Installation du serveur RADIUS sur une machine (Remote Authentication Dial-In User Service)

« Le serveur NPS effectue de manière centralisée l'authentification, l'autorisation et la gestion des connexions pour les connexions sans fil, les connexions de commutateurs d'authentification, les connexions d'accès à distance et les connexions VPN, ainsi que pour les connexions aux ordinateurs exécutant la passerelle des services Terminal Services (Passerelle TS). Lorsque vous utilisez le serveur NPS comme serveur RADIUS, vous devez configurer les serveurs d'accès réseau, tels que les points d'accès sans fil et les serveurs VPN, en tant que clients RADIUS sur le serveur NPS. Vous devez également configurer les stratégies réseau que le serveur NPS utilise pour autoriser les demandes de connexion. Vous pouvez configurer la gestion RADIUS de manière à ce que le serveur NPS enregistre les informations de gestion dans des fichiers journaux sur le disque dur local ou dans une base de données Microsoft® SQL Server™. »

Source : https://technet.microsoft.com/fr-fr/library/cc733085%28v=ws.10%29.aspx

Pour installer le serveur RADIUS, lancer l'Assistant ajout de rôles et de fonctionnalités depuis le Gestionnaire de serveur.

2	Assistant Ajout de rôles et de fonctionnalités 📃 🗖 🗙
Avant de comme Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Assistant Ajout de rôles et de fonctionnalités
	Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant. Cliquez sur Suivant pour continuer.
	<pre>< Précédent Suivant > Installer Annuler</pre>

a	Assistant Ajout de rôles et de fonctionnalités
Sélectionner le typ	pe d'installation
Avant de commencer Type d'installation	Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Sélection du serveur Rôles de serveurs	Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Fonctionnalités Confirmation	 Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
Résultats	
	< Précedent Suivant > Installer Annuler
<u>a</u>	Assistant Aiout de rôles et de fonctionnalités

Then i		Assista	init Ajout u	e roles et de lo	netionnances	
Sélectionner l	e ser	veur de (destina	ition		
Avant de commence		Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.				
Type d'installation	1)	Sélectionne	er un serveur	du pool de serveu	rs	
Sélection du serveur		O Sélectionne	er un disque	dur virtuel		
Rôles de serveurs		Pool de serv	eurs			
Fonctionnalités		F (1)				
Confirmation		Filtre :				
Résultats		Nom		Adresse IP	Système d'exploitation	
	2)	V	fr	10.1.151.132	Microsoft Windows Server 2	2012 Standard
		1 ordinateur(s)) trouvé(s)			
		Cette page pré	ésente les ser	veurs qui exécuter	t Windows Server 2012 et qui	ont été ajoutés à l'aide de la rs hors ligne et les serveurs
		nouvellement	ajoutés dont	la collection de do	nnées est toujours incomplète	ne sont pas répertoriés.
					3)	
				< <u>P</u> réc	édent Sui <u>v</u> ant >	Installer Annuler

Sélectionner le rôle « Service de stratégie et d'accès réseau ».

Restance in the second	Assistant Aiout de rôles et de fonctionnalités	_ _ ×
Sélectionner des r	ôles de serveurs	
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Services de rôle Confirmation Résultats	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélect Rôles Serveur DNS (Installé) Service de fichiers et de stockage (Installé) Services AD DS (Installé) Services AD DS (Installé) Services AD FS (Active Directory Federation Servic Services AD LDS (Active Directory Lightweight Dire Services AD RMS (Active Directory Rights Manage Services Bureau à distance Services d'activation en volume Services d'activation en volume Services de certificats Active Directory Services de stratégie et d'accès réseau Services WSUS (Windows Server Update Services)	tionné. Description Les services de stratégie et d'accès réseau fournissent le serveur NPS (Network Policy Server), l'autorité HRA (Health Registration Authority) et le protocole HCAP (Host Credential Authorization Protocol), qui favorisent le maintien de l'intégrité et de la sécurité de votre réseau.
	Assistant Ajout de rôles et de fonctionnalités	> Installer Annuler
Sélectionner des f	onctionnalités	
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Services de rôle Confirmation Résultats	Sélectionnez une ou plusieurs fonctionnalités à installer sur le se Fonctionnalités Assistance à distance Base de données interne Windows BranchCache Chiffrement de lecteur BitLocker Client d'impression Internet Client pour NFS Client TFTP Clustering avec basculement Data Center Bridging Déverrouillage réseau BitLocker Équilibrage de la charge réseau Expérience audio-vidéo haute qualité Windows	erveur sélectionné. Description L'assistance à distance vous permet (ou permet à un technicien du support technique) d'aider les utilisateurs qui rencontrent des problèmes avec leur ordinateur ou qui ont des questions relatives à celui-ci. Cette fonctionnalité permet d'afficher et de contrôler le Bureau de l'utilisateur afin de résoudre les problèmes. Les utilisateurs peuvent également demander de l'aide à des amis ou à des collègues.
	< Précédent Suivant	: > Installer Annuler



Sélectionner le service de rôle « Serveur NPS (Network Policy Server).

B	Assistant Ajout de rôles et de fonctionnalité:	s 🗖 🗖 🗙
Sélectionner des	services de rôle	
Avant de commencer	Sélectionner les services de rôle à installer pour Services de s	tratégie et d'accès réseau
Type d'installation	Services de rôle	Description
Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Services de rôle Confirmation Résultats	1) Serveur NPS (Network Policy Server) Autorité HRA (Health Registration Authority) HCAP (Host Credential Authorization Protocol)	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'intégrité des clients, ainsi que sur l'authentification et l'autorisation des demandes de connexion. Avec NPS, vous pouvez également déployer la protection d'accès réseau (NAP), une technologie de création, d'application et de mise à jour d'une stratégie d'intégrité client.
		
	< Précédent Suiv	ant > Installer Annuler

a	Assistant Ajout de rôles et de fonctionnalités
Confirmer les séle	ections d'installation
Avant de commencer	Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur
Type d'installation	Installer.
Sélection du serveur	Redémarrer automatiquement le serveur de destination, si nécessaire
Rôles de serveurs	cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces
Fonctionnalités	fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Services de stratégie et d'	Services de stratégie et d'accès réseau
Services de rôle	Serveur NPS (Network Policy Server)
Confirmation	
Resultats	
	Exporter les paramètres de configuration Spécifier un autre chemin d'accès source
	< Précédent Suivant > Installer Annuler
A	Assistant Ajout de rôles et de fonctionnalités
Progression de l'i	nstallation
Avant de commencer	Afficher la progression de l'installation
Type d'installation	1 Installation de fonctionnalité
Sélection du serveur	
Rôles de serveurs	Installation demarrée sur tr
Fonctionnalités	Services de stratégie et d'accès réseau
Services de strategie et d'	Serveur NPS (Network Policy Server)
Confirmation	
Résultats	

 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

 Exporter les paramètres de configuration

 < <u>Précédent</u>
 Sui<u>vant ></u>

 Installer
 Annuler

Une fois le rôle serveur NPS installé, il faut configurer le serveur RADIUS.



Configurer 802.1X
Sélectionner le type de connexions 802.1X
 Type de connexions 802.1X: Connexions sans fil sécurisée Lissique vous deployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy connectent via ces points d'accès. 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 sans fil qui se connectent via ces commutateurs. Mon : Connexions sans fil sécurisées Lorsque vous servir du texe par défaut ou le modifier. Connexions sans fil sécurisées 2
Précédent Suivant Terminer Annuler

On peut alors ajouter un ou plusieurs clients Radius :

	Configurer 802.1X	×
	Spécifier les commutateurs 802.1X	
	Spécifiez les commutateurs ou points d'accès sans fil 802.1X(cl	ents RADIUS)
Les clients RA des points d'ac	DIUS sont des serveurs d'accès réseau, à l'image des commutate cès sans fil. Les clients RADIUS ne sont pas des ordinateurs cli€	urs d'authentification et nts.
Pour spécifier	un client RADIUS, cliquez sur Ajouter.	
Clients RADI	JS :	
		Ajouter
		Modifier
		Supprimer
	Précédent Suivant Te	miner Annuler
	Normany diant DADUIS	x
	Nouveau client RADIUS	
Paramètres		
Sélection	ner un modèle existan <u>t</u> :	
		~
Nom et adr	esse	
Nom convit	rial :	
		
Adresse (IP	ou DNS) : 31	Várifier 21
- Secret parts	ané	
Secret parta Sélectionne	aqé ez un <u>m</u> odèle de secrets partagés existant :	<u></u>
Secret parts Sélectionne Aucun	agé ez un <u>m</u> odèle de secrets partagés existant :	Adresse :
Secret parts Sélectionne Aucun	aqé ez un <u>m</u> odèle de secrets partagés existant :	Adresse -
Secret parta Sélectionne Aucun Pour taper automatiqu	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c	Adresse : 231 3) Pour identifier le client à
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c US avec le même secret partagé entré ici. Les secrets parta la casse.	Adresse - 231 3) Pour identifier le client à liste suivante.
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent	agé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c US avec le même secret partagé entré ici. Les secrets parta la casse.	Adresse 231 3 Pour identifier le client à liste suivante. Adresse I <u>P</u> :
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c US avec le même secret partagé entré ici. Les secrets parta la casse.	Adresse 231 3) Pour identifier le client à liste suivante. Adresse I <u>P</u> : 231 5
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez o US avec le même secret partagé entré ici. Les secrets parta la casse.	Adresse 231 3 Pour identifier le client à liste suivante. Adresse I <u>P</u> :
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent © Manuel Secret part ••••••• Confirmez la	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c US avec le même secret partagé entré ici. Les secrets parta la casse. <u>G</u> énérer agé : 7) e secre partagé :	Adresse 231 3) Pour identifier le client à liste suivante. Adresse I <u>P</u> : 231 5
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent © Manuel Secret part Confirmez la	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez o US avec le même secret partagé entré ici. Les secrets parta la casse. <u>G</u> énérer agé : 7) e secre partagé : 8)	Adresse 231 3 Pour identifier le client à liste suivante. Adresse I <u>P</u> :
Secret parta Sélectionne Aucun Pour taper automatiqu client RAD respectent © Manuel Secret part Confirmez la	aqé ez un <u>m</u> odèle de secrets partagés existant : manuellement un secret partagé, cliquez sur Manuel. Pour g ement un secret partagé, cliquez sur Générer. Vous devez c US avec le même secret partagé entré ici. Les secrets parta la casse. <u>G</u> énérer agé : 7) a secre partagé : 8)	Adresse 231 3) Pour identifier le client à liste suivante. Adresse I <u>P</u> : 231 5

Configurer 802.1X		x			
Configurer une méthode d'authentif	ication			-	-
Sélectionnez le type de protocole EAP pour cette stratégie. Type (basé sur la méthode d'accès et la configuration réseau) : Microsoft: PEAP (Protected EAP) 1	2)		en application s clients, ainsi que	ur l'ensemble du sur l'authentifica	réseau de tion et
	Modi Sélectionnez le certificat identité auprès du client, stratégie de demande de Certificat délivré à : Nom convivial : Émetteur : Date d'expiration ;	fier les que le sa Un cert connex	s propriétés erveur doit utilise ificat configuré pr idon remplacera ce . fr . fr . fr . fr	EAP Protégé r comme preuve our EAP Protégé e certificat. 3)	de son dans la
5) Précédent Suivant	Activer la reconnexion Déconnecter les client Types EAP Mot de passe sécurisé (E Ajouter Modif	AP-MSC	hiffrement forcé HAP version 2) Supprimer	4) ок	Monter Descendre Annuler

Il faut ensuite ajouter le ou les groupes d'utilisateurs autorisés à s'authentifier :

Configurer 802.1X	x
Spécifier des groupes d'utilisateurs L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou fonction du paramètre d'autorisation d'accès de la stratégie réseau.	non en
Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.	
Groupes 1) Ajout WifiRadius Supp	er rimer
Sélectionnez un groupe ?	x
Sélectionnez le type de cet objet :	
un groupe Types d'objets	
À partir de cet emplacement :	_
Emplacements	·
Entrez le nom de l'objet à sélectionner (<u>exemples</u>) : <u>WifiRadius</u> 2) 3) Vérifier les nor	ns
Avancé 4) OK Annule	:
5) Précédent Suivant Terminer Annuk	ər

	Configurer 802.1X ×
	Configurer les contrôles du trafic
	Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.
Si vos clients R l'affectation de Si vous configu demandes de c	ADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. rez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les onnexion authentifiées et autorisées.
Si vous n'utilise	z pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.
Configuration Pour configur	du contrôle du trafic er les attributs de contrôle du trafic, cliquez sur Configurer. 1) Configurer
	Précédent Suivant Terminer Annuler

Attributs RADIUS standard Pour envoyer des attribut RADIUS standard, puis o n'est pas envoyé aux clio RADIUS pour connaître RADIUS pour connaître	Attributs spécifiques ts supplémentaires au cliquez sur Modifier. Sents RADIUS. Consu les attributs nécessa	ues au fournisseur ux clients RADIUS, sélectionnez un attribut 5 vous ne configurez pas d'attribut, celui-ci litez la documentation de votre client ires.
Attribute		
Nom	Valeur	
Filter-Id	<non configurée=""></non>	
Tunnel-Type	<non configurée=""></non>	
Tunnel-Medium-Type	<non configurée=""></non>	
Tunnel-Pvt-Group-ID	<non configurée=""></non>	
Tunnel-Assignment-ID	<non configurée=""></non>	
Description :		
		Modifier

	Configurer 802.1X X	
	Configurer les contrôles du trafic Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.	
Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées. Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.		
Configuration of Pour configure	du contrôle du trafic er les attributs de contrôle du trafic, cliquez sur Configurer. Configurer	
	Précédent Suivant Terminer Annuler	

Configurer 802.1X	x	
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. Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration. Pour modifier la configuration, cliquez sur Précédent. Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer. 		
Clients RADIUS : 231) Stratégie de demande de connexion : Connexions sans fil sécurisées Stratégies réseau : Connexions sans fil sécurisées		
Détails de la configuration		
Précédent Suivant Terminer Annuler		

Les clients RADIUS Peuvent aussi être ajoutés en utilisant Powershell. Pour cela, il faut créer un fichier CSV dans lequel on indique :

- Le nom convivial du point d'accès : il permet d'identifier le point d'accès dans la liste des clients
- Son adresse IP
- La clé secrète liée au point d'accès (si celle-ci est la même partout, inutile de la préciser dans ce fichier, elle peut être renseignée directement dans le script, voir exemple ci-dessous)

```
# New-NpsRadiusClient -Address "ADRESSE_IP_DU_POINT_D_ACCES" -Name "NOM_CONVIVIAL"
# -NapCompatible $True -SharedSecret "CLE_SECRETE"
# On renseigne le chemin d'accès au fichier CSV
$filepath = "c:\liste_pa.csv"
# On utilise la fonction d'import de CSV
Import-CSV $filepath -delimiter ";" -Header NAME,IP | Foreach-Object{
    # Pour chague ligne du fichier, on ajoute un nouveau client RADIUR
    New-NpsRadiusClient -Address $_.IP -Name $_.NAME -SharedSecret Clés3crèt3
}
```