

Présentation de solution Radius et son installation

Auteurs : Carvalho Tom, Bagassien Stephen, Dez Sofiane Référence : Assurmer Date : 24/10/2023



DIFFUSION

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

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de page
V1.0	24/10/2023	Carvalho Tom Bagassien Stephen Dez Sofiane	Présentation de solution Radius et son installation	12

COORDONNEES

Nom	E-mail	Téléphone
Carvalho Tom	tom.carvalho@assurmer.fr	01.47.10.00.00
Bagassien Stephen	stephen.bagassien@assurmer.fr	01.47.10.00.00
Dez Sofiane	<u>sofiane.dez@assurmer.fr</u>	01.45.10.00.00

SOMMAIRE

Table des matières

Guide a l'utilisateur à la connexion WIFI Errei	ır ! Signet non défini
---	------------------------

Présentation du fonctionnement d'une solution Radius

Radius, qui signifie Remote Authentication Dial-In User Service, est un protocole d'authentification et d'autorisation largement utilisé dans les réseaux informatiques, en particulier dans les réseaux sans fil et les réseaux d'accès à distance.

Pour comprendre le fonctionnement de RADIUS, nous pouvons diviser le processus en trois parties principales : l'authentification, l'autorisation et l'accounting.

Authentification

Lorsqu'un utilisateur tente de se connecter à un réseau protégé par Radius, la première étape consiste en une demande d'authentification. Cette demande est généralement initiée par le serveur d'accès réseau, tel qu'un point d'accès WIFI, lorsque l'utilisateur essaie de se connecter. Le serveur d'accès réseau envoie alors une demande d'authentification au serveur Radius.

Le serveur Radius reçoit la demande et vérifie les informations d'identification fournies par l'utilisateur. Ces informations peuvent inclure un nom d'utilisateur et un mot de passe, ou d'autres types d'informations d'identification telles que des certificats numériques. Le serveur Radius utilise alors sa base de données interne ou se connecte à d'autres sources d'authentification, telles que des bases de données LDAP ou Active Directory, pour valider les informations d'identification de l'utilisateur.

Une fois que l'utilisateur a été authentifié avec succès, le serveur RADIUS envoie une réponse au NAS, indiquant si l'authentification a réussi ou échoué.

Autorisation

Après avoir authentifié l'utilisateur, le serveur Radius peut également être utilisé pour déterminer les autorisations que cet utilisateur a sur le réseau. Cela peut inclure des informations telles que les services auxquels l'utilisateur est autorisé à accéder, les limitations de bande passante, les restrictions d'accès à certaines ressources, etc.

Le serveur Radius envoie ces informations d'autorisation au serveur d'accès réseau sous forme de réponse à la demande initiale. Le serveur d'accès réseau utilise ensuite ces informations pour configurer les paramètres de la session réseau de l'utilisateur conformément aux politiques définies.

Accounting

Enfin, le protocole Radius prend également en charge la fonction d'accounting, qui consiste à enregistrer les détails des sessions réseau des utilisateurs. Cela inclut des informations telles que les heures de début et de fin de session, la quantité de données transférées pendant la session, etc. Ces informations peuvent être utilisées à des fins de facturation, de surveillance de l'utilisation du réseau, ou à des fins de sécurité et de conformité.

Radius est donc un protocole d'authentification et d'autorisation largement utilisé dans les réseaux informatiques pour contrôler l'accès des utilisateurs au réseau et pour enregistrer les détails de leurs sessions. Il offre une solution centralisée et sécurisée pour gérer l'accès aux réseaux, ce qui en fait un choix populaire dans de nombreux environnements réseau.

Procédure d'installation et de configuration de la solution Radius sous Windows server 2019

I. Installation du service Radius sur le serveur

a. Aller dans le gestionnaire de serveur, cliquer sur gérer puis Ajouter des rôles et fonctionnalités



b. Sélectionner le rôle Services de stratégie et d'accès réseau, puis Ajouter des fonctionnalités

electionner des	roles de serveurs	Assistant Ajout de rôles et de fonctionnalités
Avant de commencer Type d'installation	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélection Rôles	Ajouter les fonctionnalités requises pour Services de stratégie et d'accès réseau ?
Rôles de serveurs Fonchervalités Cambrigation Résultats		Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.
1	Services de déploiement Windows Services de fichiers et de stockage (2 sur 12 install Services de stratègie et d'accès résolu Services WSUS (Windows Servier Update Services) V	 ✓ Inclure les outils de gestion (si applicable) ✓ Inclure des forst insultités

d. Ajouter le rôle Serveur NPS



Configurer Radius pour une borne WIFI

- a. Lancer le service et faire un clic droit sur NPS
- b. Cliquer sur Inscrire un serveur dans l'Active Directory

0	Serveur NPS	5 (1
Fichier Actio	n Affichage ?	
	Importer la configuration Exporter la configuration	7
a Str	Démarrer le service NPS Arrêter le service NPS Inscrire un serveur dans Active Directory	* # *
Þ 🏂 Pre	Propriétés Affichage	
Pia Ge ⊳ 🛃 Ge	Aide	

- d. Faire un clic droit sur Client RADIUS pour créer un nouveau client Radius sur la console NPS
- e. Rentrer la configuration souhaitée

🛞 NPS (Local)	Clients RADIUS	
Clients et serveurs RADIUS 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	N
Stratégies Stratégies de demande de connexion Stratégies récenu	Nom convivial Adresse IP Fabricant du périphérique Compatible avec la protection d'accès réseau (NAP) Éta wap41e5c0 192.168.90.39 RADIUS Standard No Ad	at ctivé
 Stratégies de contrôle d'intégrité November d'accès réseau 		
Gestion	Propriétés de wap41e9c0	
Figure 1 Gestion des modèles	Paramètres Avanoé	
	Activer ce client RADIUS	
	Sélectionner un modèle existant	
	APWap307	
	Nom et advassa	
	Nom convivial :	
	Wap41e9oD	
	Adresse (IP ou DNS) :	
	192.168.90.39 Vérilier	
	Secret partagé	
	Sélectionnez un modèle de secrets partagés existant :	
	Aucun	
	Pour taper manuelement 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 : eve	
	OK Annuler Appiquer	

f. Créer une nouvelle Stratégie de réseau et la nommer



g. Ajouter le groupe utilisateurs du domaine

			Proprietes de Win_Cisco
ue d'ensemble	Conditions	Contraintes	Paramètres
Configurez les c Si la demande c demande de co stratégies suppl	conditions de de connexion nnexion ne ré émentaires se	cette stratégie répond aux co ipond pas aux raient configu	réseau. onditions, le serveur NPS utilise cette stratégie pour autoriser la demande de connexion. Si la « conditions, le serveur NPS ignore cette stratégie et en évalue d'autres, dans l'hypothèse où des urées.
Condition		Valeur	
🏭 Groupes (d'utilisateurs	AIS\Utit	sateurs du domaine
)escription de l la condition Gr	a condition : oupes d'utilisi	ateurs spécifie	que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

- h. Sélectionner MS-CHAP v2 et MS-CHAP pour l'authentification par mot de passe
- i. Monter le Extended Authentication Protocol qui sert pour le transport des données nécessaires à l'authentification

			P	opriétés de W	/ifi_Cisco			
/ue d'ensemble	Conditions	Contraintes	Paramètres					
Configurez les c Si la demande d Contraintes :	ontraintes de le connexion	cette stratégi ne répond par	e réseau. s à toutes les c	ontraintes, l'accès n	éseau est refusé.			
Méthode Délai d'ir Délai d'ir	a d'authentifi nactivité xpiration de	ication	Autorisez I spécifiées Les types l'ordre dar Types de	accès uniquement de protocoles EAP s s lequel ils sont listé rotocoles EAP :	aux clients qui s'auth iont négociés entre le s.	entifient à l'a serveur NP	ide des S et le c	méthodes client dans
ID de la	station appel	ée	Microsof	PEAP (Protected	EAP)			Monter
Restricti	ons relatives aux heures	s aux	4					Descendre
Type de	port NAS		Ajoute Méthodes Auther L'ul Auther Auther Auther Auther Autoris	Modifier d'authentification m tification chiffrée Mi lisateur peut modific fification chiffrée Mi stateur peut modific tification chiffrée (C tification chiffrée re s clients à se co uniquement l'intégri	Supprimer oins sécurisées : crosoft version 2 (MS rr le mot de passe apr r le mot de passe apr HAP) e (PAP, SPAP) nnecter sans négocia té de l'ordinateur	-CHAP v2) ès son expira ès son expira	ation ation ode d`au	thentification
					[ОК		Annuler Appliquer

j.

k. Dans type de port NAS sélectionner Sans fil – IEEE 802.11

	Nouvelle stratégie réseau
Configure Les contraintes s doivent se confi Server) rejette au configurer de co	r des contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion rmer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Poli itomatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas ntraintes, cliquez sur Suivant.
Configurez les contraintes de cette Si la demande de connexion ne ré Contraintes -	s stratégie réseau. pond pas à toutes les contraintes, l'accês réseau est refusé.
Contraintes Contraintes Contraintes Contraintes Contraintes Délai d'inactivité Délai d'expiration de session ID de la station appelée Restrictions relatives aux jours et aux heures Type de port NAS	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 Asynchrone (Modem) RNIS synchrone Synchrone (ligne T1) Vituel (VPN) Types de tunnels pour connexions 802.1X standard Ethemet FDDI Øsnefit - IEEE 802.11 Token Ring Autres ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique
	ADSL-DNT - Multi tonalité discrète DSL asymétrique Asynchrone (Modem) Câble V Précédent Suivant Terminer

Installation et configuration d'une autorité de certification

a. Installation du rôle adcs et outil de gestion



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



- d. Sur la page Services de rôle, sélectionner Autorité de certification et cliquer sur Suivant
- e. Sur le type d'installation, sélectionner Autorité de certification d'entreprise et cliquer sur Suivant
- f. Sur la page type d'autorité de certification, sélectionner Autorité de certification racine
- g. Sur la page Clé privée, sélectionner Créer une nouvelle clé privée et cliquer sur Suivant
- h. Sur la page Chiffrement, entrer les informations comme suit (Recommandation NIST et globalsign : longueur de clé minimal 2048 et algorithme SHA256)

hiffrement pour	l'autorité de certification	,	SERVEUR DE DESTINATIO
informations d'identificati. Services de rôle Type d'installation	Spécifier les options de chiffrement	-	ongueur de la clé
Type d'AC	RSA#Microsoft Software Key Storage Provider		1048
Cié privée	Sélectionnez l'algorithme de hachage pour signer les certif	icats émis pa	r cette AC :
Cofferent Nom de l'AC Période de validité Esse de données de certi Confirmation Programme Alexan	SHA256 SHA304 SHA312 SHA1 Autorisez l'interaction de l'administrateur lonque l'auto privée.	eité de certif	ication accède à la clé
	En savoir plus sur le chiffrement		

- i. Sur la page Nom de l'autorité de certification, accepter les valeurs par défaut et cliquer sur Suivant
- j. Donner un nom au certificat

6	Configuration des services de certificats Active Directory	- 0 ×
Nom de l'autorité	de certification	YEUR DE DESTINATION
informations didentificati Services de rôle Type d'installation Type d'AC Cié privée Chiffrement Nom de tAC Période de validité Base de données de cert Confirmation Proventor Knuttes	Spécifier le nom de l'AC Tapez un nom commun pour identifier cette autorité de certification. Ce no certificate émis par l'autorité de certification. Les valeurs des suffixes du nor automatiquement, mais elles sont modifiables. Nom commun de cette AC :	m est ajouté à tous les. n unique sont générées
	En savoir plus sur le nom de l'autorité de certification	
	< Précédent Sumant > Co-	figurer Annuler

- k. Sur la page Période de validité, par défaut la valeur est de 5 année, cliquer sur Suivant
- I. Sur la page Base de données de certificats, cliquer sur Suivant
- m. Sur la page Confirmation, passer en revue les informations fournies et cliquer sur Configurer

Sélection du certificat autosigné sur la console NPS

- a. Aller dans Console NPS, stratégie d'accès réseau, propriétés de la stratégie wifi, dans l'onglet contraintes
- b. Sélectionner Microsoft PEAP
- c. Cliquer sur Modifier
- d. Sélectionner le certificat serveur autosigné
- e. Cliquer sur OK pour valider

	Propriétés de Will_Cisco	X	Ticats délivrés	-
e d'avaentile Conditions Contraine	Fearline		Modifier les propriètes EAP Protégé	2.
Cardigant les contractes de cette stratégie viseou. 15 le demande de connection en réport pas à tables les contractes, l'acces viseou en refuei. Contractes Contractes Contractes Contractes			Selectornes le certifiad que le serveur duit utilise come preuve de son dente autries du dent. Un certificar configuré pour 50 Present dens le manage de desente de convesion resplaces o crimitades Certificar défent à .	
 Celes d'anactivité Celes d'anactivité Celes d'anactivité Celes d'anactivité appelée Restrictions relatives aux liseur et aux Ameres Tope de part 1465 	As types de protocoles EAP and négociés porte la servieur NFS et la client dans Trade de protocoles EAP (************************************		Bretter : Dele dispiration : 13/01/2021 13:37:56 Chatter is a dente aans delffessent faruet Trons EAP Apute: Huddle: Supprise: OK konder O	
	OK Ander but	100		