Mathieu URGIN Clément MONTMAYEUR

Installation et configuration du protocole Radius sur Windows Server 2022

AssurMer 13.11.2024 Validé par DSI AssurMer

v1.1

Sommaire :

- P0 Introduction et prérequis
- P1 Installation et configuration du service de certificat
- P2 Installation et configuration du service NAP
- P3 Configuration de la borne WiFi
- P4 Dépannage

P0 – Introduction et prérequis

La mise en place du protocole radius sur l'infrastructure d'AssurMer permettra entre autres d'authentifier les utilisateurs sur la/les borne(s) Wifi du réseau via leurs sessions utilisateur, ce qui permettra de gérer les accès de chaque utilisateur.

Pour cela, nous avons mis en place un serveur Active Directory sous Windows Serveur 2022 dans le domaine assurmer.local, dans lequel nous avons créé des utilisateurs, ainsi qu'un groupe de sécurité, accordé pour l'accès au réseau Wifi,



Information AD : Nom Serveur : WSRV2K22-AD1 Adresse IP : 172.16.0.1 (Static) OS : Windows Server 2022 Standard 5 Etendu DHCP activé (1 par VLAN)



Information Borne Wifi :

Modelé : Cisco WAP371 IP : 172.16.0.10 (Static) Sécurité WAP2 - Entreprise

P1 – Installation et configuration du service de certificat

Sur le serveur Active Directory, dans le gestionnaire de serveur, Cliquez sur « Ajoutez des rôles et fonctionnalités »

DÉMARRAGE	1 Configurer ce serveur local
VAPIDE .	2 Ajouter des rôles et des fonctionnalités
	3 Ajouter d'autres serveurs à gérer
OUVEAUTÉS	4 Créer un groupe de serveurs
	5 Connecter ce serveur aux services cloud

Cliquez sur suivant et sélectionnez le service de certificat active directory,

📥 Assistant Ajout de rôles et de fon	ctionnalités	- 🗆 X
Sélectionner des m Avant de commencer	Ôles de serveurs Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec	SERVEUR DE DESTINATION WSRV-AD.assurmer.local tionné.
Sélection du serveur Rôles de serveurs Fonctionnalités AD CS Services de rôle Confirmation Résultats	Attestation d'intégrité de l'appareil Hyper-V Serveur de télécopie Serveur DHCP (Installé) Servicer UNS (Installé) Services Mel (IIS) Services AD DS (Installé) Services AD DS (Installé) Services AD DS (Active Directory Rights Manager Services AD RMS (Active Directory Rights Manager Services AD RMS (Active Directory Rights Manager Services dativation en volume Services dativation en volume Services de certificats Active Directory (AD FS) Services de tederation Active Directory (AD FS) Services WSUS (Windows Server Update Services) Windows Deployment Services	Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.
	< Précédent	Installer Annuler

Puis cliquez sur « Suivant » puis « Installer

			_
< Précédent Su	uivant >	nstaller Annu	ler

Dans le gestionnaire de serveur, dans la partie notification, cliquez sur « Configurez les services de certificats Active Directory,



Ici, vous pouvez définir les identifiants utilisés pour la configuration du service, dans notre cas nous utiliserons l'identifiants par default du domaine, cliquez sur suivant,

Lonfiguration des services de	certificats Active Directory	_		×
Informations d'id	entification	SERVEUR DE I WSRV-AD.a	DESTINAT issurmer.l	'ION local
Informations d'identificati Services de rôle Confirmation	Spécifier les informations d'identification pour services de rôle	configurer l	85	
	Pour installer les services de rôle suivants, vous devez être membre local : Utiliser l'autorité de certification autonome Inscription de l'autorité de certification via le Web Répondeur en ligne Pour installer les services de rôle suivants, vous devez être membre d'entreprise : Autorité de certification d'entreprise Service Web Istratégie d'inscription de certificats Service Web Istratégie d'inscription de certificats Service Web Istratégie d'inscription de certificats Service d'inscription de périphériques réseau	du groupe Admin du groupe Admin	istrateurs	
	Informations d'identification : ASSURMER\Administrateur	Modifier		
	En savoir plus sur les rôles de serveur AD CS	/		
	< Précédent Suivant >	Configurer	Annul	er

Ensuite, cochez « Autorité de certification », et faites suivant,



Laissez « Autorité de certification d'entreprise » coché, puis faites suivant,

L Configuration des services de certificats Active Directory Type d'installation Spécifier le type d'installation de l'AC Informations d'identificati... Services de rôle Les autorités de certification d'entreprise peuvent utiliser les services de domaine Ac Type d'AC Autorité de certification d'entreprise Clé privée Les autorités de certification d'entreprise doivent être membres d'un domaine et Chiffrement O Autorité de certification autonome Nom de l'AC Les autorités de certification autonomes peuvent être membres d'un groupe de t Période de validité Base de données de certi. Confirmation

Faites de même pour le type d'autorité de certification, cochez « Autorité de certification racine » puis, faites suivant,



Cliquez maintenant sur « Crée une clef privée » celle-ci servira au serveur radius pour l'authentification, puis cliquez sur suivant,

ᡖ Configuration des services de certificats Active Directory

Clé privée	
Informations d'identificati Services de rôle Type d'installation Type d'AC Clé privée	Spécifier le type de la clé privée Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée. Ocréer une clé privée Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	 Utiliser la clé privée existante Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC. Sélectionner un certificat et utiliser sa clé privée associée Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée. 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.

Ici, on définit le type de chiffrement utilisé pour l'authentification par certificat,

Le chiffrement SHA256 étant déjà très sécurisé, avec une longueur de clé de 2048, c'est le moyen le plus adapté dans notre situation, cliquez ensuite sur suivant,

L Configuration des services de cen	tificats Active Directory		- o ×
Chiffrement pour	l'autorité de certification		SERVEUR DE DESTINATION WSRV-AD.assurmer.local
Informations d'identificati Services de rôle	Spécifier les options de chiffrement		
Type d'installation	Sélectionnez un fournisseur de chiffrement :		Longueur de la dé :
Type d'AC	RSA#Microsoft Software Key Storage Provider	•	2048
Clé privée	Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :		
Chiffrement	(SHA256)		
Nom de l'AC	SHA384		
Période de validité	SHA512		
Base de données de certi	SHA1		
Confirmation	MD5 MD4		
	MD2		
	Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.		

Dans cette partie, laissons les valeurs par default, cliquez sur suivant,

📠 Configuration des services de certificats Active Directory

Nom de l'autorité	de certification
Informations d'identificati	Spécifier le nom de l'AC
Services de rôle	
Type d'installation	Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées autor
Type d'AC	Nom commun de cette AC :
Clé privée	assurmer-WSRV-AD-CA
Chiffrement	
Nom de l'AC	Suffixe du nom unique :
Période de validité	DC=assurmer,DC=local
Base de données de certi	Aperçu du nom unique :
Confirmation	CN=assurmer-WSRV-AD-CA,DC=assurmer,DC=local

Ici on peut définir la période de validité du certificat avant d'être renouvelé, 2 ans est un bon compromis sécurité/praticité,



Cliquez sur suivant, puis « Configurer » et enfin « Close »

La configuration du service de certificat Active Directory est maintenant terminé.

P2 – Installation et configuration du service NAP

Dans cette seconde partie, nous installons le service permettant de gérer les politiques d'accès réseau (NAP).

Cela inclut la configuration des règles pour authentifier et autoriser les utilisateurs ou appareils.

Retournez dans le gestionnaire de serveur et une ajoutez une nouvelle fonctionnalité,



Sélectionnez « Service de stratégie et d'accès réseau, puis faites « Suivant »

Avant de commencer	COLES DE SELVEULS Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.	WSRV-AD.assurmer.local
Type d'installation	Rôles	Description
Sélection du serveur Rôles de serveurs Fonctionnalités Services de stratégie et d' Confirmation Résultats	Accès à distance Attestation d'intégrité de l'appareil Hyper-V Serveur DHCP (Installe) Serveur DNS (Installe) Services AD DDS (Installe) Services Bureau à distance Services d'activation en volume Services de certificats Active Directory (AD FS) Services de fédération Active Directory (AD FS) Services de fédération Active Directory (AD FS) Services de stratégie et d'accés réseau Services WSUS (Windows Server Update Services) Windows Deployment Services	Les services de stratègie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

Puis « Installer »



Passons ensuite à la configuration du NAP, dans le gestionnaire de service cliquez sur « Service de stratégie et d'accès réseau (NPAS) et faites un clic droit sur le nom de machine, puis Serveur NPS,

📠 Gestionnaire de serveur		
Gestionnai	re de serveur • Services de stratégie	et d'accès réseau (NPAS)
 Tableau de bord Serveur local Tous les serveurs AD CC 	SERVEURS Tous les serveurs 1 au total	
AD CS	Nom du serveur Adresse IPv4 Facilité de gestion	Dernière mise à jour Activation de W
I∎I AD DS ÎE DHCP a DNS a Services de fichiers et d ▷ I Services de stratégie et	WSRV-AD 172.16.0.5 En ligne - Compteurs de perform.	Ajouter des rôles et fonctionnalités Ajouter des rôles et fonctionnalités Arrêter le serveur local Gestion de l'ordinateur Connexion Bureau à distance Windows PowerShell
		Configurer l'association de cartes réseaue 3
	ÉVÉNEMENTS Tous les événements 0 au total	Serveur NPS (Network Policy Server) Gérer en tant que Démarrer les compteurs de performances Actualiser
	Filtrer P 🗎 🔻 🗎	Copier
	Nom du serveur ID Gravité Source Journal Date et heure	

Choisissez « Serveur RADIUS pour les connexions câblées ou sans fil 802.1X, et cliquez sur Configurez 802.1X,



Sélectionnez « Connexions sans fils sécurisé, et donnez le nom que vous souhaitez, cliquez ensuite sur suivant,



Dans cette partie de la configuration nous ajoutons le client radius, et dans ce cas, la borne Wifi, Cliquez donc sur « Ajouter » et renseignez les informations de la bornes Wifi que vous possédez,

Configurer 80.	2.1X	×	Nouveau client RADIUS
	Spécifier les commutateurs 802.1X Spécifiez les commutateurs ou points d'accès sans fil 802.1X(clients RADIUS)		Paramètres Sélectionner un modèle existant :
Les clients R/ des points d'a Pour spécifier Clients RADI	ADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentifica ccès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients. : un client RADIUS, cliquez sur Ajouter.	ion et ent	Nom et adresse 2 Nom convivial 2 (WAP371-B1-BA1=) Adresse (IP ou DNS): 3
	(Ao	ter)	(172 16.0 10) Vértier
	Mod	ner	Sélectionnez un modèle de secrets partagés existant :
	Sup	primer	Aucun
	2		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. automatique de la construction de la construction de la construction anuel de la construction de la construction de la construction anuel de la construction de la construction de la construction anuel de la construction de la construction de la construction automatique de la construction de la construction de la construction continuez le secret partagé : continuez le secret partagé : automatique de la construction
	Précédent Suivant Terminer Ann	uler	OK Annuler

Définissez :

- Le nom de la borne
- Son adresse IP
- Le mot de passe qu'utilisera la borne pour se connecter au radius

Cliquez ensuite sur OK, puis Suivant

Pour la méthode d'authentification, sélectionnez « Microsoft : PEAP » puis cliquez sur « Suivant »

Configurer 802.1X	×
Configurer une méthode d'authentification	
Sélectionnez le type de protocole EAP pour cette stratégie.	
Type (basé sur la méthode d'accès et la configuration réseau) :	
Microsoft: PEAP (Protected EAP)	Configurer
1	
× ²	
Précédent Suivant Terminer	Annuler

Ici nous ajoutons le groupe utilisateur qui permettra l'accès pour les utilisateurs au Wifi de l'entreprise,

Cliquez sur « Ajouter », sélectionnez le groupe accès crée pour cela puis faites « OK » puis « Suivant »

onfigurer au	2.1X		
	Spécifier des	s groupes d'utilisateu	irs
	L'accès des utilisate fonction du paramè	eurs membres du ou des groupes s tre d'autorisation d'accès de la stra	sélectionnés sera autorisé ou non atégie réseau.
our sélection ratégie s'app	rer des groupes d'utilisa lique à tous les utilisateu	teurs, cliquez sur Ajouter. Si aucun g urs.	roupe n'est sélectionné, cette
Groupes			Ajouter Supprimer
Sélectionne	z un groupe		×
Sélectionne	z le type de cet objet :		
un groupe			Types d'objets
À partir de c	et emplacement :		
assumer.lo	cal		Emplacements
Entrez le nor	n de l'objet à sélectionn	er (exemples) :	
Entrez le nor Acces-WifiF	n de l'objet à sélectionn	er (<u>exemples</u>) :	Vérifier les noms
Entrez le nor Acces-WifiF	n de l'objet à sélectionn	er (<u>exemples</u>) :	Vérifier les noms
Entrez le nor Acces-WifiF Avancé	n de l'objet à sélectionn	er (<u>exemples</u>) : 3	Vérfier les noms

Faites « Suivant » et Enfin « Terminer »

P3 – Configuration de la borne WiFi

Maintenant que le radius est correctement configuré pour accueillir la borne WiFi, ainsi que les utilisateurs, configurons la borne Wifi en elle-même,

Branchez la borne Wifi sur votre infrastructure, dans le manuel d'utilisation, récupérez l'adresse IP par défaut de la borne, et connectée un poste configuré sur la même plage d'IP que la borne,

Dans le cas de la borne Cisco WAP371, l'adresse IP par default est la 192.168.1.245,

Via un navigateur accéder à l'interface utilisateur, le mot de passe par default est « cisco »

uluulu. Wireless Access Point		Userna Passer		
			Login	
 2014 David Spokens, Inc. All rights minimud. Cloca, The Cloca Significant Cloca Systems are registered trademarks or trademarks of Cloca 	Systems, Inc. and/or its attilutes in the United States and certain (other countries.		

Ignorez l'utilitaire de configuration de base, et allez dans la partie « LAN » puis « VLAN and IPV4 Adress »

cisco WAP371	Wireless-AC/N Dual	Radio Access Point with Single Point Setup
Getting Started	VI AN and IPv/ Addres	ee
Run Setup Wizard	VLAN and IPV4 Addres	55
 Status and Statistics 	Global Settings	
 Administration 	MAC Address	70:01:05:21:17:20
LAN	WAG AUGIESS.	10.01.05.31.11.50
Port Settings	Untagged VLAN:	Enable
VLAN and IPv4 Address	Lintaged VLANUD:	1 (Range 1, 4004 Default 1)
IPv6 Tunnel	Undagged VLAN ID.	(Range, 1 - 4034, Delauir, 1)
LLDP	Management VLAN ID:	1 (Range: 1 - 4094, Default: 1)
 Wireless 		
 System Security 	IPv4 Settings	
Client QoS	Connection Tune:	O DHCP
SNMP	Connection Type:	Static IP
Single Point Setup	Static IP Address:	172 16 0 10
Captive Portal		
	Subnet Mask:	255 . 255 . 255 . 0

Ici, changez l'adresse IP de la borne par l'adresse souhaité, ici nous choisirons 172.16.0.10/24, puis appliquez la configuration,

Ensuite, reconnectez-vous à la borne sur sa nouvelle adresse IP, et dans la partie « Administration » puis « User Accounts » changez le mot de passe par defaut de la borne,

▲ Etape Importante : L'utilisation de mot de passe faible constitue environ 30% des attaques cyber malveillante

cisco WAP371 V	1 Wireless-AC/N Dual Radio Access Point with Single Point Setup	
Getting Started Run Setup Wizard	User Accounts	
 Status and Statistics 	User Account Table	
Administration	User Name User Level New Password Confirm New Password Password Strength Meter	
System Settings	Cisco Read/Write Access	
Time Settings	Add Edit Delete	
Lug descrigts Email Adat LED Daplay HTTP-HTTPS Service Management Access Cont Manage Timware Download/Backup Configuration Rebod Discovery - Bonjour Packet Capture Support Information > LAN Wireless > System Security > Cleft OoS > SIMUP > Single Point Setup > Captive Portal	Save Contraction of the second	

Après cela fait nous pouvons configurer le réseau étendu, allez dans « Wireless » puis « Networks », dans SSID Name, choisissez le nom de vos réseaux Wifi étendu, modifier le VLAN du réseau, et dans le type de sécurité, choisissez « WPA Entreprise » pour faire fonctionner l'authentification utilisateur,

cisco WAP371	Nirele	ss-AC	/N Du	ual Rac	lio Access Point with S	ingle Point	Setup			
Getting Started	Netw	orks								
Run Setup Wizard										
 Status and Statistics 	Select	the radio in	nterface fi	rst, and then	enter the configuration parameters.					
 Administration 	Radio	c 🔿 Rad	io 1 (5 GH	łz)						
► LAN		Rad	io 2 (2.4 C	3Hz)						
🖸 Wireless	Virt	ual Access	Points (SSIDs)						
Radio 2 Roque AP Detection		VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
(Networks)				40	ASSURMER-Particuliers-MCC		WPA Enterprise 🗸	Disabled ~		
Wireless Multicast Forward Scheduler							Show Details			
Scheduler Association	0	1	12	30	ASSURMER-Business-MCC	2	WPA Enterprise ~	Disabled ~		
Bandwidth Utilization MAC Filtering					Lines and the second		Show Details			
WDS Bridge	0	2	87	20	ASSURMER-Compta-MCC		WPA Enterprise ~	Disabled ~		
WorkGroup Bridge							Show Dataile			
 System Security 			-		1	1		1		
 Client QoS 	U	3	124	10	ASSURMER-Direction-MCC	C	WPA Enterprise V	Disabled ~		
SNMP							Show Details			
Single Point Setup		4	0	1	ASSURMER-Administration-MCC	1	WPA Enterprise 🗸	Disabled \sim		
Captive Portal							Show Details			
	C	Add	Edit	Del	ieto .					
	Sav	/e								

Effectuez la même manipulation pour le réseau en 2,4Ghz,

Networks
Select the radio interface first, and then enter the configuration parameters.
Radio: 🔘 Radio 1 (5 GHz)
Radio 2 (2.4 GHz)

Dans la dernière étape, configurez l'authentification de la borne sur le radius, rendez-vous dans la partie « System Security » puis « Radius Server »

cisco WAP371	Wireless-AC/N Dual Radio Access	Point with Single Point Setup
Getting Started		
Run Setup Wizard	RADIUS Server	
 Status and Statistics 	Server IP Address Type: IPv4	
 Administration 	O IPv6	
LAN Wireless	Server IP Address-1: (172.16.0.1) (x	oc.aoc.aoc.)
System Security	Server IP Address-2:	0.000.000.000)
RADIUS Server 802.1X Supplican 2	Server IP Address-3:	0000000000)
WPA-PSK Complexity	Server IP Address-4: (x)	000000000000000000000000000000000000000
Client QoS	Key-1: (F	lange: 1 - 64 Characters)
SNMP Single Point Setup	Key-2: (F	tange: 1 - 64 Characters)
Captive Portal	Key-3:	lange: 1 - 64 Characters)
	Кеу-4: (Я	tange: 1 - 64 Characters)
	RADIUS Accounting: Z Enable	
	Save	

Renseigner l'adresse IPV4 du serveur Radius configuré précédemment, ainsi que le mot de passe que vous avez choisi (voir page 13) et faites « Save »

Désormais, le réseau configuré précédemment devrais apparaitre dans les réseau Wifi,

Pour donner l'accès à un utilisateur, attribuez lier le groupe « Acces-WifiPro »

nvironn	ement	Sessions	Co	ntrôle	à distanc	e P	rofil des se	ervices	Bureau à dis	tance	CO
énéral	Adress	e Com	ote P	rofil	Téléph	ones	Organis	ation	Membre de	Appe	l entr
Membre	e de :										
Nom						Dos	sier Servic	es de d	domaine Acti	ve Direc	tory
Acces	-WifiPro					assu	irmer.local	/Assur	Mer/Groupes	(
٢.											>
< Ajou	iter	Supp	rimer	_			_	_			>
< Ajou	iter	Supp	rimer								>
< Ajou	ter	Supp	rimer	s du d	omaine			_			>
< Ajou Groupe	ter principa	Supp I : Utiliz	rimer sateurs	s du de	omaine est pas u	tile de	e modifier l	e grou	pe principal, t	sauf si v	vous
< Ajou Groupe Défini	tter principa r le grou	Supp I : Utilit pe princip	rimer sateurs al	s du de Il n' disp	omaine est pas u posez de	tile de client:	e modifier l	e grou h ou d	pe principal, : 'applications	sauf si v compat	vous
< Ajou Groupe Défini	tter principa r le grou	Supp I : Utilit pe princip	rimer sateurs al	s du du II n' disp PO	omaine est pas u posez de SIX.	tile de client:	e modifier l s Macintos	e grou h ou d	pe principal, i 'applications	sauf si v compat	> vous ibles
< Ajou Groupe Défini	ter principa r le grou	Supp I : Utilis	rimer sateurs al	s du d Il n' disp PO	omaine est pas u posez de SIX.	tile de	e modifier l s Macintos	e grou h ou d	pe principal, l'applications	sauf si v compat	> vous ibles

Désormais, vous pourrez vous connecter via les identifiants cette utilisateur sur ce réseau Wifi,

P3 – Dépannage

En cas de problème, voici un guide des problèmes les plus courant que vous pourrez rencontrer :

1 - « Nous n'avons pas pu nous connecter à ce réseau »



Solutions : Vérifier le paramétrage telle que :

- Mot de passe d'authentification de la borne sur le radius
- Certificat utilisateur
- Mot de passe utilisateur

2 – « Connecté pas d'internet »



Vérifier que votre serveur DHCP est actif et qu'il est configuré sur le bon VLAN,

3 – Pas d'accès aux machines sur le réseau



Vérifier que votre réseau Wifi étendu est configuré sur le bon VLAN