Configuration de 802.1x - PEAP avec FreeRadius et WLC 8.3

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Configuration Diagramme du réseau Installer httpd Server et MariaDB Installer PHP 7 sur CentOS 7 Installer FreeRADIUS **FreeRADIUS** WLC en tant que client AAA (Authentication, Authorization, and Accounting) sur FreeRADIUS FreeRADIUS en tant que serveur RADIUS sur WLC **WLAN** Ajouter des utilisateurs à la base de données FreeRADIUS Certificats sur freeRADIUS Configuration du périphérique final Importer un certificat FreeRADIUS Créer un profil WLAN Vérification Processus d'authentification sur WLC Dépannage

Introduction

Ce document décrit comment configurer un réseau local sans fil (WLAN) avec la sécurité 802.1x et le protocole PEAP (Protected Extensible Authentication Protocol) en tant que protocole EAP (Extensible Authentication Protocol). FreeRADIUS est utilisé comme serveur RADIUS (Remote Authentication Dial-In User Service) externe.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Linux
- Éditeur Vim
- Contrôleurs LAN sans fil AireOS (WLC)

Remarque : ce document est destiné à donner aux lecteurs un exemple de configuration requise sur un serveur FreeRADIUS pour l'authentification PEAP-MS-CHAPv2. La configuration du serveur FreeRADIUS présentée dans ce document a été testée dans les travaux pratiques et a fonctionné comme prévu. Le centre d'assistance technique Cisco (TAC) ne prend pas en charge la configuration du serveur RADIUS gratuit.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CentOS7 ou Red Hat Enterprise Linux 7 (RHEL7) (1 Go de RAM recommandé et au moins 20 Go de disque dur)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Diagramme du réseau



Installer httpd Server et MariaDB

Étape 1. Exécutez ces commandes pour installer le serveur httpd et MariaDB.

[root@tac-mxwireless ~]# yum -y update [root@tac-mxwireless ~]# yum -y groupinstall "Development Tools" [root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb Étape 2. Démarrez et activez httpd (Apache) et le serveur MariaDB.

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb

Étape 3. Configurez les paramètres MariaDB initiaux pour le sécuriser.

[root@tac-mxwireless ~] #mysql_secure_installation

Note: Exécutez toutes les parties de ce script. Il est recommandé pour tous les serveurs MariaDB en production. Lisez attentivement chaque étape.

In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none): OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation.

Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! - Removing privileges on test database... ... Success! Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB! Etape 4. Configurez la base de données pour freeRADIUS (utilisez le même mot de passe configuré à l'étape 3).

[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius" [root@tac-mxwireless ~]# mysql -u root -p -e "show databases" [root@tac-mxwireless ~]# mysql -u root -p MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword"; MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q Bye

Installer PHP 7 sur CentOS 7

Étape 1. Exécutez ces commandes pour installer PHP 7 sur CentOS7.

```
[root@tac-mxwireless ~]# cd ~
[root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh
[root@tac-mxwireless ~]# sudo bash setup-ius.sh
[root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common
[root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel
php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear
[root@tac-mxwireless ~]# sudo apachectl restart
```

Installer FreeRADIUS

Étape 1. Exécutez cette commande pour installer FreeRADIUS.

[root@tac-mxwireless ~]# yum -y install freeradius freeradius-utils freeradius-mysql freeradiussqlite

Étape 2. Faites radius.service démarrer après mariadb.service.

Exécutez cette commande :

```
[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service
Ajouter une ligne dans la section [unité]:
```

After=mariadb.service [Unité] doit ressembler à ceci :

[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target After=mariadb.service

Étape 3. Démarrez et activez freeradius pour démarrer au démarrage.

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service

Étape 4. Activez le pare-feu pour la sécurité.

[root@tac-mxwireless ~]# systemctl enable firewalld [root@tac-mxwireless ~]# systemctl start firewalld [root@tac-mxwireless ~]# systemctl status firewalld

Étape 5. Ajoutez des règles permanentes à la zone par défaut pour autoriser les services http, https et radius.

```
[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius'
[root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success
Étape 6. Rechargez le pare-feu pour que les modifications prennent effet.
```

[root@tac-mxwireless ~]# firewall-cmd --reload

FreeRADIUS

Afin de configurer FreeRADIUS pour utiliser MariaDB, suivez ces étapes.

Étape 1. Importez le schéma de base de données RADIUS pour remplir la base de données RADIUS.

[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/modsconfig/sql/main/mysql/schema.sql

Étape 2. Créez un lien logiciel pour Structured Query Language (SQL) sous /etc/raddb/modsenabled.

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ Étape 3. Configurez le module SQL /raddb/mods-available/sql et modifiez les paramètres de connexion à la base de données pour qu'ils correspondent à votre environnement.

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql La section SQL doit être similaire à ceci.

sql {

driver = "rlm_sql_mysql"
dialect = "mysql"

Connection info:

server = "localhost"

```
port = 3306
login = "radius"
password = "radpass" # Database table configuration for everything except Oracle radius_db =
"radius" } # Set to 'yes' to read radius clients from the database ('nas' table) # Clients will
ONLY be read on server startup. read_clients = yes # Table to keep radius client info
client_table = "nas"
```

Étape 4. Modifiez le droit du groupe de /etc/raddb/mods-enabled/sql en radiusd.

[root@tac-mxwireless ~] # chgrp -h radiusd /etc/raddb/mods-enabled/sql

WLC en tant que client AAA (Authentication, Authorization, and Accounting) sur FreeRADIUS

Étape 1. Modifiez /etc/raddb/clients.conf afin de définir la clé partagée pour le WLC.

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf Étape 2. En bas, ajoutez l'adresse IP du contrôleur et la clé partagée.

client{ secret = shortname = }

FreeRADIUS en tant que serveur RADIUS sur WLC

IUG:

Étape 1. Ouvrez l'interface utilisateur graphique du WLC et accédez à **SECURITY > RADIUS > Authentication > New** comme indiqué dans l'image.

ahaha		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	n Home
Security	RADIUS Authentication Servers	Apply New
▼ AAA General	Auth Called Station ID Type 🛛 🗛 MAC Address:SSID 🛛 🗸	
 RADIUS Authentication 	Use AES Key Wrap 🗌 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Accounting Fallback	MAC Delimiter V	
DNS	Framed MTU 1300	

Étape 2. Complétez les informations du serveur RADIUS comme indiqué dans l'image.

RADIUS Authentication Servers > New					
Server Index (Priority)	2 ~				
Server IP Address(Ipv4/Ipv6)	a.b.c.d				
Shared Secret Format	ASCII 🗸	•			
Shared Secret	•••••				
Confirm Shared Secret	•••••				
Key Wrap	(Designed for a constraint of the second	r FIPS customers and requires a key wrap compliant RADIUS server)			
Port Number	1812				
Server Status	Enabled \sim				
Support for CoA	Disabled $$				
Server Timeout	10 second:	5			
Network User	🗹 Enable				
Management	🗹 Enable				
Management Retransmit Timeout	2 seconds				
IPSec	Enable				

CLI :

> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>

WLAN

IUG:

Étape 1. Ouvrez l'interface utilisateur graphique du WLC et accédez à **WLANs > Create New >** Goas présenté dans l'image.

،، ،،، ،، cısco	<u>M</u> ONITOR <u>W</u> LANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs							
▼ WLANS WLANS ▶ Advanced	Current Filter: No	ne [<u>Cha</u>	nge Filter] [Cl	<u>ear Filter]</u>			Create Ne	ew 🗸 Go

Étape 2. Choisissez un nom pour l'identificateur SSID (Service Set Identifier) et le profil, puis cliquez sur Applyas comme indiqué dans l'image.

WLANs > New		< Back	Apply
Туре	WLAN ~		
Profile Name	profile-name		
SSID	SSID-name		
ID	2 ~		

CLI :

> config wlan create <id> <profile-name> <ssid-name> Étape 3. Attribuez le serveur RADIUS au WLAN.

CLI :

> config wlan radius_server auth add <wlan-id> <radius-index>
IUG:

Accédez à **Security > AAA Servers** et choisissez le serveur RADIUS souhaité, puis cliquez sur **Apply** comme indiqué dans l'image.

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
		^
Select AAA servers below to override use of default servers on this WLAN		
RADIUS Servers		
RADIUS Server Overwrite interface Enabled		
Authoptication Service: Accounting Service: FAD Department		
Finabled Penabled Finabled		
Server 1 IP:172.16.15.8, Port:1812 V None V		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 🔽 Interim Interval 0 Seconds		~
<	2	>

Étape 4. Augmentez éventuellement la durée de la session.

CLI :

>	config	wlan	session-timeout	<wlan-id></wlan-id>	<session-timeout-seconds></session-timeout-seconds>
IL	JG:				

Accédez à **Avancé > Activer le délai d'attente de session >** cliquez sur **Appliquer** comme indiqué dans l'image.

WL	ANs > Edit 'ise-p	rof				< Back	Apply
6	eneral Security	QoS Policy-Mapping	Adva	inced			
	Allow AAA Override	Enabled		DHCP		_	
	Coverage Hole Detection	🗹 Enabled		DHC) Server	Override	
	Enable Session Timeout	28800 Session Timeou (secs)	1	DHCI Assig	9 Addr. Inment	Required	
	Aironet IE	Enabled		OEAP			
	Diagnostic Channel <u>18</u>	Enabled		Split	Tunnel	Enabled	
	Override Interface ACL	IPv4 None 🗡	IPv6 None ∨	Manage	ment Frame Pr	rotection (MFP)	
	Layer2 Acl	None \vee					
	URL ACL	None 🗸		MFP	Client Protectio	n 🛃 Optional 🗸	
	P2P Blocking Action	Disabled \lor		DTIM Pe	eriod (in beacor	n intervals)	
	Client Exclusion ²	Enabled 60 Timeout Value (secs)		802.:	11a/n (1 - 255)) 1	
	Maximum Allowed Clients <u>^g</u>	0		802.: NAC	11b/g/n (1 - 25	55) 1	
<	Static IP Tunneling	□		NAC	State None	$\overline{\mathbf{v}}$	>

Étape 5. Activez le WLAN.

CLI :

```
> config wlan enable <wlan-id>
IUG:
```

Naviguez jusqu'à **Général > Statut > Cliquez sur Activé > Cliquez sur Appliquer** comme indiqué dans l'image.

LANs > Edit 'ssid-r	ame'	< Back
ieneral Security	QoS Policy-Mapping Advanced	
Profile Name	ssid-name	
Туре	WLAN	
SSID	ssid-name	
Status	Enabled	

Ajouter des utilisateurs à la base de données FreeRADIUS

Par défaut, les clients utilisent des protocoles PEAP, mais freeRadius prend en charge d'autres méthodes (non couvertes dans ce guide).

Étape 1. Modifiez le fichier /etc/raddb/users.

est le nom d'utilisateur et Cisco123 le mot de passe.

user1 Cleartext-Password := <Cisco123> Étape 3. Redémarrez FreeRadius.

[root@tac-mxwireless ~]# systemctl restart radiusd.service

Certificats sur freeRADIUS

FreeRADIUS est fourni avec un certificat d'autorité de certification (CA) par défaut et un certificat de périphérique qui sont stockés dans le chemin /etc/raddb/certs. Le nom de ces certificats est ca.pem et server.pem. server.pem est le certificat que les clients reçoivent lorsqu'ils passent par le processus d'authentification. Si vous devez attribuer un autre certificat pour l'authentification EAP, vous pouvez simplement les supprimer et enregistrer les nouveaux dans le même chemin avec ce même nom exact.

Configuration du périphérique final

Configurez un ordinateur portable Windows pour qu'il se connecte à un SSID avec l'authentification 802.1x et PEAP/MS-CHAP (version Microsoft du protocole d'authentification à échanges confirmés) version 2.

Pour créer le profil WLAN sur la machine Windows, deux options sont disponibles :

- 1. Installer le certificat auto-signé sur l'ordinateur pour valider et approuver le serveur RADIUS libre afin de terminer l'authentification
- Ignorez la validation du serveur RADIUS et faites confiance à tout serveur RADIUS utilisé pour effectuer l'authentification (non recommandé, car il peut devenir un problème de sécurité). La configuration de ces options est expliquée sur la configuration du périphérique final - Créer le profil WLAN.

Importer un certificat FreeRADIUS

Si vous utilisez les certificats par défaut installés sur freeRADIUS, suivez ces étapes afin d'importer le certificat EAP du serveur freeRADIUS dans le périphérique final.

Étape 1. Obtenez le certificat de FreeRadius :

[root@tac-mxwireless ~]# cat /etc/raddb/certs/ca.pem

----BEGIN CERTIFICATE----

MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEw1Tb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydG1maWNhdGUgQXV0aG9yaXR5MB4X DTE3MDDzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBgNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh bXBsZSBJbmMuMSAwHgYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3



Étape 2. Copier et coller la sortie de l'étape précédente dans un fichier texte et modifier l'extension en .crt

Étape 3. Double-cliquez sur le fichier et sélectionnez **Installer le certificat...** comme le montre l'image.



Étape 4. Installez le certificat dans le magasin **Autorités de certification racine de confiance** comme indiqué sur l'image.

Certificate Import Wizard	8							
Certificate Store								
Certificate stores are system areas where certifica	ites are kept.							
Windows can automatically select a certificate store, or you can specify a location for the certificate.								
 Automatically select the certificate store bas Place all certificates in the following store 	sed on the type of certificate							
Certificate store:								
Salact Cartificata Stara	Browse							
Select the certificate store you want to use.								
Personal	Back Next > Cancel							
OK Cancel	ОК							

Créer un profil WLAN

Étape 1. Cliquez avec le bouton droit sur l'icône Démarrer et sélectionnez **Panneau de configuration** comme indiqué dans l'image.

Programs and Features
Mobility Center
Power Options
Event Viewer
System
Device Manager
Network Connections
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)
Task Manager
Control Panel
File Explorer
Search
Run
Shut down or sign out
Desktop
👔 אין

Étape 2. Accédez à **Réseau et Internet > Centre Réseau et partage> cliquez sur Configurer une nouvelle connexion ou un nouveau réseau** comme indiqué dans l'image.



Étape 3. Sélectionnez **Connexion manuelle à un réseau sans fil** et cliquez sur Suivant comme indiqué dans l'image.

	-		×
🔶 👙 Set Up a Connection or Network			
Choose a connection option			
			-
Connect to the Internet			
 Set up a broadband or dial-up connection to the internet. 			
with the second			
Set up a new router or access point.			
Manually connect to a wireless network			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
	Next	G	ral
	Next	Car	icei

Étape 4. Entrez les informations avec le nom du SSID et du type de sécurité WPA2-Enterprise, puis cliquez sur **Suivant** comme indiqué dans l'image.

			-		×
÷	Manually connect to a	wireless network			
	Enter information f	or the wireless network you want to add			
	Network name:	SSID-name			
	Security type:	WPA2-Enterprise ~			
	Encryption type:	AES			
	Security Key.	Hide character	5		
	Start this connection	on automatically			
	Connect even if the Warning: If you set	e network is not broadcasting ect this option, your computer's privacy might be at risk			
		N	ext	Can	cel

Étape 5. Sélectionnez **Modifier les paramètres de connexion** afin de personnaliser la configuration du profil WLAN comme indiqué dans l'image.

– 🗆 🗙	
	 See Manually connect to a wireless network
	Successfully added ise-ssid
	→ Change connection settings
e settings.	Open the connection properties so that I can change the settings.
Close	
e settings. Close	→ Change connection settings Open the connection properties so that I can change the settings.

Étape 6. Accédez à l'onglet **Sécurité** et cliquez sur **Paramètres** comme indiqué dans l'image.

ise-ssid Wireless Network Properties $ imes$				×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	hentication method:	_	_	
Microsoft: Protected I	EAP (PEAP)	Settin	igs	
Remember my credentials for this connection each time I'm logged on				
Advanced settings				
		ОК	Car	ncel

Étape 7. Choisissez si le serveur RADIUS est validé ou non.

Si oui, activez Vérifier l'identité du serveur en validant le certificat et à partir des Autorités de certification racines de confiance : sélectionnez le certificat auto-signé de freeRADIUS.

Après cela, sélectionnez **Configurer** et désactiver **Utiliser automatiquement mon nom de connexion et mon mot de passe Windows...**, puis cliquez sur **OK** comme indiqué dans les images.

Protected EAP Properties	×
When connecting:	
Verify the server's identity by validating the certificate	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Eggine & Oktob International Control International	^
En la secta de la social de la	
Example Certification Authority	
Fermet Dopt Contillanting Frida	
 E. A. Bibliock Internation (1977) Supplied (1977) E. J. S. Sono (1977) Statistic Sciences (1977) 	
< >>	*
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified	\sim
Select Authentication Method:	_
Secured password (EAP-MSCHAP v2) Configu	re
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
OK Cano	el
CAP MISCHAPV2 Properties X	
When connecting:	
Automatically use my Windows logon name and password (and domain if any).	
OK Cancel	

Étape 8. Configurez les informations d'identification de l'utilisateur.

Une fois de retour à l'onglet Sécurité, sélectionnez **Paramètres avancés**, spécifiez le mode d'authentification en tant qu'**authentification utilisateur** et enregistrez les informations d'identification configurées sur freeRADIUS afin d'authentifier l'utilisateur, comme indiqué dans les images.

ise-ssid Wireless Network Properties				×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network au	thentication method:			
Microsoft: Protected	EAP (PEAP)	Settin	igs	
Remember my credentials for this connection each time I'm logged on				
	_			
Advanced settings	5			
		ОК	Cano	cel

Advanced settings		×	
802.1X settings 802.11 settings	_		
Specify authentication mode:			
User authentication	✓ Save of	redentials	
Delete credentials for all us	sers		
Enable single sign on for this n	etwork		
Perform immediately befor	e user logon		
O Perform immediately after	user logon		
Maximum delay (seconds):	10	- A	
Allow additional dialogs to sign on	be displayed during	single	
This network uses separate	e virtual LANs for m	achine	
and user authentication			
	OK	Cancel	
			4
findows Security			
Save credentials			
Saving your credentials allo	WE YOUR COMP	uter to conne	act to the network
when you're not logged on	(for example,	to download	updates).
user1			
cisco			
	•		

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

OK

Х

Cancel

Processus d'authentification sur WLC

Exécutez les commandes suivantes afin de surveiller le processus d'authentification pour un utilisateur spécifique :

> debug client <mac-add-client> > debug dot1x event enable > debug dot1x aaa enable

Pour lire facilement les sorties du client de débogage, utilisez l'outil Wireless debug analyzer :

Analyseur de débogage sans fil

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.