Authentification 802.1X / RADIUS avec attribution dynamique de VLAN

Groupe 3 – RIOCA - Maxime et Souhir

PARTIE 1 – DOCUMENT DE CONFIGURATION

Quand une manip est la même pour plusieurs services ou postes, on montre un seul exemple (la Compta). Les autres ont été faits pareil. Pour les switchs, on montre les deux.

1. Contexte et étude préalable

Maintenant chaque utilisateur doit se connecter avec son compte AD avant d'avoir le réseau. Il arrive tout seul dans le VLAN de son service, peu importe le port ou l'étage.

1.1 Problématique

- Avant, le VLAN dépendait du port. Si un salarié changeait de bureau ou d'étage, il se retrouvait dans le réseau d'un autre service.
- N'importe quel appareil branché sur une prise avait accès au réseau, sans aucun contrôle.

1.2 Principe de la solution : 802.1X avec RADIUS

Rôle 802.1X	Équipement	Fonction
Supplicant	Poste client Windows	Envoie l'identité de l'utilisateur ou du PC (EAP)
Authentificateur	Switchs SWRDC et SW1ER	Bloque le port et fait passer les messages vers le RADIUS
Serveur d'authentification	NPS sur srv-ad-rioca	Vérifie le compte dans l'AD, choisit la stratégie et renvoie le VLAN

Comment se passe une connexion :

1. Quand on branche le PC, le port est bloqué. Seuls les messages d'authentification (EAPOL) passent.
2. Le PC s'authentifie en PEAP. Un tunnel TLS est créé avec le certificat du serveur, puis le mot de passe est vérifié en EAP-MSCHAP v2.
3. Le switch envoie tout ça au serveur NPS en RADIUS (UDP 1812).
4. Le NPS vérifie le compte dans l'AD et prend la première stratégie réseau qui correspond au groupe.
5. Le NPS répond Access-Accept avec 3 attributs : Tunnel-Type = VLAN, Tunnel-Medium-Type = 802 et Tunnel-Pvt-Group-ID = numéro du VLAN.
6. Le switch ouvre le port dans ce VLAN et le PC récupère son IP en DHCP.

Le port ne s'ouvre qu'après l'accord du serveur NPS



Avant l'accord de NPS, seul le trafic EAPOL traverse le port.

Échange 802.1X entre les 3 acteurs

Le switch ne décide rien, il fait juste passer les messages. C'est le NPS qui accepte ou refuse et qui donne le VLAN.

1.3 Moyens mis en œuvre

Élément	Détail
Serveur	srv-ad-rioca (172.19.100.2), Windows Server 2025 sur Hyper-V : AD DS, DNS, AD CS (autorité de certification d'entreprise racine) et NPS
Switch rez-de-chaussée	SWRDC, Cisco Catalyst 2960-Plus, IOS 15.2, 172.19.70.2
Switch 1er étage	SW_1ER_GRP3, Cisco Catalyst 2960-X (WS-C2960X-24TS-L), IOS 15.2, 172.19.70.3
Cœur de réseau	SwCoeur (Catalyst 3650) : routage inter-VLAN, passerelles en .254
Postes	Windows 10/11 joints au domaine RIOCA.LOCAL

On n'a rien acheté : on a utilisé les rôles de Windows Server et les switchs qu'on avait déjà.

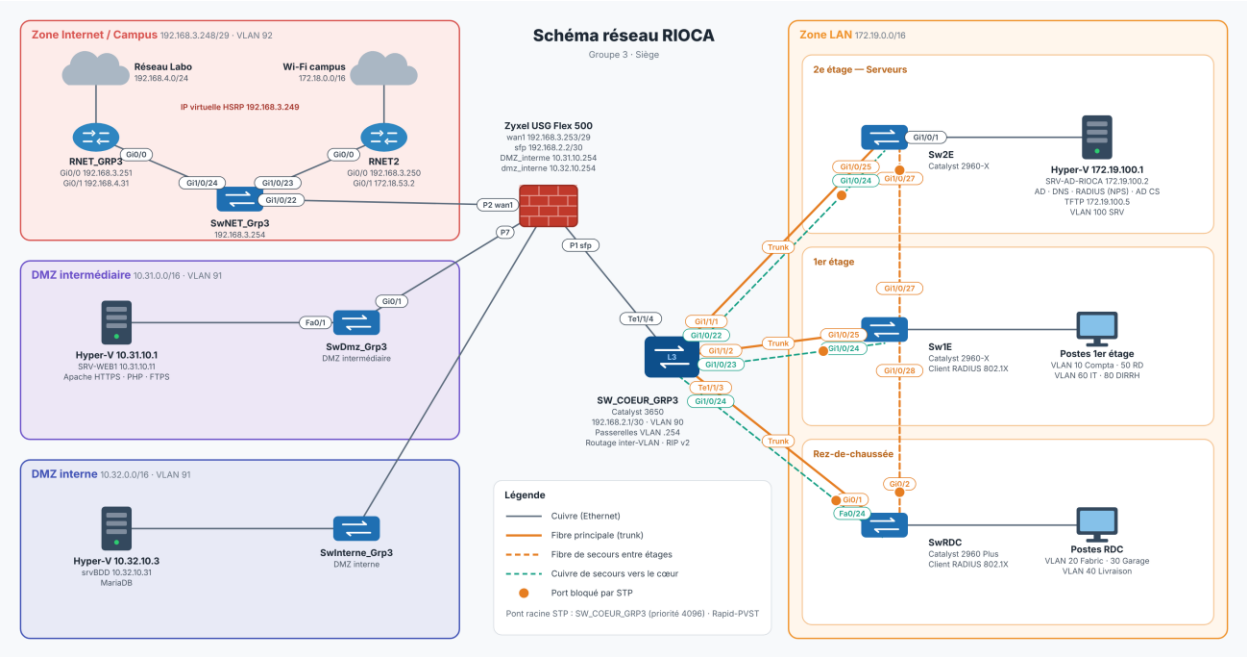
1.4 Impact sur l'infrastructure existante

- Les ports restent fermés tant que l'utilisateur n'est pas authentifié. Un PC qui n'est pas configuré en 802.1X n'a plus du tout accès au réseau.
- Le VLAN mis sur chaque port devient juste un VLAN par défaut. Le vrai VLAN est donné par le NPS selon le groupe AD.
- Tous les VLAN utilisateurs doivent exister sur les deux switchs, sinon la mobilité ne marche pas.
- Si le serveur NPS est en panne, plus personne ne peut se connecter (voir les améliorations).
- Le SSH sur les switchs marche toujours avec le compte local, même sans RADIUS.
- On n'a pas touché au routage inter-VLAN, au DHCP ni aux trunks.

2. Architecture

Le serveur srv-ad-rioca a maintenant 4 rôles : AD DS, DNS, AD CS et NPS (RADIUS). Les deux switchs sont ses clients RADIUS.

2.1 Schéma réseau mis à jour



2.2 Équipements concernés

Équipement	Rôle dans la solution	Adresse IP	VLAN
srv-ad-rioca	Serveur RADIUS (NPS), AD DS, DNS, AD CS	172.19.100.2/24	100 (SRV)
SWRDC	Client RADIUS, authentificateur 802.1X	172.19.70.2/24	70 (ADM)
SW_1ER_GRP3	Client RADIUS, authentificateur 802.1X	172.19.70.3/24	70 (ADM)
SwCoeur	Routage inter-VLAN, passerelles	172.19.X.254/24	Tous

Flux en plus : RADIUS en UDP 1812 (authentification) et UDP 1813 (comptabilisation), des switchs vers 172.19.100.2.

2.3 Correspondance groupes AD et VLAN

Service	Groupe AD	VLAN	Réseau	Passerelle
Comptabilité – Paie	COMPTA	10 (compta)	172.19.10.0/24	172.19.10.254
Atelier de fabrication	FABRIC	20 (Fabric)	172.19.20.0/24	172.19.20.254
Garage	GARAGE	30 (GARAGE)	172.19.30.0/24	172.19.30.254
Livraison	LIVR	40 (LIVR)	172.19.40.0/24	172.19.40.254
Recherche & Développement	RD	50 (RD)	172.19.50.0/24	172.19.50.254
Infrastructure & Système	IT	60 (IT)	172.19.60.0/24	172.19.60.254

Service	Groupe AD	VLAN	Réseau	Passerelle
Direction & Ressources humaines	DIRRH	80 (DIRRH)	172.19.80.0/24	172.19.80.254

Les VLAN 70 (ADM) et 100 (SRV) ne sont jamais donnés par le NPS.

2.4 VLAN par défaut des ports d'accès

Switch	Ports	VLAN par défaut	Remarque
SWRDC	Fa0/1 à Fa0/8	20	802.1X actif
SWRDC	Fa0/9 à Fa0/18	30	802.1X actif
SWRDC	Fa0/19 à Fa0/23	40	802.1X actif
SWRDC	Gi0/1	Trunk	Lien vers SwCoeur, sans 802.1X
SW1ER	Gi1/0/1 à Gi1/0/4	10	802.1X actif
SW1ER	Gi1/0/5 à Gi1/0/9	50	802.1X actif
SW1ER	Gi1/0/10 à Gi1/0/14	60	802.1X actif
SW1ER	Gi1/0/15 à Gi1/0/19	80	802.1X actif
SW1ER	Gi1/0/25	Trunk	Lien vers SwCoeur, sans 802.1X

Les autres ports sont éteints (shutdown). Le VLAN par défaut sert seulement si le NPS accepte quelqu'un sans renvoyer de VLAN.

3. Configuration du serveur srv-ad-rioca

Sur le serveur on a l'autorité de certification, qui sert pour PEAP, et le NPS, qui décide de l'accès et du VLAN.

3.1 Autorité de certification (AD CS)

- Rôle AD CS installé en autorité de certification d'entreprise racine.
- On a fait un certificat ordinateur pour srv-ad-rioca avec le modèle « Contrôleur de domaine », dans la console mmc (Ordinateur local > Personnel).
- Ce certificat sert à authentifier le serveur. Il est envoyé aux PC quand le tunnel PEAP s'ouvre.
- Les PC du domaine font confiance à notre autorité tout seuls, car elle est publiée dans l'AD.

3.2 Installation de NPS

- Installation du rôle « Services de stratégie et d'accès réseau ».
- On a inscrit le NPS dans l'AD (clic droit sur NPS (Local) > Inscrire un serveur dans Active Directory) pour qu'il puisse lire les comptes.
- Ouverture des ports RADIUS dans le pare-feu Windows :

```
New-NetFirewallRule -DisplayName "RADIUS Authentification" -Direction Inbound -
Protocol UDP -LocalPort 1812 -Action Allow
New-NetFirewallRule -DisplayName "RADIUS Comptabilisation" -Direction Inbound -
Protocol UDP -LocalPort 1813 -Action Allow
```

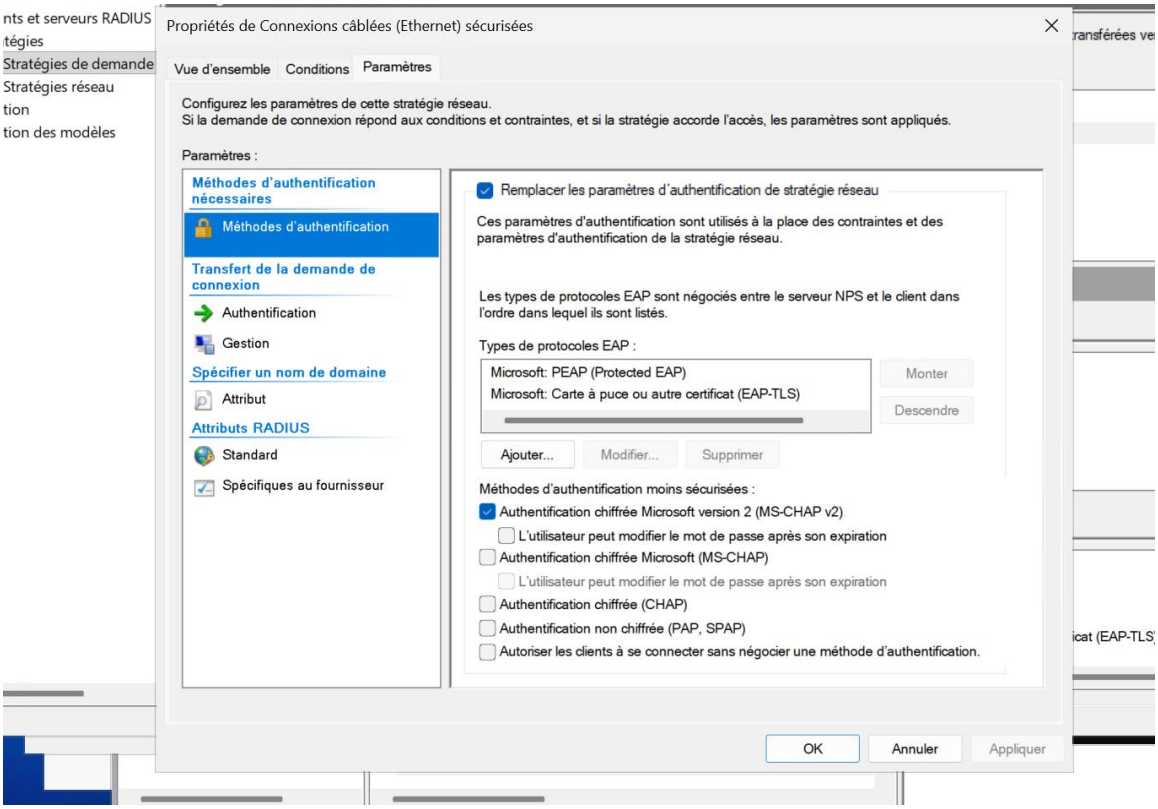
3.3 Clients RADIUS

Nom convivial	Adresse IP	Secret partagé
switchRDC	172.19.70.2	Voir le document des comptes
SW1ER	172.19.70.3	Voir le document des comptes

Il faut mettre l'IP du switch dans le VLAN 70. Si la requête vient d'une autre IP, le NPS l'ignore.

3.4 Stratégie de demande de connexion

- Stratégie « Connexions câblées (Ethernet) sécurisées », faite avec l'assistant « Connexions filaires 802.1X sécurisées ».
- Condition : type de port NAS = Ethernet.
- Les demandes sont traitées par ce serveur.
- Méthodes d'authentification : on a coché « Remplacer les paramètres d'authentification de stratégie réseau ». Comme ça les méthodes sont réglées une seule fois ici, pour toutes les stratégies.
- Types EAP dans l'ordre : Microsoft: PEAP en premier (certificat de srv-ad-rioca, méthode interne EAP-MSCHAP v2), puis Microsoft: Carte à puce ou autre certificat (EAP-TLS, en secours, voir 5.4).
- On a aussi coché MS-CHAP v2 dans les méthodes moins sécurisées.



3.5 Stratégies réseau

Le NPS lit les stratégies dans l'ordre et prend la première qui correspond. Il faut donc mettre nos stratégies avant les deux stratégies par défaut, qui refusent tout. Entre nos stratégies l'ordre ne change rien, car chaque utilisateur est dans un seul groupe.

Ordre	Stratégie	Groupe en condition	Accès	VLAN renvoyé
1	Compta	RIOCA\COMPTA	Accorder	10
2	IT	RIOCA\IT	Accorder	60
3	Fabric	RIOCA\FABRIC	Accorder	20
4	Ordinateurs_Domaine	RIOCA\Ordinateurs du domaine (Groupes Windows)	Accorder	60
5	Garage	RIOCA\GARAGE	Accorder	30
6	LIVR	RIOCA\LIVR	Accorder	40
7	RD	RIOCA\RD	Accorder	50
8	DIRRH	RIOCA\DIRRH	Accorder	80
9	Connexions au serveur Microsoft de Routage et Accès distants	Serveur d'accès Microsoft	Refuser	–
10	Connexions à d'autres serveurs d'accès	Toutes les demandes	Refuser	–

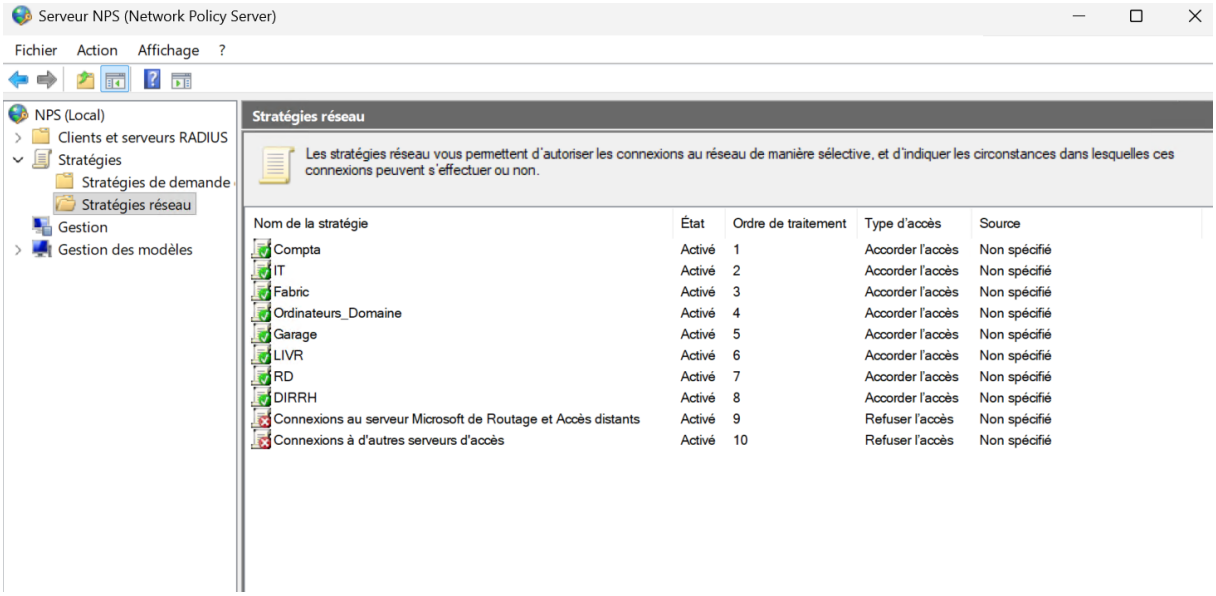
La stratégie Ordinateurs_Domaine authentifie le PC lui-même avant l'ouverture de session. Elle sert pour EAP-TLS (5.4). En PEAP mode utilisateur, c'est seulement le compte de l'utilisateur qui est envoyé.

Réglages pareils pour chaque stratégie de service :

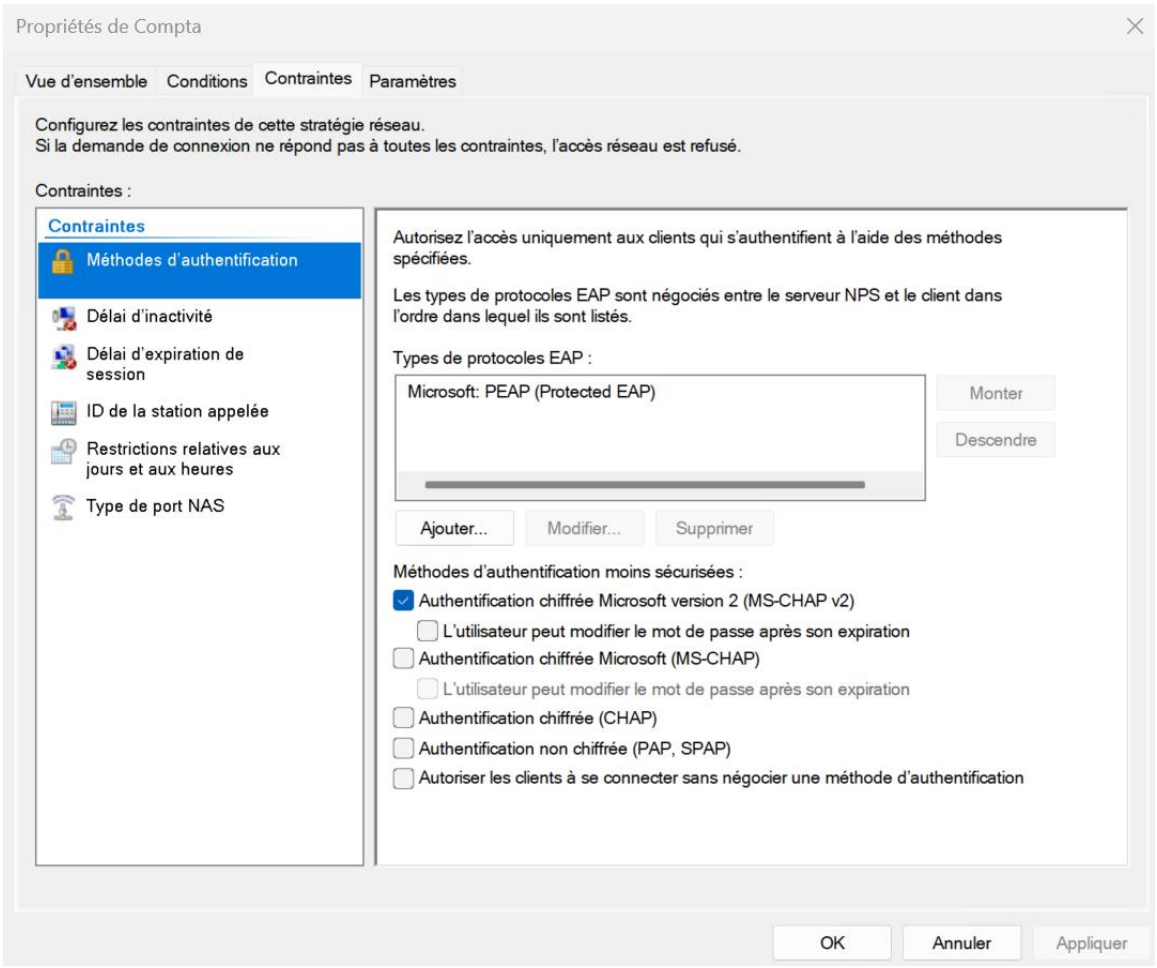
- **Vue d'ensemble** : stratégie activée, « Accorder l'accès », type de serveur d'accès réseau = Non spécifié.
- **Conditions : Groupes d'utilisateurs = le groupe du service.**
- **Contraintes : type de port NAS = Ethernet. Les méthodes sont dans la stratégie de demande de connexion (3.4).**
- **Paramètres > Attributs RADIUS > Standard** :

Attribut	Valeur
Tunnel-Medium-Type	802 (inclut tous les médias 802 et le format canonique Ethernet)
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Pvt-Group-ID	Numéro du VLAN du service (10, 20, 30…)

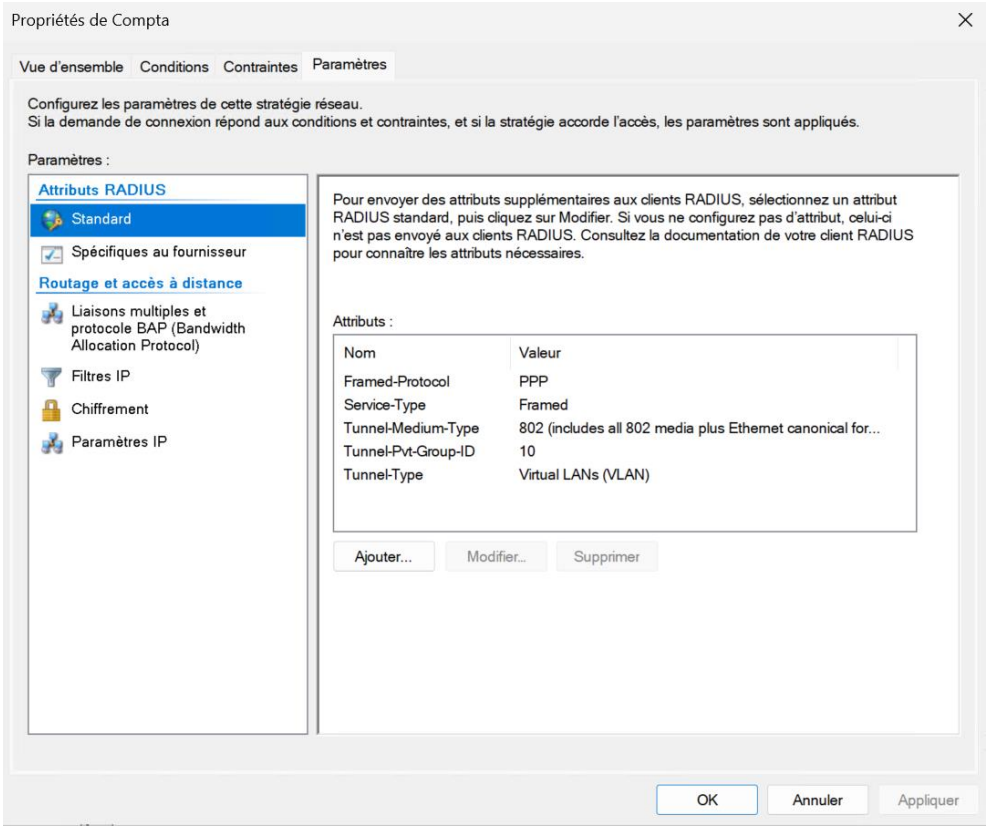
On montre seulement la stratégie Compta. Les autres sont pareilles, il n'y a que le groupe et le VLAN qui changent.



Contraintes de la stratégie Compta :



Paramètres de la stratégie Compta : le VLAN 10 est renvoyé avec Tunnel-Pvt-Group-ID.



3.6 Comptes utilisateurs

- Chaque utilisateur est dans le groupe de sécurité de son service. Le NPS regarde les groupes, pas les OU.
- Onglet « Appel entrant » du compte : « Contrôler l'accès via la stratégie réseau NPS » (c'est la valeur par défaut).

Exemple : le groupe COMPTA avec le compte deniz. Les autres services sont faits pareil.

4. Configuration des switchs SWRDC et SW1ER

Les deux switchs ont la même config globale, il n'y a que les ports qui changent. Les trunks vers le SwCoeur n'ont pas de 802.1X.

4.1 Configuration globale (identique sur les deux switchs)

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa session-id common
dot1x system-auth-control
!
radius server serveur-nps
 address ipv4 172.19.100.2 auth-port 1812 acct-port 1813
 key <secret partagé>
```

4.2 Ports d'accès du SWRDC

```
interface range FastEthernet0/1 - 24
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
```

4.3 Ports d'accès du SW1ER

```
interface range GigabitEthernet1/0/1 - 19
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
```

On a gardé les switchport access vlan qui étaient déjà sur les ports. Ils servent de VLAN par défaut (voir 2.4).

4.4 Rôle de chaque commande

Commande	Rôle
`aaa new-model`	Active le modèle AAA du switch
`aaa authentication login default local`	Connexion console et SSH avec le compte local admin-it, sans RADIUS
`aaa authorization exec default local`	Donne le privilège 15 du compte local : on arrive direct en mode enable
`aaa authentication dot1x default group radius`	Envoie les authentifications 802.1X au serveur RADIUS
`aaa authorization network default group radius`	Le switch peut appliquer ce que renvoie le NPS, dont le VLAN
`aaa session-id common`	Même numéro de session pour tous les échanges AAA
`dot1x system-auth-control`	Active le 802.1X sur l'ensemble du switch
`radius server serveur-nps`	Déclare le serveur NPS, ses ports et le secret
`authentication port-control auto`	Le port reste fermé tant que l'authentification n'a pas marché
`dot1x pae authenticator`	Le port joue le rôle d'authentificateur (obligatoire en IOS 15)
`dot1x timeout tx-period 10`	Redemande l'identité du PC toutes les 10 s au lieu de 30 s

Commande	Rôle
`spanning-tree portfast`	Le port passe direct en transmission, sans attendre le spanning-tree

5. Configuration des postes clients

Chaque PC Windows doit être configuré en supplicant, sinon il reste bloqué sur le port. C'est la même config sur tous les PC, on en montre un.

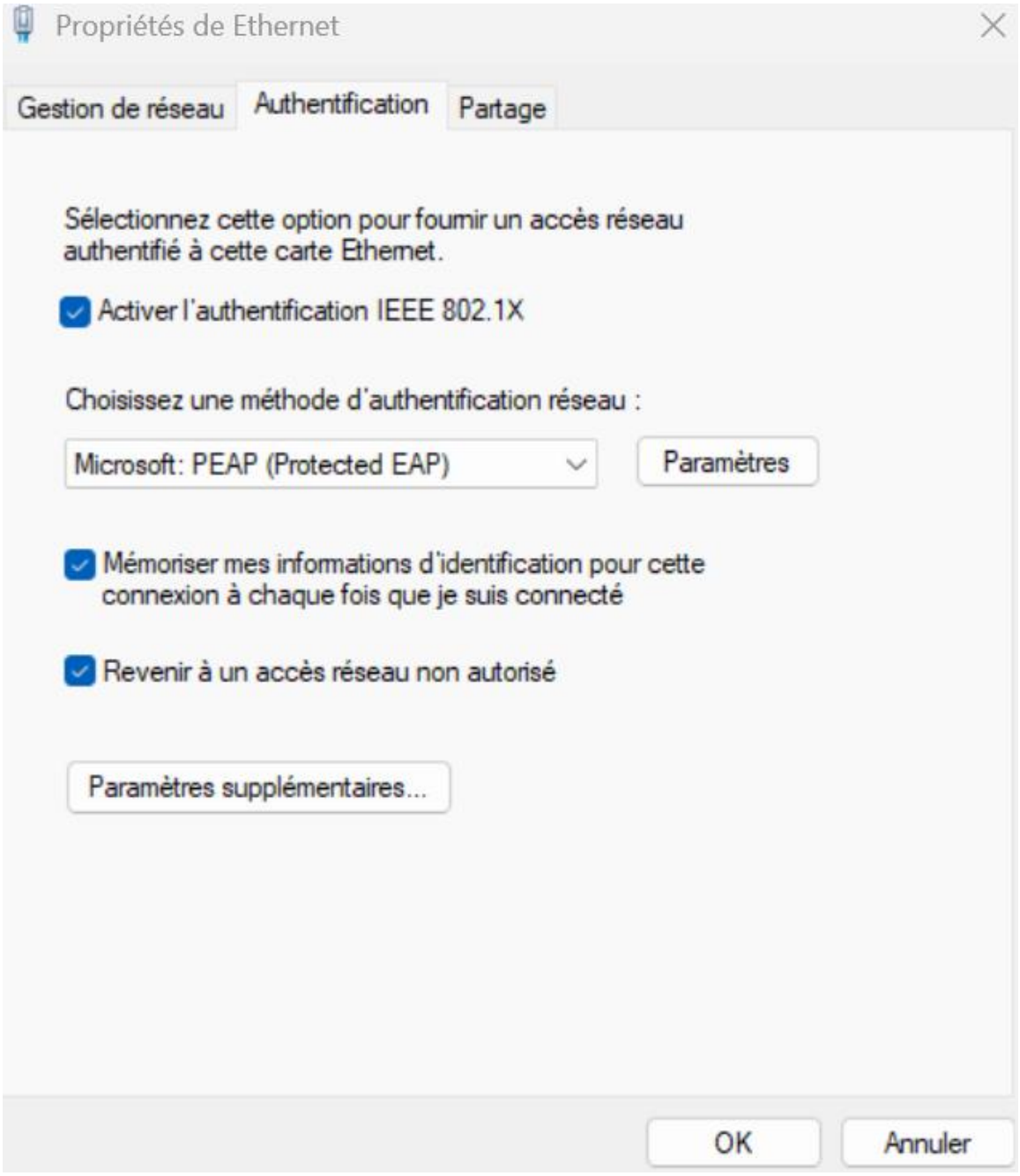
5.1 Service d'authentification filaire

Le service « Configuration automatique de réseau câblé » (dot3svc) est désactivé de base. On l'a mis en automatique et démarré.

```
Set-Service dot3svc -StartupType Automatic
Start-Service dot3svc
```

5.2 Paramètres de la carte Ethernet (onglet Authentification)

Paramètre	Valeur
Authentification IEEE 802.1X	Activée
Méthode d'authentification	Microsoft: PEAP (Protected EAP)
Méthode interne PEAP	EAP-MSCHAP v2, « Utiliser automatiquement mon nom et mot de passe Windows » décoché (voir anomalie A14)
Mode d'authentification (paramètres supplémentaires)	Authentification utilisateur
Mémoriser mes informations d'identification	Coché : la première fois, l'utilisateur tape RIOCA\compte et son mot de passe. C'est gardé seulement pour sa session Windows
Vérifier l'identité du serveur en validant le certificat	Décoché pendant les tests. À recocher avec RIOCA-SRV-AD-RIOCA-CA (voir améliorations)
Réseaux locaux virtuels distincts	Non coché : c'est le switch qui gère le VLAN, pas le PC



Résultat : sur n'importe quel PC, chaque utilisateur arrive dans le VLAN de son service avec son propre compte. La première fois sur un PC, il doit taper son identifiant et son mot de passe.

5.3 Poste hors domaine (PC personnel)

Un PC hors domaine ne connaît pas notre autorité de certification ni les comptes AD. Il faut faire des réglages en plus.

Paramètre	Valeur
Vérifier l'identité du serveur en validant le	Décoché car le PC ne connaît pas notre autorité. Le

Paramètre	Valeur
certificat	mieux : importer le certificat racine RIOCA et laisser coché
Activer la confidentialité de l'identité	Décoché : le NPS doit recevoir le vrai nom du compte
EAP-MSCHAP v2 > Utiliser automatiquement mon nom et mot de passe Windows	Décoché : le compte Windows local n'existe pas dans l'AD
Mode d'authentification	Authentification utilisateur, avec RIOCA\compte enregistré
Compte utilisé	Un compte nominatif d'un service, jamais l'admin du domaine

5.4 Solution de secours : EAP-TLS par certificats

Si PEAP ne marche pas, on a aussi configuré et testé l'authentification par certificat (T9). Aucun mot de passe n'est envoyé et le PC a le réseau dès l'écran de connexion.

- AD CS : deux modèles copiés. RIOCA_Ordinateur_8021X (copie de « Ordinateur », inscription auto pour Ordinateurs du domaine) et RIOCA_Utilisateur_8021X (copie de « Utilisateur », sans l'e-mail dans le sujet, inscription auto pour Utilisateurs du domaine). Les deux sont publiés sur RIOCA-SRV-AD-RIOCA-CA.
- GPO GPO_AutoEnroll_Certificats liée au domaine : « Client des services de certificats - Inscription automatique » activé côté ordinateur et côté utilisateur.
- NPS : EAP-TLS ajouté dans la stratégie de demande de connexion (3.4), et stratégie Ordinateurs_Domaine (VLAN 60) pour le PC.
- PC : méthode « Microsoft: Carte à puce ou autre certificat », « Utiliser un certificat sur cet ordinateur », mode « Authentification utilisateur ou ordinateur ».

Limite : un nouvel utilisateur doit d'abord récupérer son certificat depuis un PC déjà connecté au réseau.

6. Améliorations possibles

Le gros point faible, c'est qu'on a un seul serveur NPS. S'il tombe, plus personne ne peut se connecter.

Amélioration	Intérêt
Second serveur NPS, déclaré comme deuxième serveur RADIUS sur les switchs	Plus de point unique de panne, comme pour le HSRP
Clé de registre BlockNtlmv1SSO = 0 déployée par GPO (Préférences > Registre)	Remet l'envoi automatique du mot de passe Windows bloqué par KB5127648. Plus besoin de le taper la première fois
Configuration 802.1X des postes déployée par GPO (stratégies de réseau câblé IEEE 802.3)	Plus besoin de configurer chaque PC à la main

Amélioration	Intérêt
VLAN « parking » sans routage ni DHCP comme VLAN par défaut des ports	Un utilisateur accepté sans VLAN n'arrive dans aucun réseau
Secret RADIUS long, distinct des autres mots de passe, et `service password-encryption`	Plus de sécurité sur les échanges et sur la config
Comptabilisation RADIUS (`aaa accounting dot1x default start-stop group radius`)	Garde une trace des connexions et déconnexions
MAB (authentification par adresse MAC)	Pour brancher des imprimantes ou appareils qui ne font pas de 802.1X
« Vérifier l'identité du serveur » recoché avec l'autorité RIOCA-SRV-AD-RIOCA-CA	Empêche un faux serveur RADIUS de récupérer les mots de passe
Credential Guard réactivé sur les postes	Marche avec les identifiants mémorisés et EAP-TLS, et protège les mots de passe en mémoire

PARTIE 2 – RAPPORT DE TESTS

7. Méthode et outils de vérification

Pour chaque test on regarde 3 choses : le switch (état du port), le NPS (accepté ou refusé) et le PC (IP reçue).

Niveau	Outil	Ce qu'il montre
Switch	`show authentication sessions interface <port> details`	État Authorized / Unauthorized, utilisateur, VLAN attribué (Server Policies > Vlan Group)
Switch	`show aaa servers`	État du serveur RADIUS et compteurs de requêtes, acceptations, refus et délais dépassés
Switch	`ping 172.19.100.2`	Joignabilité du serveur NPS
Serveur	Observateur d'événements > Affichages personnalisés > Rôles de serveurs > Services de stratégie et d'accès réseau	Événement 6272 (accès accordé) ou 6273 (refusé), avec le code de raison et la stratégie appliquée
Serveur	`Get-WinEvent -FilterHashtable @{LogName='Security'; Id=6273} -MaxEvents 1`	Détail du dernier refus
Serveur	`netsh nps show np`	Ordre, état, conditions et attributs de toutes les stratégies réseau

Niveau	Outil	Ce qu'il montre
Serveur	`Get-ADPrincipalGroupMembership <utilisateur>`	Groupes de l'utilisateur testé
Poste	`ipconfig /all`	Adresse IP obtenue dans le réseau du VLAN attendu

8. Tests réalisés

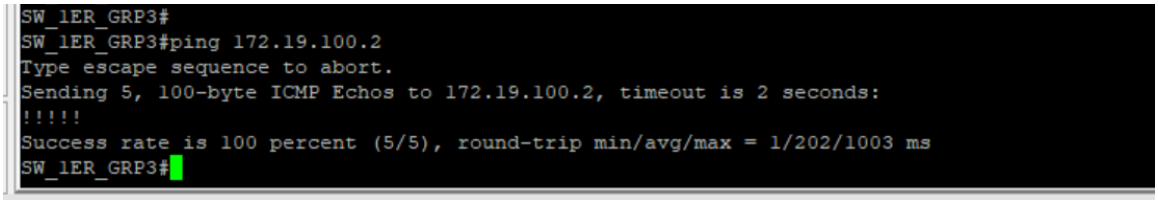
L'objectif est atteint : un utilisateur arrive dans le VLAN de son service même sur un port d'un autre VLAN, et aussi sur l'autre switch (T3 et T4). Les stratégies changent seulement par le groupe et le VLAN, donc on les a vérifiées en T5 au lieu de faire un test par service.

N°	Test	Procédure	Résultat attendu	Résultat obtenu	Statut
T1	Joignabilité du serveur NPS	`ping 172.19.100.2` depuis SWRDC et SW1ER	100 % de réponses	5/5 réponses sur les deux switchs	OK
T2	Dialogue RADIUS switch / NPS	`show aaa servers` après une connexion	Serveur UP, réponses reçues, aucun délai dépassé	State UP, requêtes traitées, 0 timeout	OK
T3	Même utilisateur sur les deux switchs	deniz (COMPTA) sur SWRDC Fa0/11 (port en VLAN 30 par défaut), puis sur SW1ER Gi1/0/1	Authorized et VLAN 10 sur les deux switchs, IP en 172.19.10.x, événement 6272	SWRDC : Authorized, VLAN 10. SW1ER : Authorized, Vlan Group : Vlan 10, IP 172.19.10.1	OK
T4	Autre service, VLAN différent du port (SW1ER)	souhir (IT) sur SW1ER Gi1/0/1, port en VLAN 10 par défaut	Authorized, VLAN 60, IP en 172.19.60.x	Authorized, Vlan Group : Vlan 60, IP 172.19.60.3	OK
T5	Configuration des stratégies de service	`netsh nps show np` sur srv-ad-rioca	8 stratégies d'accès activées, avant les stratégies par défaut, chacune avec son VLAN	Compta, IT, Fabric, Ordinateurs_Domaine, Garage, LIVR, RD, DIRRH en ordre 1 à 8, activées, Source non spécifiée	OK
T6	Refus d'un compte non autorisé	Connexion avec un compte membre d'aucun groupe de	Unauthorized, événement 6273, stratégie « Connexions à	Compte RIOCA\test : Unauthorized sur SW1ER Gi1/0/1, aucune adresse IP	OK

N°	Test	Procédure	Résultat attendu	Résultat obtenu	Statut
		service	d'autres serveurs d'accès »	attribuée	
T7	Accès SSH d'administration	SSH depuis un poste du VLAN IT vers SW1ER avec admin-it	Connexion acceptée, arrivée directe en mode privilégié (#)	Connexion acceptée, arrivée directe en mode privilégié (SW_1ER_GRP3#)	OK
T8	Plusieurs utilisateurs sur le même poste (PEAP)	PC-USER-GRP3 sur SW1ER Gi1/0/13 : session de deniz (COMPTA), puis de souhir (IT)	Chaque utilisateur dans le VLAN de son service	deniz : Authorized, VLAN 10. souhir : Authorized, Vlan Group : Vlan 60, IP 172.19.60.4	OK
T9	Solution de secours EAP-TLS	PC-USER-GRP3 sur SW1ER Gi1/0/13 en EAP-TLS : écran de connexion, puis session de deniz	Poste en VLAN 60 avant la session, puis deniz en VLAN 10	host/pc-user-grp3.RIOCA.local : Authorized, VLAN 60. deniz@RIOCA.local : Authorized, VLAN 10, IP 172.19.10.1	OK

Preuves :

T1 - SW1ER : ping de 172.19.100.2, 5 sur 5.



T2 - SWRDC : show aaa servers (extrait).

```
RADIUS: id 1, priority 1, host 172.19.100.2, auth-port 1812, acct-port 1813
     State: current UP, duration 17289s, previous duration 0s
     Dead: total time 0s, count 0
     Authen: request 1, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 1, challenge 0
```

Le serveur répond, sans timeout. Ce premier essai a été refusé, on l'a corrigé après (anomalie A3).

T3 - SW1ER Gi1/0/1 : deniz (COMPTA) est authentifié, le NPS donne le VLAN 10, IP 172.19.10.1.

```
SW_1ER_GRP3#show authentication sessions interface GI1/0/1 details
            Interface:  GigabitEthernet1/0/1
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.10.1
            User-Name:  RIOCA\deniz
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  198s
    Common Session ID:  AC1346030000001201744E1F
      Acct Session ID:  Unknown
               Handle:  0xEA000002
       Current Policy:  POLICY_Gi1/0/1

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 10

Method status list:
      Method            State

      dot1x              Authc Success
```

T3 - SWRDC Fa0/11 : même résultat sur le switch du RDC, deniz en VLAN 10.

```
SWRDC#show authentication sessions interface Fa0/11 details
            Interface:  FastEthernet0/11
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.10.1
            User-Name:  deniz
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  78s
    Common Session ID:  AC1346020000000F0040C700
      Acct Session ID:  Unknown
               Handle:  0xB9000003
       Current Policy:  POLICY_Fa0/11

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 10

Method status list:
      Method            State

      dot1x             Authc Success
```

T4 - SW1ER Gi1/0/1 : souhir (IT), sur un port en VLAN 10, est mis en VLAN 60 et a l'IP 172.19.60.3.

```
SW_1ER_GRP3(config-if)#end
SW_1ER_GRP3#show authentication sessions interface Gi1/0/1 details
            Interface:  GigabitEthernet1/0/1
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.60.3
            User-Name:  RIOCA\souhir
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  52s
    Common Session ID:  AC1346030000000F01570572
      Acct Session ID:  Unknown
               Handle:  0x4B000001
       Current Policy:  POLICY_Gi1/0/1

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 60

Method status list:
      Method            State

      dot1x              Authc Success
```

T5 - Liste des stratégies et ordre : voir la capture en 3.5.

T6 - SW1ER Gi1/0/1 : le compte RIOCA\test n'est dans aucun groupe de service. Il reste Unauthorized, sans IP.

```
SW_1ER_GRP3#show authentication sessions interface Gi1/0/1 details
            Interface:  GigabitEthernet1/0/1
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  RIOCA\test
               Status:  Unauthorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  394s
    Common Session ID:  AC1346030000001901A6D326
      Acct Session ID:  Unknown
               Handle:  0x38000008
       Current Policy:  POLICY_Gi1/0/1

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

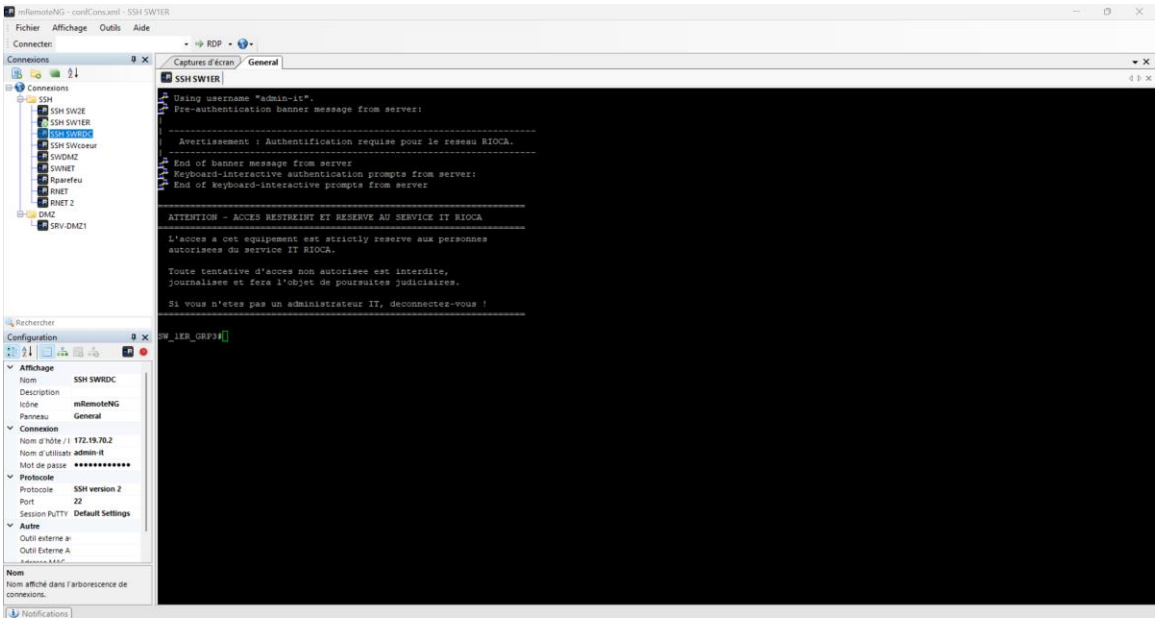
Method status list:
      Method            State

      dot1x              Running
```

L'événement 6273 sur srv-ad-rioca (extrait) :

```
Nom de compte :                 RIOCA\test
Nom convivial du client :       switch1erE
Nom de stratégie réseau :       Connexions à d'autres serveurs d'accès
Code raison :                   65
```

T7 - SW1ER : connexion SSH avec admin-it, on arrive direct en mode privilégié (SW_1ER_GRP3#).



T8 - SW1ER Gi1/0/13 : sur le même PC, deniz puis souhir ont chacun le VLAN de leur service.

```
SW_1ER_GRP3#show authentication sessions interface Gi1/0/13 details
            Interface:  GigabitEthernet1/0/13
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.60.4
            User-Name:  souhir
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  191s
    Common Session ID:  AC13460300000002F01611130
      Acct Session ID:  Unknown
               Handle:  0xCD000020
       Current Policy:  POLICY_Gi1/0/13

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 60
```

T9 - SW1ER Gi1/0/13 : en EAP-TLS, le PC est authentifié avec son certificat avant la session (VLAN 60), puis deniz avec le sien (VLAN 10).

```
SW_1ER_GRP3#show authentication sessions interface Gi1/0/13 details
            Interface:  GigabitEthernet1/0/13
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.60.3
            User-Name:  host/pc-user-grp3.RIOCA.local
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  52s
    Common Session ID:  AC1346030000001B0092E98A
      Acct Session ID:  Unknown
               Handle:  0xC200000D
       Current Policy:  POLICY_Gi1/0/13

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 60

Method status list:
      Method            State

      dot1x              Authc Success

SW_1ER_GRP3#
SW_1ER_GRP3#
```

```
SW_1ER_GRP3#show authentication sessions interface Gi1/0/13 details
            Interface:  GigabitEthernet1/0/13
          MAC Address:  fc34.9780.541d
         IPv6 Address:  Unknown
         IPv4 Address:  172.19.10.1
            User-Name:  deniz@RIOCA.local
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  118s
    Common Session ID:  AC1346030000001B0092E98A
      Acct Session ID:  Unknown
               Handle:  0xC200000D
       Current Policy:  POLICY_Gi1/0/13

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 10

Method status list:
      Method            State

      dot1x              Authc Success
```

9. Anomalies rencontrées et corrections

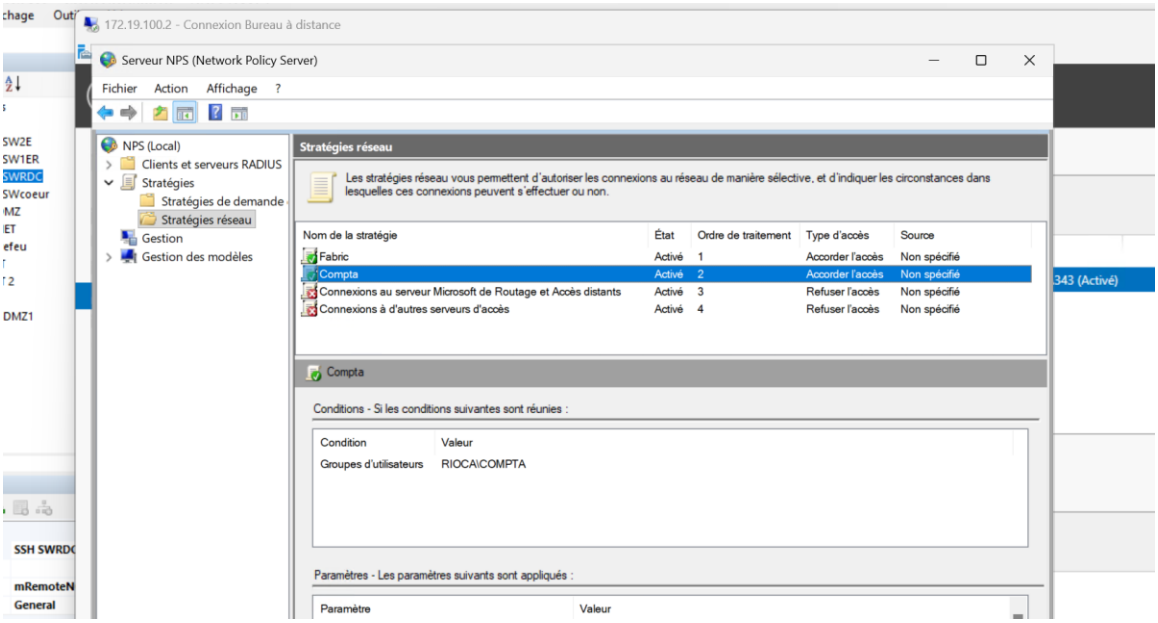
On a eu 14 problèmes pendant la mise en place et les tests. La plupart venaient des stratégies NPS, on les a trouvés avec l'observateur d'événements.

N°	Symptôme	Diagnostic	Cause	Correction
A1	Port orange en permanence, aucune trace côté NPS	`show aaa servers` : le switch n'envoyait aucune requête au serveur	`dot1x pae authenticator` manquant : en IOS 15, `port-control auto` tout seul ne lance pas l'EAP	Ajout de `dot1x pae authenticator` sur les ports d'accès
A2	Configuration AAA incomplète	Relecture du `show running-config`	`aaa authorization network default group radius` manquant : le switch n'aurait pas mis le VLAN du NPS	Commande ajoutée
A3	Refus immédiat (1 reject, 0 challenge)	Événement 6273, code 65, stratégie appliquée « Connexions à d'autres serveurs d'accès »	Les stratégies par défaut passaient avant Compta et Fabric, et l'une d'elles prend toutes les demandes	Stratégies de service remontées en haut de la liste
A4	Stratégie Compta sans configuration PEAP	`netsh nps show np` : attribut EAP-Configuration absent	Certificat et méthode interne non sélectionnés dans les contraintes	Contraintes > PEAP : certificat de srv-ad-rioca et EAP-MSCHAP v2
A5	Utilisatrice du service Fabric refusée, PC en APIPA	6273, code 65 ; `netsh nps show np` : « Source de la stratégie » = 10 et 20	« Type de serveur d'accès réseau » mis sur « Spécifique au fournisseur » avec le numéro de VLAN. En plus, les copies de stratégie étaient désactivées	Remis sur « Non spécifié », copies activées, copie en trop supprimée
A6	SSH vers SWRDC accepté, mais `enable` refusé	Arrivée en mode utilisateur (>)	Avec aaa new-model, le privilège 15 du compte local ne marche plus sans autorisation exec, et il n'y a pas d'enable secret	`aaa authentication login default local` et `aaa authorization exec default local`
A7	Erreurs dans les notes de départ	Comparaison avec les `show running-config` et le schéma	IP du NPS notée 172.19.70.1 au lieu de 172.19.100.2, et brouillage MAC Hyper-V noté comme nécessaire alors que	Documentation corrigée

N°	Symptôme	Diagnostic	Cause	Correction
		réseau	RADIUS c'est juste de l'UDP routé	
A8	Postes du VLAN IT bloqués sur « Vérification de vos informations d'identification » (SW1ER)	`show authentication sessions` : aucune méthode lancée ; `show run interface Gi1/0/13`	`dot1x pae authenticator` manquant sur `Gi1/0/10 à 14` : la commande avait été tapée sur une plage avec les ports éteints `Gi1/0/20 à 24`, elle a planté et on est sorti du mode `interface`	Commandes refaites sur interface range Gi1/0/1 - 19, seulement les ports d'accès
A9	PC hors domaine refusé (« Nous n'avons pas pu nous connecter à ce réseau »)	User-Name = anonymous ; 6273, code 8 (compte inexistant)	Option PEAP « Activer la confidentialité de l'identité » : le PC envoie « anonymous », et le NPS cherche ce nom dans l'AD	Option décochée, identifiants RIOCA\compte enregistrés sur le PC
A10	PC personnel refusé avec le compte Administrateur	User-Name = rioca\Administrateur ; stratégie appliquée = stratégie par défaut	Le compte n'appartient à aucun groupe de service	Connexion avec un compte nominatif du groupe IT. On n'enregistre jamais le compte admin du domaine sur un PC
A11	Tous les utilisateurs du poste placés dans le VLAN IT	User-Name = RIOCA\souhir quel que soit l'utilisateur connecté	Identifiants de souhir enregistrés pour tout le PC (Paramètres supplémentaires > Enregistrer ident.)	Identifiants supprimés, chacun se connecte avec son compte
A12	Aucune authentification avant l'ouverture de session	show authentication sessions : méthode N/A, aucune trame EAPOL reçue	dot3svc en démarrage manuel : il ne démarre qu'à l'ouverture de session	Service passé en démarrage automatique (5.1)
A13	Échec avec « Utiliser automatiquement mon nom et mot de passe	Journal NPS : réponses Access-Challenge sans suite, aucun événement 6272	On pensait à Credential Guard (il bloque MS-CHAP v2 avec les identifiants Windows)	Credential Guard désactivé : ça n'a rien changé, on a continué côté PC (A14)

N°	Symptôme	Diagnostic	Cause	Correction
	Windows »	ou 6273		
A14	Même échec pour le compte ordinateur et pour les utilisateurs	Wired-AutoConfig, événement 15514 : raison 0x50005, erreur 0x80070285, blocage de 600 s	Mise à jour Windows KB5127648 (octobre 2026) : elle bloque l'envoi automatique des identifiants Windows en PEAP-MSCHAP v2	Case « Utiliser automatiquement … » décochée et identifiants mémorisés par utilisateur (5.2). EAP-TLS en secours (5.4)

Après la correction A3, les stratégies de service passent avant les deux stratégies par défaut (capture prise quand il n'y avait que Fabric et Compta).



À retenir : le code 65 parle de l'onglet « Appel entrant » du compte, mais la vraie cause était dans « Nom de stratégie réseau ». Si c'est une stratégie par défaut, ça veut dire qu'aucune de nos stratégies n'a correspondu.

10. Bilan

La solution marche sur les deux switchs. Les utilisateurs se connectent avec leur compte AD et ont le VLAN de leur service, peu importe le port ou l'étage.

- Objectif atteint : mobilité testée au RDC (T3) et entre les deux switchs (T4).
- Sécurité : un PC ou un compte pas autorisé n'a plus aucun accès.
- Administration : le SSH sur les switchs ne dépend pas de RADIUS.
- Plusieurs utilisateurs sur le même PC : chacun a le VLAN de son service (T8). Le secours par certificats marche aussi (T9).
- À faire en priorité : un deuxième serveur NPS, pour ne plus dépendre d'un seul serveur.