ADRAR FORMATION

Restructuration Réseau

MARAVAL Liam
04/10/2024

Ce document sera décomposé en plusieurs chapitres :

1.Contexte : Définition des besoins ainsi que le choix de solutions en réponse à la demande client.
2.Mise en place des configurations réseau : Partie technique des configurations réseaux.
3.Mise en place des serveurs : Partie technique des configurations systèmes.
4.Conclusion du projet

Table des matières

1. Contexte

1.1 Demandes du client

Le centre de formation de l'ADRAR fait appel à nos services afin de restructurer et sécuriser son réseau.

Voici la configuration de l'infrastructure actuellement :

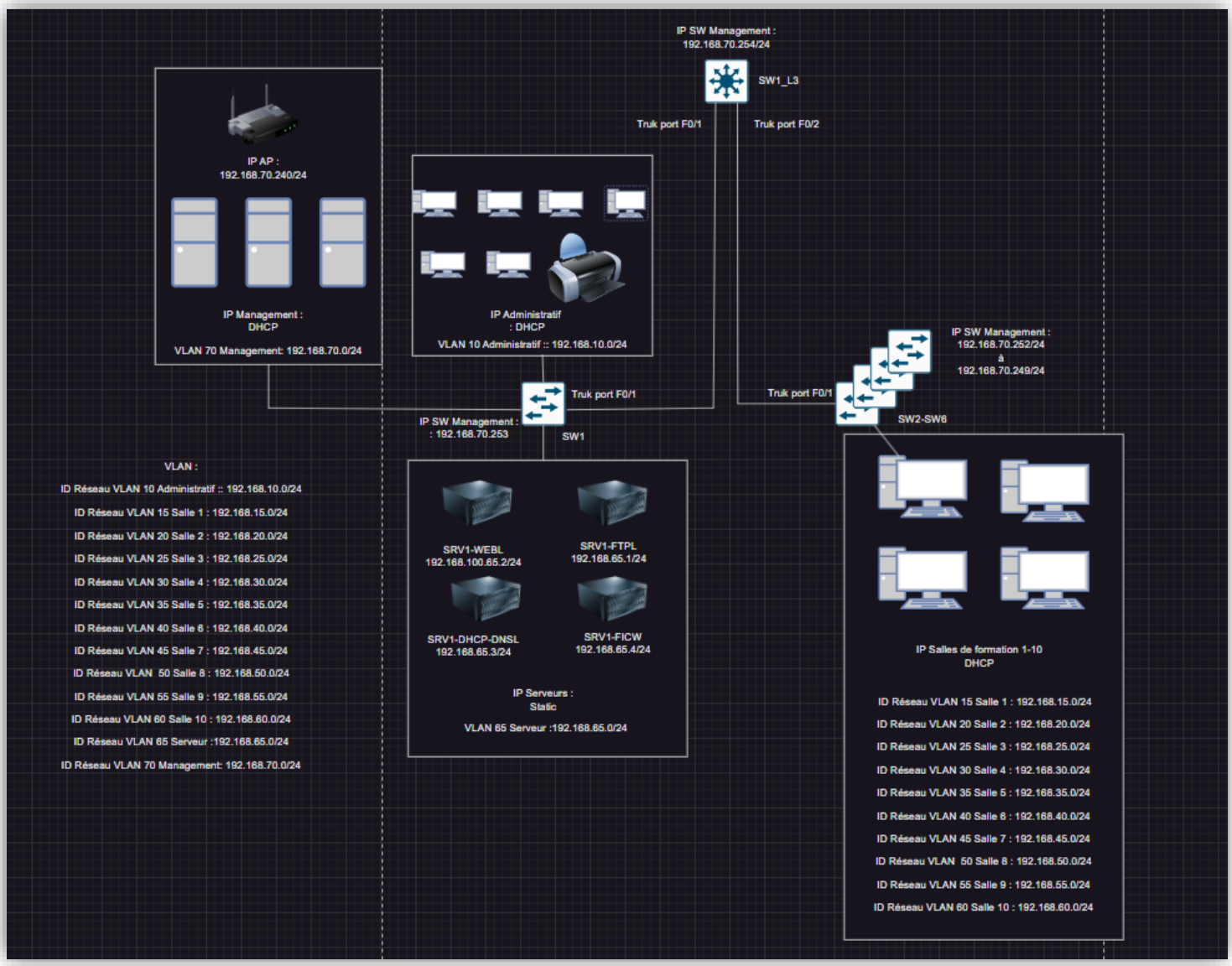
- Un sous réseau 192.168.100.0/24
- 10 salles de formations avec 20 postes clients
- Un service administratif avec 20 postes clients
- Un serveur comprenant tous les services réseaux

Voici les souhaits de l'ADRAR concernant l'évolution :

- Un sous-réseau réservé au personnel administratif, postes utilisateurs, administrateur IT, imprimantes ainsi qu'un point d'accès WIFI
- Un sous-réseau réservé aux serveurs
- Un sous-réseau pour chaque salle de formation (pour représenter les salles vous ferez un sous-réseau formation)
- Un serveur Windows, accessible uniquement à partir du sous-réseau administratif
- Un serveur Web (Linux) hébergeant 2 sites web, www.adrar.lan et www.adrar-form.lan accessible à TOUS
- Un serveur FTP (Linux) accessible uniquement depuis le post de l'administrateur IT du réseau administratif
- Les salles de formations ne peuvent pas accéder au sous-réseau du personnel administratif mais l'administrateur IT peut accéder aux postes des salles.

1.2 Evolution du réseau

Afin de mieux comprendre la mise en place de la nouvelle infrastructure réseau, veuillez-vous référer au nouveau schéma effectué (cf : Diagramme Réseau) :



Nous allons donc mettre en place plusieurs VLANs afin de segmenter et sécuriser le réseau par service/usage :

- Un VLAN « Administratif » qui compte 50 postes
- Un VLAN par salle de formation nommé « Salle-X » qui compte 20 postes chacun
- Un VLAN « Serveurs » qui compte 4 serveurs
- Un VLAN « Management » qui servira au administrateur du SI qui compte 2 postes
- Un VLAN « Natif » pour changer le VLAN par défaut

Nous avons rajouté un VLAN Management cela étant plus cohérent et sécurisé d'isoler l'administration des différents périphériques.

Ces besoins ont été calculés avec l'ADRAR en incluant de potentielles évolutions comme un nombre de périphériques plus important.

Nous avons choisi de mettre en place des VLANs en 192.168.X.0/24 pour les VLAN utilisateurs afin de faciliter la compréhension du réseau.
En ce qui concerne les VLAN « Serveurs » et « Management » ils seront en 192.168.X.0/28.
Le nombre de 254 hôtes par VLAN est amplement suffisant, même si des grosses évolutions arrivent à l'avenir chez l'ADRAR.
Le 3eme octets correspond à l'ID du VLAN afin de faciliter la lecture réseau.

Voici comment sont définis les plans d'adressage des VLANs :

ID Réseau VLAN 10 Administratif : 192.168.10.0/24
ID Réseau VLAN 15 Salle_1 : 192.168.15.0/24
ID Réseau VLAN 20 Salle_2 : 192.168.20.0/24
ID Réseau VLAN 25 Salle_3 : 192.168.25.0/24
ID Réseau VLAN 30 Salle_4 : 192.168.30.0/24
ID Réseau VLAN 35 Salle_5 : 192.168.35.0/24
ID Réseau VLAN 40 Salle_6 : 192.168.40.0/24
ID Réseau VLAN 45 Salle_7 : 192.168.45.0/24
ID Réseau VLAN 50 Salle_8 : 192.168.50.0/24
ID Réseau VLAN 55 Salle_9 : 192.168.55.0/24
ID Réseau VLAN 60 Salle_10 : 192.168.60.0/24
ID Réseau VLAN 65 Serveur :192.168.65.0/28
ID Réseau VLAN 70 Management : 192.168.70.0/28

Tous les VLANs seront clients DHCP sauf :

- Les 7 Switches ainsi que le point d'accès Wifi sur lesquels nous mettons une IP fixe dans le VLAN 70 afin de pouvoir les administrer
- Les serveurs qui seront en IP fixe pour assurer l'accès aux ressources clients

Pour effectuer le routage inter-VLAN nous avons mis en place un Switch L3 Core.
Cette solution a été choisie pour sa facilité d'administration, sa capacité évolutive et aussi pour sa scalabité.

Pour les Switches d'accès nous avons mis en place des Cisco Catalyst 2960L – 48ports.
En effet, ce modèle convient parfaitement pour les petits/moyens réseau, il dispose des fonctions de base comme la gestion des VLANs, ports POE, QOS tout en continuant de recevoir des mises à jour de sécurité, le tout à un prix abordable.

Concernant le Switch L3 Core nous avons choisi le modèle Cisco Catalyst 3560CX – 12 ports. Celui-ci a été choisi en 12 ports ce qui est amplement suffisant et permettra, si nécessaire, une extension simplifiée du réseau. Il assure les fonctions de base d'un Switch tout en effectuant du routage.

Le nommage des Switches a été effectué ainsi : SWX – « X » représentant le numéro du Switch, celui-ci étant à incrémenter à chaque nouvel équipement mis en place.

Pour le Switch de niveau 3 nous avons rajouté « –L3 », exemple : SW1-L3 = 1er switch de niveau 3 du réseau.

Voici un tableau récapitulatif de l'assignation des ports par Switch :

SW1 : 192.168.70.253/24

Mode	Port de début	Port de fin
TRUNK 10,15,65,70,99	FastEthernet 0/1	FastEthernet 0/1
Access VLAN 65	FastEthernet 0/2	FastEthernet 0/12
Access VLAN 10	FastEthernet 0/13	FastEthernet 0/39
Access VLAN 70	FastEthernet 0/40	FastEthernet 0/45
Trunk 10,15,70,99	FastEthernet 0/46	FastEthernet 0/46

SW2 : 192.168.70.252/24

Mode	Port de début	Port de fin
Trunk VLAN 15-60,70,99	FastEthernet 0/1	FastEthernet 0/1
Access VLAN 15	FastEthernet 0/2	FastEthernet 0/24
Access VLAN 20	FastEthernet 0/25	FastEthernet 0/47
Trunk VLAN 15-60,70,99	FastEthernet 0/48	FastEthernet 0/48

SW1-L3 : 192.168.70.254/24

Mode	Port de début	Port de fin
Trunk VLAN 10,15,65,70,99	FastEthernet 0/1	FastEthernet 0/1
Trunk VLAN 15-60,70,99	FastEthernet 0/2	FastEthernet 0/2

1.3 Sécurisation du réseau

Afin de renforcer la sécurité ainsi que de limiter les accès à certaines ressources sensibles, comme les serveurs, nous allons mettre en place des ACLs sur le SW1-L3 (cf Diragramme réseau).
Une fois les ACLs en place sur l'interface du VLAN, Cisco refuse automatiquement tous les flux, ainsi, toutes les règles présentes seront « permit ».

Celles-ci seront amenées à évoluer dans le temps mais il est préférable de fermer tous les accès et d'ouvrir les flux nécessaires aux besoins.
Voici un tableau récapitulatif par VLANs des autorisations actuelles :

Nom du VLAN	Source	Port Source	Destination	Port Destination
Vlan 10 Administratif	ID Réseau VLAN 10 :192.168.10.0/24	Any	ID Réseau VLAN 70 : 192.168.70.0/28	Retour ICMP : Echo-reply
Vlan 10 Administratif	ID Réseau VLAN 10 :192.168.10.0/24	Port client :gt 1024	Serveur Web : 192.168.65.2/32	Port Web : 443

Vlan 10 Administratif	ID Réseau VLAN 10 :192.168.10.0/24	Port client :gt 1024	Serveur DNS : 192.168.65.3/32	Port DNS : 53
Vlan 10 Administratif	ID Réseau : any	Port client DHCP : 68	ID réseau : Any	Port DHCP : 67
Vlan 10 Administratif	ID Réseau VLAN 10 :192.168.10.0/24	Port client :gt 1024	Serveur de fichier : 192.168.65.4/32	Port SMB : 445

Nom du VLAN	Source	Port Source	Destination	Port Destination
Vlan 15 Salle_1	ID Réseau VLAN 15 :192.168.15.0/24	Any	ID Réseau VLAN 70 : 192.168.70.0/28	Retour ICMP : Echo-reply
Vlan 15 Salle_1	ID Réseau VLAN 15 :192.168.15.0/24	Port client :gt 1024	Serveur Web : 192.168.65.2/32	Port Web : 443
Vlan 15 Salle_1	ID Réseau VLAN 15 :192.168.15.0/24	Port client :gt 1024	Serveur DNS : 192.168.65.3/32	Port DNS : 53
Vlan 15 Salle_1	ID Réseau : any	Port client DHCP : 68	ID réseau : Any	Port DHCP : 67

Nom du VLAN	Source	Port Source	Destination	Port Destination
Vlan 65 Serveurs	ID Réseau VLAN 65 :192.168.65.0/28	Any	ID Réseau VLAN 70 : 192.168.70.0/28	Retour ICMP : Echo-reply
Vlan 65 Serveurs	Serveur SFTP :192.168.65.1/32	Port SFTP Personnalisé : 4422	ID Réseau VLAN 70 : 192.168.70.0/28	Port client :gt 1024
Vlan 65 Serveurs	Serveur DHCP :192.168.65.3/32	Port serveur DHCP : 67	ID réseau all VLANs : 192.168.0.0/16	Port serveur DHCP : 67
Vlan 65 Serveurs	Serveur de Fichier :192.168.65.4/32	Port SMB : 445	ID Réseau VLAN 10 :192.168.10.0/24	Port client :gt 1024
Vlan 65 Serveurs	Serveur DNS :192.168.65.3/32	Port DNS : 53	ID réseau all VLANs : 192.168.0.0/16	Port client :gt 1024
Vlan 65 Serveurs	Serveur Web :192.168.65.2/32	Port Web : 443	ID réseau all VLANs : 192.168.0.0/16	Port client :gt 1024

Nom du VLAN	Source	Port Source	Destination	Port Destination
Vlan 70 Management	ID Réseau VLAN 70 :192.168.70.0/28	Any	ID réseau all VLANs : 192.168.0.0/16	ICMP : Echo
Vlan 70 Management	ID Réseau VLAN 70 :192.168.70.0/28	Port client :gt 1024	Serveur SFTP : 192.168.65.1/32	Port SFTP Personnalisé : 4422

Vlan 70 Management	ID Réseau : Any	Port client DHCP : 68	ID Réseau : Any	Port serveur DHCP : 67
Vlan 70 Management	ID Réseau VLAN 70 :192.168.70.0/28	Port client :gt 1024	Serveur DNS : 192.168.65.3/32	Port DNS : 53
Vlan 70 Management	ID Réseau VLAN 70 :192.168.70.0/28	Port client :gt 1024	Serveur Web : 192.168.65.2/32	Port Web : 443

Pour tout détails techniques concernant les ALCs merci de vous référer à la partie **2.3 Configuration du SW1-L3**

1.4 Configuration des serveurs

Comme demandé par l'ADRAR nous avons configuré plusieurs serveurs :

SRV1-FTPL	192.168.65.1/28	Debian 12	SFTP
SRV1-WEBL	192.168.65.2/28	Debian 12	Apache2 : www.adrar.lan et www.adrar-form.lan
SRV1-DHCP-DNSL	192.168.65.3/28	Debian 12	DHCP/DNS
SRV1-FICW	192.168.65.4/28	Windows Server 2019	Serveur de fichiers

Pour la stratégie de nommage nous avons choisi : SRV + numéro du serveur pour le services hébergé - nom du service + 1ere lettre de l'OS.
Ce qui donne par exemple **SRV1-FTPL** (1er serveur FTP en Linux)

Concernant le SRV1-FICW, l'ADRAR ne nous ayant pas précisé le besoin concernant le service hébergé par ce serveur, nous leur avons suggéré un serveur de fichier.
Ce rôle étant natif au OS Windows serveur, cela est cohérent d'avoir un espace de travail partagé pour le personnel administratif.
Nous avons mis en place des dossiers pour les 20 utilisateurs avec un quota de 50Go chacun ainsi qu'une sécurité NTFS adaptée.
Dans le cas de besoins supplémentaires, nous assurerons l'installation d'autres services ainsi que la sécurisation des flux nécessaires.

Pour l'OS des serveurs Linux nous avons choisi Debian 12.
Cet OS ,réputé pour sa stabilité, est très documenté ce qui facilitera les futures évolutions et l'administration au quotidien.
Le serveur de fichier est quant à lui en Windows serveur 2019 ce choix étant imposé par l'ADRAR.

Concernant le dimensionnement des VMs Linux nous avons choisi :

- RAM 8Go
- 1 CPU
- Stockage 50Go

Pour le serveur de fichier Windows :

- RAM 8Go
- 2 CPU
- Stockage 2TO

Ces dimensionnements ont été calculés approximativement au vu de la charge de travail et peuvent être revus en cas de sur/sous consommation.

2. Mise en place des configurations réseau

2.1 Configuration du SW1

Nous allons commencer par configurer les paramètres de base du switch, comme son nom, mot de passe, chiffrement, sécuriser les lignes VTY et port COM (les mots de passe n'apparaitront pas en clair dans ce document) :

```
enable
conf t
hostname SW1
ip domain-name adrar.local
username admin password *****
enable password *****
crypto key generate rsa
1024
service password-encryption
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
login local
transport input ssh
exit
line con 0
login local
end
```

Une fois cela fait nous allons déclarer nos VLANs et ajoutons l'IP sur le VLAN 70 pour administrer le switch mais également désactiver l'interface du VLAN par défaut :

```
conf t
interface vlan 1
shutdown
no ip address
exit
vlan 10
name Administratif
exit
vlan 15
name Salle_1
exit
vlan 65
name Serveurs
exit
vlan 70
name Management
vlan 99
name Natif
```

```
exit
interface vlan 70
ip address 192.168.70.253 255.255.255.240
exit
```

Maintenant, nous allons assigner nos ports à nos VLAN, effectuer le trunk avec le Switch Core ainsi qu'un autre trunk sur le port 47 pour notre point d'accès ainsi que déclarer notre VLAN Natif (Pour plus de détail sur le point d'accès se rendre au chapitre **2.4 Configuration du point d'accès Wifi**) :

```
interface fa0/1
switchport mode trunk
switchport trunk allow vlan 10,15,65,70,99
switchport trunk native vlan 99
exit
interface range fa0/13-39
switchport mode access
switchport access vlan 10
exit
interface range fa0/40-45
switchport mode access
switchport access vlan 70
exit
interface range fa0/2-12
switchport mode access
switchport access vlan 65
exit
interface fa0/46
switchport mode trunk
switchport trunk allow vlan 10,15,70,99
switchport trunk native vlan 99
exit
```

2.2 Configuration du SW2-6

Sur les SW2 à SW6 nous allons reprendre les mêmes paramétrages de base que dans le SW1.

Dans cet exemple nous ne montrerons que la configuration du SW2 et ne déclarerons que le VLAN 15 Salle_1, les étapes étant identiques pour les autres Switches et VLANs.

Une fois les configurations de base appliquées, nous déclarons les VLANs nécessaires et ajoutons l'IP sur le VLAN 70.

```
enable
conf t
vlan 15
name Salle_1
exit
interface vlan 70
ip address 192.168.70.252 255.255.255.240
```

Une fois cela fait, nous assignons les interfaces et effectuons les trunks :

```
interface fa0/1
switchport mode trunk
switchport trunk allow vlan 15,20,25,30,35,40,45,50,55,60,70,99
switchport trunk native vlan 99
exit
interface range fa0/2-24
switchport mode access
switchport access vlan 15
```

```
exit
interface range fa0/25-47
switchport access vlan 20
exit
interface fa0/48
switchport mode trunk
switchport trunk allow vlan 15,20,25,30,35,40,45,50,55,60,70,99
switchport trunk native vlan 99
```

2.3 Configuration du SW1-L3

Comme pour les Switches précédents nous effectuons les configurations de base.

Nous lui déclarons maintenant les VLANs (Comme ci-dessus, nous gardons uniquement le VLAN 15 Salle_1 pour les salles de formation) :

```
vlan 10
name Administratif
exit
vlan 15
name Salle_1
vlan 65
name Serveurs
exit
vlan 70
name Management
vlan 99
name Natif
exit
```

Nous associons les IP aux VLANs qui serviront au routage ainsi que le Relay DHCP pour nos clients DHCP :

```
interface vlan 10
ip address 192.168.10.254 255.255.255.0
ip helper-address 192.168.65.3
exit
interface vlan 15
ip address 192.168.15.254 255.255.255.0
ip helper-address 192.168.65.3
exit
interface vlan 65
ip address 192.168.65.254 255.255.255.240
ip helper-address 192.168.65.3
exit
interface vlan 70
ip address 192.168.70.254 255.255.255.240
ip helper-address 192.168.65.3
```

Nous effectuons les trunks et activons le routage :

```
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allow vlan 10,15,65,70,99
switchport trunk native vlan 99
interface fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
switchport trunk allow vlan 15,20,25,30,35,40,45,50,55,60,70,99
switchport trunk native vlan 99
exit
ip routing
end
```

Nous allons ajouter les ACLs définies dans la partie **1.3 Sécurisation du réseau** de ce document, pour plus de détails merci de vous référer à ce chapitre :

```
ip access-list extended VLAN10
permit icmp 192.168.10.0 0.0.0.255 192.168.70.0 0.0.0.15 echo-reply
permit tcp 192.168.10.0 0.0.0.255 gt 1024 host 192.168.65.2 eq 443
permit udp 192.168.10.0 0.0.0.255 gt 1024 host 192.168.65.3 eq domain
permit UDP any eq 68 any eq 67
permit tcp 192.168.10.0 0.0.0.255 gt 1024 host 192.168.65.4 eq 445
exit
ip access-list extended VLAN15
permit icmp 192.168.15.0 0.0.0.255 192.168.70.0 0.0.0.15 echo-reply
permit tcp 192.168.15.0 0.0.0.255 gt 1024 host 192.168.65.2 eq 443
permit udp 192.168.15.0 0.0.0.255 gt 1024 host 192.168.65.3 eq domain
permit UDP any eq 68 any eq 67
exit
ip access-list extended VLAN65
permit icmp 192.168.65.0 0.0.0.255 192.168.70.0 0.0.0.15 echo-reply
permit tcp host 192.168.65.1 eq 4422 192.168.70.0 0.0.0.15 gt 1024
permit UDP host 192.168.65.3 eq 67 192.168.0.0 0.0.255.255 eq 67
permit tcp host 192.168.65.4 eq 445 192.168.10.0 0.0.0.255 gt 1024
permit udp host 192.168.65.3 eq domain 192.168.0.0 0.0.255.255 gt 1024
permit tcp host 192.168.65.2 eq 443 192.168.0.0 0.0.255.255 gt 1024
exit
ip access-list extended VLAN70
permit icmp 192.168.70.0 0.0.0.255 192.168.0.0 0.0.255.255 echo
permit tcp 192.168.70.0 0.0.0.255 gt 1024 host 192.168.65.1 eq 4422
permit UDP any eq 68 any eq 67
permit udp 192.168.70.0 0.0.0.255 gt 1024 host 192.168.65.3 eq domain
permit tcp 192.168.70.0 0.0.0.255 gt 1024 host 192.168.65.2 eq 443
```

Nous assignons maintenant les ACLs aux différents VLANs :

```
interface vlan 10
ip access-group VLAN10 in
exit
interface vlan 15
ip access-group VLAN15 in
exit
interface vlan 65
ip access-group VLAN65 in
exit
interface vlan 70
ip access-group VLAN70 in
exit
```

2.4 Configuration du point d'accès Wifi

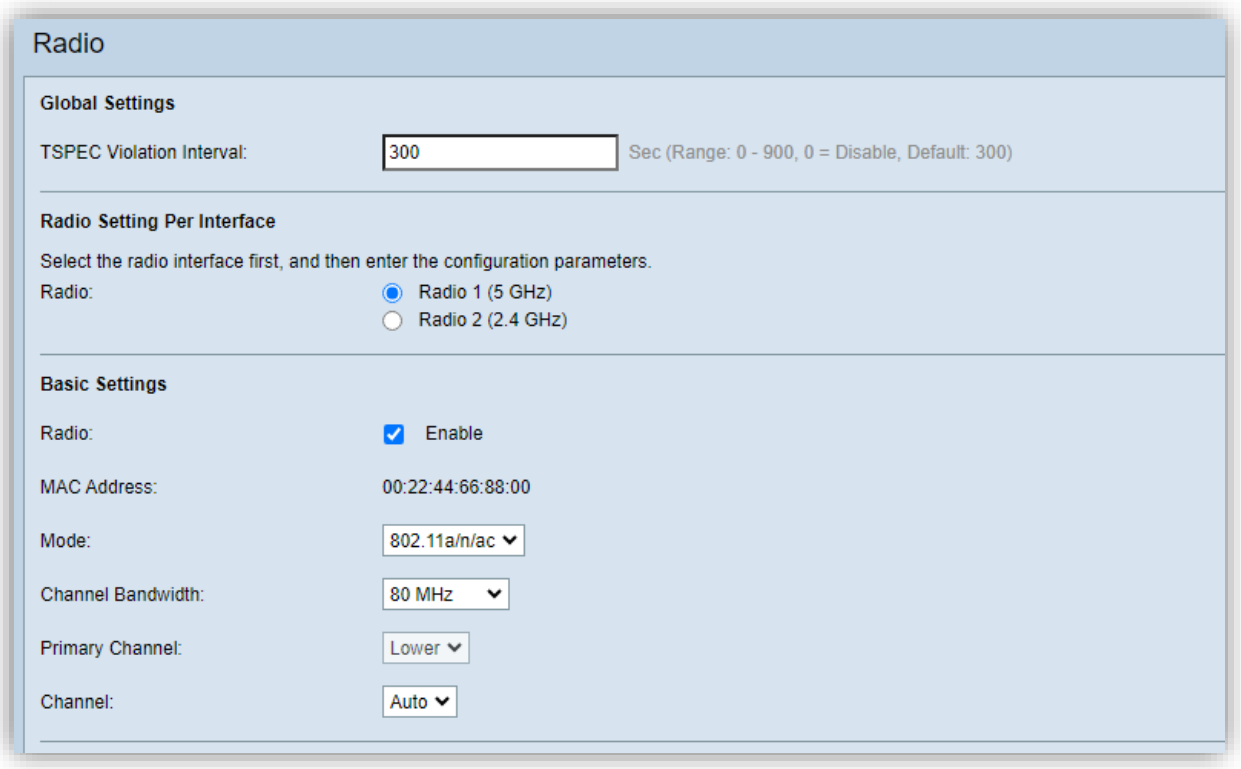
Nous allons mettre en place un point d'accès Wifi appartenant au VLAN 70 de Management, qui diffusera deux SSID dans deux VLANs différents :

- Wifi_Administratif : pour le Vlan 10 Administratif
- Wifi_Salle1 : pour le Vlan 15 Salle_1

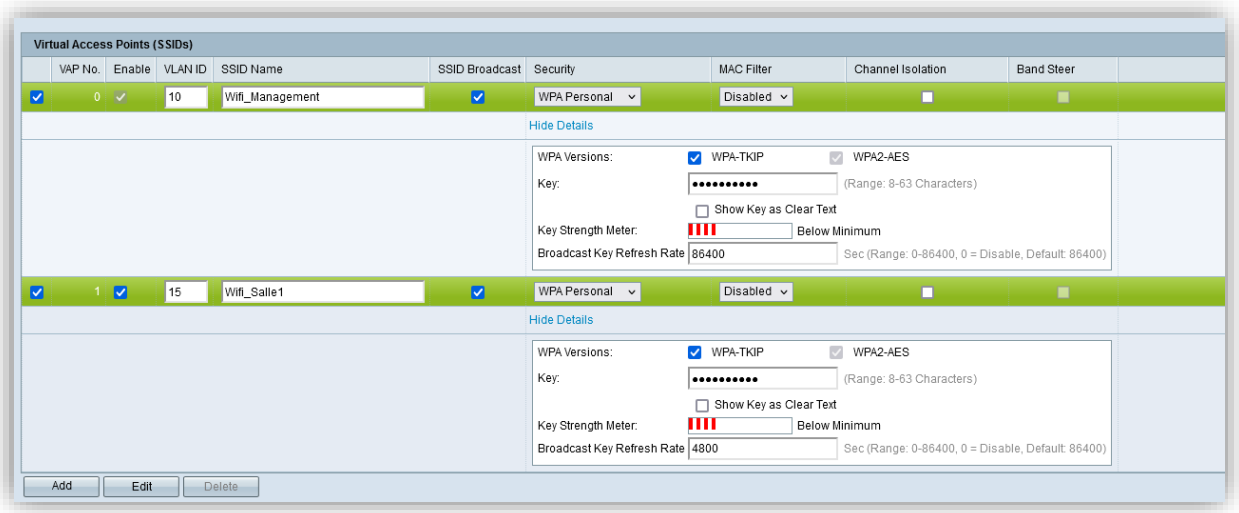
Nous commençons par nous connecter sur le point d'accès via son IP par défaut qui est 192.168.1.245/24.

Une fois sur la GUI nous configurons les paramètres de base, changeons de mot de passe d'administration et le nom du point d'accès.

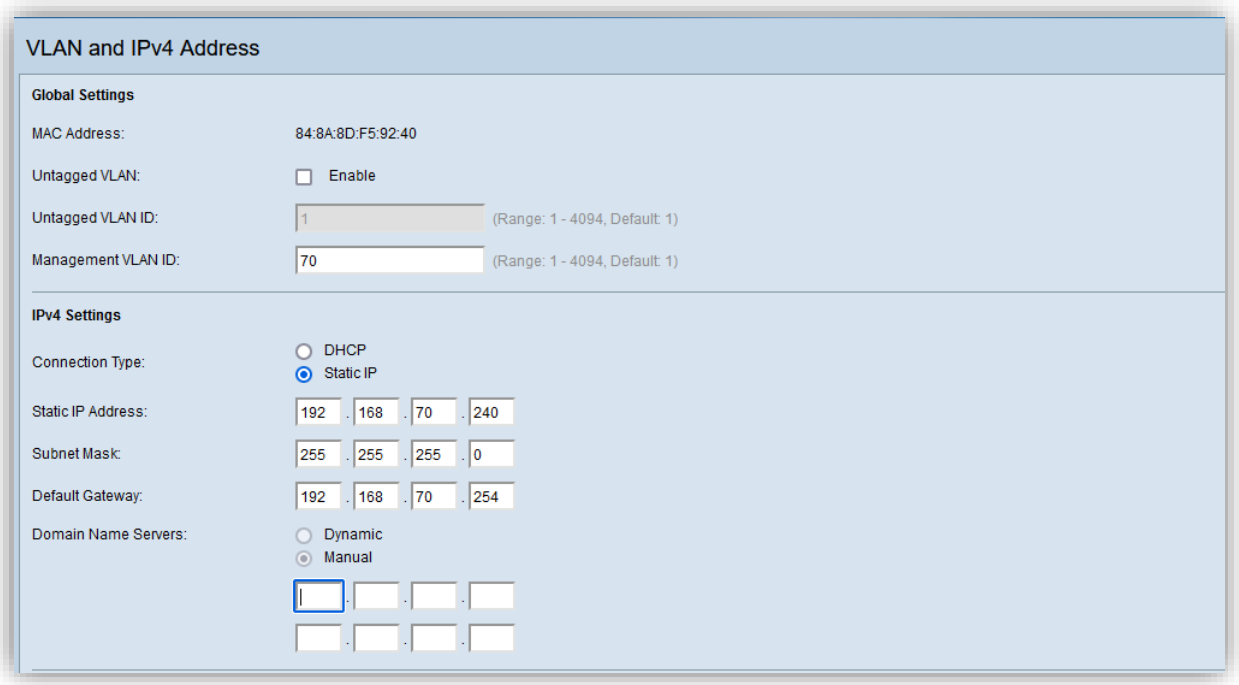
Nous allons activer le paramètre **« Radio »** pour que le point d'accès puisse diffuser ses SSID :



Nous pouvons maintenant configurer nos deux SSID avec les ID VLANs correspondants ainsi qu'une clé de sécurité WPA Personnal, ne disposant pas de serveur Radius pour le WPA Enterprise :



Nous lui assignons son IP en décochant la case « Untagged VLAN » pour que les trames soient tagguées et ainsi permettre la communication des différents VLANs par Wifi :



Nous avons effectués les tests nécessaires au bon fonctionnement du Wifi pour nos deux SSID.

3. Mise en place des serveurs

Pour toutes informations concernant l'IP, le nom du serveur, l'OS ou le service hébergé sur le serveur merci de vous référer au chapitre **1.4 Configuration des serveurs** de ce document.

3.1 Configuration du serveur DNS

Pour notre serveur DNS nous avons fait le choix d'installer Bind9 pour plusieurs raisons :

- Sa stabilité
- Ses performances qui permettent de gérer de grandes quantités de requêtes
- Ses mises à jours régulières
- Son évolutivité car adapté au besoin de petites comme de grandes entreprises
- Sa documentation très complète étant l'un des services DNS les plus utilisés

Nous allons configurer notre serveur DNS avec les zones suivantes :

adrar.local
zone inversée adrar.local
adrar.lan (Site WEB)
adrar-form.lan (Site WEB)

Nous commençons par installer le service DNS et sauvegarder les fichiers de configuration de base :

```
apt install bind9
cd /etc/bind
cp named.conf.options named.conf.options.sav
cp named.conf.local named.conf.local.sav
```

Nous éditons le fichier de configuration « **named.conf.options »** et renseignons les redirecteurs **:**

```
nano /etc/bind/named.conf.options
```

```
forwarders {
                1.1.1.1;
                 8.8.8.8;
        };
```

Nous allons copier le fichier de configuration de zone, le renommer et ensuite enregistrer nos entrées DNS :

```
cp db.empty db.adrar.local
```

```
;
; Zone file for adrar.local
;
; The full zone file
;
$TTL 3D
@       IN      SOA     srv1-dhcp-dnsl.adrar.local. root.adrar.local. (
                        202410011       ; serial, todays date + todays
serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds
;
@       IN      NS      srv1-dhcp-dnsl@adrar.local.
srv1-ftpl.      IN      A       192.168.65.1
srv1-webl.      IN      A       192.168.65.2
srv1-dhcp-dnsl. IN      A       192.168.65.3
srv1-ficw.      IN      A       192.168.65.4
```

Concernant les paramètres :

- $TTL : Durée de vie des enregistrements DNS
- SOA : Serveur qui fait autorité sur la zone
- Serial : Version du fichier
- Refresh : Taux de rafraîchissement pour la synchronisation des fichiers de configuration entre serveur DNS
- Retry : Délai d'attente apres un **« resfresh »** échoué
- Expire : Délai d'expiration de la zone en cas d'échec de résolution de la zone
- Minimun : Durée de mis en cache minimum pour les réponses négatives du serveur DNS

Nous effectuons les mêmes opérations pour la zone inversée « **db.inverse.adrar.local** » :

```
;
; Zone file for reverse adrar.local
;
; The full zone file
;
$TTL 3D
@       IN      SOA     adrar.local. root.adrar.local. (
                        200608081       ; serial, todays date + todays
serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; minimum, seconds
;
@       IN      NS      srv1-dhcp-dnsl@adrar.local.
1       IN      PTR     srv1-ftpl.
2       IN      PTR     srv1-webl.
3       IN      A       srv1-dhcp-dnsl.
4       IN      A       srv1-ficw.
```

Nous allons éditer le fichier « **named.conf.local »** pour déclarer nos fichiers de zones directe et indirecte :

```
zone "adrar.local" {
    type master;
    file "/etc/bind/db.adrar.local";
};
zone "65.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.inverse.adrar.local";
};
zone "adrar.lan" {
    type master;
    file "/etc/bind/db.adrar.lan";
};
zone "adrar-form.lan" {
    type master;
    file "/etc/bind/db.adrar-form.lan";
};
```

Une fois cela fait nous effectuons les tests de résolution directe et inversée :

```
liam@SRV1-DHCP-DNSL:~$ nslookup srv1-webl.adrar.local
Server:         192.168.65.3
Address:        192.168.65.3#53

Name:   SRV1-WEBL.adrar.local
Address: 192.168.65.2

liam@SRV1-DHCP-DNSL:~$ nslookup 192.168.65.1
1.65.168.192.in-addr.arpa       name = SRV1-FTPL.adrar.local.
```

Tout est fonctionnel.

Nous allons donc appliquer les mêmes configurations pour les zones des sites web ww.adrar.lan et www.adrar-form.lan

3.2 Configuration du service DHCP :

Nous allons créer 4 étendues au total sur notre serveur DHCP une pour chaque VLANs ce qui donnera :

ID Réseau	1er IP	Derniere IP	Gateway	DNS
192.168.65.0/28	192.168.65.10	192.168.65.13	192.168.65.14	192.168.65.3
192.168.10.0/24	192.168.10.1	192.168.10.100	192.168.10.254	192.168.65.3
192.168.15.0/24	192.168.15.1	192.168.15.100	192.168.15.254	192.168.65.3
192.168.70.0/28	192.168.70.10	192.168.70.13	192.168.70.14	192.168.65.3

En ce qui concerne les VLANs 10,15,70, nous avons choisi de prendre des pools assez larges afin d'anticiper de futurs évolutions au sein de l'ADRAR comme un nombre de périphériques augmentant (Tablettes, PC, Smartphone, Imprimantes ect …)

Nous commençons par installer le package DHCP sur notre serveur :

```
apt install isc-dhcp-server
```

Nous assignons la carte Ethernet à nos pool DHCP IPV4 :

```
nano /etc/default/isc-dhcp-server
```

```
DHCPDv4_CONF=ens33
```

Nous allons configurer le 1er pool pour le réseau 192.168.65.0/24 :

```
nano /etc/dhcp/dhcpd.conf
```

```
#Options DNS
option domain-name « adrar.local »;
option domain-name-servers 192.168.65.3;
default-lease-time 600;
max-lease-time 7200;


#Pool DHCP VLAN 65 Serveurs
Subnet 192.168.65.0 netmask 255.255.255.240 {
        Option routers 192.168.65.14 ;
        Range 192.168.65.10 192.168.65.13 ;
}
```

Une fois cela fait nous pouvons redémarrer le service et faire nos tests via un poste client :

```
Systemctl restart isc-dhcp-server
```

```
root@SRV1-DHCPL:~# systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - LSB: DHCP server
     Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
     Active: active (running) since Sat 2024-09-21 16:42:39 CEST; 5min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 2279 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, sta>
      Tasks: 4 (limit: 2264)
     Memory: 4.8M
        CPU: 28ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─2295 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens33
```

```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : adrar.local
   Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Adresse physique . . . . . . . . . . . : 00-0C-29-B3-B3-26
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::8c40:9d80:ef0f:3c36%4(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.65.11(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Bail obtenu. . . . . . . . . . . . . . : dimanche 22 décembre 2024 12:21:57
   Bail expirant. . . . . . . . . . . . . : lundi 30 décembre 2024 12:21:56
   Passerelle par défaut. . . . . . . . . : 192.168.65.14
   Serveur DHCP . . . . . . . . . . . . . : 192.168.65.3
   IAID DHCPv6 . . . . . . . . . . . : 100666409
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-D2-99-87-00-0C-29-B3-B3-26
   Serveurs DNS. . .  . . . . . . . . . : ::1
                                 192.168.65.3
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Le poste client a bien son bail DHCP avec toutes les options indiquées.

Nous appliquons les mêmes configurations pour les autres pools :

```
#Pool DHCP VLAN 65 Serveurs
Subnet 192.168.65.0 netmask 255.255.255.240 {
        Option routers 192.168.65.14 ;
        Range 192.168.65.10 192.168.65.13 ;
}
#Pool DHCP VLAN 10 Administratif
Subnet 192.168.10.0 netmask 255.255.255.0 {
        Option routers 192.168.10.254 ;
        Range 192.168.10.1 192.168.10.100 ;
}
#Pool DHCP VLAN 15 Salle 1
Subnet 192.168.15.0 netmask 255.255.255.0 {
        Option routers 192.168.15.254 ;
        Range 192.168.15.1 192.168.15.100 ;
}
#Pool DHCP VLAN 70 Management
Subnet 192.168.70.0 netmask 255.255.255.240 {
        Option routers 192.168.70.14 ;
        Range 192.168.70.10 192.168.70.13 ;
}
```

3.3 Configuration du service Apache 2

Pour notre serveur Web nous avons fait le choix d'installer Apache2 pour plusieurs raisons :

- Celui-ci étant très utilisé il est très bien documenté
- Très flexible grâce à ces différents modules
- Réputé pour sa stabilité et sa fiabilité via des mises à jours régulières

Il permet notamment de créer plusieurs sites web accessibles sur une même IP et un même port, ce qui va nous intéresser dans notre cas.
En effet, en fonction de la requête envoyée, Apache sera capable de rediriger le trafic sur le bon site Web, hébergé sur ce que l'on appelle un « VirtualHost ».

Pour la mise en place du HTTPS, nous utiliserons des certificats auto signée mais cela n'est pas la bonne pratique, celle-ci doit être normalement faite pas une autorité de certification

Nous allons configurer 2 sites web sur notre serveur :

- www.adrar.lan
- www.adrar-form.lan

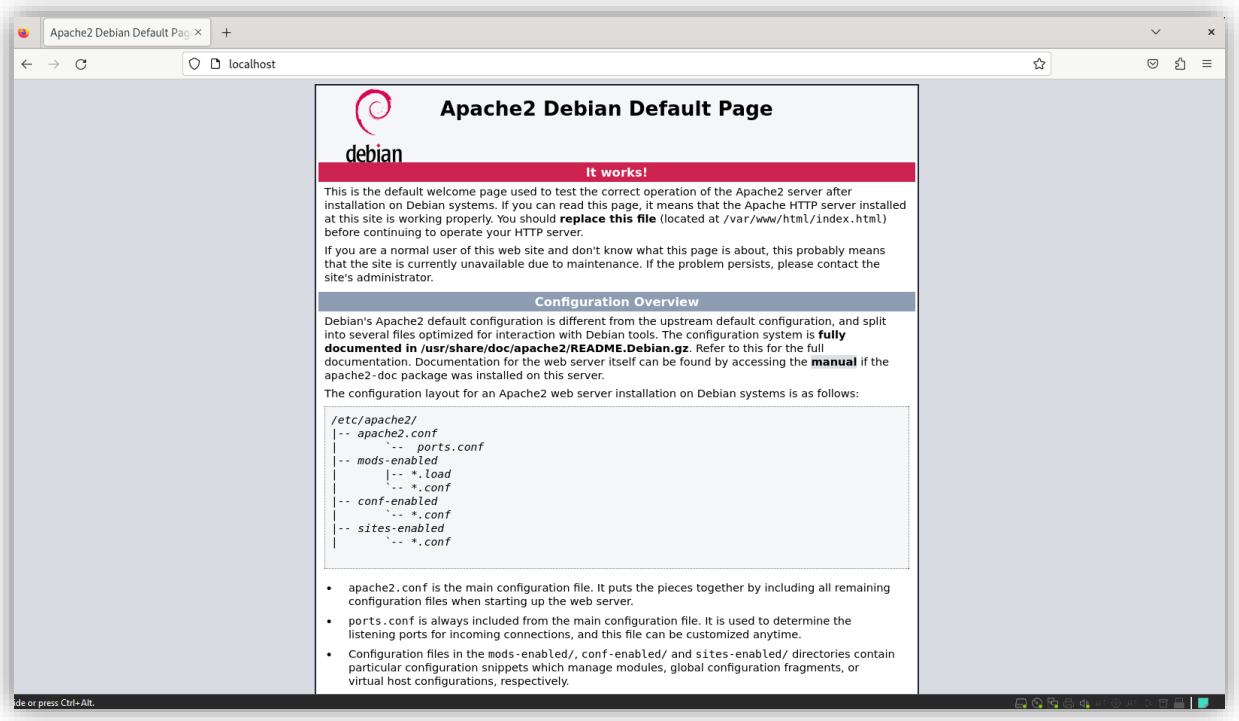
Nous installons le service **Apache2** ainsi que **opnssl** pour générer le certificat et démarrons le serveur :

```
apt install apache2
apt install openssl
systemctl start apache2
```

Nous vérifions maintenant le statut et testons la page web par défaut :

```
sudo systemctl status apache2
```

```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-09-21 09:17:55 CEST; 4min 50s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2995 (apache2)
      Tasks: 55 (limit: 2264)
     Memory: 10.6M
        CPU: 48ms
     CGroup: /system.slice/apache2.service
             ├─2995 /usr/sbin/apache2 -k start
             ├─2997 /usr/sbin/apache2 -k start
             └─2998 /usr/sbin/apache2 -k start
```



Nous allons maintenant créer les répertoires pour les certificats auto-signés ainsi que les clefs privées :

```
mkdir -p /ect/ssl/certs
mkdir -p /ect/ssl/private
```

Nous générons notre clé privée et créons le certificat basé sur la signature via cette clé :

```
openssl genrsa -out /etc/ssl/private/adrar.lan.key 2048
openssl req -new -x509 -key /etc/ssl/private/adrar.lan.key -out
/ect/ssl/certs/adrar.lan.crt -days 365
```

Nous allons créer le répertoire pour l'hôte virtuelle du site www.adrar.lan :

```
mkdir -p /var/www/adrar.lan
```

Nous pouvons maintenant créer le fichier de configuration et renseigner les différents champs pour ce site web :

```
nano /etc/apache2/sites-available/adrar.lan.conf
```

```
<VirtualHost *:443>
    ServerAdmin webmaster@adrar.lan
    ServerName adrar.lan
    ServerAlias www.adrar.lan
    DocumentRoot /var/www/adrar.lan/
    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/adrar.lan.crt
    SSLCertificateKeyFile /etc/ssl/private/adrar.lan.key
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
</VirtualHost>
```

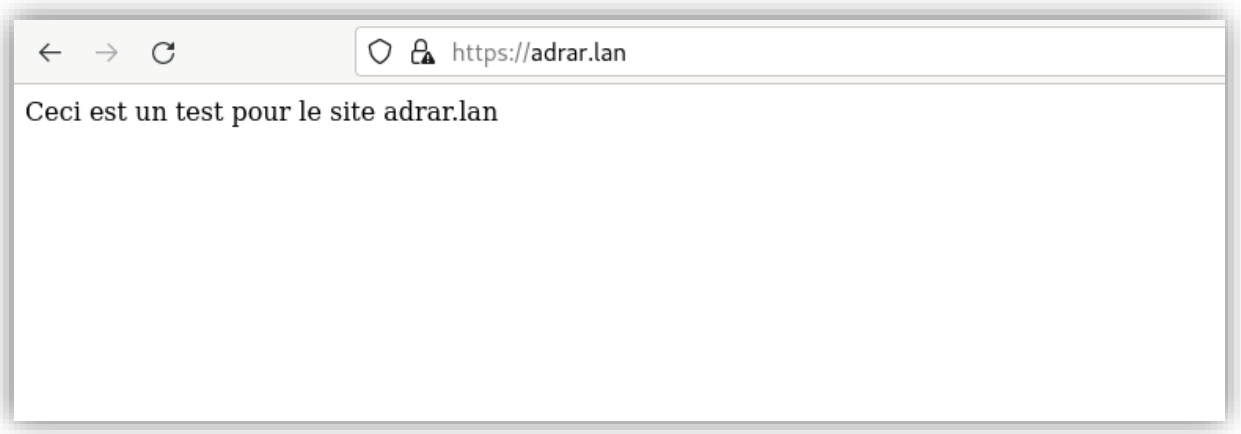
Nous pouvons désormais activer notre hôte virtuel, le module SSL et désactiver le site par défaut.

```
a2ensite adrar.lan
a2enmod ssl
a2dissite 000-default.conf
```

Nous créons le fichier index.html et renseignons le message de test **« Ceci est un test pour le site adrar.lan »** :

```
nano /var/www/adrar.lan/index.html
```

Apres redémarrage du service nous allons maintenant sur notre site web :



Le site est bien fonctionnel nous allons donc effectuer les mêmes opérations pour le site www.adrar-form.lan.

3.4 Configuration du serveur SFTP

Nous avons choisi de mettre en place du SFTP plutôt que FTP, celui-ci étant plus sécurisé notamment en assurant le chiffrement de données, des noms d'utilisateurs et mots de passe.

Pour des raisons de sécurité, nous avons modifié le port par défaut qui est le 22 pour un port personnalisé « **4422 »**

Nous allons créer un utilisateur **« Management »** pour se connecter ainsi qu'un groupe **« sftpuser »** sur lequel nous mettrons les règles de sécurité nécessaires.

Nous commençons par installer **opnssh-server** :

```
apt install openssh-server
```

Nous créons maintenant un groupe **« sftpusers »** et l'utilisateur nommé **« Management »**, appartenant à ce groupe, et lui assignons un mot de passe :

```
groupadd sftpusers
useradd -G sftpusers Management
passwd Management
```

Nous allons créer le répertoire racine du serveur SFTP ainsi qu'un sous répertoire **« Management »**. Il appartiendra à l'utilisateur du même nom afin d'avoir les permissions de lecture et écriture (le répertoire chroot ne devant pas être accessible en écriture pour des raisons de sécurité) :

```
mkdir /srv/sftp
mkir /srv/sftp/Management
chown Mangement:sftpusers /srv/sftp/Management/
```

Une fois cela fait, nous éditons le fichier **« sshd_config »** pour **:**

- Décommenter la ligne **« PasswordAuthentification yes »**
- Ajouter en fin de fichier les règles de connexions des utilisateurs du groupe « **sftpusers** » :
- Modifier le port par défaut pour mettre le **4422**

```
nano /etc/ssh/sshd_config
```

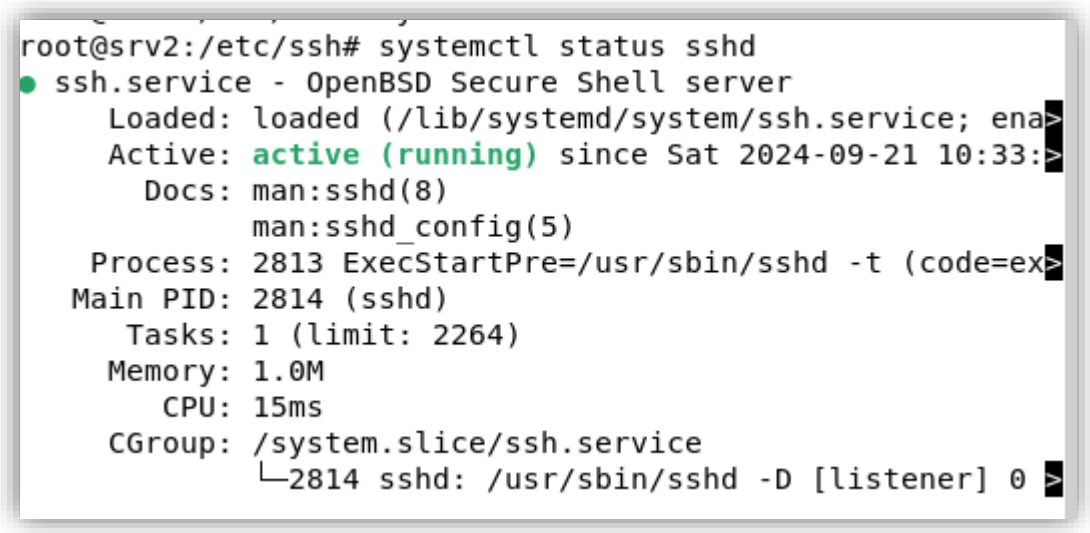
```
PasswordAuthentication yes
Port 4422
Match Group sftpusers
    X11Forwarding no
    AllowTcpForwarding no
    ChrootDirectory /srv/sftp
    ForceCommand internal-sftp
```

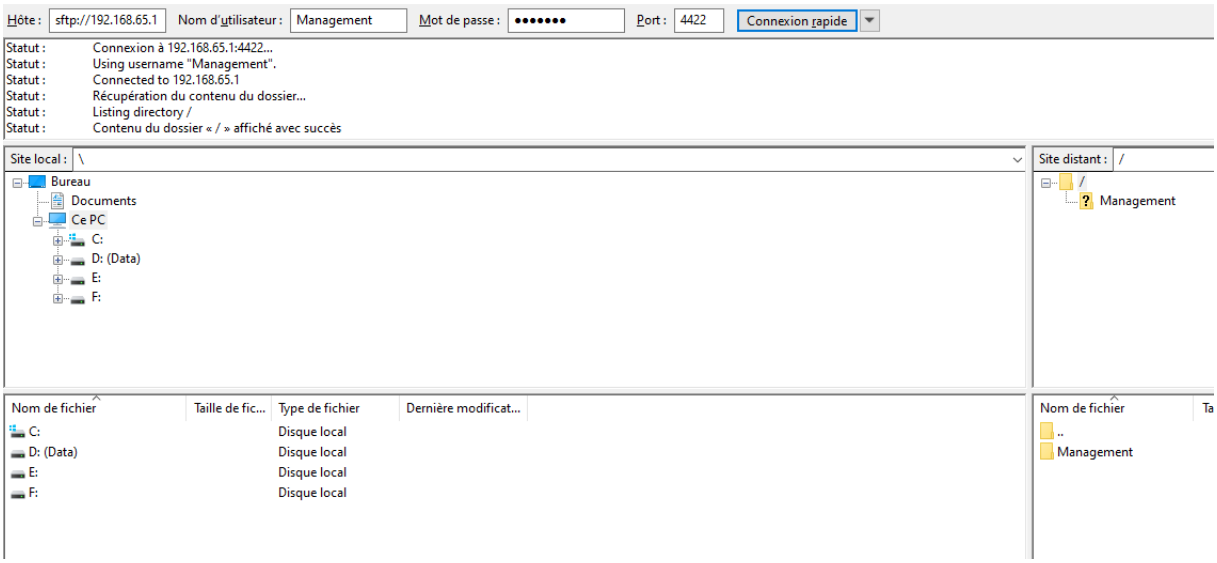
Ces règles permettent :

- AllowTcpForwarding no : Empêche de rediriger des connexions TCP de la machine locale via le serveur SSH
- ChrootDirectory /srv/sftp : Indique que les utilisateurs ne pourront accéder qu'à ce répertoire et sous répertoire via les connexions SSH
- ForceCommand internal-sftp : Cette règle force les utilisateurs du groupe à utiliser uniquement des commandes SFTP et non SSH

Nous allons redémarrer le service et effectuer nos tests via un client Filezilla :

```
systemctl restart sshd
systemctl status sshd
```





4. Conclusion du projet

Suite à ce projet, nous avons effectué une refonte complète de l'infrastructure adaptée au besoin de l'ADRAR.
Les choix du matériel ainsi que leurs configurations ont été pensés pour pouvoir évoluer facilement dans le temps.
Concernant la sécurisation des accès, nous avons mis en place une politique de sécurité affinée mais celle-ci peut être évidemment adaptée au besoin pour les évolutions futures.