Installation et Configuration du WIFI Radius

Auteur : Tom Beaumont et Ilies Salhi Reference : Assurmer Date : 14/02/2024



Page

2/10

Reference

DIFFUSION et VISAS

	Diffusion				
Société / Entité	Destinataires	Fonction	Diffusion	Pour info	
Assumer	Service IT	Procédure	Réseau		

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.0	14/02/2024	Tom Beaumont Ilies SALHI	Procédure d'installation et configuration du WIFI Radius	10

COORDONNEES

	Contacts				
Nom	E-mail	Téléphone			
Tom BEAUMONT	tom.beaumont@assurmer.fr	01.95.24.00.01			
Ilies Salhi	llies.salhi@assurmer.fr	01.95.24.00.01			





Page



Table des matières

-	Installation du service radius sur le premier serveur AD	4
-	Configuration de radius pour une borne WI-FI	5
-	Configuration d'une Autorité de certification	8
-	Sélection du certificat autosigné sur la console NPS	10





Assurmer

Installation du service radius sur le premier serveur AD



21.Sur le serveur Windows 2019, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis

« Ajouter des rôles et fonctionnalités ».

Propriétés du Gestionnaire de serveur

22.Selectionner le rôle services de stratégie et d'accès réseau et ajouter des fonctionnalités





23. Ajout du service de rôle : Serveur NPS



	Titre	Reference	Page	
<u>کې</u>	Installation d'une borne WI-FI	Assurmer	5 / 10	

Configuration de radius pour une borne WI-FI

9	Serveur N	NPS (I
Fichier Ac	tion Affichage ?	
NPS (I I I I	Importer la configuration Exporter la configuration	
⊿ _ Str	Démarrer le service NPS Arrêter le service NPS Inscrire un serveur dans Active Directory	k t
Þ 🏂 Pri	Propriétés Affichage	
N Ge	Aide	_[

23.Lancer le service et faite clic droit sur NPS

24. Inscrire le serveur dans l'Active directory sinon il sera impossible de définir les conditions liées aux groupes/utilisateurs dans la stratégie d'accès distant !

25.Création d'un nouveau client radius sur la console NPS, clic droit nouveau Nom de la borne : wap121 adresse de la borne : 192.168.1.250 secret : Que vous avez définit sur la borne en amont

WPS (Local)	Clients RADIUS	
Clients et serveurs KADIUS Clients RADIUS Groupes de serveurs RADIUS distants	Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau	L.
Stratégies de demande de connexion	Nom convivial Adresse IP Fabricant du périphérique Compatible avec la protection d'accès réseau (NAP) Éta	t
Stratégies de demande de contrexion Stratégies réseau Stratégies de contrôle d'intégrité	wap41e9c0 192.168.90.39 RADIUS Standard No Acti	ivé
Notection d'accès réseau Le Gestion	Propriétés de wap41e9c0	
🛃 Gestion des modèles	Paramètres Avancé	
	Activer ce client RADIUS	
	Sélectionner un modèle existant :	
	APWap307	
	Nom et adresse	
	(hap41eSc)	
	Adresse (IP ou DNS) :	
	192.168.90.39 Vérfier	
	Secret partagé	
	Selectionnez un modele de secrets partages 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	

26.Configuration de la stratégie réseau nouvelle stratégie réseau – nom de la stratégie : Wifi



	Titre	Reference	Page	
2	Installation d'une borne WI-FI	Assurmer	6 / 10	



27.Nous ajouterons le Groupes utilisateurs du domaine

ratégies supp	lémentaires se	aient configu	ées.			5			
Condition	1	Valeur							
Groupes	d'utilisateurs	AIS\Utilis	ateurs du dor	naine					
escription de	la condition :								
escription de a condition G	la condition : roupes d'utilisa	teurs spécifie	que l'utilisate	ur qui tente d'é	tablir la connex	ion doit appa	rtenir à l'ur	n des groupes se	électionnés.
scription de	la condition :	hum márifa	ave Datherte	a a chada d'à	table la concern	an dell mon	at a second at 10 and		Unationalis

28.Selectionner MS-CHAP v2 et MS-CHAP pour authentification par mot de passe.



	Titre	Reference	Page	
<u>ک</u>	Installation d'une borne WI-FI	Assurmer	7 / 10	-

29. Monter Le protocole Extended Authentication Protocol sert pour le transport des données nécessaire à l'authentification.

nfigurez les c la demande d	ontraintes de le connexion	cette stratégi ne répond pa	réseau. à toutes les contraintes, l'accès réseau est ref	fusé.	
ntraintes : Contraintes Méthode S Délai d'ir	s d'authentifi nactivité xpiration de	cation	Autorisez l'accès uniquement aux clients q spécifiées. Les types de protocoles EAP sont négocié l'ordre dans lequel ils sont listés. Types de protocoles EAP :	ui s'authentifient à l'aide des is entre le serveur NPS et le d	méthodes client dans
De la Restricti jours et <i>i</i>	station appel ons relatives sux heures port NAS	ée aux	Microsoft: PEAP (Protected EAP)	admer des : on 2 (MS-CHAP v2) asse après son expiration CHAP) passe après son expiration AP) is négocier une méthode d'au ateur	Monter Descendre

30.Type de port NAS - dans rubrique 801.1X , sélectionner Sans fil – IEEE 802.11 si ce n'est pas un accès sans fil, la demande de connexion est rejetée.

	Configurer	des contraintes
	Les contraintes s	ont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion
24	doivent se confo Server) rejette au configurer de cor	rmer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Polic tomatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas traintes, cliquez sur Suivant.
Configurez les	contraintes de cette	stratégie réseau.
Si la demande	e de connexion ne rép	oond pas à toutes les contraintes, l'accès réseau est refusé.
Contraintes	-	
Contraintes	\$	Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie
🥦 Délai d	inactivité	
🔒 Délai d	expiration de	Types de tunnels pour connexions d'accès à distance et VPN standard
Design ID de la	n station	RNIS synchrone
appelée	e	Synchrone (ligne T1)
Restric	tions relatives	Types de typels pour connevions 802 1X standard
heures	irs et aux	Ethemet
Type d	e port NAS	FDDI
		Token Ring
		Autres
		ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
		ADSL-DMT - Multi-tonalite discrete DSL asymetrique
		Câble V
		Précédent Suivant Terminer Annuler

ESIEE[it]



Configuration d'une Autorité de certification

< Précédent Suivant >



32. Démarrer le gestionnaire de serveur, et cliquez sur l'icône drapeau en haut à droite pour démarrer la configuration.

traduction d'adresses réseau

Installer

Annuler

33.Sur la page Services de rôle, sélectionnez Autorité de certification et cliquez sur Suivant.

• Sur la page Type d'installation, sélectionnez Autorité de certification d'entreprise et cliquez sur Suivant.

• Sur la page Type d'autorité de certification, sélectionnez Autorité de certification racine

Sur la page Clé privée, sélectionnez Créer une nouvelle clé privée et cliquez sur Suivant.



	Titre	Reference	Page	
<u>ک</u>	Installation d'une borne WI-FI	Assurmer	9 / 10	

• Sur la page Chiffrement, entrez les informations comme suit. (Recommandation NIST et globalsign : longueur de clé minimal 2048 et algorithme SHA256)

E.	Configuration des services de certificats Active Dire	ectory	×
Chiffrement p	oour l'autorité de certification	SERVEU	IR DE DESTINATION SRV2012.ais.local
Informations d'identi Services de rôle	ificati Spécifier les options de chiffrement	Inner	r de la clé :
Type d'installation	RSA#Microsoft Software Key Storage Provider	▼ 2048	0.
Clé privée	Sélectionnez l'algorithme de hachage pour signer les certific	cats émis par cette	AC:
Chimrement	SHA256 (2)	~	
Nom de l'AC	SHA384	=	
Periode de validit	e SHA512	101	
Base de donnees de Confirmation Progression Résultats	Certi Autorisez l'interaction de l'administrateur lorsque l'autor privée.	ité de certification	accède à la clé
	En savoir plus sur le chiffrement Précédent	> Configu	urer Annuler

35.Sur la page Nom de l'autorité de certification, acceptez les valeurs par défaut et cliquez sur Suivant.

36.Donné un nom au certificat

Norm de rautorite	de certification	SRV2012.ais.local	
Informations d'identificati	Spécifier le nom de l'AC		
Services de rôle			
Type d'Installation	Tapez un nom commun pour identifier cette autorité de c	certification. Ce nom est ajouté à tous les	
Type d'AC	certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont généré automatiquement, mais elles sont modifiables.		
Clé privée			
Chiffrement	Nom commun de cette AC :		
Nom de l'AC	ais-SRV2012-CA		
Période de validité	Suffixe du nom unique :		
Base de données de certi	DC=ais,DC=local		
Confirmation	Aperçu du nom unique :		
	CN=ais-SRV2012-CA,DC=ais,DC=local		
	En savoir plus sur le nom de l'autorité de certification		

37.Sur la page Période de validité, par défaut la valeur est de 5 année cliquez sur Suivant.





38.Sur la page Base de données de certificats, cliquez sur Suivant.

39.Sur la page Confirmation, passez en revue les informations fournies et cliquez sur Configurer.

Sélection du certificat autosigné sur la console NPS

40.Console NPS – stratégie d'accès réseau – propriétés de la stratégie wifi onglet contraintes

41.Sélectionner Microsoft PEAP

42.Modifier

43.Sélectionner le certificat serveur autosigné. 44.OK pour valider

	k [ficats délivrés]	-
e d'entemble Conditions Contraintes Paramètres onfigurez les contraintes de cette stratégier réleau. I a demandé de connection ne répond pas à touelle les contraintes, l'accès réseau est refusé ontraintes Contraintes Méthodes d'authentification Délai d'authentification de session Delai station appelée Restrictions relatives aux jours et aux heures Type de port NAS Méthodes d'authentification mons sécurisées Méthodes d'authentification mons sécurisées Authentification chifrée Microaft vanno 2 (MS-CHAP v2) Lutilisateur peut modifier le mot de passe après son expiration Authentification chifrée (CHAP) Authentification chifrée (CHAP) Control restriction de passe après son expiration Méthodes d'authentification chifrée (CHAP) Authentification chifrée (Modifier les propriétés EAP Protégé Selectornez le certificat que le serveur doit utiliser comme preuve de son identité auprès du cient. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacers ce certificat. Certificat delivré à : SRV2012.ais.local Nom convival : SRV2012.ais.local Emetiteur : ais-SRV2012.CA Date d'expiration : 15/01/2021 15:57:56 Activer la reconnexion rapide Déconnecter les clents sans chiffrement forcé Types EAP Motifier Supprimer OK Armuler Agouter Modifier Supprimer OK Armuler	

