Note externe

Dir2S – Informatique et Télécoms
Département Production
Agence Exploitation Télécoms
Ratton Jordan

Projet Fortification

Identification : Présentation-Fortification

Version : 1

Nb. de pages : 14

Résumé / Avertissement
Ce document a pour but de présenter le Projet Fortification

Document(s) associé(s) et annexe(s) :

Version	Date d'application	Nature de la modification	Annule et remplace
V1	13/06/2025	Version Initiale	

Accessibilité

☑ Libre ☐ Interne ☐ Restreinte ☐ Confidentielle

SOMMAIRE

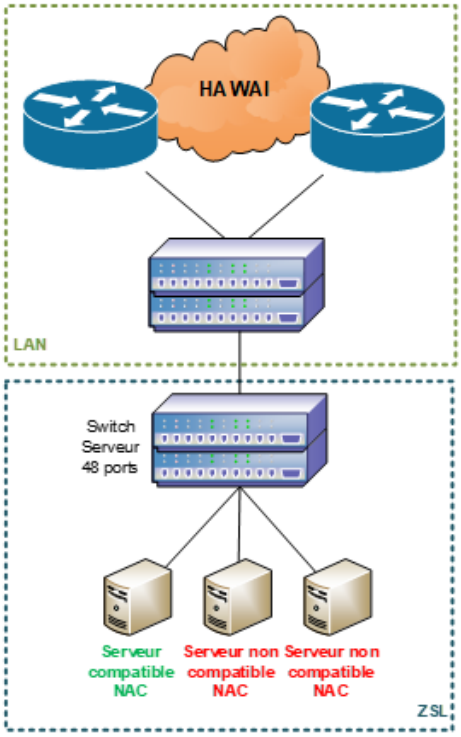
1 — Définition et contexte

1.1. Projet Fortification c'est quoi ?

Le projet Fortification consiste à sécuriser et optimisé la ZSL des sites RITA (sites migrés de CISCO en ARUBA) en ajoutant un cluster de firewall et en remplaçant ou supprimant le switch serveur qu'on verra ensuite.

ZSL : zone réseau composée de 1 à x VLAN, l'incorporation de switch n'est qu'un moyen de communication et d'interfaçage
Cluster de firewall : Ensemble de pare-feu configurés comme un seul système, si l'un d'eux tombe en panne, l'autre prend le relais, permettant une sécurité permanente. Le firewall permet de filtrer les flux entrants et sortants.

1.2. Contexte



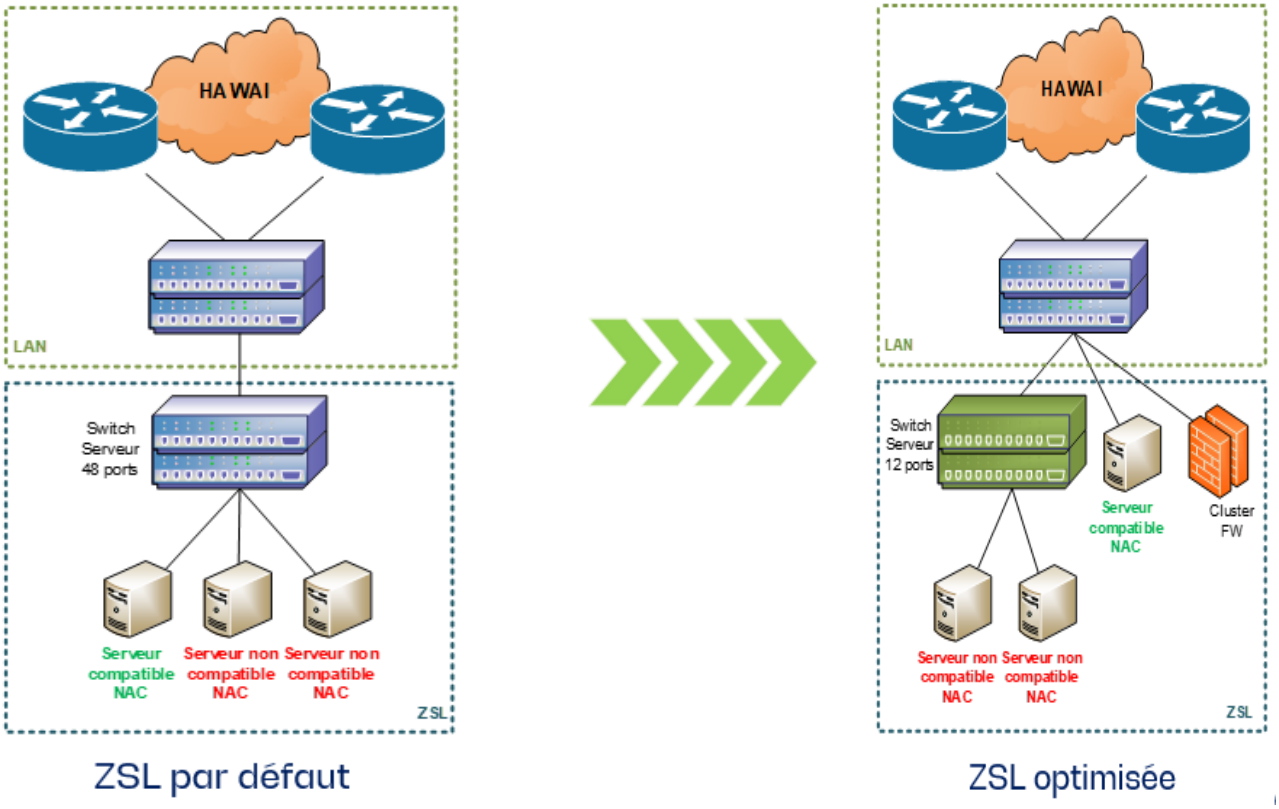
ZSL par défaut

Ci-dessus nous voyons la disposition de la ZSL et de la partie LAN avant la fortification. La ZSL est composée d'un switch serveur 48 ports permettant de relier les serveurs (compatible ou non en NAC) au switch cœur. Cependant, elle n'est pas vraiment optimisée et sécurisée, c'est là que la Fortification intervient.

Nous avons 2 cas, soit le site possède des serveurs non compatibles NAC et/ou compatibles NAC soit le site possède seulement des serveurs compatibles NAC.

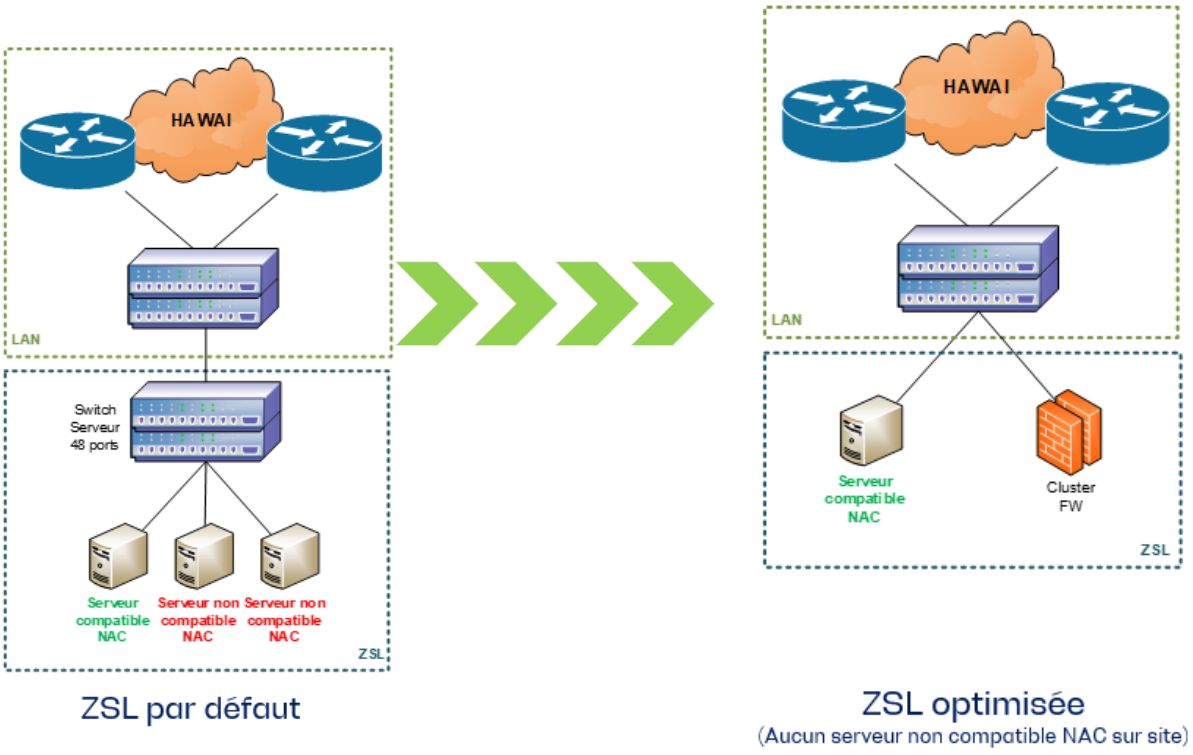
Le ***NAC*** (Network Access Control ou Contrôle d'Accès Réseau) est une technologie qui contrôle et sécurise l'accès des appareils à un réseau informatique. Il vérifie si un appareil est autorisé et respecte certaines règles de sécurité avant de le laisser se connecte.

Le 1er cas, le site possède des serveurs non compatibles NAC et/ou compatibles NAC, nous aurons cette topologie après fortification :



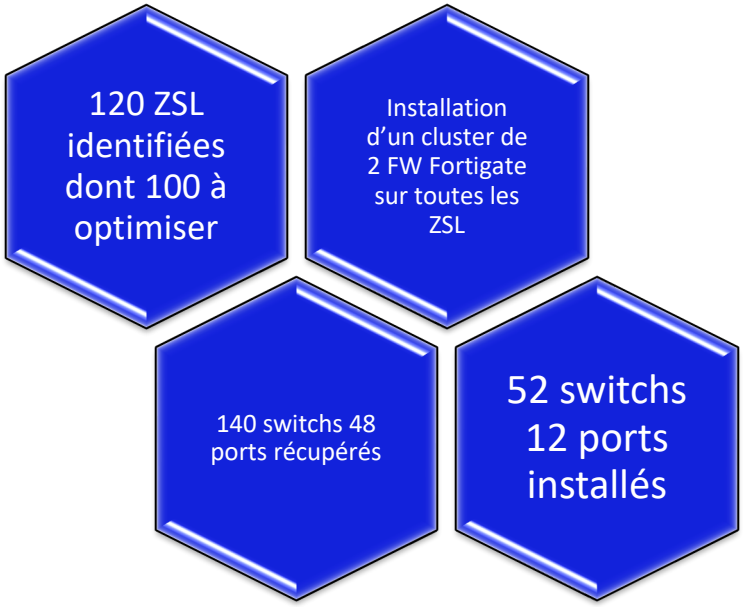
Le switch serveur 48 ports sera remplacé par un switch serveur 12 ports servant à relier les serveurs non compatibles NAC au switch cœur de réseau, s'il y a des serveurs compatibles NAC, alors ils seront directement reliés au switch cœur, c'est donc ça l'optimisation de la ZSL.
Pour la sécurisation c'est simple, on ajoute tout simplement un cluster de firewall sur le switch cœur pour sécuriser cette ZSL.

Le 2ème cas, le site possède seulement des serveurs compatibles NAC, nous aurons cette topologie après Fortification :



Le switch serveur 48 ports sera tout simplement retiré et ne sera pas remplacer par un switch serveur 12 ports. Les serveurs, compatibles NAC seront directement reliés au switch cœur et le cluster de firewall également.

2 — Etats des lieux



Estimation de réductions du nombre de ports de 90% sur les ZSL déjà déployées

3 — Périmètre et acteurs

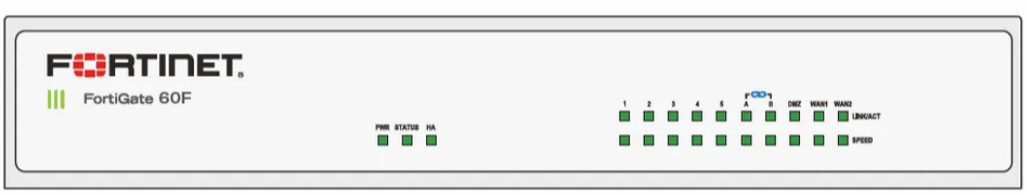
PRI	• Gère le pojet et la configuration des firewalls
TEX	• Guide à distance un technicien Econocom pour l'installation du switch, firewall et du brassage des serveurs
EXB	• Vérifie si les serveurs de bureautique remontent bien
CPT	• Vérifie si les serveurs de téléphonie remontent bien
CAIT	• C'est l'interlocuteur informatique du site qui est présent sur place et vérifie au bon déroulement de la fortification

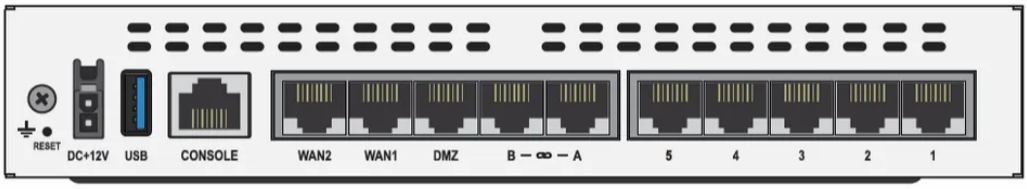
4 — Fortigate

4.1. Types firewalls

4.1.1. Fortigate 60F

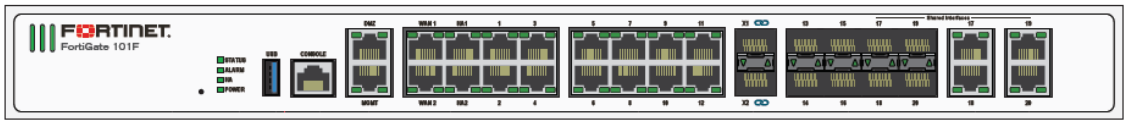
Le Fortigate 60F sera installé sur les sites où la ZSL est à moins de 1GB/s par serveur.

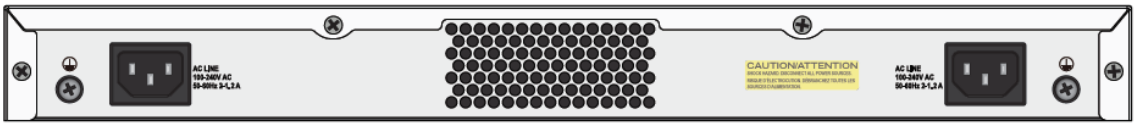




4.1.1. Fortigate 100F

Quant à lui, le Fortigate 100F sera installé sur les sites où la ZSL est à plus de 1GB/s par serveur





4.1. Pourquoi choisir Fortigate ?

Nouveau marché, prix avantageux

GESTION FACILITE

1 seul type de firewall = 1 seul outil d'exploitation FORTIMANAGER

SECURISATION

Meilleure gestion de CVE et des mises à jour

UNIFORMISATION

Permet d'uniformiser les différentes infrastructures

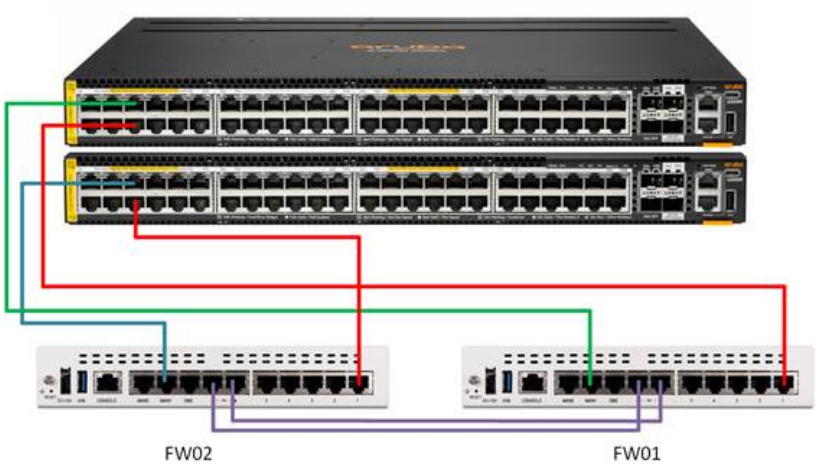
REUTILISATION

Les FW 60F pourront être utilisé pour d'autres besoins

5 — Mon rôle dans la Fortification ?

5.1. Installation des FW

La fortification se déroule à distance, je pilote un technicien Econocom présent sur place pour qu'il s'occupe de l'installation des FW et des switchs ainsi que le brassage des serveurs. Pour l'injection de configuration ou vérification des équipements, je prends la main sur son PC à distance.



J'indique au technicien comment brancher les 2FW au switch cœur, voici un exemple de câblage :
FW01 WAN1 – SC 1/1/5
FW01 port1 – SC 1/1/6
FW02 WAN1 – SC 2/1/5
FW02 port1 – SC 2/1/6
FW01 port A – FW02 port A
FW01 port B – FW02 port B

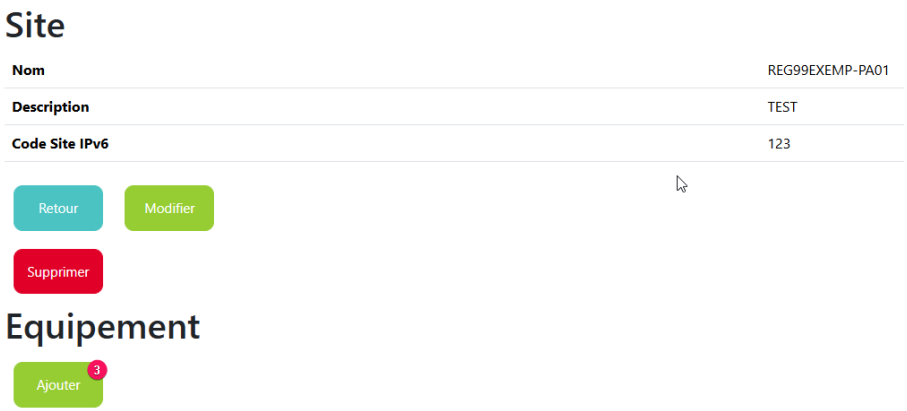
Ensuite, je vérifie si le switch cœur a la bonne configuration avec la commande *show interface*

5.1. Remplacement des switchs 48 ports

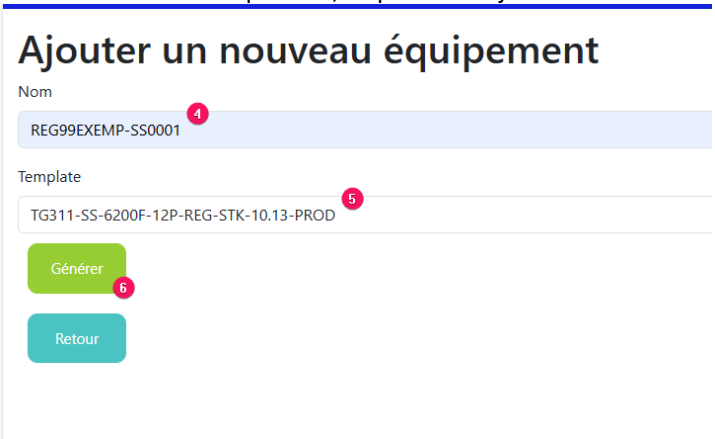
5.1.1. Création de configuration du switch

Pour la création de configuration des switchs ARUBA nous utilisons un logiciel créer en interne.

Nous allons tout d'abord sur le site en question :



Une fois sur le site en question, cliquez sur « ajouter » sous la rubrique « équipement »



On nomme l'équipement et on choisit le template **TG311-SS-12P-REG-STK-10.13-PROD**
Puis sur générer.
Une fois générée, on dépose le fichier de configuration dans un espace partagé et sécurisé avec les différents acteurs de ce projet.

Chez Enedis, nous utilisons des templates pour simplifier et standardiser la configuration des switchs. Un template est un fichier de configuration préétabli qui contient tous les paramètres nécessaires pour un type de switch donné. Il est conçu en fonction du modèle, de son utilisation et du nombre de ports. Grâce à ce système, il suffit de copier le contenu du fichier de configuration générée préalablement dans le switch pour que la configuration complète s'applique automatiquement, sans avoir à saisir chaque commande manuellement. Cette approche permet de gagner du temps, d'éviter les erreurs et d'assurer une homogénéité des configurations sur l'ensemble du parc informatique.

5.1.2. Upgrade des switchs

Avant l'installation des switchs, un upgrade est nécessaire pour qu'il soit sur la même version afin qu'ils se stacks (forme un seul et même switch).

Pour cela on met simplement ces commandes sur le switch :

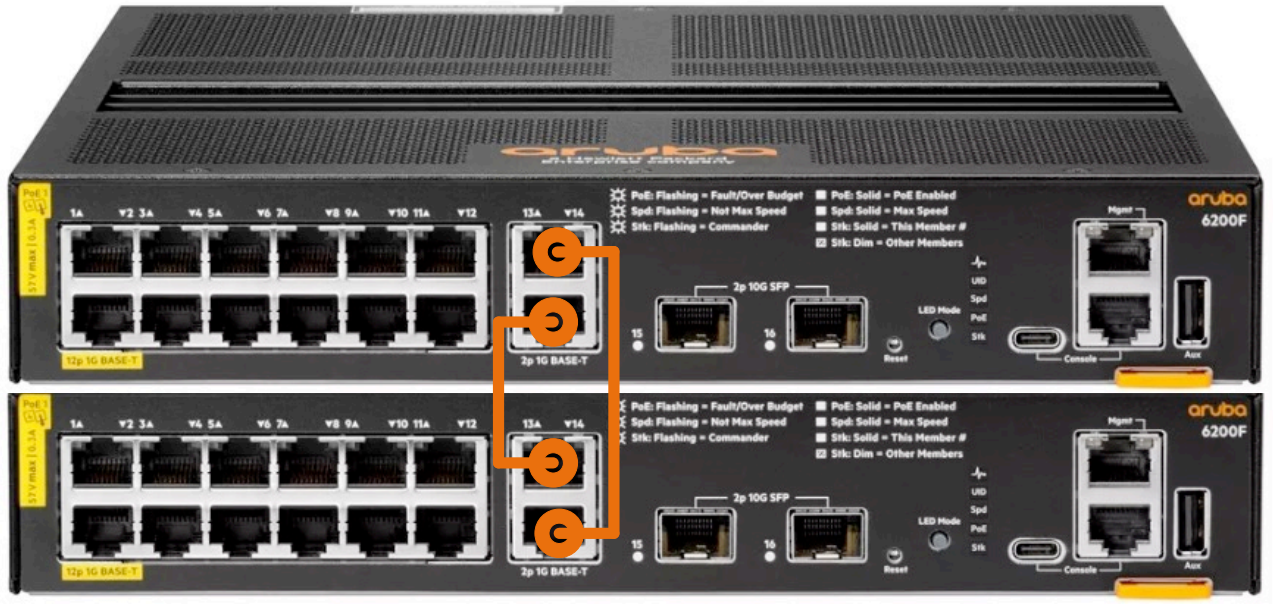
```
usb mount ->on monte l'usb sur le switch

copy usb://<nom_fichier> primary ->on copie la version présente sur la clé usb sur la partition
primaire du switch

reload -> on redémarre le switch
```

5.1.3. Injection des configurations

A distance, j'indique au technicien Econocom que les switchs doivent être branchés de cette manière :



L'injection se fait uniquement sur le switch primaire et lorsque les branchements de stack entre eux sont effectués.
Une fois les branchements fait, il suffit de mettre ces commandes :

```
usb mount -> permet d'autoriser l'usb sur le switch

copy usb://<nom_fichier> running-config : on copie la configuration générée précédemment sur la runnig-
config

write memory -> on enregistre la running-config
```

Ceci est la première méthode, la 2ème est tout simplement de faire appel au fichier sur notre serveur sftp (si on l'a mis au préalable) :

```
copy tftp:192.168.0.1//<nom_fichier> running-config
```

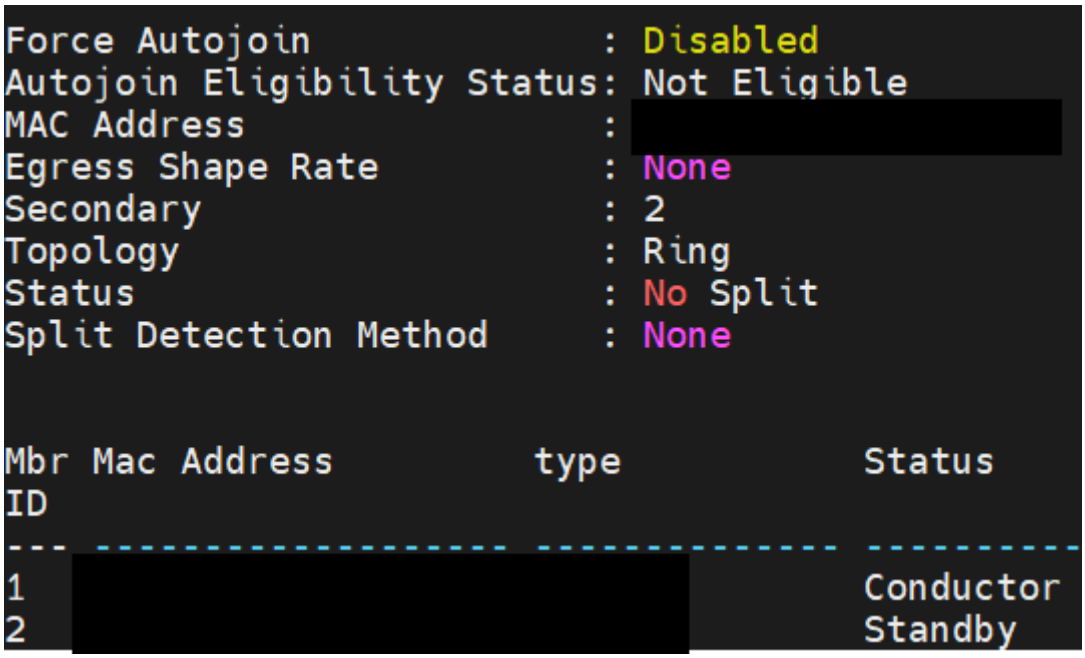
5.1.4. Ajout du switch dans un stack

Pour ajouter un switch dans un stack, nous devons vérifier que le branchement a bien été fais (voir ci-dessus), une fois fais nous mettons ces commandes :

```
Vsf force-auto-join -> cette commande permet de définir un seul et même switch virtuel composé de plusieurs switchs physiques interconnectés
```

Le switch devrait redémarrer et remonter en tant que stack, pour vérifier le stack il suffit de mettre cette commande sur le switch primaire :

```
Show vsf
```



On voit bien que la topologie est indiqué en « Ring », ce qui veut dire en « boucle » et on voit également 2 membres, un « conductor » (primaire) et le 2ème en « standby » (secondaire).

5.1.5. Brassage des serveurs sur SC et SS

Pour finir, on indique au technicien de branché les serveurs compatible NAC sur le switch cœur et les serveurs non compatible NAC sur le switch serveur.