# PROJET ASSURMER

# AUTEURS :

DE CARVALHO LOPES Bruno BELAHA Sidahmed LE CLAINCHE Killian

DATE :

07/01/2025

2025

# Sommaire

I.	Installation du serveur NPS	3
١١.	Configuration du serveur RADIUS	. 10
III.	Installation du rôle requis pour l'autorité de certifications	. 16
IV.	Configuration du serveur RADIUS + Certificats	. 22

## I. Installation du serveur NPS

Gestionnaire de serveur				- 0	
Gestionn	aire de serveur 🔸 Tablea	u de bord	· @	Gérer Outils Afficher Aide	
			>	Ajouter des rôles et fonctionnalités	
🔢 Tableau de bord	Tableau de bord BIENVENUE DANS GESTIONNAIRE DE SERVEUR				
Serveur local				Créer un groupe de serveurs	
Tous les serveurs	Co	nfigurer ce serveur local		Propriétés du Gestionnaire de serveur	
AD DS	DÉMARRAGE	5			
	RAPIDE 2	Aiouter des rôles et des fonctionnali	tés		
Services de fichiers et d P					
-	3 4	Ajouter d'autres serveurs a gerer			
	NOUVEAUTES 4	Créer un groupe de serveurs			
	5	Connecter ce serveur aux services d	oud		
			odd	Masquer	
	EN SAVOIR PLUS			Carlos Poles C	
	Rôles : 4   Groupes de serveurs : 1   N	lombre total de serveurs : 1			
	El lo pr	9= DUGD	0		
	AD DS	I∎ DHCP 1	DNS 1		
	Facilité de gestion	Facilité de gestion	Facilité de gestion		
	Événements	2 Événements	Événements		
	Services	Services	Services		
	Performances	Performances	Performances		
	Résultats BPA	Résultats BPA	Résultats BPA		
	6				
		08/01/2025 09:09			

Etape 1 : Cliquez sur « ajouter des rôles et fonctionnalités » :

Etape 2 : Cochez « Installation basée sur un rôle ou une fonctionnalité », puis cliquez sur « Suivant »

Gestion naire de serveur Gestionna Gestionna	aire de serveur • Tableau de bord Bienvenue dans gestionnaire de serveur	- C C
I Serieur local 下 Tous les serveurs II AD DS 注 DH:CP ▲ DNS ■ Serices de fichiers et d ▷	Avant de commencer Sélection du serveur Fonction nalités Confirmation Résultato Résult	strintaller des rôles et des fonctionnalités sur installer des rôles et des fonctionnalités sur nent, ou sur un disque dur virtuel hors connexion. Inctionnalité des rôles, des services de rôle et des fonctionnalités. sce infrastructure VDI (Virtual Desktop Infrastructure) pour teurs virtuels ou sur des sessions. Masquer
		Ment Suivant > Installer Annuler

#### Etape 3 : Cliquez sur « Suivant » :



Etape 4 : Cliquez sur « Ajouter des fonctionnalités » :





#### Etape 5 : Cochez la case « Services de stratégie et d'accès réseau » :





#### Etape 7 : Cliquez sur « Suivant » :







#### Etape 9 : Cliquez sur « Suivant » :



Etape 10 : Effectuez un clic droit sur « Services de stratégie et d'accès réseau » :

ionnaire de serveur		- 0
)⊛ • Gestie	onnaire de serveu 🔹 Services de stratégie et d'accès réseau (NPAS) 💿 🔹 🗐 🌇 🖼	érer Outils Afficher
ableau de bord	SERVEURS Tous les serveurs   1 au total	TÂCHES 💌
erveur local		0
us les serveurs		
) DS	Nom du serveur Adresse IPyr Facilité de gestion Dernière mise à jour Activation de Windows	
HCP	SRV-AD 172.16.0.1 En ligne - Compteurs de performances non démarré 08/01/2025 09:22:03 Non activé	
IS		
rvices de fichiers et d		
rvices de stratégie et.		
	6164199499499	
	Tous les événements   0 au total	TÂCHES 🔻
		~
	Filtrer D (II) • (II) •	۲
	Nom du serveur ID Gravité Source Journal Date et heure	

Gestionna Tableau de bord	aire de serveur • Services de stra SERVEURS Tous les serveurs   1 au total	atégie et d'accès réseau (NPAS)	• 😨   🚩 Gérer	Outils Afficher Aide
Serveur local	Filtrer 👂 🕕 🕶	® •		۲
AD DS	Nom du serveur Adresse IPv4 Facilité de gestion	Dernière mise à jour Activation	n de Windows	
<ul> <li>▲ DNS</li> <li>■ Services de fichiers et d ▷</li> <li>♥ Services de stratégie et</li> </ul>		Ajouter des rôles et fonctionnalités Arrêter le serveur local Gestion de l'ordinateur Connexion Bureau à distance Windown SpeerShell Configurer association de cartes réseau		
	ÉVÉNEMENTS Tous les événements   0 au total	Serveur NPS (Network Policy Server) Gérer en tant que Démarrei sc compteurs de performances Actualiser		TÂCHES 💌
	Filtrer 🔎 🕕 🕇	Copier		۲
	Nom du serveur ID Gravité Source Journal Date	et heure		

## Etape 11 : Cliquez sur « Serveur NPS (Network Policy Server) :



Serveur NPS Fichier Actio	(Network Policy Se n Affichage ?	rver)	/		- 0 ×
🔶 🔿 📰	2 🖬				
NPS (Lor <sup>-n</sup> ) Clier ) Strat Gesti ) Gesti	Importer la con Exporter la conf Démarrer le serv Arrêter le servic	iguration iguration ice NPS e NPS	<sup>2</sup> oloy Server Yous permet de créer et de mettre en app	ilication sur l'ensemble du réseau de votre organisation des stratégies d'acci	és réseau potant sur l'authentification et l'autorisation des
	Inscrire un serve	serveur dans Active Directory			
	Affichage		iguration dans la liste, puis cliquez sur le lien ci-dessous	uration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.	
	Aide		kions d'accès à distance ou VPN		~
		Configurer une connext	on VPN ou d'accès à distance	Informations	
		Configuration de mod	lèlos		Ŧ

### Etape 13 : Cliquez sur « OK » :

NPS (Local)	NPS (local)	
Clients et serveurs RADIUS	Mise en route Le serveur NPS (Network: Policy Server) vons permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'authentification et l'autorisation	on des
	Configuration standard	•
	Sélectionnez un scénario de configuration dans la liste, puis chures sur le lien ci-dessous pour ouver l'Assistant Scénario.  Serveur RADIUS pour les connexions d'accès à c Serveur RADIUS pour les connexions Pour permettre auxienceurs NPS (Network Policy Server)  Serveur RADIUS pour les connexions Pour permettre auxienceurs NPS (Network Policy Server) d'authentifier d'authentifier et d'autoriser les connexions proven Configurer une connexion VPN ou d'accès a Configurer une connexion VPN ou d'accès a	
	Configuration avancée	•

# II. <u>Configuration du serveur RADIUS</u>

Fta	no	1	٠
Lla	he		٠

cisco WAP371 \	Wireless-AC/N Dual Radio Access Point with Single Point Setup
Getting Started	Quetere Cettinge
Run Setup Wizard	System Settings
<ul> <li>Status and Statistics</li> </ul>	Host Name: wapf/e330 (Pange: 1.63 Charactere)
Administration	(Nalige: 1-05 Onalacters)
System Settings	System Contact : (Range: 0-255 Characters)
User Accounts Time Settings Log Settings	System Location: (Range: 0-255 Characters)
Email Alert LED Display	Save
HTTP/HTTPS Service	
Management Access Conti Manage Firmware	

## Etape 2 : Cliquez sur « Nouveau » :

😔 Serveur NPS (Net	twork Policy Ser	rver) – Ø	×
Fichier Action	Affichage ?		
(+ +) 🔂 🗹			
NPS (Local)		NPS (Local)	
🗸 🧮 Clients et ser	rveurs RADIUS	Mise Fruite	
Clients	Nouveau		
> Stratégies	Actualiser	Le serveux int's (inknown knotcy server) vous permet de creer et de mettre en application sur l'ensemble du reseau de votre organisation des stratégies d'acces reseau potant sur l'autorisation demandes de connexision.	des
Sestion			
> 🛃 Gesti 🖓 de	Aide	Configuration standard	
		Sélectionnez un scénario de configuration dans la liste, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.	
		Serveur RADIUS pour les connexions d'accès à distance ou VPN	
		Serveur FADIUS pour les connexions d'acces à distance ou VFN Lonque vous configure un serveur NPS (lieture) Policy Server la mat que serveur RADIUS pour des connexions d'accès à distance ou VPN, vous créez des stratégies réseau qui permettent au serveur NPS d'authentifier et d'autoriser les connexions provenant des serveurs d'accès réseau à distance ou VPN (également appelés clerits RADIUS).	
		Configurer une connexion VPN ou d'accès à distance	
		Configuration avancée	•
		Configuration de modèles	•
<	>	0	

Etape 3 : Renseignez le host en fonction des paramètres de la bornes, puis cliquez sur « OK » :

/ 1	
ropriétés de wapf4e330 X	
Paramètres Avancé	
Activer ce client RADIUS	
Sélectionner un modèle existant :	
Nom et adresse	
Nom convivial : wanf4e 330	
Adresse (IP ou DNS) :	
Veniles	
Secret partagé	
Sélectionnez un modèle de secrets partagés existant :	
Aucun	
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 Annuler Appliquer	

Etape 4 : Dans stratégie de réseau, faites un clic droit puis cliquez sur « Nouveau »

						/	
Serveur NPS (Network P	Serveur NPS (Network Policy Server)						
Fichier Action Afficha	age ?				/		
🗢 🔿 🖄 🔂 🖬	1						
NPS (Local)	St	ratégies rése	au	/			
✓	RADIUS						
Clients RADIUS		Les stra	tégies réseau vous permettent d'autoriser les connexi	ons au ré	éseau de manière séle	ctive, et d'indiquer	les circonstances dans lesquelles ces con
Groupes de serv	eurs RA						
✓				1	1		
Stratégies de de	mande No	om de la straté	gie	État	Ordre de traitement	Type d'accès	Source
🚰 Stratégie <u>s réceau</u>		Connerione	u serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès	Non spécifié
Gestion N	Nouveau		d'autres serveurs d'accès	Activé	999999	Refuser l'accès	Non spécifié
> 🛃 Gestion des 🛛 🛛 🛛	Exporter la lis	ste					
4	Affichage	>					
4	Actualiser						
4	Aide						
		Conditions - Si Condition	les conditions suivantes sont réunies : Valeur				

# Etape 5 : Entrez le nom de la stratégie « SSID » :

August of the former of t	_	égie réseau Snécifier le	e nom de la strat	égie réseau et le type d	e connexion
Aum de la stratégie :     SSID     Véthode de connexion réseau   Sédectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner un naleur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votr enveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.    Type de serveur d'accès réseau :     Non spécifié    Spécifique au fournisseur :   10   10         Précédent Suivant Terminer Annuler Rape 6 : Cliquer sur « Ajouter » :	A	Vous pouvez spé s'applique.	écifier le nom de votre straté	égie réseau ainsi que le type des conne	exions auxquelles la stratégie
Néthode de connexion réseau Sélectionnez le type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votr erveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié. Type de serveur d'accès réseau : Non spécifié Spécifique au fournisseur : 10 0 Précédent Suivant Terminer Annuler appe 6 : Cliquer sur « Ajouter » :	n de la s	tratégie : 🖌			
Iéthode de connexion réseau         iélectionnez le type de serveur d'accès réseau ou bien Spécifique au foumisseur, mais ces paramètres ne sont pas obligatoires. Si votreveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.         Type de serveur d'accès réseau :         Non spécifié         Spécifique au fournisseur :         10       ‡         Précédent       Suivant         Terminer       Annuler         appe 6 : Cliquer sur « Ajouter » :	0				
Non spécifié   Spécifique au fournisseur :   10   10    Précédent Suivant Terminer Annuler  ape 6 : Cliquer sur « Ajouter » :	rur dans Ty reur d'acci	ype de serveur d'acc ès réseau est un cor	nucces réseau ou bien Spécifique mmutateur d'authentification o	au foumiseur, mais ces paramètres ne su foumiseur, mais ces paramètres ne su un point d'accès sans fil 802.1X, sélec	sont pas obligatoires. Si votre tionnez Non spécifié.
Spécifique au fournisseur :	Non spéc	ifié		~	
10 1 Précédent Suivant Terminer Annuler Annuler Appe 6 : Cliquer sur « Ajouter » :	Spécifique	au fournisseur :			
Précédent Suivant Terminer Annuler	10	-			
ape 6 : Cliquer sur « Ajouter » :					
				Précédent Suivant	Terminer Annuler

	Spécifiez les o minimum, une	r <b>les conditio</b> conditions qui déterr condition est néces	<b>ns</b> minent si cette : saire.	stratégie rése	au est évaluée po	ur une demande	de connexion. A
Conditions :							
Condition		Valeur			λ		
Description de l	a condition :				Ajoqter	Modifier	Supprimer
				Précédent	Suivant	Terminer	Annuler

## Etape 7 : Sélectionnez « Groupe d'utilisateurs », puis cliquez sur « Ajouter » :

1	2	
	2	$\times$
si cette stratégie réseau est évaluée pour u	ne demande de connexion. Au	ı
	:	×
	^	•
sateur ou l'ordinateur qui tente d'établir la co	nnexion doit appartenir	
ordinateur qui tente d'établir la connexion do	it appartenir à l'un des	
utilisateur qui tente d'établir la connexion doi	t appartenir à l'un des	
indiquent les jours et les heures auxquels le ls sont basées sur le fuseau horaire du serve	s tentatives de eur NPS (Network Ajouter Annuler	,
	si cette stratégie réseau est évaluée pour u sateur ou l'ordinateur qui tente d'établir la co ordinateur qui tente d'établir la connexion do utilisateur qui tente d'établir la connexion do indiquent les jours et les heures auxquels le s sont basées sur le fuseau horaire du serve	1 2 si cette stratégie réseau est évaluée pour une demande de connexion. Au si cette stratégie réseau est évaluée pour une demande de connexion. Au sateur ou l'ordinateur qui tente d'établir la connexion doit appartenir ordinateur qui tente d'établir la connexion doit appartenir à l'un des utilisateur qui tente d'établir la connexion doit appartenir à l'un des indiquent les jours et les heures auxquels les tentatives de s sont basées sur le fuseau horaire du serveur NPS (Network Ajouter Annuler

Sélectionnez un groupe	×
Sélectionnez le type de cet objet :	
un groupe	Types d'objets
A partir de cet emplacement :	
assumer.eu	Emplacements
Entrez le nom de l'objet à sélectionner ( <u>exemples</u> ) :	
Utilisateurs du domaine	Vérifier les noms
Avancé	OK Annuler

#### Etape 9 : Cliquez sur « OK » :



#### Etape 10: Cliquez sur « Suivant » :

Nouv	elle stratégie réseau			×
	Spécifiez les o minimum, une	Des conditions conditions qui déterminant si cet condition est nécessaire	tte stratégie réseau est évaluée pou	ir une demande de connexion. Au
Con	ditions :			
	Condition	Valeur		
-	Groupes d'utilisateurs	ASSURMER\Utilisateurs du do	maine	
Desc La c	cription de la condition : ondition Groupes d'utilisate	urs spécifie que l'utilisateur qui ter	ite d'établir la connexion doit apparten Ajouter	ir à l'un des groupes sélectionnés. Modifier Supprimer
			Précédent Suivant	Terminer Annuler

# Etape 11 : Cochez la case « Accès accordé », puis cliquez sur « Suivant » :

Nouvelle stratégie réseau	× *
Spécifier l'autorisation d'accès	
Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de conne à cette stratégie.	xion correspond
Accès accordé	
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.	/
⊖ Accès refusé	
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.	
L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS) Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent au conditi	ons de la stratég
Précédent Suivant Terminer	Annuler

#### III. Installation du rôle requis pour l'autorité de certifications

# Etape 1 : Cochez la case « Services de certificats Active Directory », puis cliquez sur

Assistant Ajout de rôles et de i	ionctionnalités	
sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION SRV-AD.assurmer.eu
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le	serveur sélectionné.
Selection du serveur		Les services de sertificate Active
Rôles de serveurs	Attestation d'integrite de l'appareil     Hyper-V	Directory (AD CS) servent à créer des
Fonctionnalités	Serveur de telécopie	autorités de certification et les
Confirmation	Serveur DNCP (Installe)	émettre et gérer les certificats
Resultats	Service Guardian hôte Services AD DS (Installé) Services AD DS (Installé) Services AD DS (Active Directory Lightwei Services AD RMS (Active Directory Rights M Services d'activation en volume Services d'activation en volume Services de certificats Active Directory Services de fichiers et de stockage (2 sur 12 Services de stratégie et d'accès réseau (Inst Services WSUS (Windows Server Update Se Windows Deployment Services	diverses applications. ght Dire Managei de docur D FS) 2 install tallé) ervices

Etape 2 : Cochez la case « Autorité de certification », puis cliquez sur « Suivant » :

Assistant Ajout de rôles et de l	fonctionnalités	- 🗆 X
Sélectionner des Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	services de rôle Sélectionner les services de rôle à installer pour Services de ce Services de rôle <u>Autorité de certification</u> Inscription de l'autorité de certification via le Web Répondeur en ligne Service Web Inscription de périphérique réseau Service Web Stratégie d'inscription de certificats	SERVEUR DE DESTINATION SRV-AD.assurmer.eu entificats Active Directory Description Une autorité de certification serva émettre et gérer des certificats. Plusieurs autorités de certificator. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.

#### Etape 3 : Cliquez sur « Installer » :





#### Etape 5 : Cliquez sur « Configurer les services de certificats Active Directory »





🔁 Configuration des services de ce	rtificats Active Directory 1	/-		×
Configuration des services de cer Services de rôle 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	rtificats Active Directory 1 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	SERVEUR DE D SRV-AD	ESTINATI	X
	En savoir plus sur les roles de serveur AD CS			
	< Précédent Suivant >	Configurer	Annule	er

#### Etape 7 : Cochez la case « Autorité de certification », puis cliquez sur « Suivant » :

#### Etape 8 : Cochez la case « Autorité de certification d'entreprise » :





#### Etape 9 : Coche la case « Créer une clé privée », puis cliquez sur « Suivant » :

#### Etape 10: Laissez les paramètres par défauts et cliquez sur "Suivant"

Configuration des services de ce	rtificats Active Directory		-		$\times$
Chiffrement pour	l'autorité de certification		SERVEUR DE I SRV-AI	DESTINAT D.assurme	ION r.eu
Informations d'identificati Services de rôle	Spécifier les options de chiffrement				
Type d'installation	Sélectionnez un fournisseur de chiffrement :		Longueur de la	clé :	
Type d'AC	RSA#Microsoft Software Key Storage Provider	~	2048		~
Clé privée	Sélectionnez l'algorithme de hachage pour signer les cert	ificats émis	par cette AC :		
Chiffrement	SHA256	^			
Nom de l'AC	SHA384				
Période de validité	SHA512				
Base de données de certi	SHA1	~			
Confirmation				A In 14	
	privée.	torite de cei	rtification accede	a la cle	
Résultats					
	En savoir plus sur le chiffrement	/			
	< Précédent Suiva	nt >	Configurer	Annul	er

#### Etape 11 : Cliquez sur « Suivant » :

🚡 Configuration des services de ce	rtificats Active Directory	_		$\times$
Nom de l'autorité	de certification	SERVEUR DE DI SRV-AD.	ESTINATI assurme	ION r.eu
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	Spécifier le nom de l'AC Tapez un nom commun pour identifier cette autorité de certification. C certificats émis par l'autorité de certification. Les valeurs des suffixes de automatiquement, mais elles sont modifiables. Nom commun de cette AC : assurmer-SRV-AD-CA Suffixe du nom unique : DC=assurmer,DC=eu Aperçu du nom unique : CN=assurmer-SRV-AD-CA,DC=assurmer,DC=eu En savoir plus sur le nom de l'autorité de certification	Ce nom est ajout u nom unique sc	é à tous nt génér	les ées
	< Précédent Suivant >	Configurer	Annule	er

#### Etape 12 : Cliquez sur « Suivant » :











#### IV. <u>Configuration du serveur RADIUS + Certificats</u>

#### Etape 1 : Cliquez sur « Configurer 802.1X » :

	NPS (tocal)
	Mise en route
1	Le serveur NPS (Network Policy Server) vous permet de créer et de mettre en application sur l'ensemble du réseau de votre organisation des stratégies d'accès réseau portant sur l'authentification et l'autorisation des demandes de connexion.
	Configuration standard
	Sélectionnez un scénario de configuration dans la linte, puis cliquez sur le lien ci-dessous pour ouvrir l'Assistant Scénario.
	Serveur RADIUS pour les connexions câbléer ou sans fil 802.1X 🗸
	Serveur RADIUS pour les connexions câblées ou sans fil 802.1X Longue vous configurez un serveur NVS (Network Policy Server) en tant que serveur RADIUS pour des connexions 802.1X, vous créez des stratégies réseau qui permettent au serveur NPS d'authentifier et d'autoriser
	Configurer 802.1X
	Configuration avancée
	Configuration de modèles

Etape 2 : Sélectionnez la case « Connexion sans fil sécurisées », puis cliquez sur « Suivant » :

Configurer 802.1X 1 × 2	
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.	
O Connexions câblées (Ethemet) 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 defaut ou le modifier.	
RADIUS-WIFI	
Précédent Suivant Terminer Annuler	

Etape 3 : Confirmez le client RADIUS préalablement ajouter, puis cliquez sur « Suivant » :

Configurer 802.1X
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 et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.
Pour spécifier un client RADIUS, cliquez sur Ajouter.
Clients RADIUS :
wapf4e330 Ajouter Modifier Supprimer
Précédent Suivant Terminer Annuler
tape 4 : Cliquez sur « Configurer »
Configurer 802.1X
Configurer une méthode d'authentification
vélectionnez le type de protocole EAP pour cette stratégie.
Type (basé sur la méthode d'accès et la configuration réseau) :
Microsoft: Carte à puce ou autre certificat v Configurer

Etape 5 : Sélectionnez l'AD impacter par l'ajout, puis cliquez sur « OK » :

Précédent Suivant Terminer Annuler

i i worresta des contes o parte de des delles contrades	Propriétés d	les cartes à	puce ou des	autres certificats
---	--------------	--------------	-------------	--------------------

×

×

Ce serveur s'identifie auprès des appelants avant que la connexion ne soit réalisée. Sélectionnez le certificat que vous voulez qu'il utilise comme preuve d'identité.

Certificat délivré à :	assumer-SRV-AD-CA	~
Nom convivial :	assumer-SRV-AD-CA	
Émetteur :	assumer-SRV-AD-CA	
Date d'expiration :	08/01/2030 11:00:52	
	ОК	Annuler

#### Etape 6 : Cliquez sur « Suivant » :

Configurer 802.1X

Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Ajouter
Supprime

# Etape 7 : Cliquez sur « Suivant » :

	1		
Configurer 802	2.1X		×
	Configurer les contrôl	es du trafic	
	Utilisez des réseaux locaux virtues contrôler le trafic réseau.	(VLAN) et des listes de	contrôle d'accès (ACL) pour
Si vos clients R l'affectation de Si vous configu demandes de c	ADIUS (commutateurs d'authentification contrôles de trafic à l'aide d'attributs de rez ces attributs, le serveur NPS invite le connexion authentifiées et autorisées.	et points d'accès sans fi unnel RADIUS, vous po s clients RADIUS à appli	I) prennent en charge uvez configurer ces attributs ici. quer ces paramètres pour les
Si vous n'utilise	z pas de contrôles du trafic ou si vous s	puhaitez les configurer ult	érieurement, cliquez sur Suivant.
Configuration Pour configur	du contrôle du trafic ær les attributs de contrôle du trafic, cliqu	iez sur Configurer.	
			Configurer
			ß
	Précéde	ent Suivant	Terminer Annuler

Etape 8 : Cliquez sur « Terminer » :

Configurer 802.1X ×
Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS
Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.
<ul> <li>Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.</li> <li>Pour modifier la configuration, cliquez sur Précédent.</li> <li>Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.</li> </ul>
Stratégie de demande de connexion : RADIUS-WIFI
Stratégies réseau : RADIUS-WIFI
Details de la contriguiduon
Précédent Suivant Terminer Annuler

Etape 9: Se rediriger vers l'interface web du réseau wifi dans la page network.

## Cliquez sur « Edit »

Ne	etw	orks									
Se R	elect adio	the radio in :	nterface fi lio 1 (5 Gl lio 2 (2.4	ist, and then o Iz) GHz)	enter the configuration parameters.						
	Virt	ual Access	s Points	SSIDs)							
		VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
	<b>~</b>			1	Assurmer-LSD5		WPA Personal 🗸	Disabled $\checkmark$			
			N	/			Show Details				
	,	Add	Edit	Dele	ete						
	Sav	e									

Etape 10 : Cliquez sur « Use global RADIUS settings »

Select the radio Inter Radio:  Radio 1 Radio 2 Radio 2	lace first (5 GHz) (2.4 GH	, and then ) iz)	enter the configuration parameters.	\					
Virtual Access Po	oints (SS	SIDs)							
VAP No. En	able V	LAN ID	SSID Name	SSID Broadcast	Securi	ity	MAC Filter	Channel Isolation	Band Steer
🔽 0 🖂	1	-	Assurmer-LSD5	<ul><li>✓</li></ul>	WP.	Enterprise 🗸	Disabled V	•	
					Hide D	talls			
					WPA	Versions: 🗌 WPA-	TKIP WPA	2-AES	
						Enab	le pre-authentication		
					MFP:	Not Re	equired 🔽 Capable	Required	
					<b>V</b>	se global RADIUS se	erver settings		
					Serve	er IP Address Type:	■ IPv4 ○ IPv6		
					Serve	er IP Address-1:	0.0.0.0	(XOOLXOXLXOXLXOX)	
					Serve	er IP Address-2:		(XOOLXOXLXOXLXOX)	
					Serve	er IP Address-3:		(XXX.XXX.XXX)	
					Serve	er IP Address-4:		(XXX.XXX.XXX)	
					Key-1	t:		(Range: 1-64 Characters)	
					Key-2	2:		(Range: 1-64 Characters)	
					Key-3	3:		(Range: 1-64 Characters)	
					Key-4	4:		(Range: 1-64 Characters)	
						nable RADIUS Acco	unting		
					Active	Server:	Server IP Address-1		
					Broad	icast Key Refresh Ra	te: 86400	Sec (Range: 0-86400, 0 = D	isable, Default: 86400)
					Sessi	on Key Refresh Rate	: 0	Sec (Range: 30-86400, 0 = 1	Disable, Default: 0)
Add	Edit	De	lete						

NPS (Local)	Stratégies réseau		
Clients et serveurs RADIUS	Les stratégies réseau vous permettent d'autoriser les co	nnexions au réseau de manière sélective, et d'indiquer les circonstance	s dans les
<ul> <li>Stratégies</li> <li>Stratégies de demande</li> </ul>	Nom de la stratégie	État Ordre de traitement Type d'accès Source	
<ul> <li>Stratégies réseau</li> <li>Stratégies réseau</li> <li>Gestion</li> <li>Gestion des modèles</li> </ul>	RADIUSA Descendre Désactiver Supprimer Renommer Stratégie dupliquée	Activé 1 Accorder l'accès Non spécifié	
	Conditions Aide : Condition Valeur Type de port NAS Sans fil - Autre OU Sans fil - IEEE 802.11 Groupes Windows ASSURMER\Utilisateurs-WIFI-RADIUS	1	

# Etape 11 : Se diriger vers les "propriétés" de la stratégies réseau

Etape 12 : Cliquer sur "Type de port NAS"

Propriétés de RADIUS-WIFI		×
Vue d'ensemble Conditions Contraintes	Paramètres	
Configurez les contraintes de cette stratégie Si la demande de connexion ne répond pas Contraintes : Contraintes Méthodes d'authentification Délai d'inactivité Délai d'inactivité Délai d'expiration de session ID de la station appelée Restrictions relatives aux jours et aux heures Type de port NAS	<ul> <li>Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.</li> <li>Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.</li> <li>Types de protocoles EAP : <ul> <li>Microsoft: PEAP (Protected EAP)</li> <li>Monter</li> </ul> </li> <li>Descendre</li> </ul> <li>Authentification moins sécurisées : <ul> <li>Authentification chiffrée Microsoft version 2 (MS-CHAP v2)</li> <li>L'utilisateur peut modifier le mot de passe après son expiration</li> <li>Authentification chiffrée Microsoft (MS-CHAP)</li> <li>L'utilisateur peut modifier le mot de passe après son expiration</li> <li>Authentification chiffrée (CHAP)</li> <li>L'utilisateur peut modifier le mot de passe après son expiration</li> <li>Authentification chiffrée (PAP, SPAP)</li> <li>Authentification non chiffrée (PAP, SPAP)</li> <li>Authentification non chiffrée (PAP, SPAP)</li> <li>Autoriser les clients à se connecter sans négocier une méthode d'authentification</li> </ul></li>	
	OK Annuler Appliq	uer

# Etape 13 : Sélectionner uniquement "sans fil – IEEE 802.11"

Configurez les contraintes de cette stratégi Si la demande de connexion ne répond pa Contraintes :	e réseau. s à toutes les contraintes, l'accès réseau est refusé.
Méthodes d'authentification	Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie Types de tunnels pour connexions d'accès à distance et VPN standard
<ul> <li>Délai d'expiration de session</li> <li>ID de la station appelée</li> <li>Restrictions relatives aux jours et aux heures</li> <li>Type de port NAS</li> </ul>	Asynchrone (Mogem)     RNIS synchrone (igne T1)     Vituel (VPN)      Types de tunnels pour connexions 802.1X standard      Ethemet     FDDI     Sans fil - IEEE 802.11     Token Ring      Autres      ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique     ADSL-DMT - Multi-tonalité discrète DSL asymétrique     Asynchrone (Modem)
	Câble V

La configuration du RADIUS est terminé pour que cela fonctionne bien, certains paramètres sont à ajustées.

**Etape Annexe 1 :** Supprimez les autres stratégies de réseaux

📢 NPS (Local)	Stratégies de demande de connexion							
✓ Clients et serveurs RADIUS ☐ Clients RADIUS	Es stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont traitées localement ou si elles sont traisférées vers des serveurs RADIUS distants.							
Groupes de serveurs RA								
✓								
🚞 Stratégies de demande	Nom de la stratégie	État Ordre de traitement	Source					
Stratégies réseau	RADIUS-WIFI	Activé 1	Non spécifié					
No. Contraction	Utiliser l'authentification Windows pour tous les utilisateurs	Activé 1000000	Non spécifié					
> 🜉 Gestion des modèles								
	Utiliser l'authentification Windows pour tous les utilisateurs     Conditions - Si les conditions suivantes sont réunies :							
	Condition							
	restrictions relatives aux jours et aux neures Umanche UUUU-24:00 Lundi UUUU-24:00 Merchedi 00:00-24:00 Jeudi 00:00-24:00 Vendredi 00:00-24:00 Samedi 00:00-24:00							
	Yarametres - Les parametres survants sont appiques :							
	Paramètre Valeur							
	Fournisseur d'authentification Ordinateur local							

#### Etape Annexe 2:

🚯 NPS (Local)	Stratégies de demande de connexion							
<ul> <li>Clients et serveurs RADIUS</li> <li>Clients RADIUS</li> <li>Groupes de serveurs RA</li> <li>Stratégies</li> </ul>	Les stratégies de demande de connexion vous permettent de spécifier si les demandes de connexion sont tratées localement ou si elles sont transférées vers des serveurs RADIUS distants.							
Stratégies de demande	Nom de la stratégie	État	Ordre de tr	aitement	Source			
Stratégies réseau	RADIUS-WIFI	Activé	1		Non spécifié			
No. 10 March 1997	Utiliser l'authentifica	tion Mindowe nour toue las utilisateurs Activá	1000000		Non spécifié			
> 🛃 Gestion des modèles		Annuler						
		Couper						
		Copier						
		Coller						
		Supprimer						
	Conditions - Si le	Tout sélectionner						
		Lecture de droite à gauche						
		Afficher les caractères de contrôle Unicode						
	Restrictions rela	Insérer un caractère de contrôle Unicode >		-24:00 Mardi 00:00-24:00 Mercredi 00:00-24:00 Jeudi 00:00-24:00 Vendredi 00:00-24:00 Samedi 00:00-24:00				
		Ouvrir l'Éditeur IME						
		Reconversion						
	Paramètres - Les paramètres suivants sont appliqués :							
	Paramètre	Valeur						
	Fournisseur d'authentification Ordinateur local							

#### Etape Annexe 3:

-									
🥪 NPS (Local)	Stratégies réseau								
<ul> <li>Clients et serveurs RADIUS</li> </ul>									
Clients RADIUS	Les strategies reseau vous permettent d'autoriser les connexions au reseau de maniere selective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.								
🔡 Groupes de serveurs RA									
✓ I Stratégies									
Stratégies de demande	Nom de la stratégie Etat Ordre de tratement Type d'accès Source								
Stratégies réseau	Activé 1 Accorder l'accès Non spécifié								
Notestion	Connexions au serveur Microsoft de Routage et Accès distants								
> 💐 Gestion des modèles	Connexions à d'autres serveurs d'accès l'indice l'accès Non spécifié								
	Descendre								
	Désactiver								
	Supprimer								
	Renommer								
	🔂 Connexions au serveur Microsoft de Routage et Accès distants Straténie durbliquée								
	- Shareye daphquee								
	Conditions - Si les conditions suivantes sont réunies : Propriétés								
	A transmission of the second sec								
	Condition Valeur Alde								
	ID du fournisseur MS-RAS ^311\$								

#### Etape Annexe 4 :

