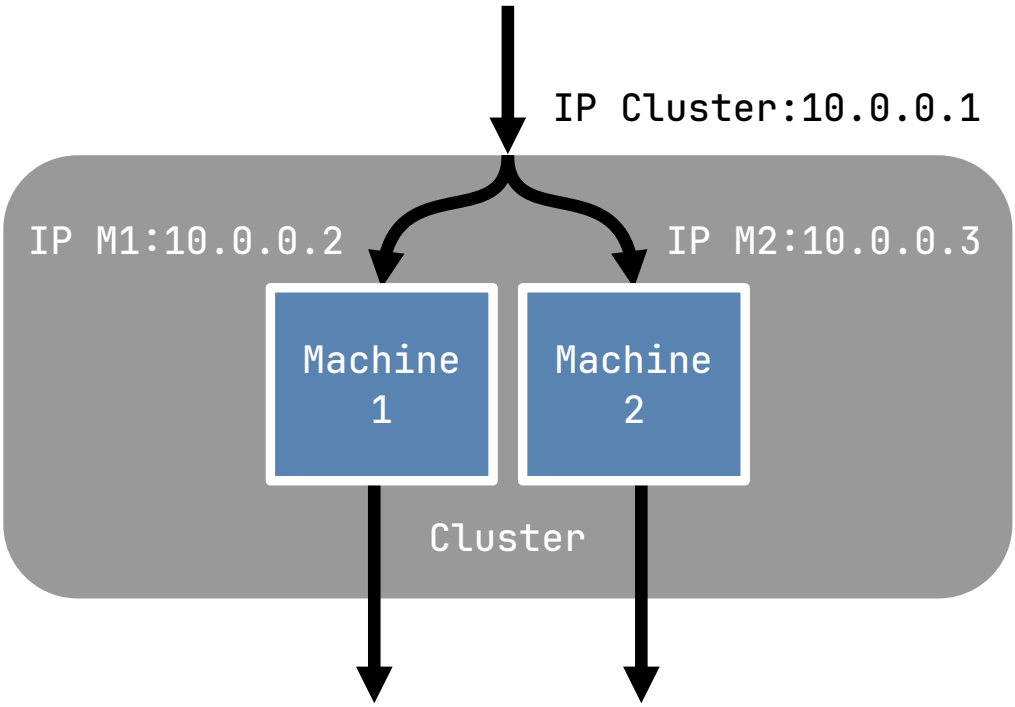
d’installation

```
curl -o webmin-setup-repo.sh \
https://raw.githubusercontent.com/webmin/webmin/master/webmin-setup-repo.sh
sudo sh webmin-setup-repo.sh
sudo apt-get install webmin
```

Le service DHCP est assuré par le serveur ISC DHCPd, le DNS est le serveur BIND9. Tout les deux sont intégré à Webmin

3. Clusters

Pour assurer un niveau de redondance suffisant pour réduire au maximum les temps de panne il faut mettre en place des clusters.



Un cluster est un regroupement de plusieurs machines en un groupe qui crée une identités fictive

3.1 HSRP

Host Standby Router Protocol (HSRP) est un protocole inventé par Cisco pour pouvoir permettre la redondance entre Routeurs, il se configure très simplement en quelques lignes sur la configuration des interfaces

Router 1 (Averell) :

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.17.1.2 255.255.255.0
ip helper-address 172.17.1.24
standby 10 ip 172.17.1.1
standby 10 priority 100
```

Routeur 2 (Jack) :

```
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.17.1.3 255.255.255.0
ip helper-address 172.17.1.24
standby 10 ip 172.17.1.1
standby 10 priority 80
```

Après l’application de cette configuration le cluster aura comme IP le 172.17.1.1 et ce sera le Routeur 1 qui sera le primaire et le Routeur 2 prendra le relais en cas de problème

3.2 CARP

Le CARP est un autre protocole de cluster à la différence que celui-ci est opensource, c’est le protocole que nous avons utilisé pour assurer la redondance des pares-feu qui sont virtualisé sur nos deux serveurs respectifs.

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	172.18.0.243/28	CARP LAN	MASTER
WAN@2	172.16.19.162/24	CARP WAN	MASTER
OPT1@3	172.18.0.1/27	CARP DMZ	MASTER

Il se configure un peux moins facilement car il faut aussi mettre en place la synchronisation entre les deux pare-feu.

Le plus gros problème que nous avons eu à régler est que les clusters CARP usurpent techniquement une adresse MAC et le Protocole ARP car le cluster est virtuel mais il référence bien à une machine. Il c’est avéré qu’après de nombreuses tentatives nous avons découvert que Hyper-V interdisait les modification et usurpation d’adresses MAC ce qui bloquais complètement toute communication du CARP car il opère à la couche 2 du modèle OSI

Après plus d’investigation nous nous sommes rendu compte que Hyper-V effectue un grand nombre de modification et d’opération à la couche 2.