Radius Linux

- Doc technique et install radius
- Procedure_Mise_A_Jour_Version_Linux
- Procedure retour arriere radius

Doc technique et install radius

Configuration et installation d’un serveur Radius

La configuration s’effectue en plusieurs étapes :

1 - Installation de NPS Windows 2022

2 - Installation de serveurs de certification

3 - Configuration dans la console Meraki (switchs et bornes wifi)

La première partie consiste à installer 4 serveurs Windows 2022 ainsi que 3 serveurs de certification (actuellement il en existe déjà un sur le domaine Vincennes, SP87).

La répartition de ces derniers est la suivante :

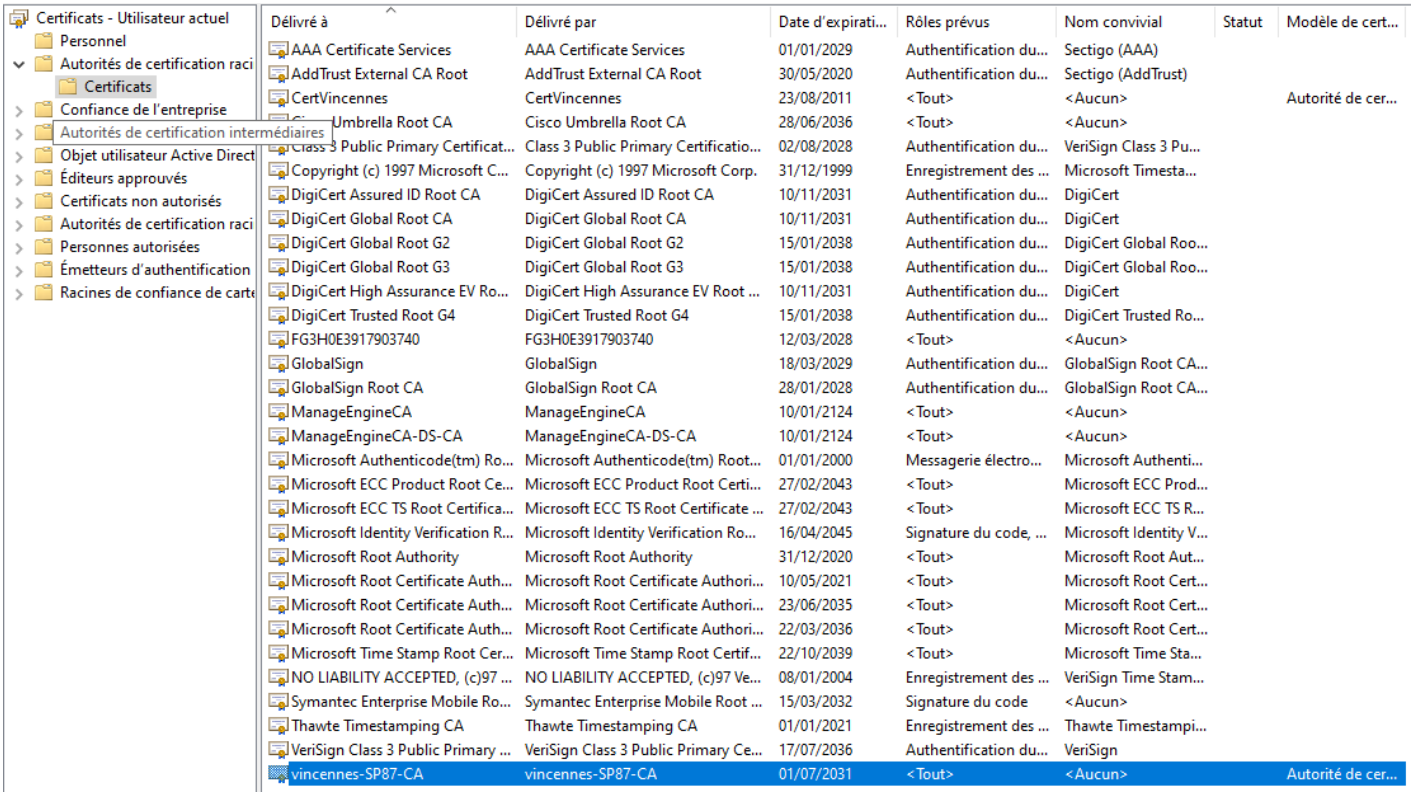
2 serveurs NPS pour l’authentification radius des agents en filaire et en wifi + 1 serveur de certification.

2 serveurs NPS pour l’authentification radius des écoles + 2 serveurs de certification

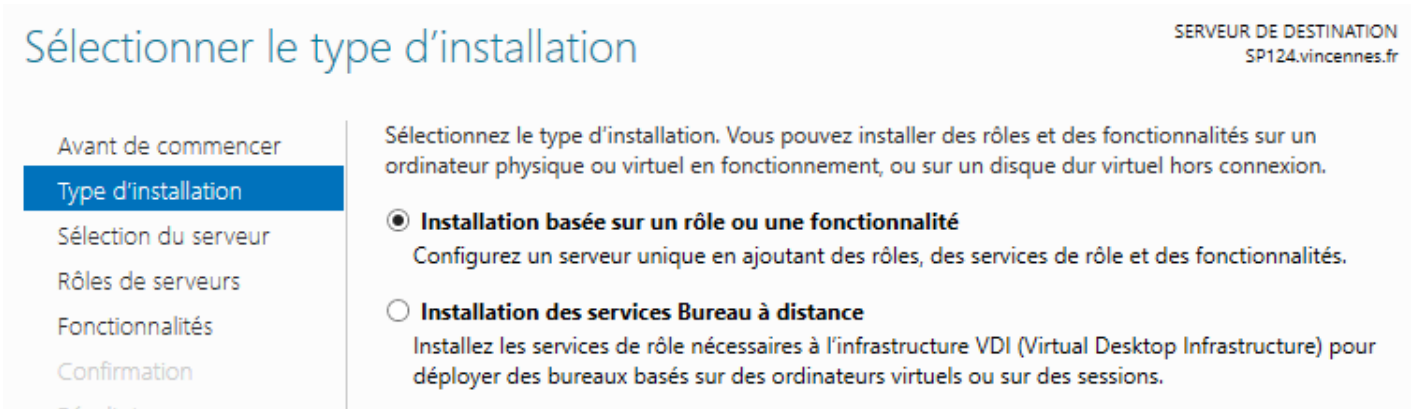
La seconde partie consiste à configurer tous les éléments dans la console web Meraki (switchs et bornes wifi)

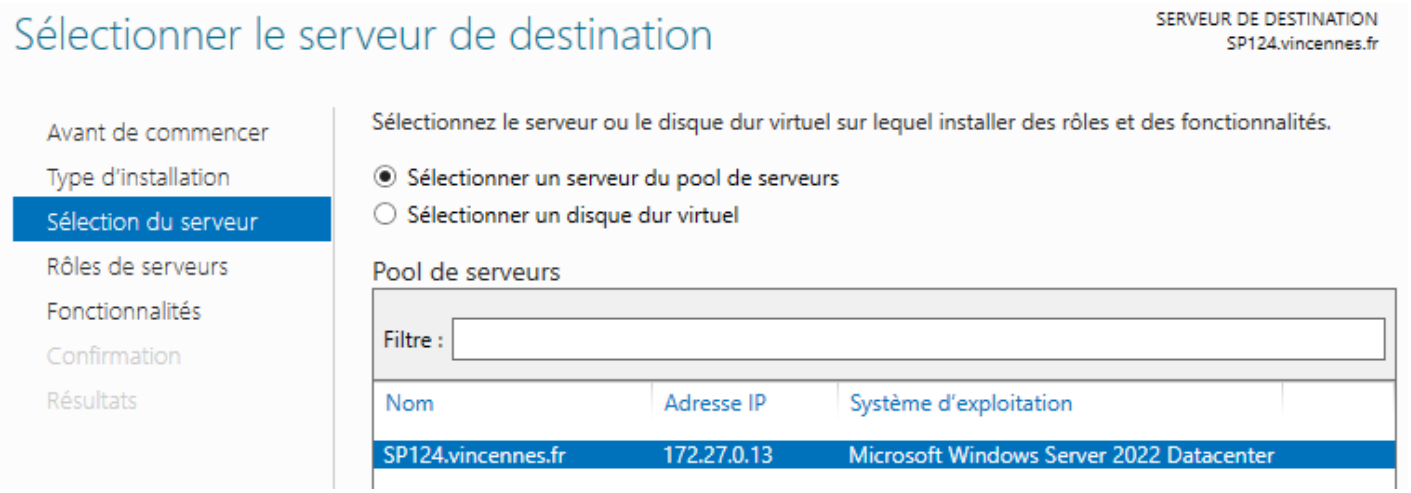
Nous avons configuré les 2 serveurs suivants : SP124 et SP125(NPS) dans le vlan système pour l’authentification sur le domaine Vincennes.fr.

1. Récupération de l’autorité de certification :

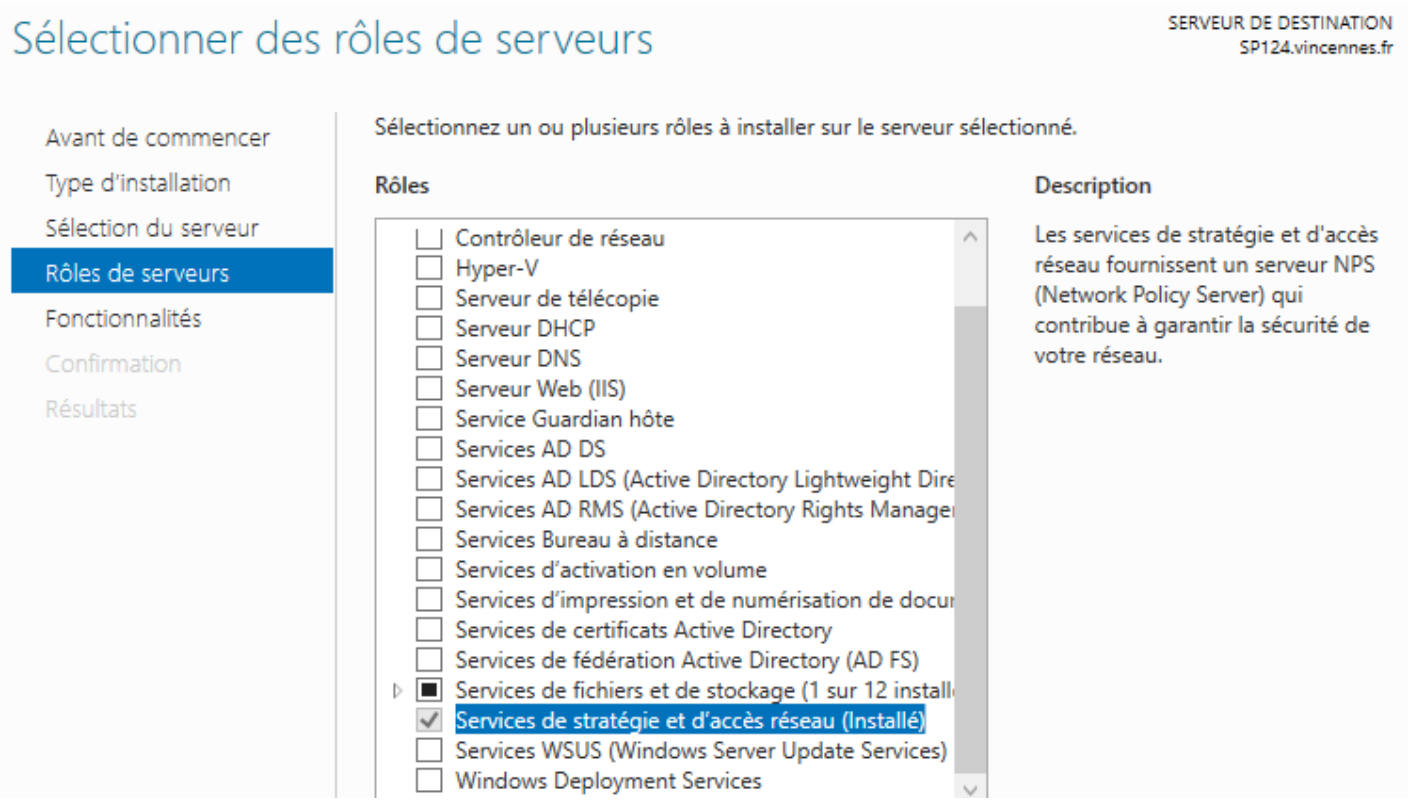


1. Ajout du rôle NPS (Network Policy Server)



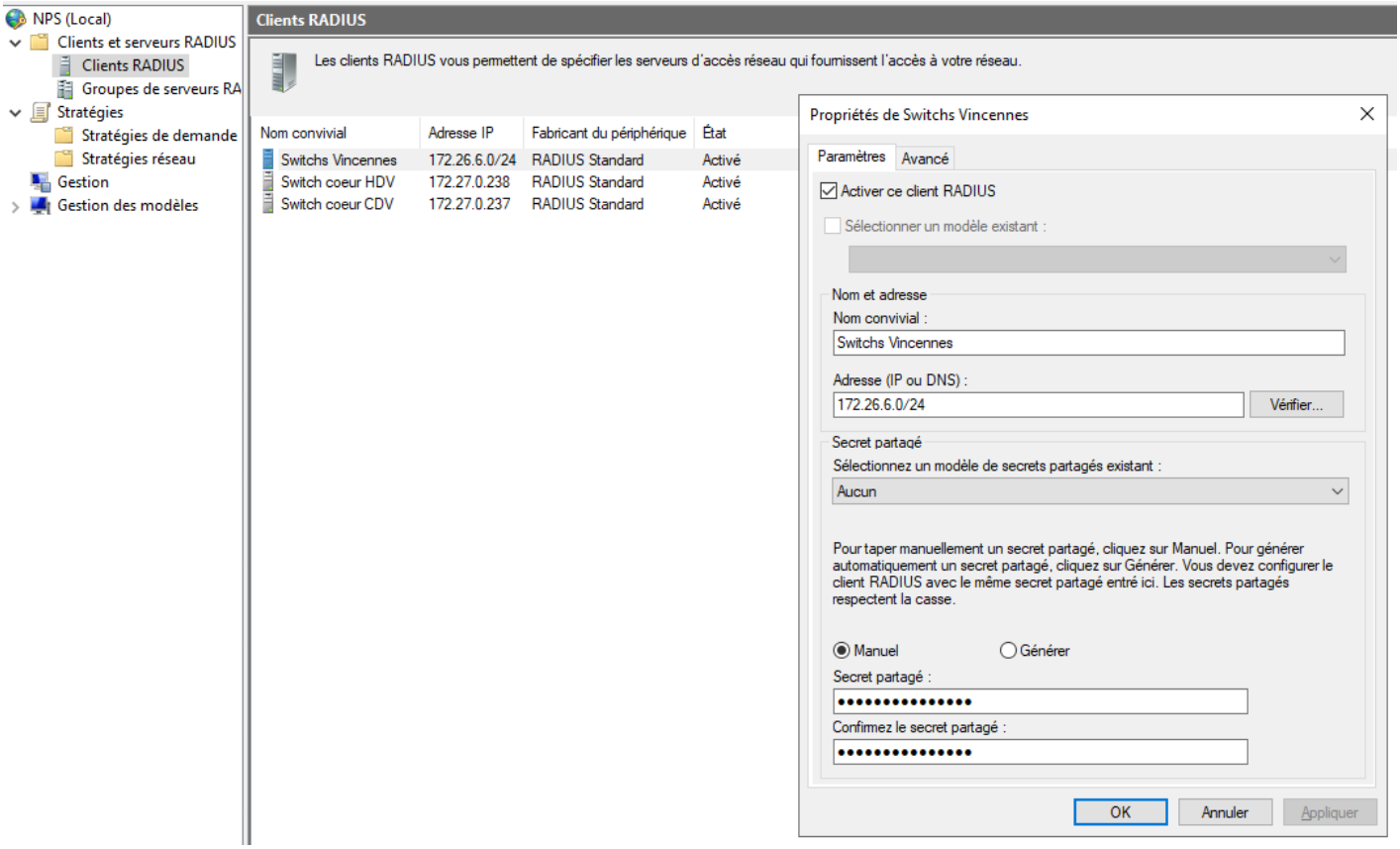


Choisir « Serveur de stratégie et d'accès réseau » puis installer



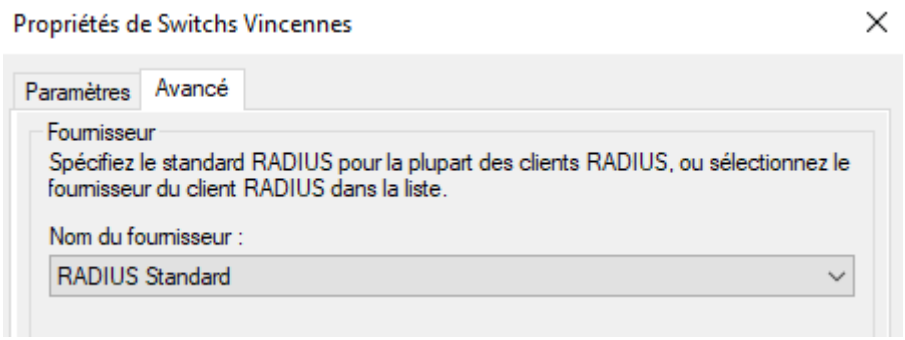
1. Configuration du NPS :

Configurer les clients radius (réseau sur lequel se trouvent les switchs et les bornes wifi)

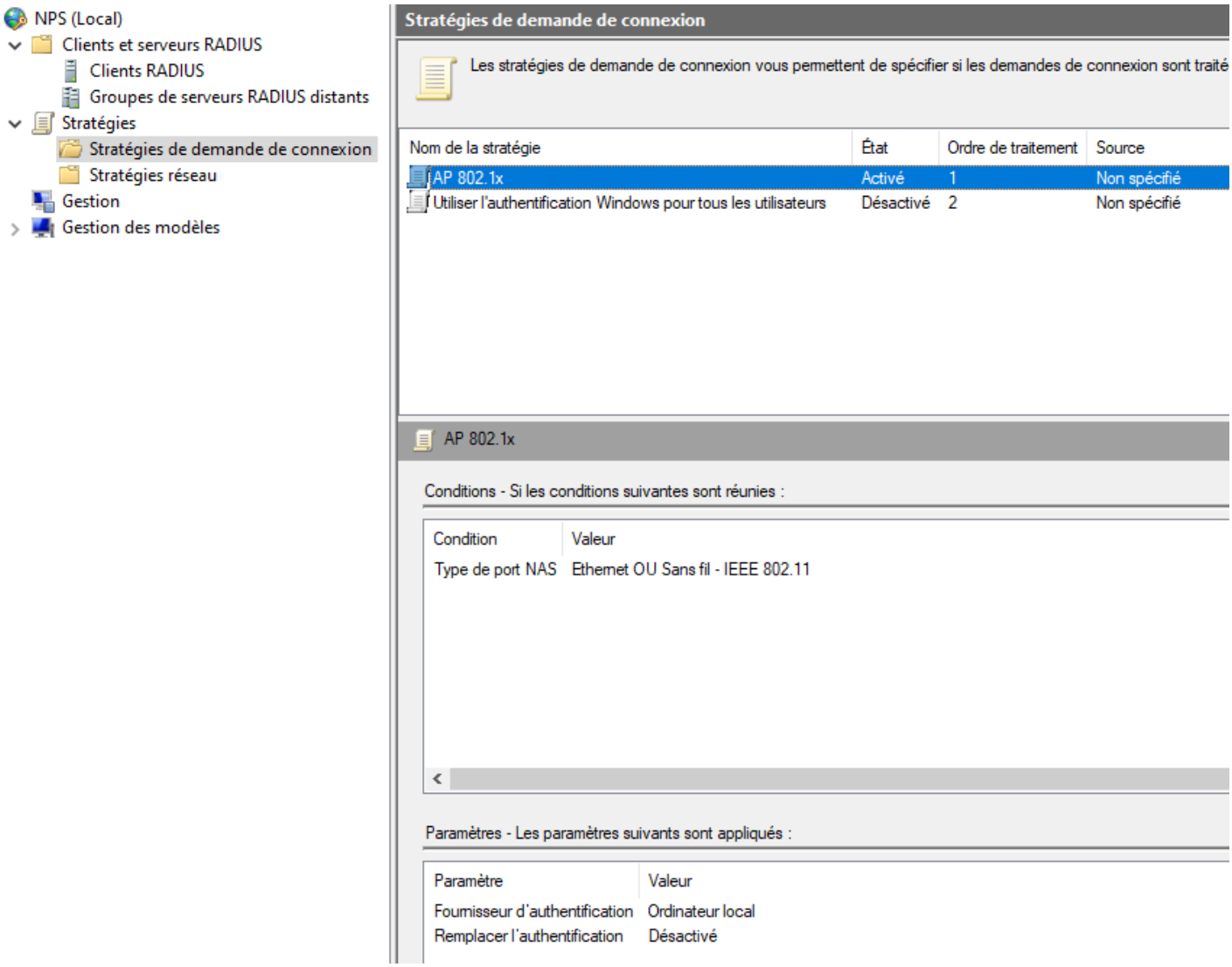


A noter que le secret partagé se trouve dans le keepass.

Onglet « Avancé »

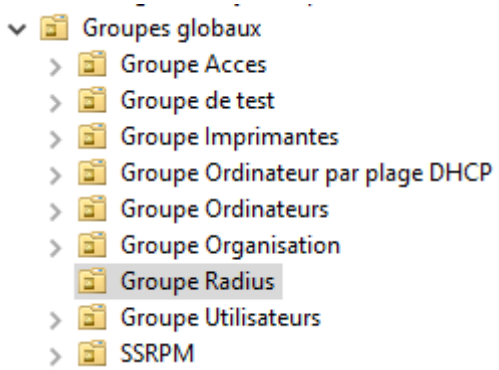


Configuration de demande de connexion : s’applique aux éléments actifs (switchs et borne wifi)



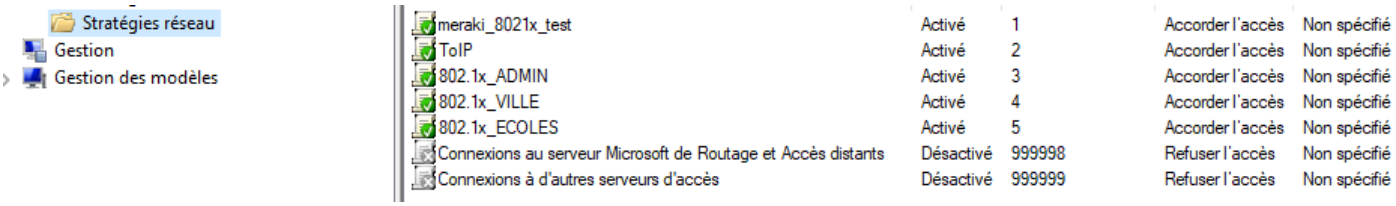
Les stratégies réseaux sont configurées de manière à orienter les réseaux vers lesquels les agents vont se connecter en fonction du groupe auxquels ils appartiennent.

Les groupes sont configurés dans l’AD :



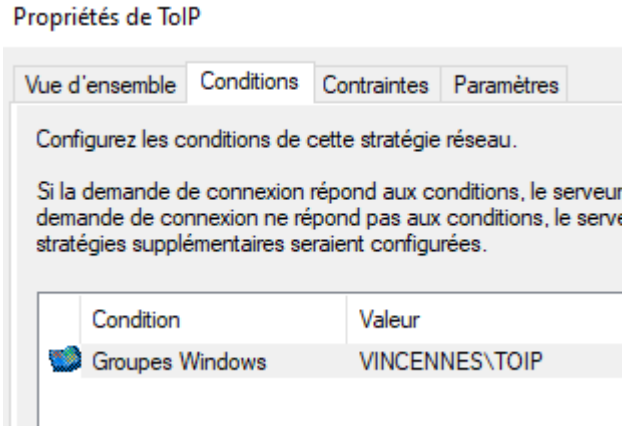
Sur les serveurs NPS du domaine Vincennes.fr, nous avons configuré 3 stratégies réseaux dans un premier temps :

ToIP, 802 1X_ADMIN et 802 1X_VILLE



Stratégie ToIP :

Comme son nom l'indique, elle permet aux téléphones de s'authentifier au serveur Radius via son ID de vlan (224) et via la méthode MD5-challenge activée sur ce dernier.



Propriétés de ToIP

Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

MD5-Challenge

Monter

Descendre

Ajouter... | Modifier... | Supprimer

Méthodes d'authentification moins sécurisées :

- [ ] Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
  - [ ] L'utilisateur peut modifier le mot de passe après son expiration
- [ ] Authentification chiffrée Microsoft (MS-CHAP)
  - [ ] L'utilisateur peut modifier le mot de passe après son expiration
- [x] Authentification chiffrée (CHAP)
- [ ] Authentification non chiffrée (PAP, SPAP)
- [ ] Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de ToIP

Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- Spécifiques au fournisseur

Routage et accès à distance

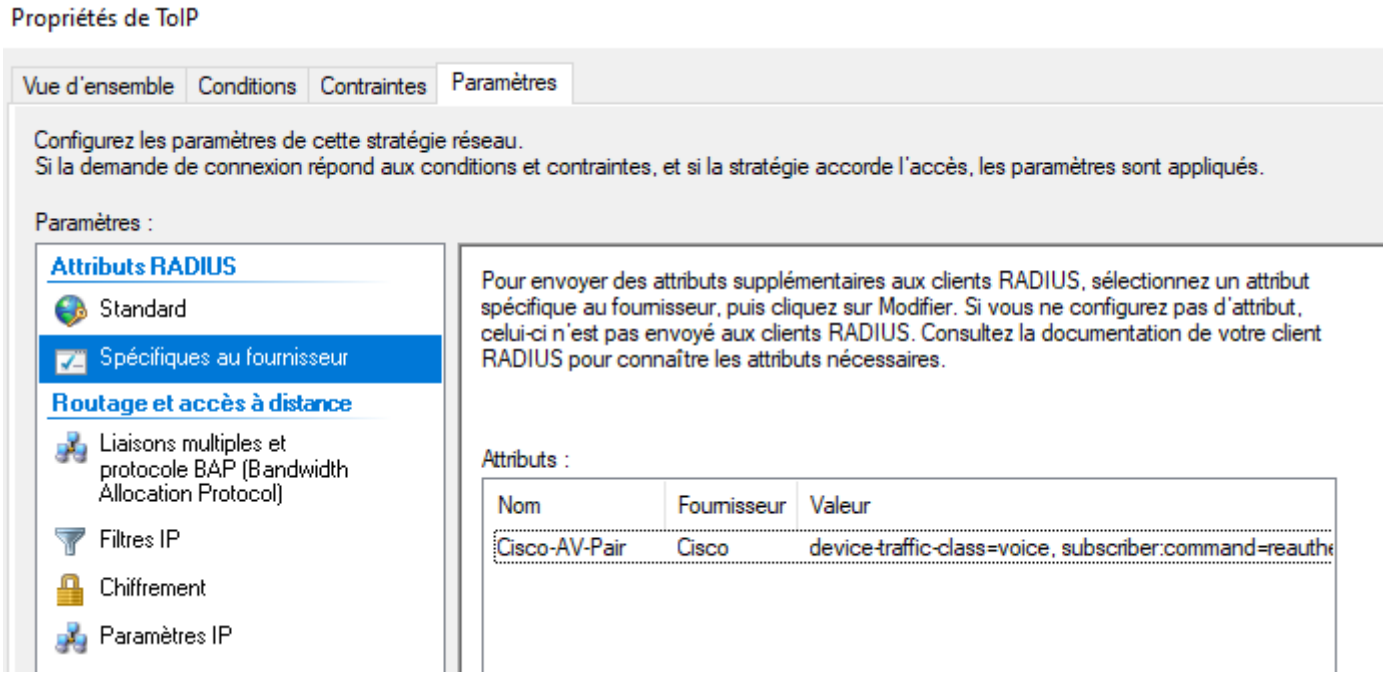
- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

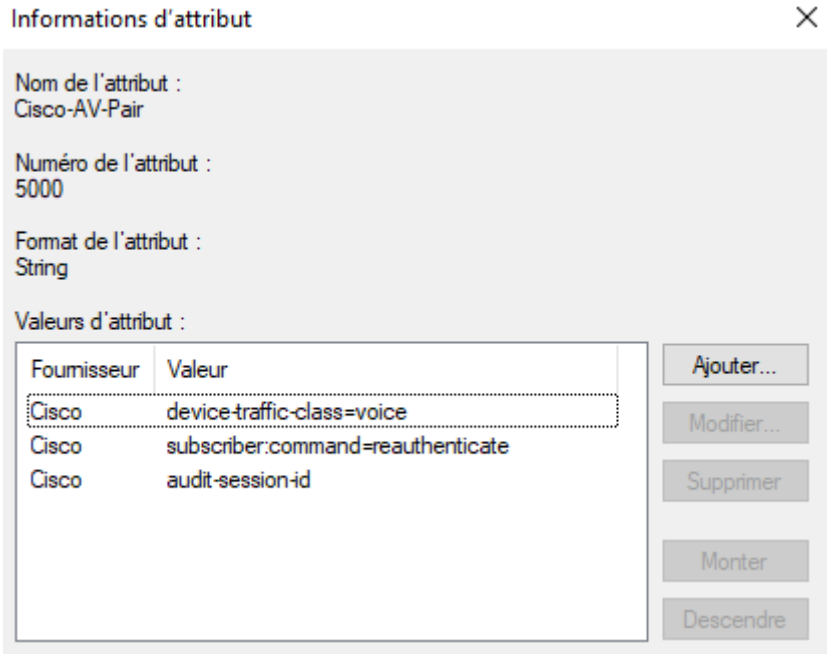
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	224
Tunnel-Type	Virtual LANs (VLAN)

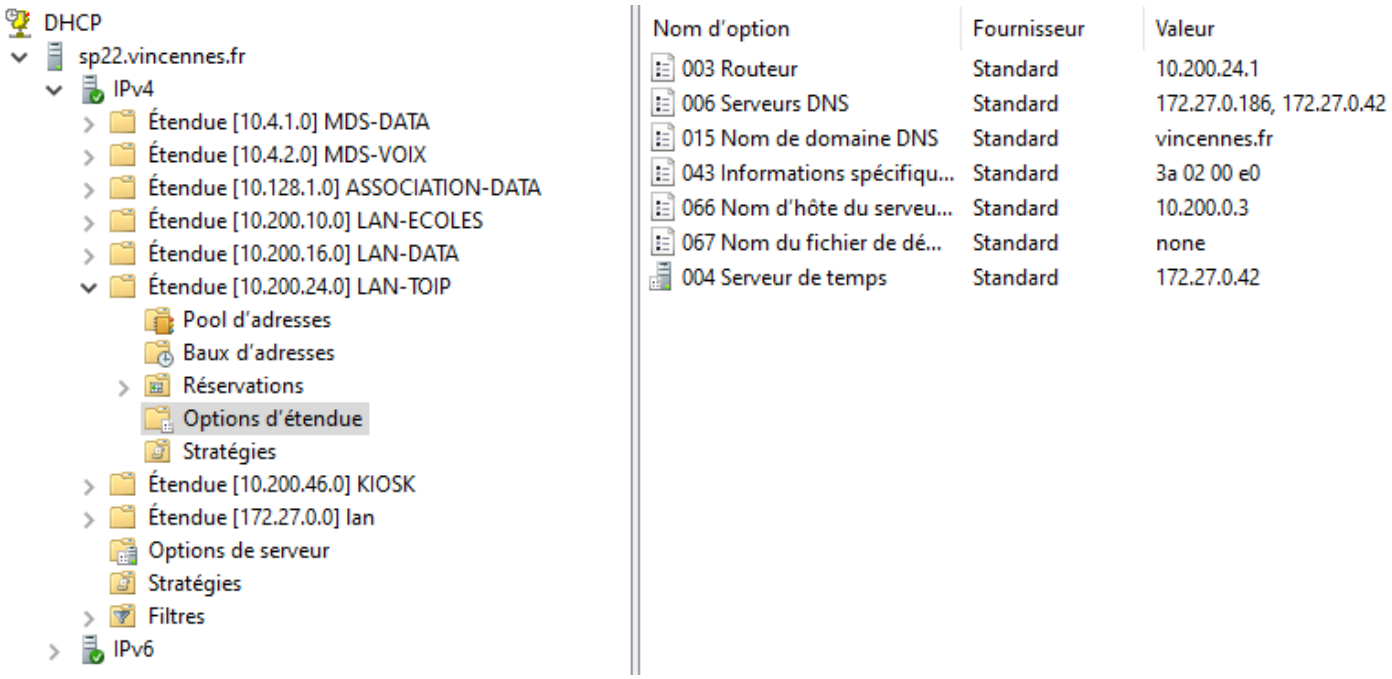
Ajouter... | Modifier... | Supprimer





A noter qu'un fichier .reg a été créé afin de rajouter une configuration supplémentaire non incluse dans les paramètres classiques.

Il a été ajouté également l'option 43 sur le Lan-Toip avec la valeur 3a 02 00 e0 dans le serveur DHCP.



« 3a 02 » correspondant a Alcatel et « 00 e0 » a l'ID du vlan voix en hexadecimal (224).

Cela permet au téléphone de se monter sans avoir l'ID du vlan de cocher dans les paramètres IP.

Stratégie ADMIN :

Cette stratégie permet l'accès du réseau aux administrateurs. La configuration du PC admin doit être en DHCP avec réservation MAC et le vlan d'admin (205) sera monté automatiquement.

802.1x_ADMIN	Activé	3	Accorder l'accès	Non spécifié
802.1x_VILLE	Activé	4	Accorder l'accès	Non spécifié
802.1x_ECOLES	Activé	5	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Désactivé	999998	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Désactivé	999999	Refuser l'accès	Non spécifié

802.1x_ADMIN

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_DINSI

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	205
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Le groupe AD dans lequel les PC Admins devront être sont ACCES_RADIUS_DINSI

Propriétés de 802.1x_ADMIN

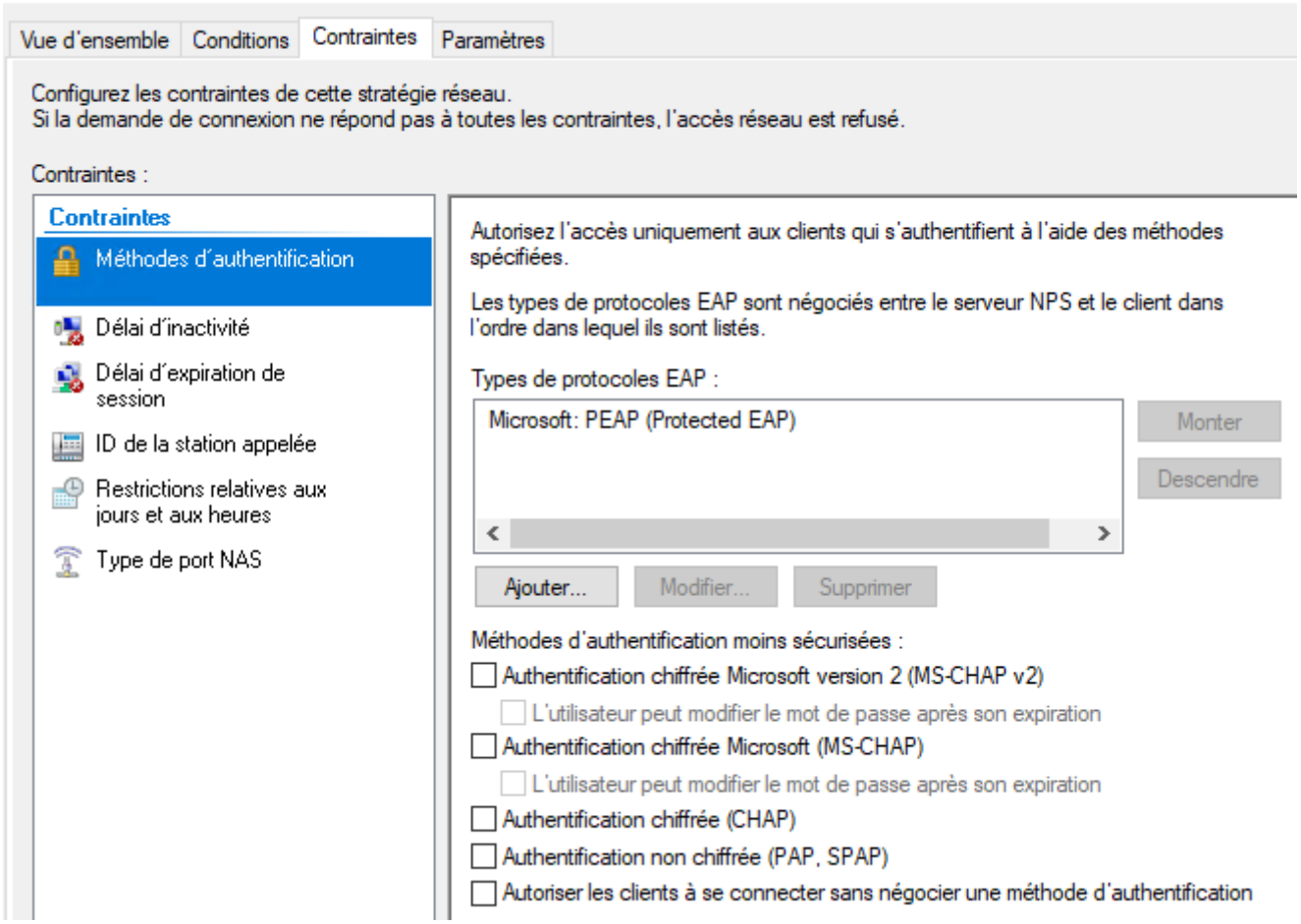
Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les conditions de cette stratégie réseau.

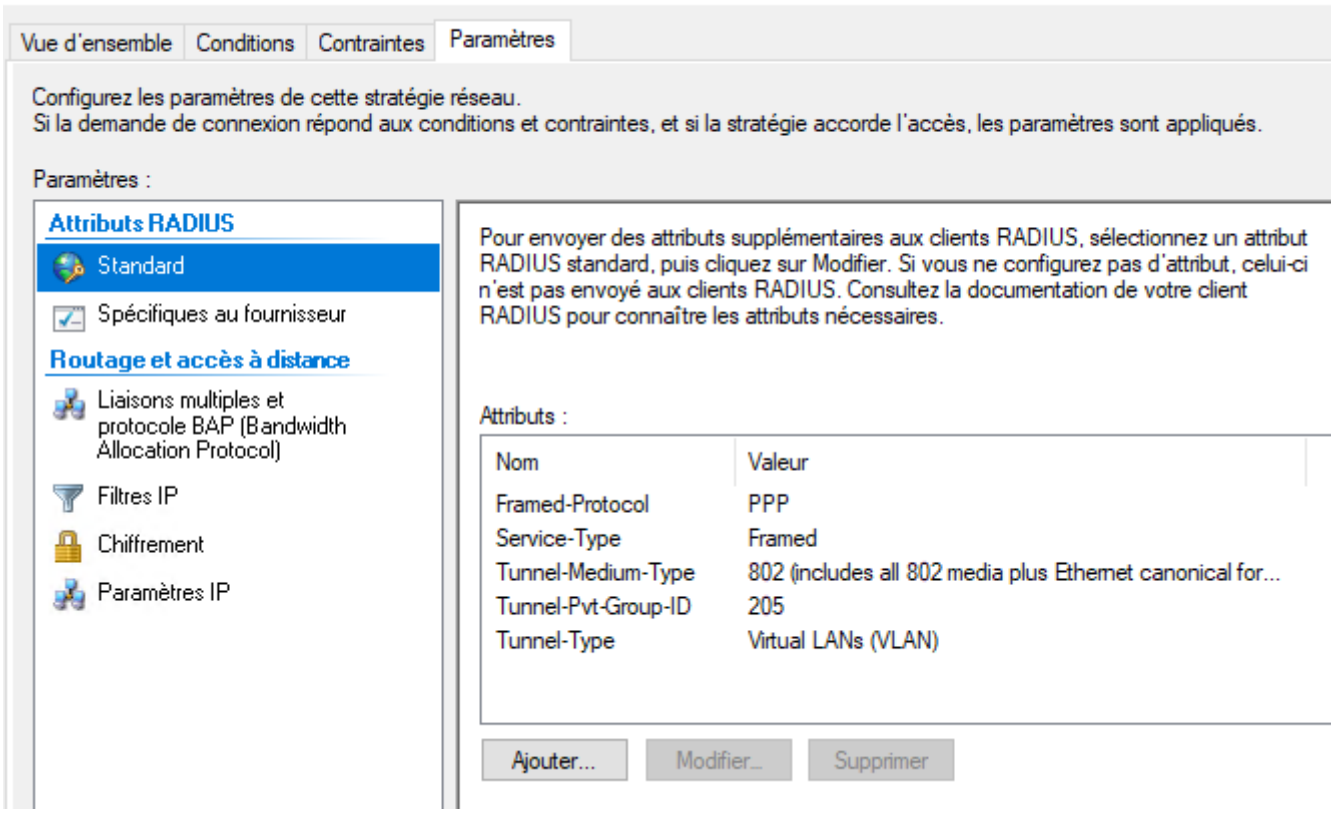
Si la demande de connexion répond aux conditions, le serveur NPS utilise cette
demande de connexion ne répond pas aux conditions, le serveur NPS ignore c
stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_DINSI

Propriétés de 802.1x_ADMIN



Propriétés de 802.1x_ADMIN



Stratégie LAN-DATA :

Cette stratégie permet aux utilisateurs standard de se connecter sur le réseau (vlan 216)

Nom de la stratégie	État	Ordre de traitement	Type d'accès	Source
meraki_8021x_test	Activé	1	Accorder l'accès	Non spécifié
ToIP	Activé	2	Accorder l'accès	Non spécifié
802.1x_ADMIN	Activé	3	Accorder l'accès	Non spécifié
802.1x_VILLE	Activé	4	Accorder l'accès	Non spécifié
802.1x_ECOLES	Activé	5	Accorder l'accès	Non spécifié

802.1x_VILLE

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_VILLE

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	audit-session-id, subscriber:command=reauthenticate
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	216
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Accès aux utilisateurs qui se trouvent dans le groupe ACCES_RADIUS_VILLE

Propriétés de 802.1x_VILLE

Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise cett
demande de connexion ne répond pas aux conditions, le serveur NPS ignore
stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'ordinateurs	VINCENNES\ACCES_RADIUS_VILLE

Propriétés de 802.1x_VILLE

Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP)

Monter

Descendre

Ajouter... | Modifier... | Supprimer

Méthodes d'authentification moins sécurisées :

- [ ] Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
  - [ ] L'utilisateur peut modifier le mot de passe après son expiration
- [ ] Authentification chiffrée Microsoft (MS-CHAP)
  - [ ] L'utilisateur peut modifier le mot de passe après son expiration
- [ ] Authentification chiffrée (CHAP)
- [ ] Authentification non chiffrée (PAP, SPAP)
- [ ] Autoriser les clients à se connecter sans négocier une méthode d'authentification

Propriétés de 802.1x_VILLE

Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

- Standard
- Spécifiques au fournisseur

Routage et accès à distance

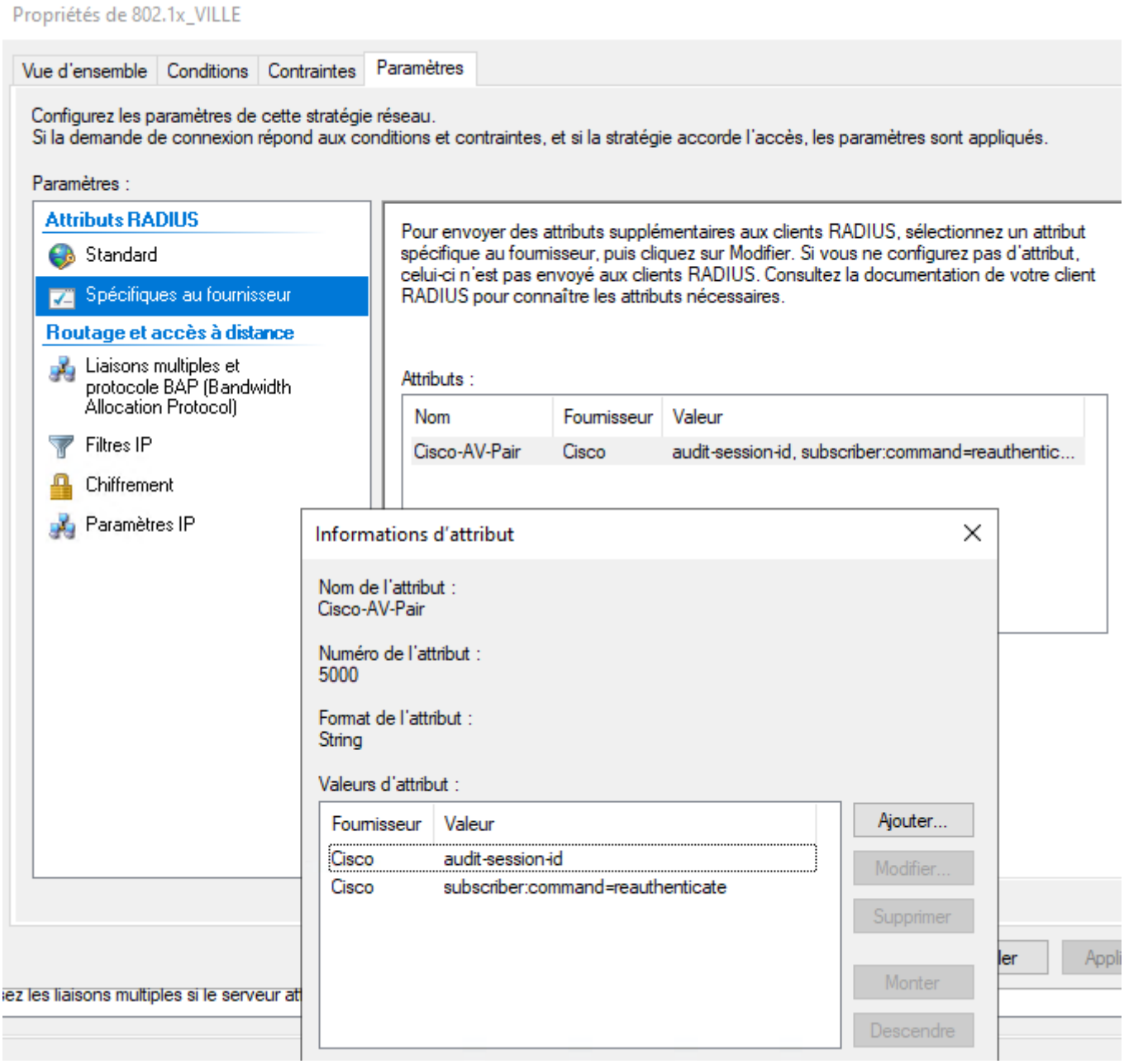
- Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)
- Filtres IP
- Chiffrement
- Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attri
RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celu
n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client
RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	216
Tunnel-Type	Virtual LANs (VLAN)

Ajouter... | Modifier... | Supprimer



Stratégie LAN_ECOLES :

2 serveurs ont été créés sur le domaine des écoles, il s'agit de SP129 et SP130.

2 serveurs de certification ont également été créés, il s'agit de SP131 et SP132.

Cette stratégie s'applique à tout le réseau des postes des écoles (Elèves, enseignants et directeur) sauf les postes des infirmeries, des gardiens ou du personnel des centres de loisirs.

ToIP	Activé	1	Accorder l'accès	Non spécifié
802.1x_ECOLE	Activé	2	Accorder l'accès	Non spécifié
802.1x_ECOLES	Désactivé	3	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Désactivé	4	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Désactivé	5	Refuser l'accès	Non spécifié

802.1x_ECOLE

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes d'ordinateurs	ECOLES\ECOLES.ORDINATEURS

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Cisco-AV-Pair	audit-session-id, subscriber:command=reauthenticate
Configuration du protocole EAP (Extensible Authentication Protocol)	Configuré
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole EAP
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical format)
Tunnel-Pvt-Group-ID	210
Tunnel-Type	Virtual LANs (VLAN)
Pourcentage de capacité du protocole BAP	Réduisez les liaisons multiples si le serveur atteint 50% pour 2 minutes

Le groupe AD dans lequel les PCs des écoles devront être est le suivant :

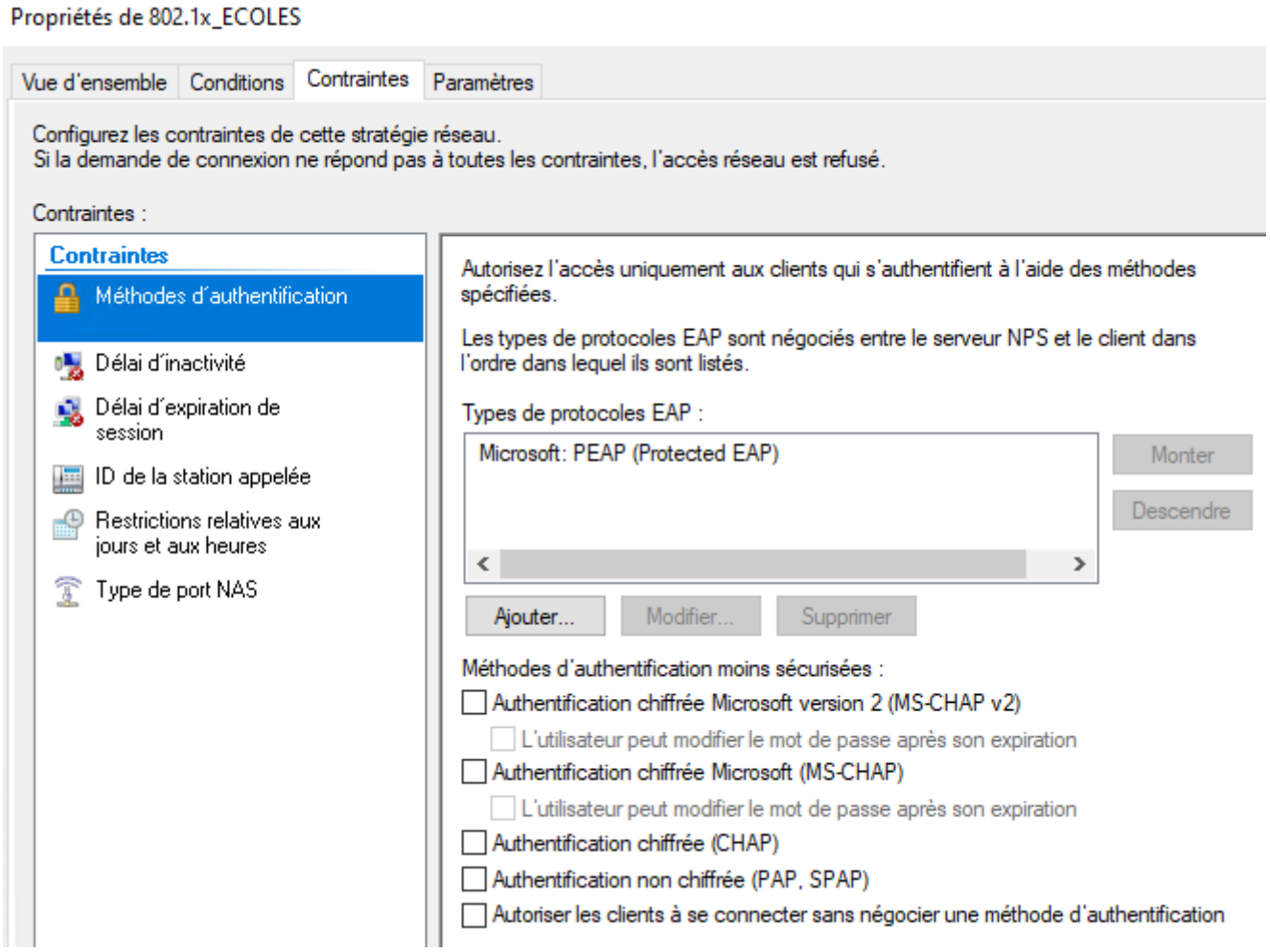
Propriétés de 802.1x_ECOLES

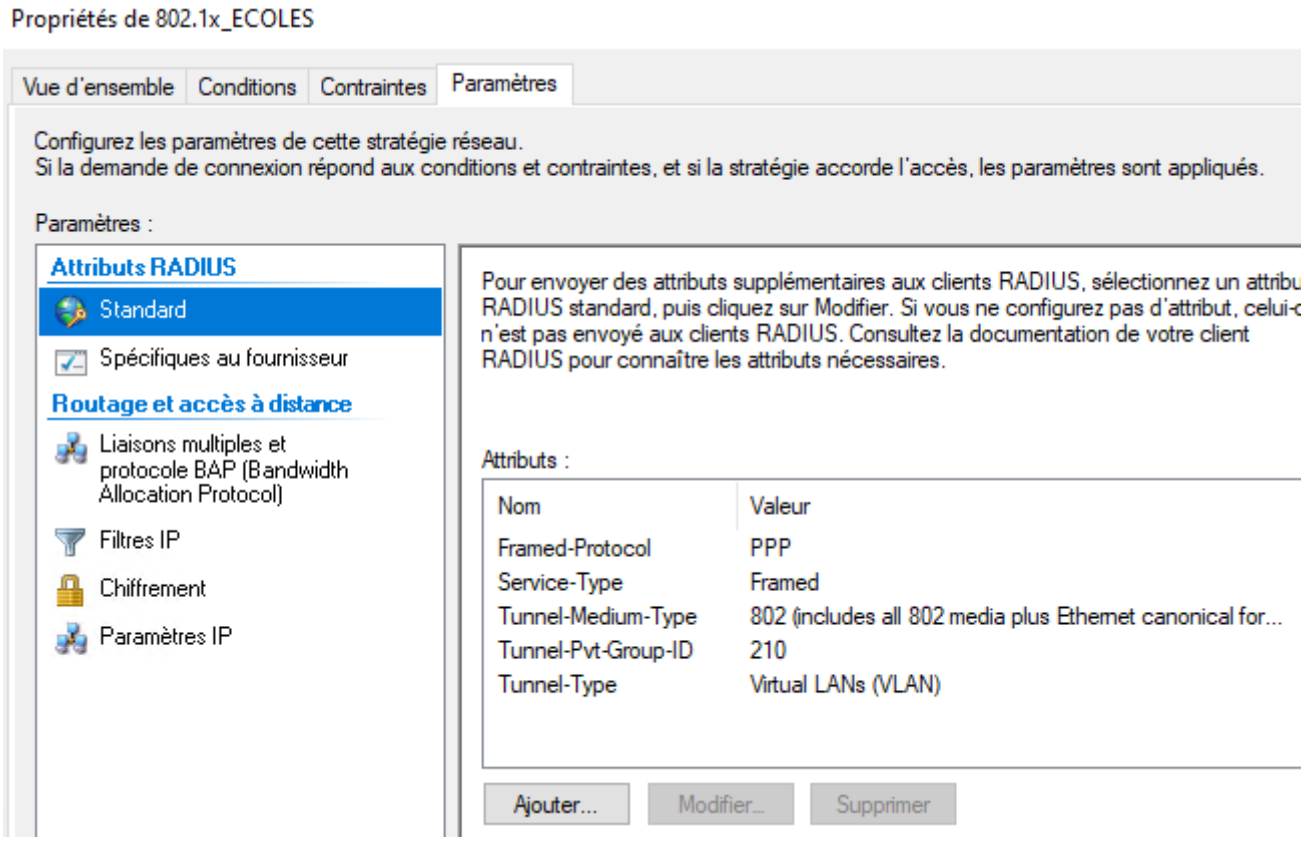
Vue d'ensemble | Conditions | Contraintes | Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur NPS utilise
demande de connexion ne répond pas aux conditions, le serveur NPS igno
stratégies supplémentaires seraient configurées.

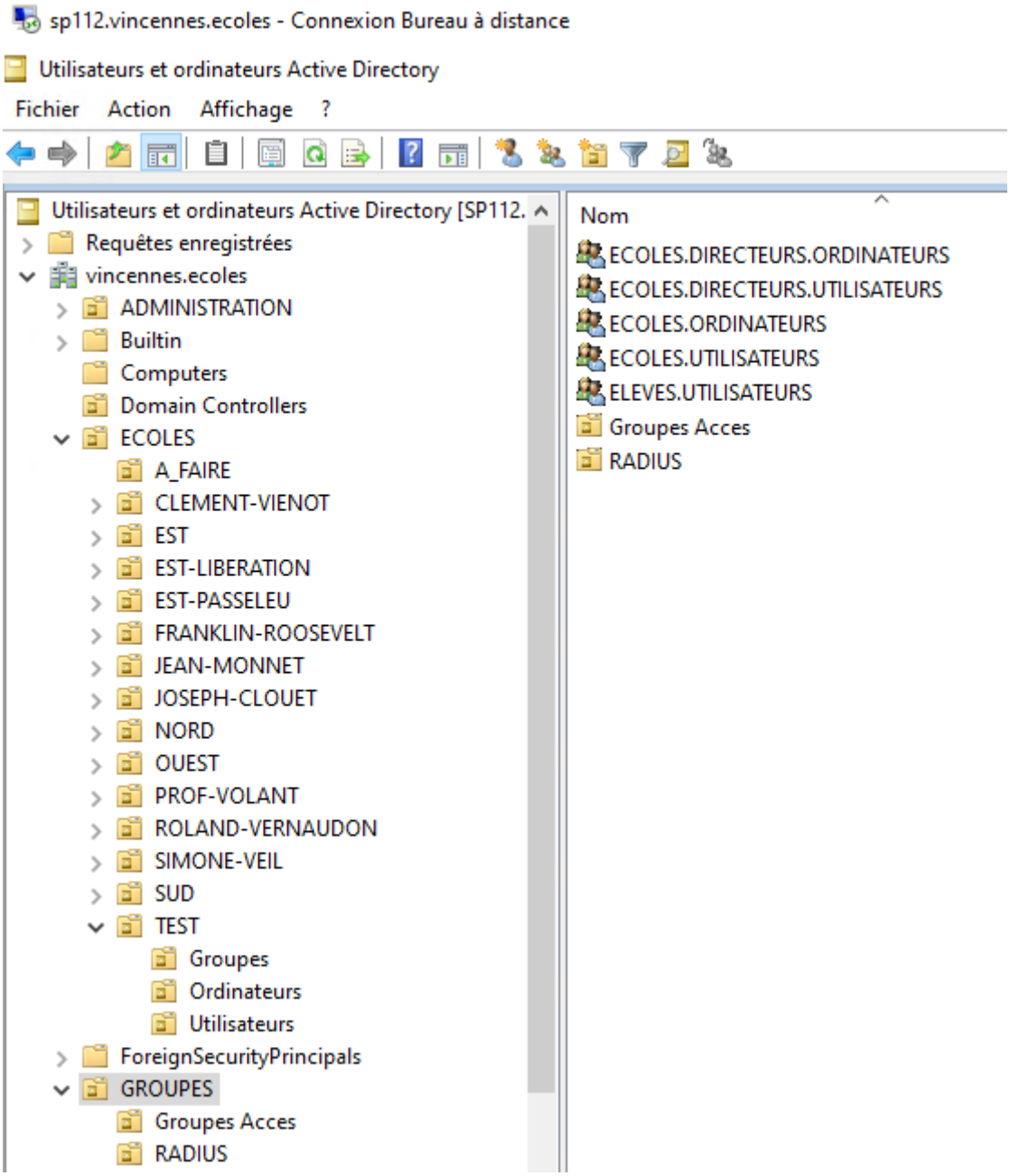
Condition	Valeur
Groupes d'ordinateurs	ECOLES\ECOLES.ORDINATEURS





Configuration sur le serveur AD des écoles :

Le PC doit être dans le groupe ECOLES.ORDINATEURS



Stratégie de groupe permettant l’activation du radius sur la carte réseau :

Activation 802.1X

Étendue | Détails | Paramètres | Délégation | État

Activation 802.1X

Données recueillies le : 19/03/2025 15:58:49 **masquer tout**

Général

masquer

Détails

masquer

Domaine	vincennes.ecoles
Propriétaire	ECOLES\Admins du domaine
Créé le	13/03/2025 19:33:58
Modifié le	13/03/2025 19:55:26
Révisions utilisateur	0 (AD), 0 (SYSVOL)
Révisions ordinateur	15 (AD), 15 (SYSVOL)
ID unique	{56010EC8-D562-4531-9F05-E5BE38160241}
État GPO	Activé

Liaisons

masquer

Emplacement	Appliqué	État du lien	Chemin d'accès
ECOLES	Non	Activé	vincennes.ecoles/ECOLES

Cette liste ne contient que les liaisons du domaine de l'objet de stratégie de groupe.

Filtrage de sécurité

masquer

Les paramètres de cet objet GPO ne s'appliquent qu'aux groupes, utilisateurs et ordinateurs suivants :

Nom
ECOLES\Ordinateurs du domaine

Délégation

masquer

Ces groupes et utilisateurs ont l'autorisation spécifiée pour cet objet de stratégie de groupe.

Nom	Autorisations acceptées	Hérité
AUTORITE NT\ENTERPRISE DOMAIN CONTROLLERS	Lecture	Non
AUTORITE NT\Système	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Administrateurs de l'entreprise	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Admins du domaine	Modifier les paramètres, supprimer, modifier la sécurité	Non
ECOLES\Ordinateurs du domaine	Lecture (à partir du filtrage de sécurité)	Non

Configuration ordinateur (activée)

masquer

Stratégies

masquer

Paramètres Windows

masquer

Paramètres de sécurité

masquer

Services système

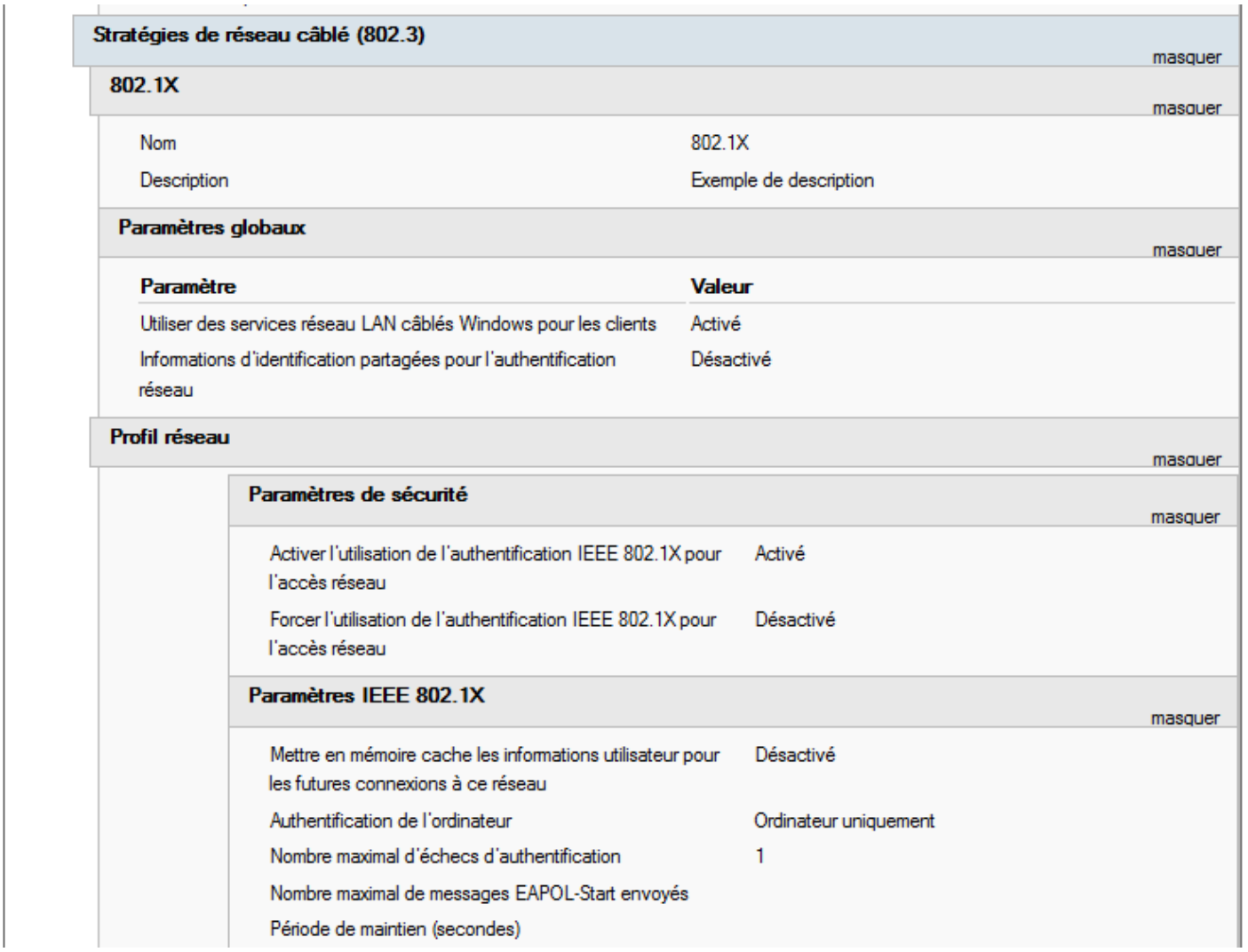
masquer

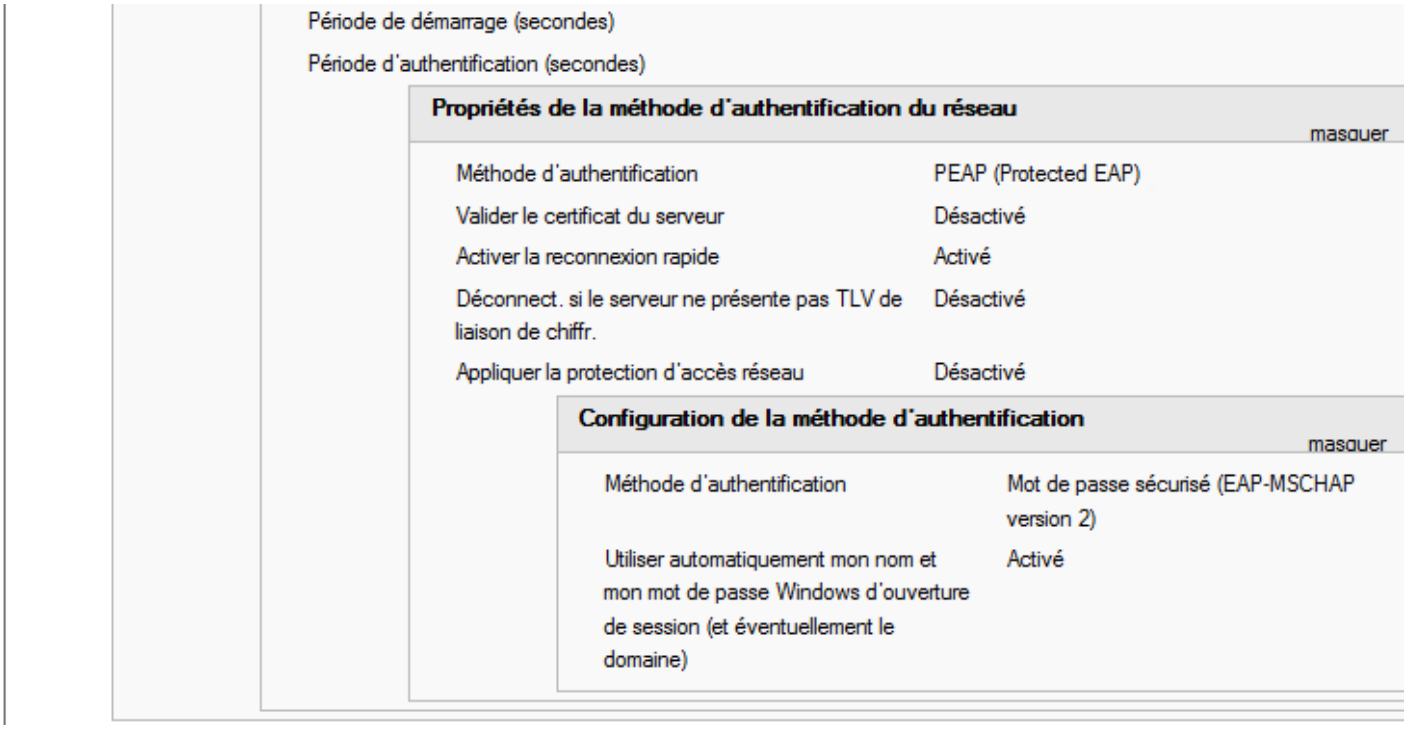
Configuration automatique de réseau câblé (Mode de démarrage : Automatique)

masquer

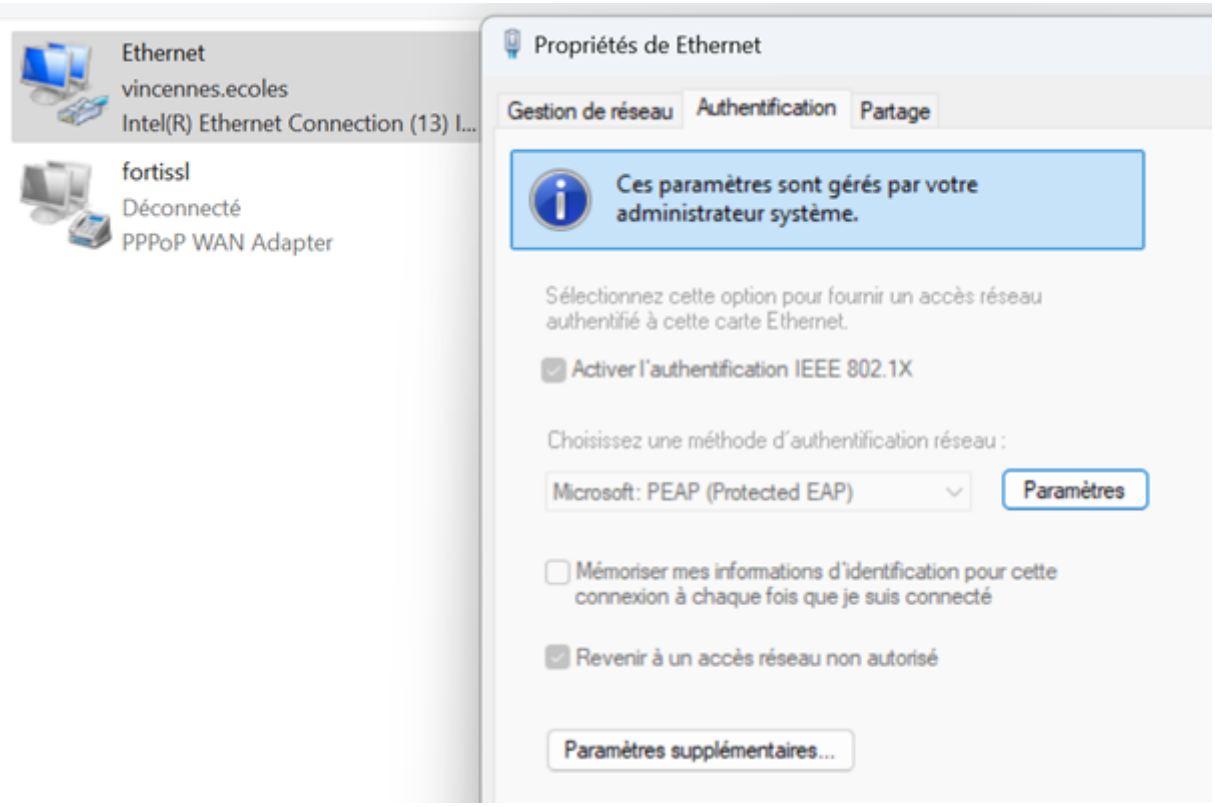
Autorisations
Aucune autorisation spécifiée

Audit
Aucun audit spécifié

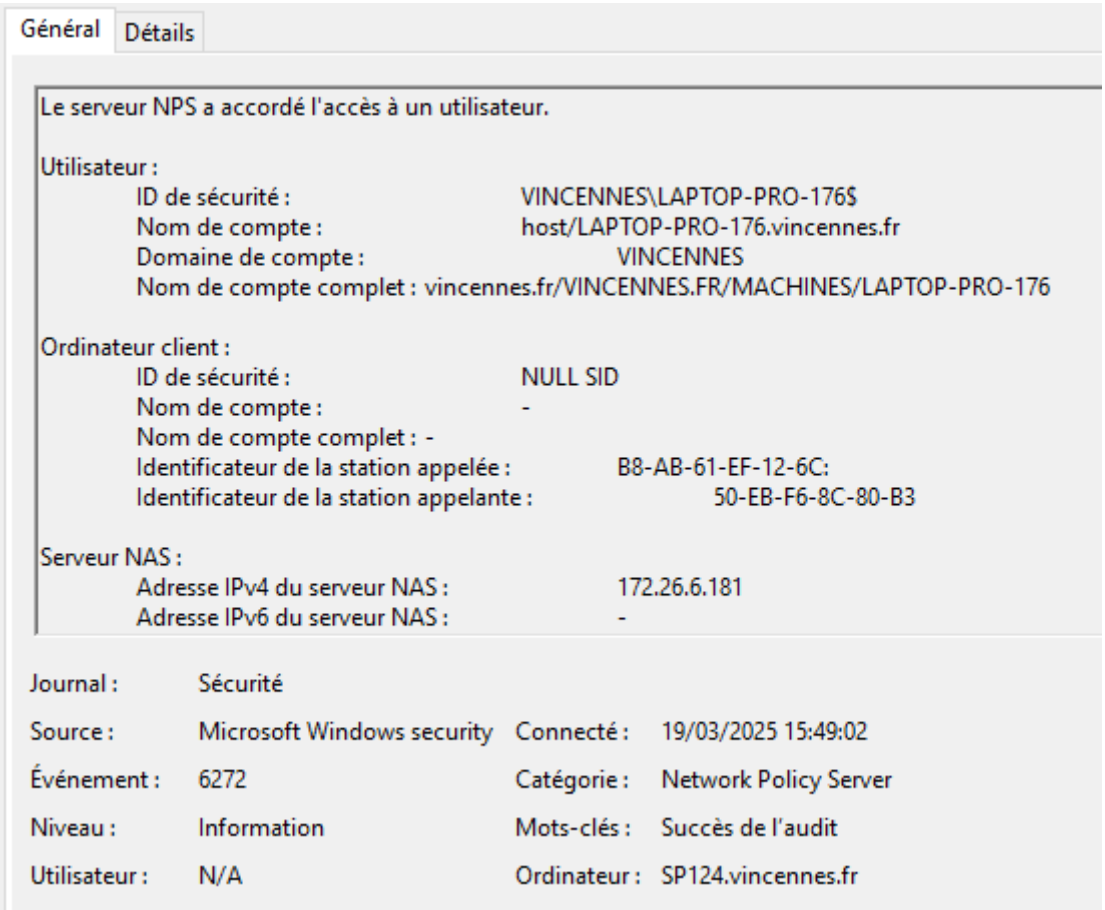




L’onglet « Authentification » apparaît suite a l’activation de la GPO « activation 802.1x »

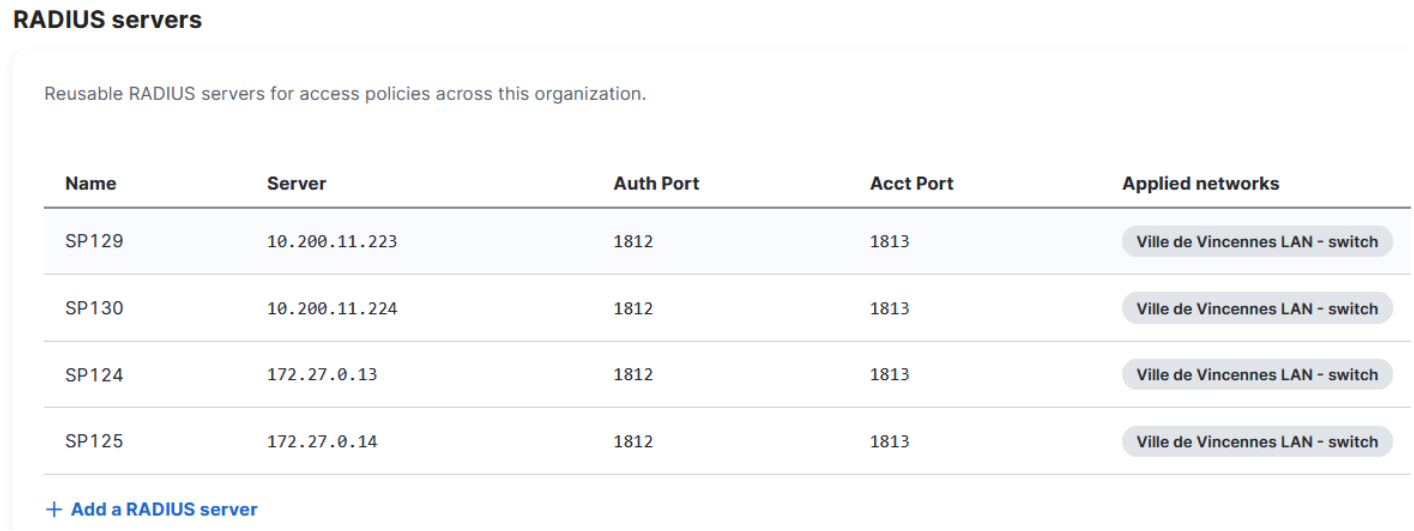


Vue de l’autorisation d’accès depuis l’observateur d’évènement :

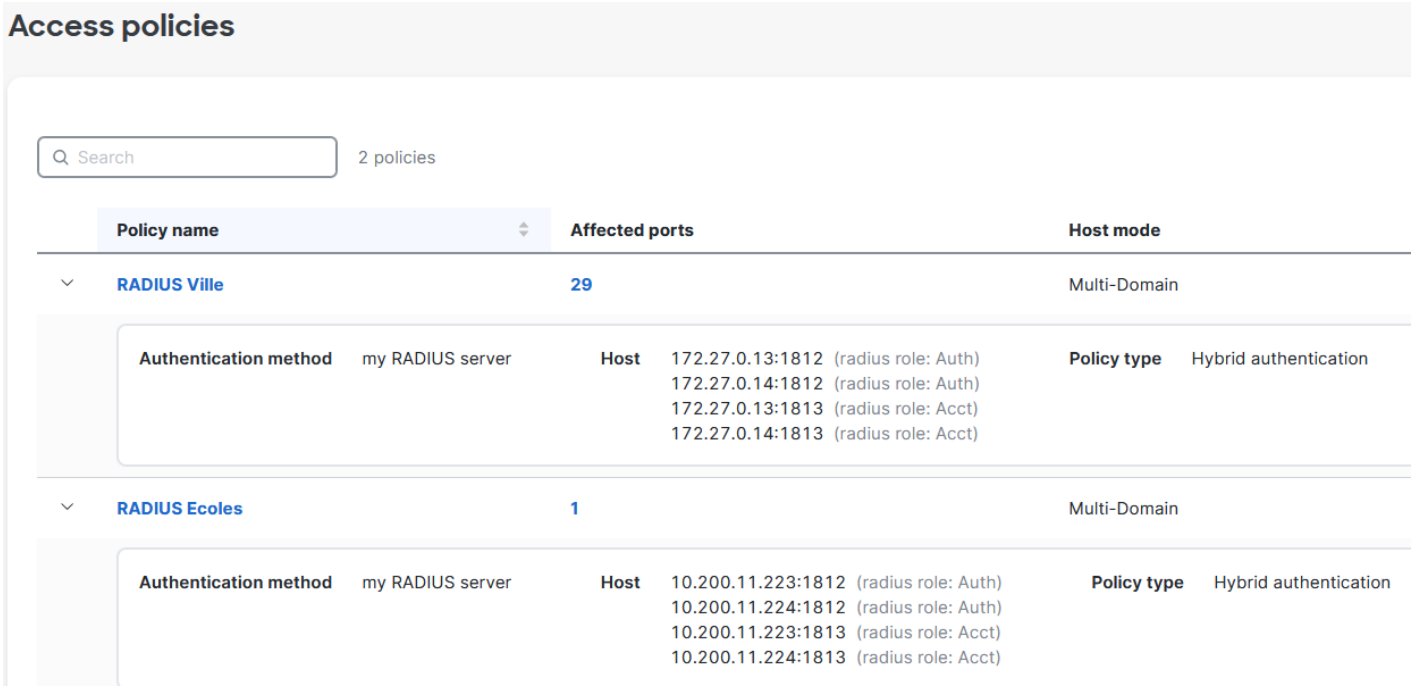


Configuration sur la console web Meraki

Il faut dans un premier temps ajouter les serveurs Radius dans la console via le menu « Organization » puis « Settings »

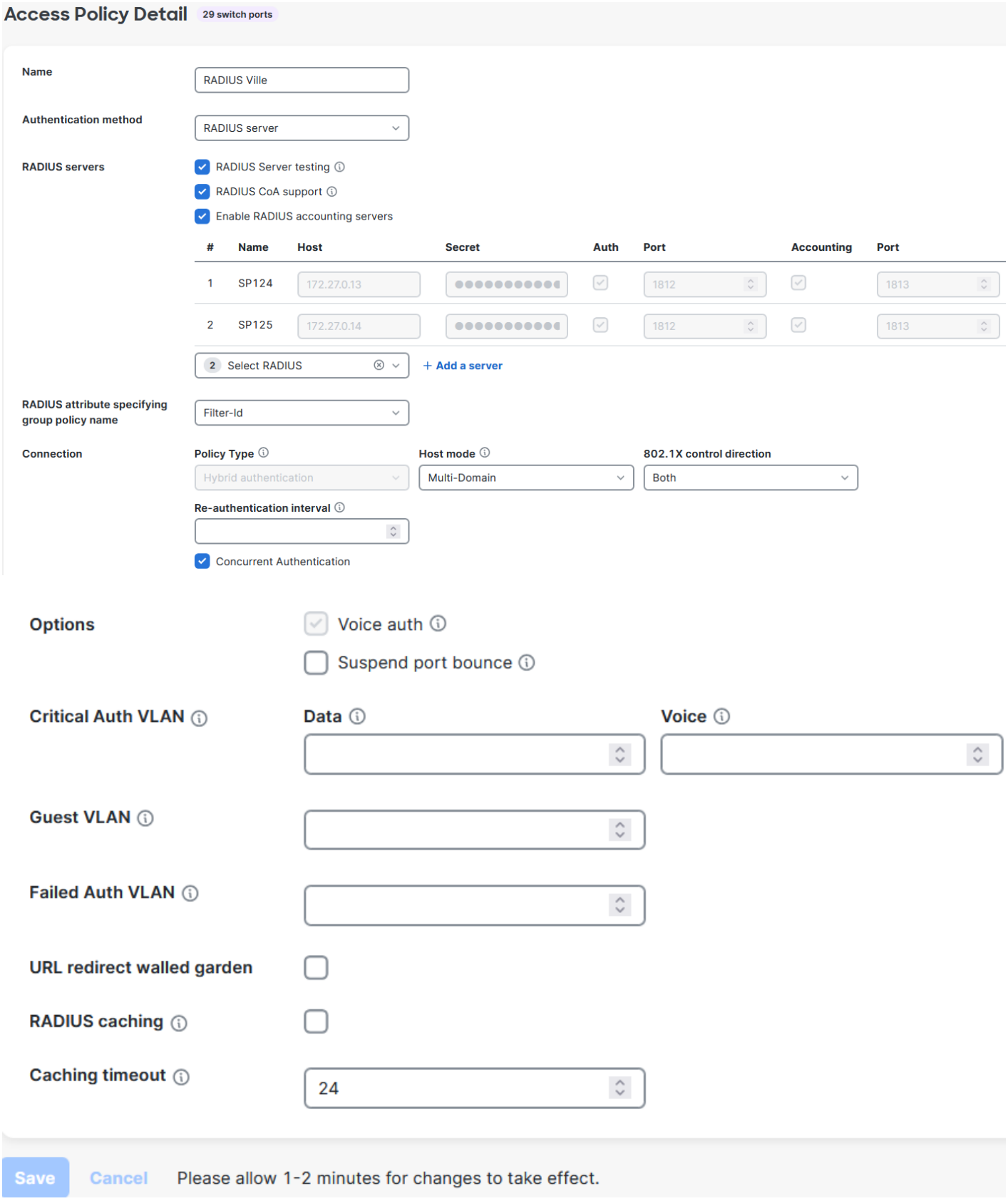


Ensuite il faut ajouter une politique d'accès via le menu « Switching » puis « Access policies »

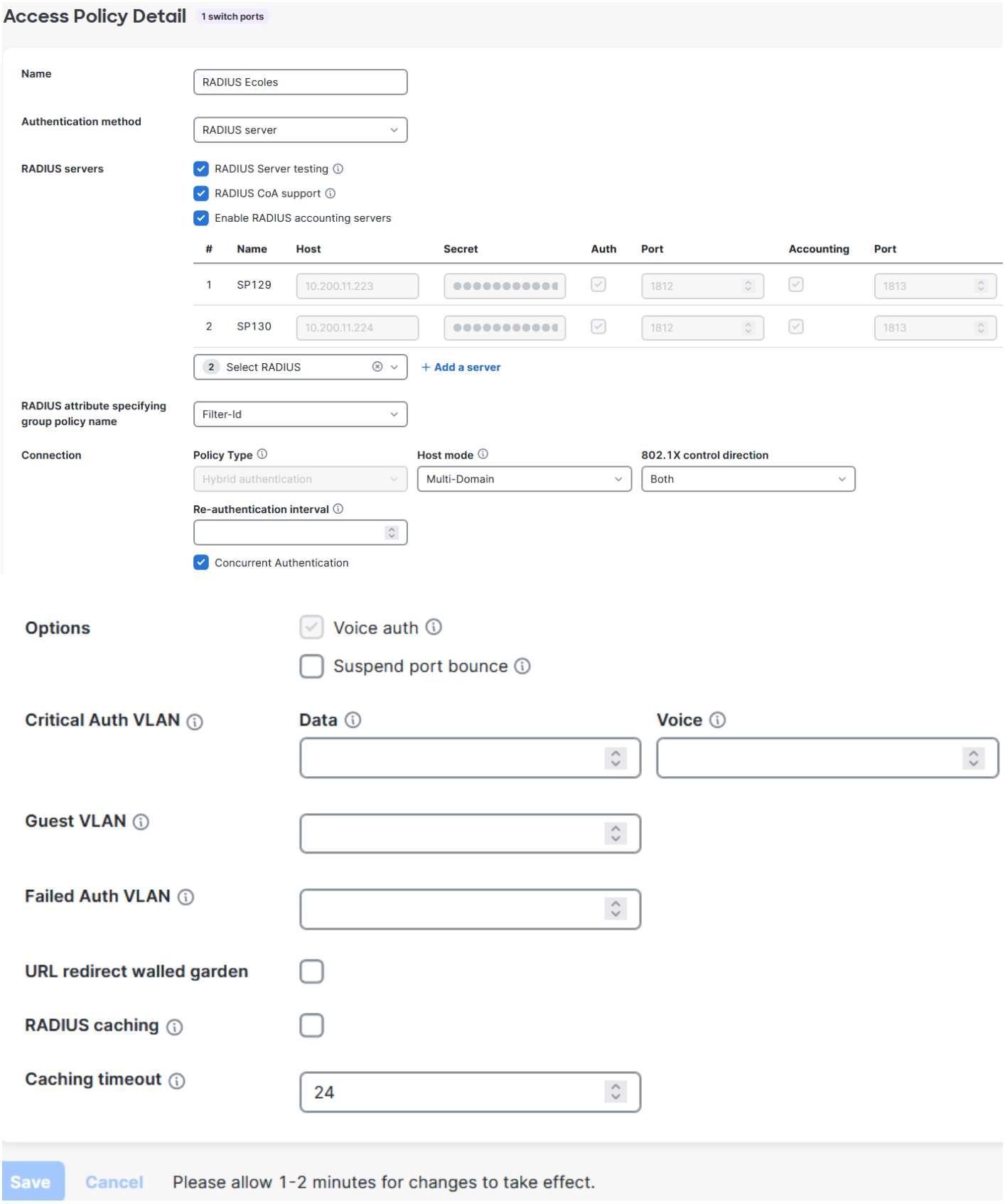


Lorsque l'on clique sur la policy, on rentre dans les détails de celle-ci :

Radius Ville :



Radius Ecoles :



Concernant la partie wireless, nous avons configuré un SSID de test nommé « Test 802.1x » dans le network Ville de Vincennes.

Test 802.1x

enabled

rename

edit settings

802.1X with custom RADIUS

None

unlimited

Local LAN

no

no

111

Disabled

no

n/a

n/a

Access control

SSID

Test 802.1x

Basic info

SSID (name) Test 802.1x

SSID status Enabled Disabled

Hide SSID

Security *WPA1/2 Enterprise with 1 RADIUS server and 1 accounting server*

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate

MAC-based access control (no encryption)
RADIUS server is queried at association time

Enterprise with
my RADIUS server

User credentials are validated with 802.1X at association time

Identity PSK with RADIUS

MAC-based Authentication

RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

Wi-Fi Personal Network (WPN) ⓘ

Enabled | Disabled

WPA encryption ⓘ

WPA1 and WPA2

802.11r is disabled due to RADIUS CoA being enabled

802.11r ⓘ

- Enabled
- Adaptive
- Disabled

802.11w ⓘ

- Enabled (allow unsupported clients)
- Required (reject unsupported clients)
- Disabled (never use)

Traffic from static IP address clients will be blocked on this SSID.

Mandatory DHCP

Enabled | Disabled

Splash page *None*

Not all splash authentication methods are compatible with WPA2-Enterprise authentication

- (•) **None (direct access)**
  Users can access the network as soon as they associate
- ( ) **Click-through**
  Users must view and acknowledge your splash page before being allowed on the network
- ( ) Sponsored guest login
  Guests must enter a valid sponsor and own email address before being allowed on the network
- ( ) Sign-on with
  Meraki Cloud Authentication
  Users must enter a username and password before being allowed on the network
- ( ) Sign-on with SMS Authentication
  Users enter a mobile phone number and receive an authorization code via SMS.
  After a trial period of 25 texts, you will need to connect with your Twilio account on the Network-wide settings page.
- ( ) **Cisco Identity Services Engine (ISE) Authentication**
  Users are redirected to the Cisco ISE web portal for device posturing and guest access
- ( ) **Endpoint management enrollment**
  Only devices enrolled in endpoint management can access this network

RADIUS *1 RADIUS server, 1 accounting server - CoA supported*

RADIUS servers

	#	Host IP	Auth port	Secret	RadSec	Test
⠿	1	172.27.0.13	1812	●●●●●●●●●●●●●	☐	Test

Add server 3 max.

RADIUS accounting servers

	#	Host IP	Acct port	Secret	RadSec
⠿	1	172.27.0.13	1813	●●●●●●●●●●●●●	☐

Add server 3 max.

⚠ Enabling RADIUS CoA disables the fast roaming features PMKsa caching, OKC, and 802.11r

☐ RADIUS testing

☑ RADIUS CoA support

RADIUS attribute specifying group policy name: Filter-Id

Advanced RADIUS settings

(NAS ID, Called-station-ID, DAS clients, EAP timers)

Called-station-ID

#	Category
1	AP MAC address
2	SSID name

Add identifier 4 max.

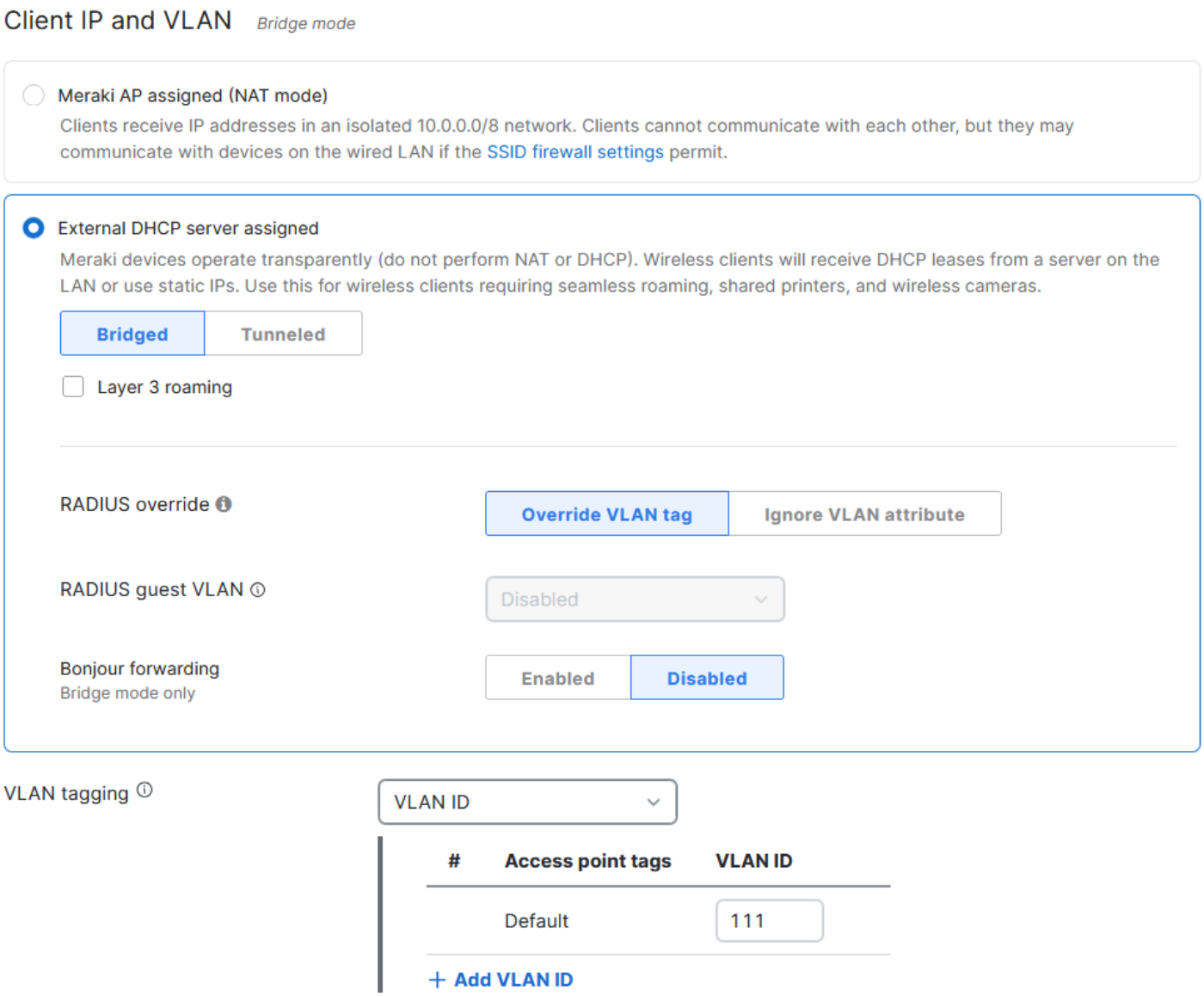
NAS ID

#	Category
1	AP MAC address
2	SSID number

Add identifier 4 max.

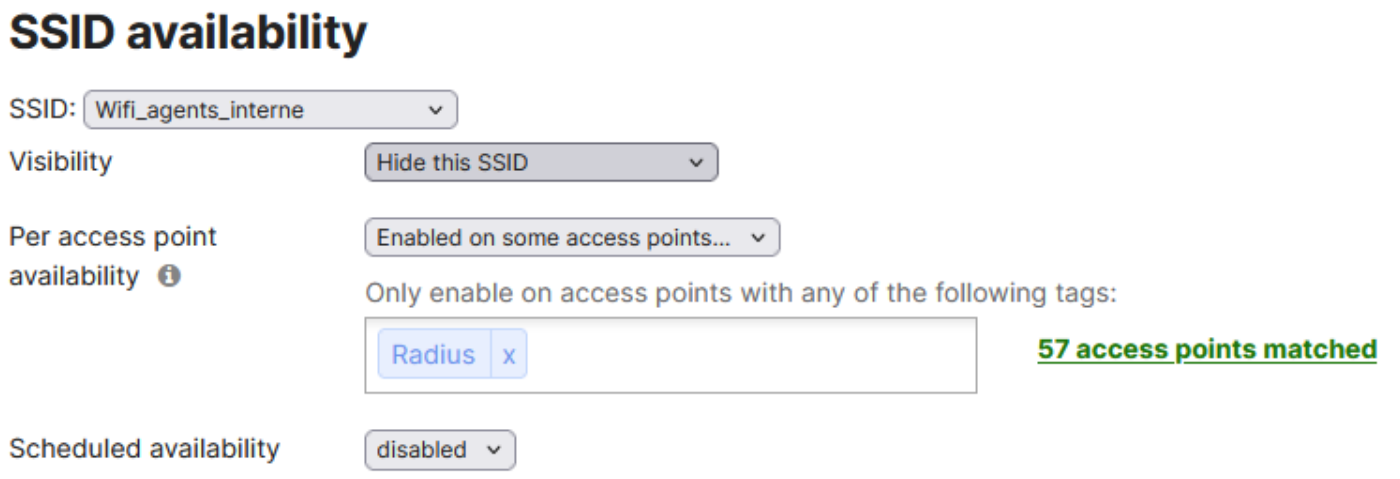
EAP timers

EAP timeout	5	second(s)
EAP max retries	5	time(s)
EAP identity timeout	5	second(s)



Le vlan assigné est le 111 ce qui correspond au wifi publique. Nous avons également pu tester en mettant le vlan 216 ce qui correspond au vlan data et cela fonctionne parfaitement.

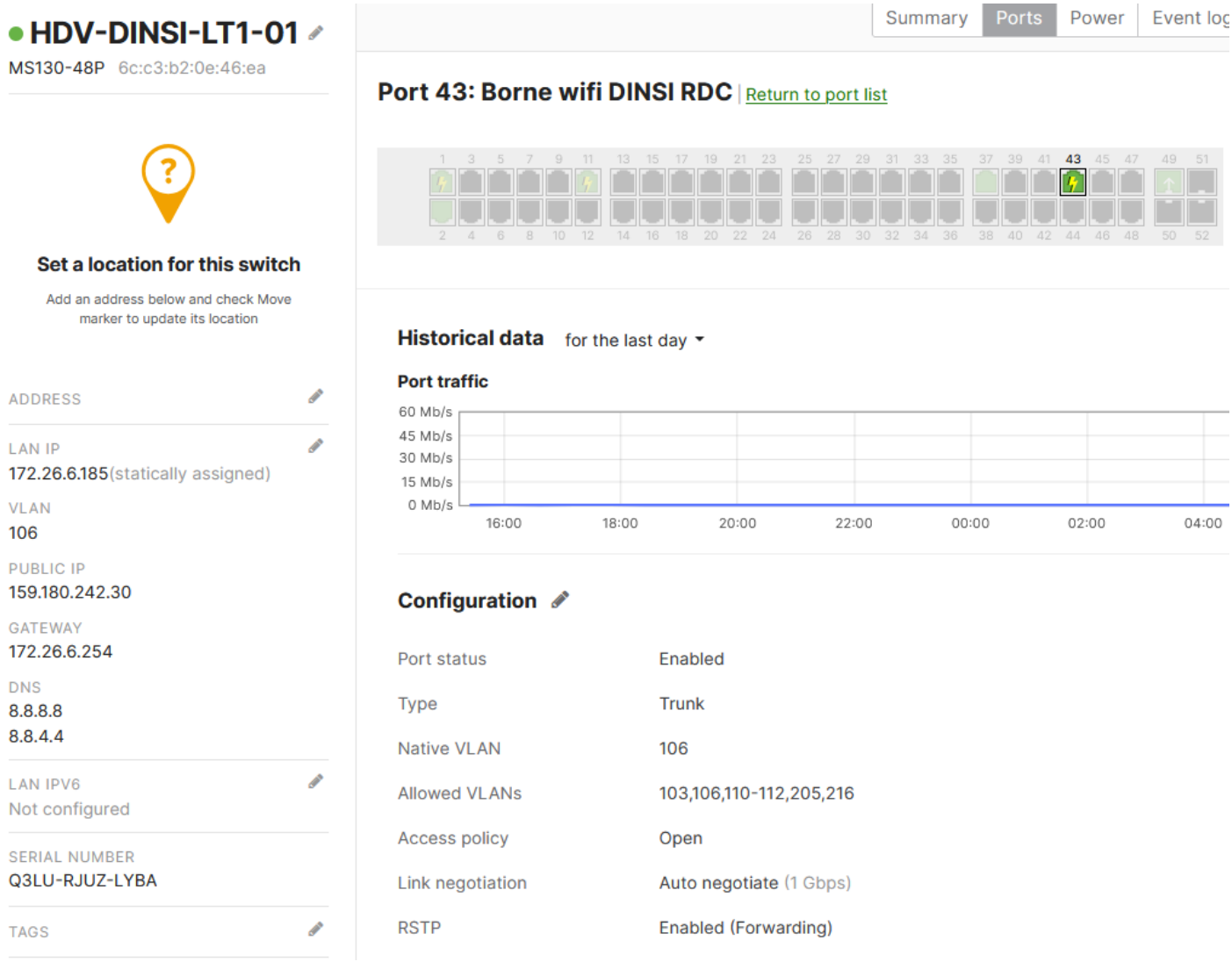
Il faut cependant par ailleurs configurer la borne pour qu'elle accepte la politique radius ce qui a été fait en taggant le SSID (Radius) puis en assignant le TAG au switch sur lequel la borne est connectée ce qui permet sa diffusion.



HDV_DSI_4E	ac:17:c8:04:21:4d	Q2KD-DAH3-B9FY	172.26.6.80	MR42	public Radius HDV
HDV_DSI_RDC	ac:17:c8:04:20:cf	Q2KD-9V23-S32C	172.26.6.81	MR42	public Radius HDV

Ensuite, il faut aller sur le port de connexion de la borne wifi (ici le port 43 du switch que nous avons taggé précédemment) et le configurer avec le vlan correspondant au SSID.

Il faut ensuite ajouter ce vlan sur le port ou est connecté la borne comme cela :



La configuration concernant les ports filaires se font de la manière suivante avec l’Access Policy et le vlan :

L’utilisateur doit absolument être intégré au bon groupe si nous voulons que la stratégie se monte correctement.

Switch / Port	HDV-DINSI-RDC-01 / 23
Name	
Port status	Enabled / Disabled
Link negotiation	Auto negotiate
Port schedule	Unscheduled
Tags	+
Port profile name	
Type	Trunk / Access
Access policy	RADIUS Ville
VLAN	1
Voice VLAN	224

Procedure_Mise_A_Jour_Version_Linux

PROCEDURE MISE A JOUR LINUX

MREMOTENG 2

SNAPSHOT 2

LINUX 4

Update and upgrade 4

Processus de mise à jour 4

VERIFICATION 7

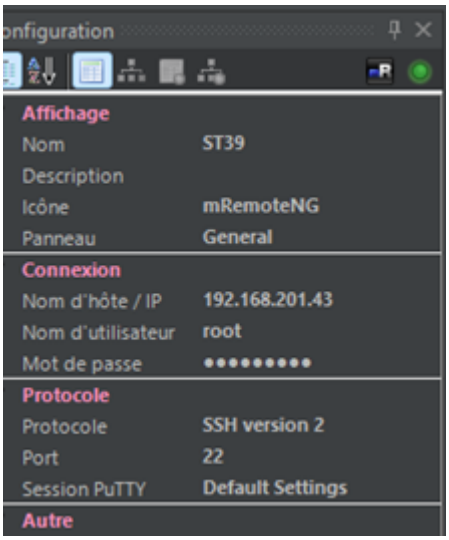
Prérequis :

- Vsphere
- MremoteNG

MREMOTENG

Installer logiciel prise en main en ligne de commande car plus pratique

Renseigner l’host, mot de passe et ID root, changer le protocole en SSH version 2



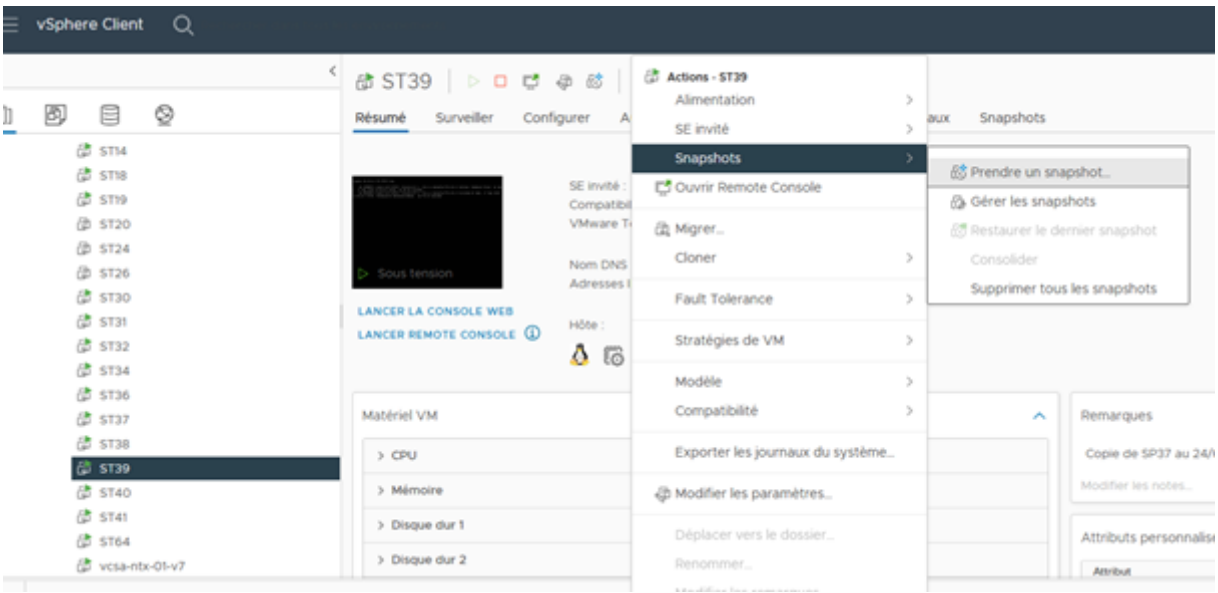
SNAPSHOT

Il est **IMPORTANT** de toujours faire une snapshot avant de commencer la mise à jour du serveur.

Se rendre sur le serveur visé sur vSphere : [Vsphere]

Dans section Inventaire, aller dans Vincennes -> MEDIATHEQUE puis rechercher le serveur.

Cliquer sur **ACTION** >> *Snapshots* >> *prendre un snapshot* >> créer



Par précaution, il est conseillé de s’assurer que la snapshot a bien été prise.

LINUX

Update and upgrade

Se connecter à la VM

Puis faire la commande apt update && apt upgrade –y (update et upgrade du Linux)

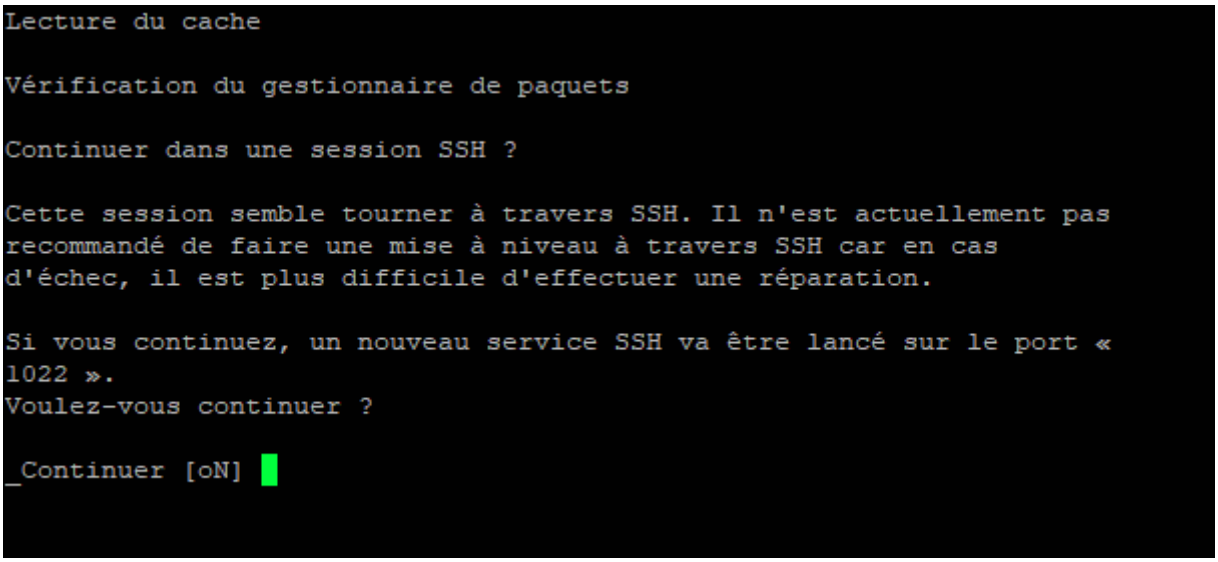
```
Last login: Wed Sep 17 11:52:00 2025 from 10.200.5.27
root@ST39:~# apt update && apt upgrade -y
```

Quand la maj se termine, redémarrer le serveur avec la commande reboot

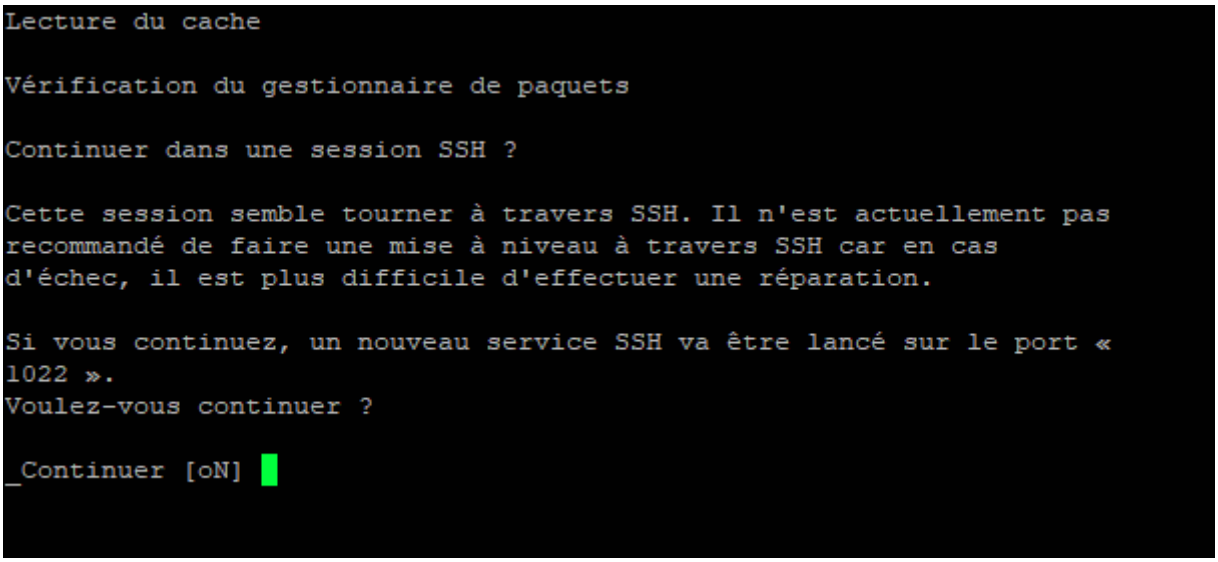
```
Found linux image: /boot/vmlinuz-5.4.0-208-generic
Found initrd image: /boot/initrd.img-5.4.0-208-generic
done
Traitement des actions différées (« triggers ») pour initramfs-tools (0.136ubuntu6.8) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-216-generic
root@ST39:~# reboot
```

Processus de mise à jour

Apres redémarrage, faire un do-release-upgrade pour débuter le processus de l’upgrade de la version.



Faire o (oui) pour continuer



Appuyer entrer continuer mise à jour

```
Lecture du cache

Vérification du gestionnaire de paquets

Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN]
```

Entrée une nouvelle fois

```
Lecture du cache

Vérification du gestionnaire de paquets

Continuer dans une session SSH ?

Cette session semble tourner à travers SSH. Il n'est actuellement pas
recommandé de faire une mise à niveau à travers SSH car en cas
d'échec, il est plus difficile d'effectuer une réparation.

Si vous continuez, un nouveau service SSH va être lancé sur le port «
1022 ».
Voulez-vous continuer ?

_Continuer [oN]
```

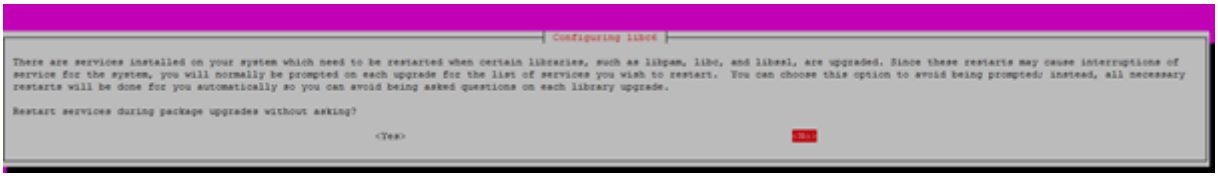
Continuer avec o (oui)

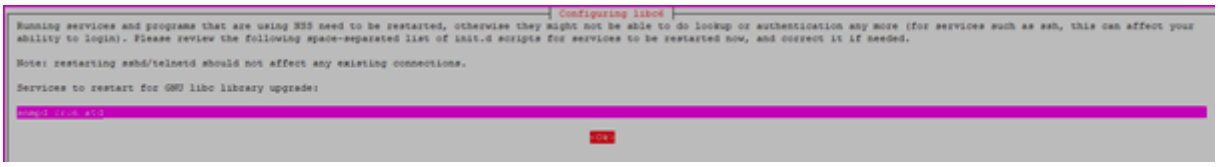
NOTE :

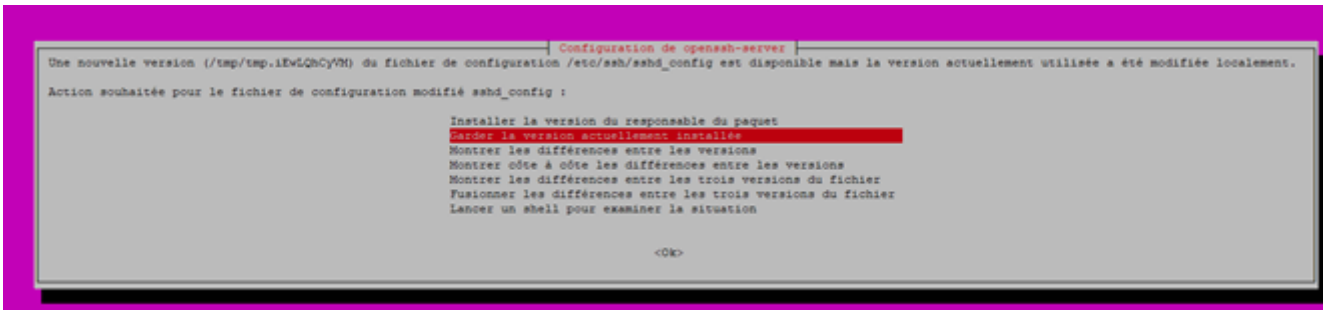
Des pop-ups apparaitront à certains moments en fonction des applications présente dans celle-ci, par précaution, les laisser par défaut.

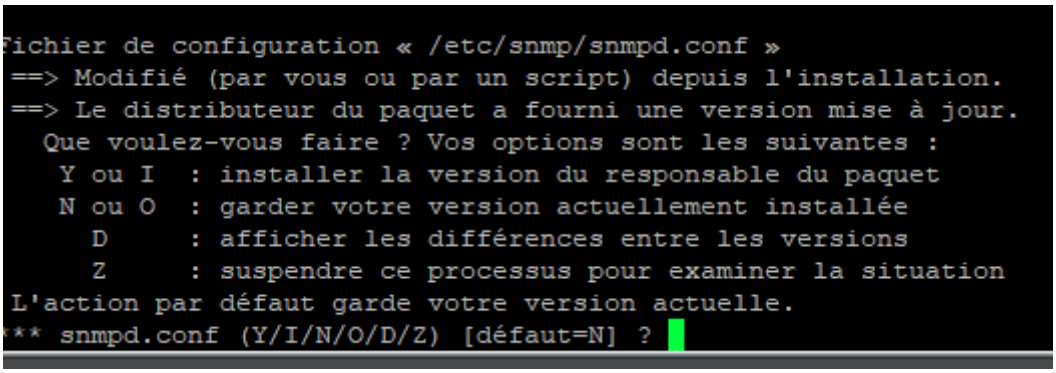
Exemple :

Dire NON en cas de perte de configuration :

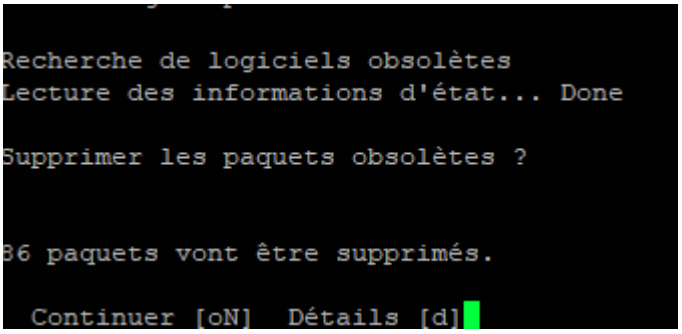




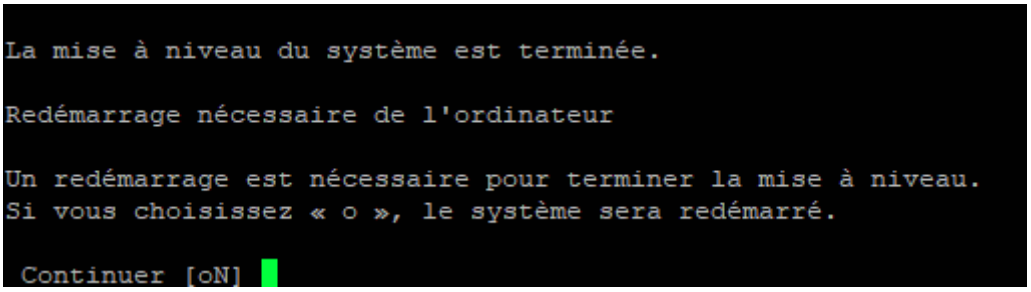




Laisser les fichiers de configuration par ***DEFAUT (N)*** si demandé



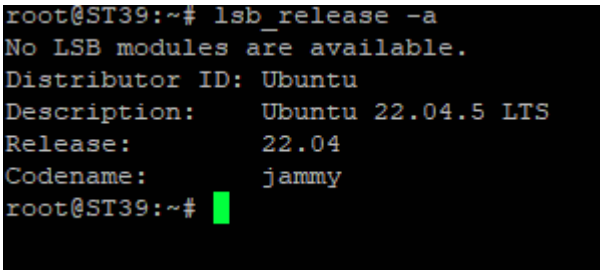
OPTIONNEL mais supprimer les données inutiles, Continuer avec o.



Redémarrage nécessaire, oui (o)

VERIFICATION

Regarder si la version s’est bien appliqué avec la commande lsb_release – a



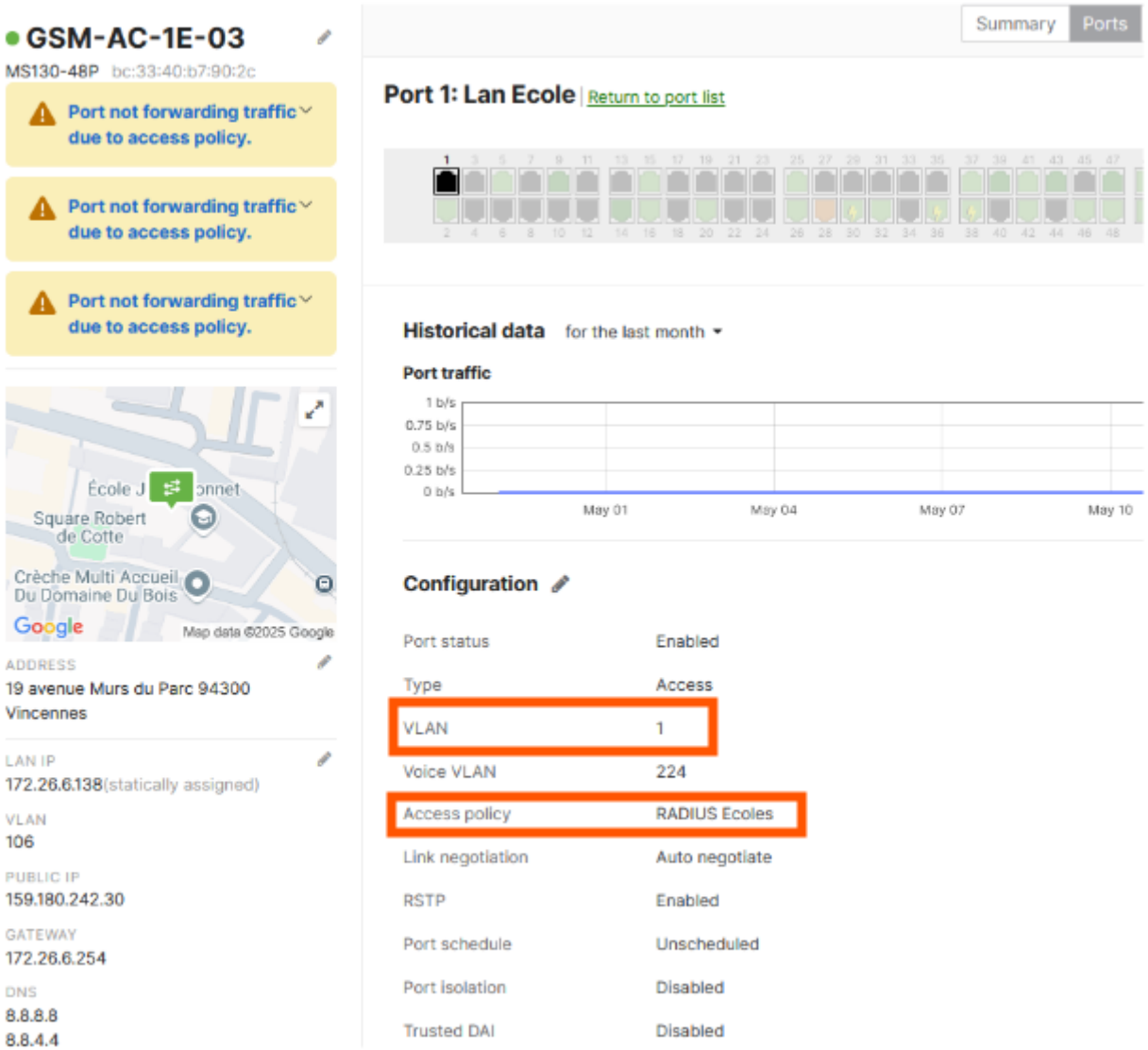
Mise à jour terminé, faire ensuite la même chose sur les prochains serveurs à mettre à jour.

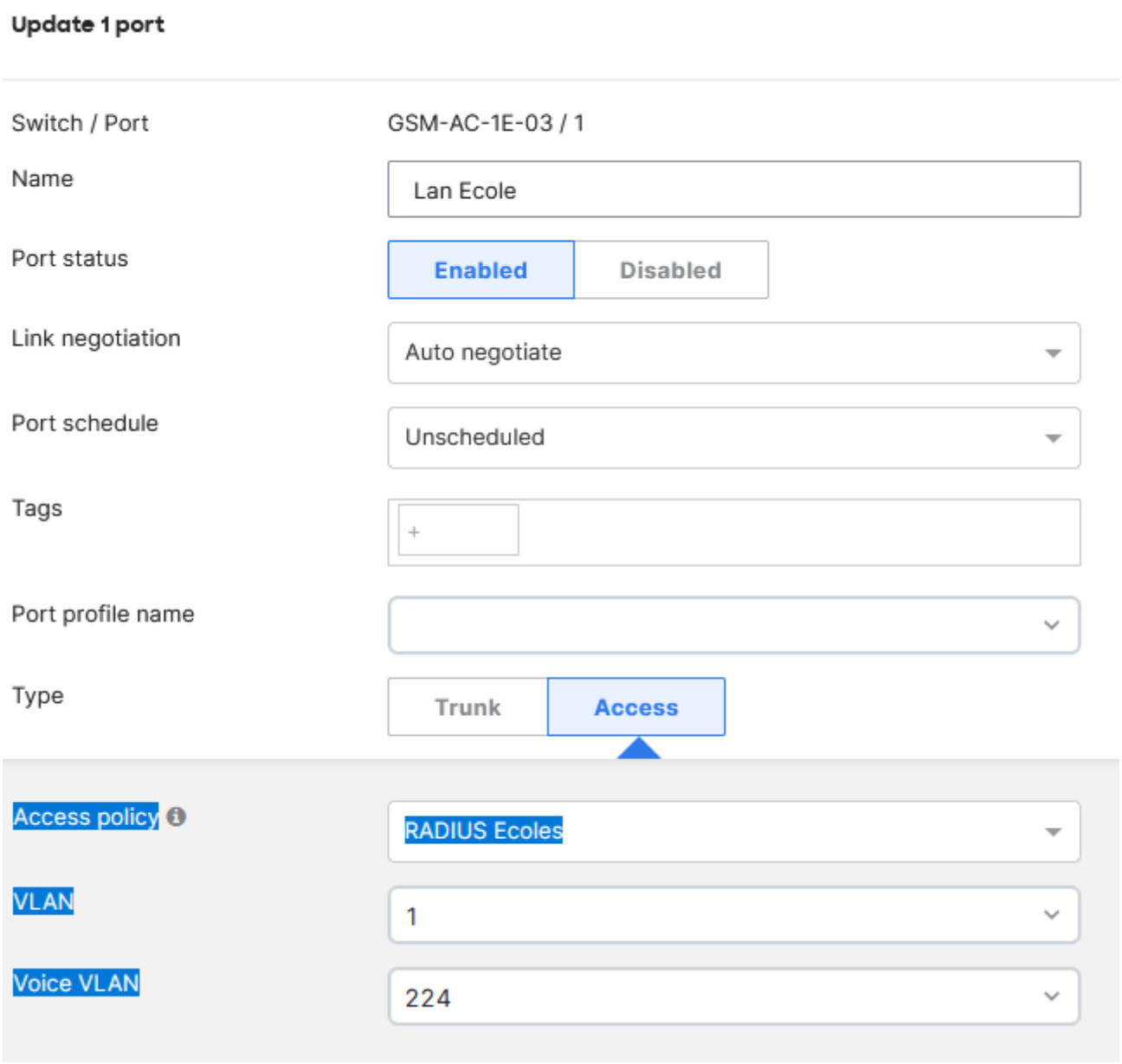
Procedure retour arriere radius

Problème avec radius

En cas de dysfonctionnement lié au serveur radius, il sera peut-être nécessaire de rebasculer en arrière la configuration actuellement en place.

Exemple de configuration sur le port 1 du switch :





Modifier l’entrée « Access Policy » et la mettre sur « Open »

Modifier l’entrée VLAN et mettre l’ID du vlan ecole (210) ou VLAN DATA (216)

Valider