# Documentation Serveur Radius

Hourlay Nolann - Le Henaff Noah

## Sommaire

Documentation	
Serveur Radius	0
Contexte	2
Installation des rôles	3
Création d'un certificat d'authentification	6
Test	21

## Contexte

On possède actuellement une infrastructure fonctionnelle similaire à une entreprise, mais sur notre routeur wifi, on souhaiterait avoir une sécurité plus forte au niveau des connexions. Pour pallier ce problème, on va installer un serveur Radius.

Un serveur RADIUS (Remote Authentication Dial-In User Service) est un serveur qui vérifie l'identité des utilisateurs qui essaient d'accéder à un réseau ou à un service informatique.

Dans notre infrastructure, on va le rattacher à notre Active Directory, les authentifications pour accéder au réseau sans fil se feront avec les comptes utilisateurs Active Directory (LDAP).

## Installation des rôles

Après avoir configuré le serveur de domaine, nous ajoutons le rôle "Services de stratégie et d'accès réseau".

📥 Assistant Ajout de rôles et de for	ctionnalités	- 🗆 X
Assistant Ajout de rôles et de for Sélectionner des r Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Confirmation Résultats	ctionnalités Ôles de serveurs Sélectionnez un ou plusieurs rôles à installer sur le serveur sélect Rôles Accès à distance Hyper-V Serveur de télécopie Serveur DHCP Serveur DNS (Installé) Serveur Web (IIS) Services AD DS (Installé) Services AD DS (Installé) Services AD DS (Installé) Services AD RMS (Active Directory Lightweight Director Services AD RMS (Active Directory Rights Management Services Bureau à distance Services Bureau à distance Services d'activation en volume Services d'activation en volume Services de certificats Active Directory Services de déploiement Windows Services de fédération Active Directory (AD FS) Services de fichiers et de stockage (4 sur 11 installé(s) Services de stratérie et d'accès réseau	- C X      SERVEUR DE DESTINATION WIN-9JS4K90CKI2.Radius.sl  tionné.  Description Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
	Services WSUS (Windows Server Update Services)	
	< Précédent Suivant	> Installer Annuler

## Ensuite, il faut installer le service de certificats Active Directory.

Sélectionner des l	rôles de serveurs sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' AD CS Services de rôle Confirmation Résultats	Rôles     Description       Accès à distance     Hyper-V       Serveur de télécopie     Les services de certificats Active       Serveur DHCP     Serveur DHCP       Serveur Web (IIS)     Services AD I (Installé)       Services AD I (Installé)     Services AD I (Installé)       Services AD LDS (Active Directory Lightweight Director)     Services AD RMS (Active Directory Rights Management)       Services d'activation en volume     Services de rédificats Active Directory       Services de déploiement Windows     Services de fédération Active Directory (AD FS)       Services de fichiers et de stockage (4 sur 11 installé(s))     Services de fichiers et de stockage (4 sur 11 installé(s))       Services WSUS (Windows Server Update Services)     Services WSUS (Windows Server Update Services)

Vous pouvez cliquer sur "suivant", jusqu'à la catégorie "Services de rôle"

Dans la catégorie "Service de rôle", vérifiez bien que la case "Autorité de certification" est cochée.



## Création d'un certificat d'authentification

Pour pouvoir créer le certificat, il faut la configuration post-déploiement :



Cliquez sur "suivant" et cochez la case "Autorité de certification".

ᡖ Configuration des services de c	ertificats Active Directory	_		×
Services de rôle	$\triangleright$	SERVEUR DE DI WIN-9JS4K90Cł	ESTINATI (12.Radiu	ON s.sl
Informations d'identificati Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	Sélectionner les services de rôle à configurer Autorité de certification Inscription de l'autorité de certification via le Web Répondeur en ligne Service d'inscription de périphériques réseau Service Web Inscription de certificats Service Web Stratégie d'inscription de certificats			
	En savoir plus sur les rôles de serveur AD CS			
	< Précédent Suivant >	Configurer	Annule	r

## Il faut choisir "Autorité de certification d'entreprise".



#### Ensuite, on choisit "Autorité de certification racine".



## Nous créons une clé privée.

📥 Configuration des services de ce	ertificats Active Directory – $\Box$ X
Clé privée	SERVEUR DE DESTINATION WIN-9JS4K90CKI2.Radius.sl
Informations d'identificati Services de rôle Type d'installation Type d'AC	Spécifier le type de la clé privée Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.
Clé privée Chiffrement	<ul> <li>Créer une clé privée</li> <li>Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.</li> </ul>
Nom de l'AC Période de validité Base de données de certi Confirmation Progression	<ul> <li>Utiliser la clé privée existante</li> <li>Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.</li> <li>Sélectionner un certificat et utiliser sa clé privée associée</li> <li>Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.</li> </ul>
Résultats	Sélectionner une clé privée existante sur cet ordinateur Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.
	En savoir plus sur la clé privée
	< Précédent Suivant > Configurer Annuler

Par la suite, nous pouvons appuyer sur "suivant" jusqu'à la création car nous laissons tout par défaut.

Nous pouvons voir que la configuration du certificat est réussie.

Résultats	SERVEUK DE DESTINATION WIN-9JS4K90CKI2.Radius.sl
Informations d'identificati Services de rôle	Les rôles, services de rôle ou fonctionnalités ci-après or kété configurés :
Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC	Autorité de certification S Configuration réussie En savoir plus sur la configuration de l'autorité de certification
Periode de Validite Base de données de certi Confirmation Progression Résultats	

Maintenant, on va exporter le certificat. Pour cela, ouvrez "l'autorité de certification".



#### Faites clic droit, propriété sur le nom de votre serveur.

Vous arriverez ici :	Propriétés de : Radius-W	/IN-9JS4K90CKI2-	.CA		? ×	
	Extensions	Stockage	Lo <sup>2</sup> Geo	tionnaires de ce	artificate	
	Agents d'inscription	Audit	Agents de réc	upération	Sécurité	-
	Général	Module de stra	tégie	Module de	e sortie	
	- Autorité de certification	1				
	Nom :	Radius-WIN-9JS4	K90CKI2-CA			
	Certificats d'autorité de	e certification :				
	Certificatin <sup>®</sup> 0					
			Affich	er le certificat		
	Paramètres de chiffren	nent				
	Fournisseur :		(ey Storage	Provider		
		SHA256				
	Algorithme de hachag	e:				
		ОК А	nnuler	Appliquer	Aide	
			💂 Certifica	t		×
Cliquer sur Afficher	le certificat, ensu	lite sur dét	ail. Général Dé	tails Chemin d'accès d	de certification	
			Afficher :	<tout></tout>	~	]
			Champ		Valeur	^
			Versior	n o de série	V3 12251bb693dfc0	b04c883185f
			Algorit	hme de signature hme de hachage de l…	sha256RSA sha256	
			Valide	eur à partir du	Radius-WIN-9JS lundi 28 avril 202	#K90CKI2-CA, 5 16:07:55
			Objet	jusqu au	Radius-WIN-915	4K90CKT2-CA
			I	Modifier les pro	priétés Copi	er dans un fichier
						10 ок

Cliquez sur "Copier dans un fichier".

Créer un dossier, et placer la certification dedans. Laisser les valeurs par défaut.

🟹 cert	28/04/2025 16:34	Certificat de sécur	11

## Configuration des éléments d'authentification

Sur le routeur wifi, dans Wireless puis Wireless Security. Renseigner certains éléments :

- mode de sécurité : WPA2 Entreprise
- adresse IP du serveur RADIUS
- Clé partagée

					Wir	eless-G Broa	dbanc
	Setup	Wireless	Security	Access Re	strictions	Applications & Gaming	Ad
	Basic Wirele	ss Settings	Wireless :	Security	VVireles	s MAC Filter	Adv
curity	B						
	Security Mode	•	WPA2 Ente	rprise 🛩			
	WPA Algorithm	IS :	TKIP+AES	~			
	RADIUS Serve	er Address :	10.29.	232 . 225			
	RADIUS Port :		1812				
	Shared Key :		salut				
	Key Renewal	limeout :	3600	secon	ds		
				Save Settin	gs Car	ncel Changes	

Ensuite, on se retrouve sur l'AD. Il faut ouvrir la console NPS.



Faites clic droit sur NPS local et cliquez sur "Inscrire un serveur dans un

Active Directory".	🚯 Serveur NPS (N	letwork Policy Se	rver)			-		×
	Fichier Action	Affichage ?						
	🗢 🄿  🖬							
	NPS (Local)		NPS (Local)					
	> 🦰 Clients	Importer la con	figuration					
	> J Stratéc	Exporter la conf	figuration					
	> 🛃 Gestio	Démarrer le sen	vice NPS		licy Server) vous permet de créer et de mettre en application des stratégies d'accès réseau portant sur l'authentification	on sur l'e et l'autor	nsemble o risation de	du es
		Arrêter le servic	e NPS					
		Inscrire un serve	eur dans Active Directory					<b>A</b>
		Propriétés						
		Affichage		>	uration dans la liste, puis cliquez sur le lien ci-dessous pour	ouvrir l'/	Assistant	
		Aide			ns d'accès à distance ou VPN	$\sim$		
			Serveur RADIUS pou Lorsque vous configurez un connexions d'accès à distar d'authentifier et d'autoriser le appelés clients RADIUS). Configurer une connex distance	r les serveu ice ou es con ion VF	connexions d'accès à distance ou VPN Ir NPS (Network Policy Server) en tant que serveur RADIU VPN, vous créez des stratégies réseau qui permettent au s nexions provenant des serveurs d'accès réseau à distance N ou d'accès à Informations	S pour d erveur N ou VPN	es IPS (égaleme	ent
			Configuration avancé	e				•
			Configuration de mod	lèles				•
	Contient des comm	andes permettan	t de personnaliser cette fenêt	re.				

#### Après, nous allons sélectionner plusieurs informations.



### Ensuite, cochez la case "Connexions sans fil sécurisé" et renseignez un nom

:

Configurer 802.1X

#### Sélectionner le type de connexions 802.1X



#### Type de connexions 802.1X : © Connexions sans fil sécurisées

Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.

Connexions câblées (Ethernet) sécurisées

Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethemet qui se connectent via ces commutateurs.

#### Nom :

Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.

SSID-BINOME-2

Précédent	Suivant	Terminer	Annuler

×

# Maintenant, on clique sur "Ajouter" :

Configurer 802.1X	$\times$
Spécifier les commutateurs 802.1X Spécifiez les commutateurs ou points d'accès sans fil 802.1X(clients RADIUS)	
Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification e des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.	t
Pour spécifier un client RADIUS, cliquez sur Ajouter.	
Clients RADIUS : Ajouter Modifier Supprime	
Précédent Suivant Terminer Annuler	

Par la suite, il faut renseigner des informations sur le Routeur Wifi comme son nom, son adresse IP et ne pas oublier de renseigner le secret partagé.

Nouveau client RADIUS	×
Paramètres	
Sélectionner un modèle existant :	
Nom et adresse	
Nom convivial :	
SSID-BINOME-2	
Adresse (IP ou DNS) :	
192.2.10.11 Vérifier	
Secret partagé	
Sélectionnez un modèle de secrets partagés existant :	_
Aucun	1
Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.	
Manuel     Générer	
Secret partagé :	
•••••	
Confirmez le secret partagé :	
OK Annul	er

Ensuite, il faut choisir le type "Microsoft : PEAP (Protected EAP).



Il faut cliquer sur "configurer" et choisir le certificat créé précédemment.

Modifier les propriétés EAP Protégé X				
Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du client. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacera ce certificat.				
Certificat délivré à :	WIN-9JS4K90CKI2.Radius.sl	$\sim$		
Nom convivial :	WIN-9JS4K90CKI2.Radius.sl			
Émetteur :	Radius-WIN-9JS4K90CKI2-CA			
Date d'expiration :	28/04/2026 23:39:10			

Maintenant, on va choisir le groupe d'utilisateurs concerné. Dans notre cas, c'est "utilisateurs du domaine".

Sélectionnez un groupe	×				
Sélectionnez le type de cet objet :					
un groupe	Types d'objets				
À partir de cet emplacement :					
Radius.sl	Emplacements				
Entrez le nom de l'objet à sélectionner (exemples) :					
Utilisateurs du domaine	Vérifier les noms				
Avancé	OK Annuler				

Quand cela est fait, cliquer sur suivant, puis terminer.

Il ne faut surtout pas oublier de mettre une règle de filetage sur le pare-feu car d'origine, il bloque les requêtes d'authentification.

```
netsh advfirewall firewall add rule name="RADIUS Authentication" dir=in
action=allow protocol=UDP localport=1812
```

C:\Users\Administrateur>netsh advfirewall firewall add rule name="RADIUS Authentication" dir=in action=allow protocol=U alport=1812 Ok.

## Test

Pour tester la connexion au réseau wifi, sur l'appareil, on va rechercher notre réseau wifi.



Pour se connecter, il vous nous demande un login et mot de passe d'un

compte Active Directory.

10.12				
Mot de passe de « SSID-BINOME-2 »				
Annuler	Saisir			
Nom d'utilis	ateur			
Mot de pass	se			
Le WPA/WPA2 (TKIP) n'est pas considéré comme sécurisé.				
S'il s'agit bien de votre réseau Wi-Fi, configurez votre routeur de façon à ce qu'il utilise le type de sécurité WPA2 (AES) ou WPA3.				
	P Mots de passe			
a z e	r t y	u i o p		
q s d	f g h	j k l m		
\$ w >	k c v b	n ′ 🛛		
123	espace	suivant		
<b>;;;</b>		Ų		

Une fois que vous avez entré les éléments nécessaires, ils vont vous demander si vous faites confiance au certificat. Mettez "Se fier" car c'est le certificat que vous avez créé précédemment.



Une fois accepté, vous serez connecté au réseau wifi.