Dépannage de l'accès sans fil défini par logiciel sur Cisco DNA Center

Table des matières

- Introduction
- Fiche de présentation des commandes pour le fabric
- Configuration push WLC AireOS à partir de Cisco DNA Center
- Push de configuration WLC à partir de Cisco DNA Center
  - Comment vérifier si Map-Server est accessible ?
  - Debug Fabric Map-Server Connectivity
  - Comment vérifier que le fabric est activé et quel est le résultat attendu ?
- Configuration WLAN diffusée depuis Cisco DNA Center
- Débogage des problèmes sans fil
  - Débogage de jonction AP/Formation de tunnel d'accès Débogage
  - Débogage client
    - Débogage WLC
    - Débogage de périphérie de fabric
    - Débogage du point d'accès
  - Débogage de cas d'utilisation
    - Débogage CWA du client
    - Débogage DHCP du client
    - Débogage des performances du client sur AP
- Intégration AP
  - Méthode/étapes traditionnelles :
    - Mise en service Plug-and-Play/point d'accès sans intervention
- Informations connexes

Introduction

Ce document décrit les questions fréquentes sur le sans fil et comment dépanner l'accès défini par logiciel sur Cisco DNA Center.

Fiche de présentation des commandes pour le fabric

Il s'agit de la fiche de commande pour le fabric sur le noeud de contrôle, le noeud de périphérie, le contrôleur de réseau local sans fil (WLC) et le point d'accès (AP).

Noeud de contrôle :

- show lisp instance-id <L2 ap instance id> ethernet server - Mappage de l'identification MAC vers EID (Endpoint Identification)
- show lisp instance-id <L3 ap instance id> ipv4 server - Mappage IP/EID

- show lisp instance-id 8188 ethernet server address-resolution - Mappage MAC vers IP pour un ID d'instance spécifique
- show lisp site
- show tech-support
- show tech-support lisp

Noeud de périphérie :

- show lisp instance-id <L2 ap instance id> ethernet database wlc
- show lisp instance-id <L2 client instance id> ethernet database wlc
- show access-tunnel summary
- show platform software fed switch active ifm interfaces access-tunnel
- show platform software access-tunnel switch active R0
- show platform software access-tunnel switch active R0 statistics
- show platform software access-tunnel switch active F0
- show platform software access-tunnel switch active F0 statistics
- show platform software object-manager switch active F0 statistics
- show platform software object-manager switch active F0 pending-issue-update
- show platform software object-manager switch active F0 pending-ack-update
- show platform software object-manager switch active F0 error-object
- show tech-support
- show tech-support lisp

WLC (AireOS) :

- show fabric ap summary
- show fabric summary
- show fabric map-server summary
- show run-config
- Commandes show run-config
- show tech

WLC (IOS-XE)

- show ap summary
- show fabric ap summary
- show wireless fabric summary
- show wireless client summary
- show tech-support wireless
- show tech-support wireless fabric
- show tech-support lisp (si Fabric in a Box ou Embedded Wireless exécuté sur les gammes 9300/9400/9500)
- show tech-support (si Fabric in a box ou Embedded wireless exécuté sur 9300/9400/9500)

Point d'accès:

- show ip tunnel fabric
- show tech-support

Configuration push WLC AireOS à partir de Cisco DNA Center

Ici, il montre le push de configuration AireOS WLC de Cisco DNA Center après le provisionnement (Remarque : Utilisation de la référence comme 3504 WLC).

show radius summary après le provisionnement WLC :

```
(sdawlc3504) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Accounting Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled
Fallback Test:
    Test Mode..... Passive
    Probe User Name..... cisco-probe
    Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
RADIUS Authentication Framed-MTU..... 1300 Bytes

Authentication Servers

Idx  Type  Server Address    Port    State     Tout  MgmtTout  RFC3576  IPSec - state/Profile Name/Radi
---  ----  ----------------  ------  --------  ----  --------  -------  ------------------------------
1  * NM    192.168.2.193     1812    Enabled   2     5         Enabled   Disabled - /none
2    M     172.27.121.193    1812    Enabled   2     5         Enabled   Disabled - /none
```

La commande WLAN Config Push est affichée sous show wlan summary.

```
(sdawlc3504) >show wlan summary

Number of WLANs..... 7

WLAN ID  WLAN Profile Name / SSID                                                  Status    Interface Na
-------  -------------------------------------------------------------------------  --------  ------------
1        Test / Test                                                               Enabled   management
17       dnac_guest_F_global_5dfbd_17 / dnac_guest_206                             Disabled  management
18       dnac_psk_2_F_global_5dfbd_18 / dnac_psk_206                               Disabled  management
19       dnac_wpa2__F_global_5dfbd_19 / dnac_wpa2_206                              Enabled   management
20       dnac_open__F_global_5dfbd_20 / dnac_open_206                              Enabled   management
21       Test!23_F_global_5dfbd_21 / Test!23                                       Disabled  management
```

Push de configuration WLC à partir de Cisco DNA Center

Ici, il montre le push de configuration WLC de Cisco DNA Center après l'ajout du WLC au fabric.

Comment vérifier si Map-Server est accessible ?

show fabric map-server summary après l'ajout du WLC au fabric.

```
(sdawlc3504) >show fabric map-server summary

MS-IP     Connection status

-------------------------------

192.168.4.45    UP

192.168.4.66    UP
```

Debug Fabric Map-Server Connectivity

La connectivité du plan de contrôle (CP) peut être interrompue ou interrompue pour diverses raisons.

- Si le CP est tombé. (ce qui n'est pas le cas ici)
- Noeuds intermédiaires descendant qui connectent le WLC au PC, par exemple, un routeur de fusion.
- Si la connectivité CP au WLC a été interrompue en raison d'une liaison interrompue. Il peut s'agir d'un WLC à un voisin immédiat ou d'un CP à un voisin immédiat vers le WLC.

show fabric map-server detailed

show fabric TCP creation-history <IP Map-Server>

Débogages pouvant fournir des informations supplémentaires

debug fabric lisp map-server tcp enable

debug fabric lisp map-server all enable

Comment vérifier que le fabric est activé et quel est le résultat attendu ?

show fabric summary après l'ajout du WLC au fabric.

```
(sdawlc3504) >show fabric summary

Fabric Support..................................... enabled

Enterprise Control Plane MS config
-------------------------------------

Primary Active MAP Server
IP Address..................................... 192.168.4.45
```

```
Secondary Active MAP Server
IP Address..................................... 192.168.4.66

Guest Control Plane MS config
------------------------------

Fabric TCP keep alive config
----------------------------

Fabric MS TCP retry count configured ............ 3
Fabric MS TCP timeout configured ............... 10
Fabric MS TCP keep alive interval configured .... 10
Fabric Interface name configured ............... management

Fabric Clients registered ..................... 0

Fabric wlans enabled .......................... 3

Fabric APs total Registration sent ............ 30

Fabric APs total DeRegistration sent .......... 9

Fabric AP RLOC reguested ...................... 15

Fabric AP RLOC response received .............. 30

Fabric AP RLOC send to standby ................ 0

Fabric APs registered by WLC .................. 6

VNID Mappings configured: 4

Name                             L2-Vnid     L3-Vnid     IP Address/Subnet
-------------------------------  ----------  ----------  ---------------------------------
182_10_50_0-INFRA_VN             8188        4097        182.10.50.0 / 255.255.255.128
10_10_10_0-Guest_Area            8190        0           0.0.0.0 / 0.0.0.0
182_10_100_0-DEFAULT_VN          8191        0           0.0.0.0 / 0.0.0.0
182_11_0_0-DEFAULT_VN            8189        0           0.0.0.0 / 0.0.0.0

Fabric Flex-Acl-tables           Status
-------------------------------- -------
DNAC_FABRIC_FLEX_ACL_TEMPLATE    Applied

Fabric Enabled Wlan summary
WLAN ID  SSID                             Type  L2 Vnid     SGT     RLOC IP          Clients  VNID Nam
-------  -------------------------------  ----  ----------  ------  ---------------  -------  --------
 19      dnac_wpa2_206                    WLAN  8189        0       0.0.0.0          0         182_11_
 20      dnac_open_206                    WLAN  8189        0       0.0.0.0          0         182_11_
```

Configuration WLAN diffusée depuis Cisco DNA Center

La diffusion de la configuration WLAN depuis Cisco DNA Center est affichée sous show fabric wlan summary après l'ajout du WLC au fabric et le pool d'adresses IP client est attribué au WLAN (Fabric Wireless LAN) sous Provisionnement > Fabric > Host Onboarding.

show fabric wlan summary après le provisionnement du fabric.

```
(sdawlc3504) >show fabric wlan summary

WLAN ID  SSID                             Type  L2 Vnid     SGT     RLOC IP          Clients  VNID Nam
-------  -------------------------------  ----  ----------  ------  ---------------  -------  --------
 19      dnac_wpa2_206                    WLAN  8189        0       0.0.0.0          0         182_11_
 20      dnac_open_206                    WLAN  8189        0       0.0.0.0          0         182_11_
```

Débogage des problèmes sans fil

Débogage de jonction AP/Formation de tunnel d'accès Débogage

1. Vérifiez si AP a obtenu l'adresse IP.

show ip dhcp snooping binding → On Fabric Edge

S'il n'affiche pas d'IP pour l'interface AP connectée, veuillez activer ces débogages sur le commutateur et vérifier si AP obtient IP ou non.

debug ip dhcp snooping packet

debug ip dhcp snooping event

Exemple de fichier journal joint ci-dessous →

Exemple :

```
Floor_Edge-6#sh ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
0C:75:BD:0D:46:60 182.10.50.7 670544 dhcp-snooping 1021 GigabitEthernet1/0/7 → AP interface should be havi
```

2. Vérifiez si AP rejoint WLC.

- show ap summary → Sur WLC
- show ap join stat summary → Sur WLC

Si AP n'a jamais rejoint WLC, activez ces débogages sur WLC.

- debug capwap events enable
- debug capwap errors enable

3. Si AP forme CAPWAP mais qu'aucun tunnel d'accès n'est formé entre AP et Switch, veuillez effectuer ces vérifications

Étape 1. Les AP dans le WLC ont-ils des IP RLOC ou non, sinon, veuillez cocher le point 1 ici.

1. Afin de rendre le protocole du plan de contrôle de fabric plus résilient, il est important qu'une route spécifique vers le WLC soit présente dans la table de routage globale de chaque noeud de fabric. La route vers l'adresse IP du WLC doit être soit redistribuée dans le protocole IGP sous-jacent à la frontière ou configurée statiquement à chaque noeud. En d'autres termes, le WLC ne devrait pas être accessible via la route par défaut.

Étape 2. Si les AP dans le WLC montrent les RLOC corrects et sous show fabric summary il montre le RLOC demandé avec le RLOC reçu tout bon, veuillez vérifier ces étapes

2. Vérifiez sur le noeud Plan de contrôle, show lisp instance-id <L2 ap instance id> ethernet server→ Il doit contenir Base Radio MAC pour AP.

Vérifiez sur le noeud Périphérie du fabric, show lisp instance-id <L2 ap instance id> ethernet database wlc → Il doit contenir Base Radio MAC pour AP et non l'adresse MAC Ethernet du point d'accès.

Si les 2 commandes ci-dessus n'affichent pas l'adresse MAC radio de base du point d'accès et que les tunnels d'accès ne se forment pas. Activez debug lisp control-plane all sur Control plane et recherchez Base Radio MAC dans logging.

Remarque : debug lisp control-plane all on Control plane is very chatty, veuillez désactiver la journalisation de la console avant d'activer les débogages.

Si vous voyez un échec d'authentification comme indiqué ici, vérifiez la clé d'authentification entre le WLC et le noeud CP.

```
Dec  7 17:42:01.655: LISP-0: MS Site EID IID 8188 prefix any-mac SVC_VLAN_IAF_MAC site site_uci, Regist

Dec  7 17:42:01.659: LISP-0: Building reliable registration message registration-rejected for IID 8188
```

Comment vérifier la clé d'authentification sur la configuration du fabric entre WLC et CP.

Sur WLC, veuillez vérifier sur GUI sous Controller > Fabric Configuration > Control Plane > (Pre Shared Key)

On CP, please check on switch using sh running-config | b map-server session CP#sh running-config | b map-server session map-server session passive-open WLC site site_uci description map-server configured from apic-em authentication-key

(Ensure that the Pre shared key on WLC should match with this authentication key on CP)

Remarque : En règle générale, Cisco DNA Center appuie sur cette clé. Ne la modifiez que si nécessaire et connaissez la configuration du protocole CP/WLC.]

---

4. Vérifie et affiche les commandes générales pour les tunnels d'accès.

- show access-tunnel summary

```
Floor_Edge-6#sh access-tunnel summary

Access Tunnels General Statistics:
 Number of AccessTunnel Data Tunnels = 5


Name SrcIP SrcPort DestIP DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac4 192.168.4.68 N/A 182.10.50.6 4789 0
Ac24 192.168.4.68 N/A 182.10.50.5 4789 0
Ac19 192.168.4.68 N/A 182.10.50.8 4789 0
Ac15 192.168.4.68 N/A 182.10.50.7 4789 0
Ac14 192.168.4.68 N/A 182.10.50.2 4789 0


Name IfId Uptime
------ ---------- --------------------
Ac4 0x00000037 2 days, 20:35:29
Ac24 0x0000004C 1 days, 21:23:16
Ac19 0x00000047 1 days, 21:20:08
Ac15 0x00000043 1 days, 21:09:53
Ac14 0x00000042 1 days, 21:03:20
```

- show platform software fed switch active ifm interfaces access-tunnel

```
Floor_Edge-6#show platform software fed switch active ifm interfaces access-tunnel
Interface                   IF_ID               State
------------------------------------------------------------
Ac4                         0x00000037          READY
Ac14                        0x00000042          READY
Ac15                        0x00000043          READY
Ac19                        0x00000047          READY
Ac24                        0x0000004c          READY

Floor_Edge-6#
```

Si les tunnels d'accès sous la commande b) sont supérieurs à a), c'est un problème. Ici, les entrées Fed n'ont pas été effacées correctement par Fabric Edge et il y a donc plusieurs entrées de tunnel d'accès sur Fed par rapport à IOS. Comparez Dest IP après l'exécution de la commande indiquée ici. Si plusieurs tunnels d'accès partagent la même adresse IP de destination, c'est le problème de la programmation.

- show platform software fed switch active ifm if-id <Chaque AP IF-ID>

Remarque : Chaque IF-ID peut être récupéré à partir de la commande précédente.

```
Floor_Edge-6#show platform software fed switch active ifm if-id 0x00000037
Interface IF_ID         : 0x0000000000000037
Interface Name          : Ac4
Interface Block Pointer : 0xffc0b04c58
Interface State         : READY
Interface Status        : ADD
Interface Ref-Cnt       : 2
Interface Type          : ACCESS_TUNNEL
        Tunnel Type       : L2Lisp
        Encap Type        : VxLan
        IF_ID             : 0x37

        Port Information
        Handle ............ [0x2e000094]
        Type ............... [Access-tunnel]
        Identifier ........ [0x37]
        Unit ............... [55]
        Access tunnel Port Logical Subblock
                Access Tunnel id  : 0x37
                Switch Num        : 1
                Asic Num          : 0
                PORT LE handle    : 0xffc0b03c58
                L3IF LE handle    : 0xffc0e24608
                DI handle         : 0xffc02cdf48
                RCP service id    : 0x0
                HTM handle decap  : 0xffc0e26428
                RI handle decap   : 0xffc0afb1f8
                SI handle decap   : 0xffc0e26aa8
                RCP opq info      : 0x1
                L2 Brdcast RI handle  : 0xffc0e26808
                GPN               : 3201
                Encap type        : VXLAN
                L3 protocol       : 17
                Src IP            : 192.168.4.68
                Dest IP           : 182.10.50.6
                Dest Port         : 4789
                Underlay VRF      : 0
                XID cpp handle    : 0xffc03038f8
        Port L2 Subblock
                Enabled ............. [No]
                Allow dot1q ......... [No]
                Allow native ........ [No]
                Default VLAN ........ [0]
                Allow priority tag ... [No]
                Allow unknown unicast  [No]
                Allow unknown multicast[No]
                Allow unknown broadcast[No]
                Allow unknown multicast[Enabled]
                Allow unknown unicast  [Enabled]
                IPv4 ARP snoop ....... [No]
                IPv6 ARP snoop ....... [No]
                Jumbo MTU ............ [0]
                Learning Mode ........ [0]
        Port QoS Subblock
                Trust Type ..................... [0x7]
                Default Value .................. [0]
                Ingress Table Map .............. [0x0]
                Egress Table Map ............... [0x0]
                Queue Map ...................... [0x0]
        Port Netflow Subblock
        Port CTS Subblock
```

```
                Disable SGACL ..................... [0x0]
                Trust ............................. [0x0]
                Propagate ......................... [0x1]
        %Port SGT ......................... [-180754391]
Ref Count : 2 (feature Ref Counts + 1)
IFM Feature Ref Counts
        FID : 91, Ref Count : 1
No Sub Blocks Present
```

- show platform software access-tunnel switch active R0

```
Floor_Edge-6#show platform software access-tunnel switch active R0
Name     SrcIp            DstIp             DstPort   VrfId    Iif_id
-----------------------------------------------------------------------
Ac4      192.168.4.68     182.10.50.6        0x12b5  0x0000  0x000037
Ac14     192.168.4.68     182.10.50.2        0x12b5  0x0000  0x000042
Ac15     192.168.4.68     182.10.50.7        0x12b5  0x0000  0x000043
Ac19     192.168.4.68     182.10.50.8        0x12b5  0x0000  0x000047
Ac24     192.168.4.68     182.10.50.5        0x12b5  0x0000  0x00004c
```

- show platform software access-tunnel switch active R0 statistics

```
Floor_Edge-6#show platform software access-tunnel switch active R0 statistics
Access Tunnel Counters   (Success/Failure)
----------------------------------------
Create                  6/0
Create Obj Download     6/0
Delete                  3/0
Delete Obj Download     3/0
NACK                    0/0
```

- show platform software access-tunnel switch active F0

```
Floor_Edge-6#show platform software access-tunnel switch active F0
Name     SrcIp            DstIp             DstPort  VrfId    Iif_id    Obj_id  Status
-------------------------------------------------------------------------------------------
Ac4      192.168.4.68     182.10.50.6        0x12b5  0x000  0x000037  0x00d270  Done
Ac14     192.168.4.68     182.10.50.2        0x12b5  0x000  0x000042  0x03cbca  Done
Ac15     192.168.4.68     182.10.50.7        0x12b5  0x000  0x000043  0x03cb9b  Done
Ac19     192.168.4.68     182.10.50.8        0x12b5  0x000  0x000047  0x03cb6b  Done
Ac24     192.168.4.68     182.10.50.5        0x12b5  0x000  0x00004c  0x03caf4  Done
```

- show platform software access-tunnel switch active F0 statistics

```
Floor_Edge-6#show platform software access-tunnel switch active F0 statistics
Access Tunnel Counters   (Success/Failure)
-----------------------------------------
Create                  0/0
Delete                  3/0
HW Create               6/0
HW Delete               3/0
Create Ack              6/0
Delete Ack              3/0
NACK Notify             0/0
```

- show platform software object-manager switch active f0 statistics

```
Floor_Edge-6#show platform software object-manager switch active f0 statistics
Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 987
Stale-objects: 0
Resolve-objects: 3
Error-objects: 1
Paused-types: 0
```

- show platform software object-manager switch active f0 pending-issue-update
- show platform software object-manager switch active f0 pending-ack-update
- show platform software object-manager switch active f0 error-object

5. Traces et débogages à collecter.

Étape 1 : collecte des journaux d'archivage avant d'activer les suivis/débogages

request platform software trace archive target flash:<Nom du fichier>

```
Floor_Edge-6#request platform software trace archive target flash:Floor_Edge-6_12_14_18
Waiting for trace files to get rotated.
Creating archive file [flash:Floor_Edge-6_12_14_18.tar.gz]
Done with creation of the archive file: [flash:Floor_Edge-6_12_14_18.tar.gz]
```

Étape 2. Augmentez la mémoire tampon de journalisation et désactivez la console.

```
Floor_Edge-6(config)#logging buffered 214748364
Floor_Edge-6(config)#no logging console
```

Étape 3. Définition des traces

- set platform software trace forwarding switch active R0 access-tunnel verbose
- set platform software trace forwarding switch active F0 access-tunnel verbose
- set platform software trace fed switch active ifm_main debug
- set platform software suivi fed switch active access_tunnel verbose
- set platform software trace forwarding-manager switch active F0 aom verbose

Étape 4 : activation des débogages

- debug l2lisp all
- debug lisp control-plane all
- debug platform software l2lisp events

Étape 5. shutdown/no shut port d'interface où AP est connecté.

Étape 6. Collecter les journaux d'archivage comme à l'étape 1. avec un nom de fichier différent.

Étape 7. Rediriger le fichier journal vers la mémoire flash.

Floor_Edge-6#show logging | redirect flash:<Nom du fichier>

```
Floor_Edge-6#show logging | redirect flash:console_logs_Floor_Edge-6_12_14_18
```

Débogage client

Debug Wireless client's issues on SDA FEW peut devenir délicat.

Veuillez suivre ce workflow pour éliminer un périphérique à la fois.

1. WLC

2. Périphérie du fabric

3. Point d'accès (si le débogage sur la périphérie du fabric pointe vers le point d'accès)

4. Noeud Intermédiaire/Frontière. (En cas de problème de chemin de données)

5. Noeud Plan de contrôle. (En cas de problème de chemin de contrôle)

Débogage WLC

Pour les problèmes de connectivité client, commencez le débogage en collectant des informations sur le WLC qui incluent les commandes show et les débogages.

Commandes show du WLC AireOS :

- show run-config
- show tech
- show wlan summary
- show wlan <id> —> Collectez ce résultat pour tous les SSID, au moins 1 pour les SSID en fonctionnement et hors fonctionnement
- show fabric summary
- show fabric map-server summary
- show client summary
- show client detail <mac_id>

Commandes de débogage WLC AireOS :

- debug client <mac1> —> Client assoc, roaming, debugs.
- debug fabric client detail enable —> Cette commande fournit des informations sur les messages d'enregistrement du fabric

Débogage de périphérie de fabric

Une fois débogué sur le WLC et observé, il n'y a aucun problème lié au chemin du plan de contrôle pour le client. Le client passe de Assoc, Authentication, et exécute l'état avec le balisage SGT ou les paramètres AAA corrects, passez à cette étape pour isoler davantage le problème.

Une autre chose à vérifier est que la programmation du tunnel d'accès est correcte comme décrit dans la section de débogage AP ci-dessus.

Commandes show pour vérifier :

Rechercher l'ID d'instance lisp de couche 2 à partir de (show client detail <mac_id> from above)

<#root>

```
show lisp instance-id
```

```
        ethernet database wlc
```

```
 --> This lists all WLC associated clients for that specific L2 lisp instance ID. A number of sources sh
show lisp instance-id
```

```
        ethernet database wlc
```

--> This shows the detail for the specific client

show device-tracking database | i Vl

--> Find Specific SVI where the client is connected and needs to be present.

show device-tracking database | i

--> Find the client entry, should be against correct VLAN, Interface, State, and Age.

show mac address-table dynamic vlan

--> The entry for the mac should match the device-tracking database, if it does please check mac addre

show ip dhcp snooping binding vlan

show ip arp vrf

show mac address-table vlan

show platform software fed switch active matm macTable vlan

--> If this is correct, programming for wireless client is happening correctly on local swit

show platform software matm switch active F0 mac

Commandes de débogage sur Fabric Edge

Nécessité de collecter les traces Fed en cas de problème dans la programmation de l'entrée client sur Fabric Edge. Il y a 2 façons de faire la même chose après avoir activé ces débogages.

Les commandes debugs et set doivent être activées quelle que soit la méthode.

- set platform software trace fed switch active all-modules emergency
- set platform software suivi fed switch active l2_fib_entry verbose
- set platform software suivi fed switch active l2_fib_adj verbose
- set platform software trace fed switch active injection verbose
- set platform software trace fed switch active matm verbose

debug (Veillez à désactiver la journalisation de la console et à augmenter la mémoire tampon de journalisation)

- debug device-tracking
- debug lisp control-plane all
- debug platform fhs all
- debug platform software l2lisp events
- debug matm all

Méthode 1. Collecter les journaux de suivi radio actifs pour un client spécifique après l'activation des débogages.

✎ Remarque : en cas de problème DHCP, veuillez ne pas utiliser cette méthode]

Attendez que le problème se reproduise

- debug platform condition mac <mac-id> control-plane
- debug platform condition start
- debug platform condition stop
- request plate soft trace filter-binary wireless context mac <mac-id>

Redirigez les journaux de la console vers la mémoire flash une fois le problème reproduit.

Méthode 2. Collecter les journaux de suivi des archives après l'activation des débogages.

Attendez que le problème se reproduise

request platform software trace archive

Collectez le fichier pour décoder les journaux et analyser les journaux d'alimentation, ios et fman

pour le mac client.

Redirigez les journaux de la console vers la mémoire flash une fois le problème reproduit.

Débogage du point d'accès

Débogages sur les modèles AP 2800/3800/1562 :

Pour les problèmes côté AP, assurez-vous de collecter toutes les commandes et les journaux WLC show avant de collecter les journaux côté AP et de les attacher à SR.

Veuillez suivre ces étapes afin de déboguer les problèmes liés aux données du côté client.

1. Collectez les commandes AP show : (2 à 3 fois, avant et après la fin des tests)

- show clock
- terme len 0
- terme mon
- show tech
- show logging
- show controllers nss stats show controllers nss status
- show ip tunnel fabric

Si vous rencontrez un problème avec CWA, veuillez collecter les journaux ci-dessous en plus des commandes principales. Les commandes ci-dessous doivent être collectées une fois avant et après la fin du test.

- show client access-lists pre-auth all <mac client>
- show client access-lists post-auth all <mac client>
- show ip access-lists
- show controller d [0/1] client
- show capwap cli detail rcb
- show tech support

2. Débogages AP (filtre par adresse MAC)

Problèmes de chemin de données client :

- debug dot11 client datapath eapol addr <mac>
- debug dot11 client datapath dhcp addr <mac>
- debug dot11 client datapath arp addr <mac>

Suivis AP client :

- config ap client-trace address add <mac>
- config ap client-trace output console-log enable
- config ap client-trace filter all enable
- config ap client-trace filter probe disable
- config ap client-trace start

- terme mon
- exec-timeout 0 0

Problèmes liés aux CWA :

- debug capwap client avc all
- debug capwap client acl
- debug client <client mac>
- debug dot11 client level info address <mac>
- debug dot11 client level events address <mac>
- debug flexconnect pmk

Débogage de cas d'utilisation

Débogage CWA du client

Points à noter :

- Lors du déploiement de CWA dans SDA, utilisez toujours DNAC pour déployer la configuration.
- Une fois déployé à l'aide de DNAC, la stratégie d'autorisation, la stratégie d'authentification et le profil d'autorisation seront également déployés sur ISE par DNAC.
- Les identités pour l'authentification doivent être configurées manuellement comme pour Dot1x

Renseignez-vous sur l'étape à laquelle le problème est observé.

Étape 1. Le client obtient-il une adresse IP et passe-t-il à Webauth Pending ?

1. Si oui, passez à l'étape suivante.
2. Si la réponse est non, le problème se situe au stade de la connexion initiale.
3. Vérifiez la configuration sur WLC et AP.
4. Vérifier que l'ACL est poussée sur l'AP et correspond à ce qui est sur le WLC
5. Si la liste de contrôle d'accès n'est pas poussée correctement, rechargez l'AP et assurez-vous qu'il s'agit d'un état intermédiaire où la configuration n'est pas poussée. Une fois confirmé sur 1 point d'accès, assurez-vous que le provisionnement des points d'accès est effectué via DNAC.

Étape 2. Le client peut-il charger la page de redirection ?

1. Si oui, passez à l'étape suivante.
2. Si la réponse est non, le problème peut se situer à plusieurs endroits.
3. Vérifiez la configuration sur WLC et AP.
4. Vérifier que l'ACL est poussée sur l'AP et correspond à ce qui est sur le WLC
5. Si la liste de contrôle d'accès n'est pas poussée correctement, rechargez l'AP et assurez-vous qu'il s'agit d'un état intermédiaire où la configuration n'est pas poussée. Une fois confirmé sur 1 point d'accès, assurez-vous que le provisionnement des points d'accès est effectué via DNAC.

6. Vérifiez l'accessibilité du WLC à ISE et du commutateur où AP est connecté à ISE. Assurez-vous qu'aucun pare-feu ne se trouve entre
7. Vérifiez que le DNS est correctement configuré.

Étape 3. Le client peut-il voir la page Web, mais le problème est de se connecter et de réussir ?

1. Assurez-vous de vérifier à nouveau les configurations des étapes 1 et 2.
2. Assurez-vous que le profil d'autorisation, la stratégie d'authentification et la stratégie d'autorisation sont corrects.
3. Vérifier les journaux ISE Live
4. Assurez-vous que le nom d'utilisateur/mot de passe est correctement configuré dans les identités ISE.
5. Collectez les débogages sur WLC et AP comme ci-dessous si tout semble bien.

1. Débogages sur WLC :

- Recueillez les commandes show suivantes pour AireOS et Polaris respectivement :

AireOS:

- show run-config
- show wlan summary
- show wlan <id_for_Guest>
- show flexconnect acl summary
- show flexconnect acl detailed <ACl_from_previous_command>

Polaris :

- show running
- show tech-support wireless
- show tech-support wireless fabric
- show wlan summary
- show wlan id <id_for_guest>
- show ap name <AP_name> config general
- show running-config ACL | sec
- show wireless profile flex summary
- show wireless profile flex detailed <profile_name_from_above>

- Activez ces débogages sur AireOS et Polaris.

AireOS:

- debug client <client_mac>
- debug aaa all enable
- Reproduisez le problème
- Collecter les journaux de console/ssh/telnet

Polaires (9300/9400/9500) :

set platform software trace wncd switch active r0 all-modules debug

Reproduisez le problème

show platform software trace message wncd switch active R0 reverse | rediriger la mémoire flash : <nom du fichier>

request platform software trace archive

Collecter les deux fichiers à partir de la mémoire flash

2. Débogages sur AP :

Collecter les informations ACL :

show ip access-lists

Collecter les débogages ci-dessous du point d'accès :

- debug capwap client avc all
- debug capwap client acl
- debug client <client mac>
- debug dot11 client level info address <mac>
- debug dot11 client level events address <mac>
- debug flexconnect pmk

Débogage DHCP du client

Certains problèmes peuvent être débogués en utilisant ces débogages.

1. Ne pas voir les messages de détection DHCP sur le commutateur.

2. Le client sans fil ne reçoit pas l'offre DHCP. La détection DHCP est observée sous debug ip dhcp snooping packet logs.

3. Recueillez la capture de paquets sur le port connecté au point d’accès, le port de liaison ascendante et le port connecté au serveur DHCP côté fusion.

Les commandes Debugs/Show qui peuvent être :

1. Vérifiez sur Cisco DNA Center si le SSID est attribué au pool IP.

2. Vérifiez si le WLAN est activé sur le WLC.

3. Vérifiez si les radios sont activées et si les réseaux 802.11a et 802.11b sont activés.

Débogage des performances du client sur AP

1. Réduisez le problème au câblé ou au sans fil, ou affectez les deux. Testez le même trafic sur un client connecté au réseau sans fil sur le même VNID et testez le même trafic sur le réseau câblé sur le même VNID.

2. Si les clients filaires du fabric sur le même VLAN ne rencontrent pas de problèmes, mais que les clients sans fil le sont, le problème se situe du côté du point d'accès.

3. Pour déboguer du côté du point d'accès en cas de problème lié aux performances du client ou au trafic, assurez-vous que la connectivité du client n'est pas le problème, pour commencer.

4. Assurez-vous, en utilisant le client de débogage sur le WLC, que le client observe une dégradation pendant l'itinérance, le délai d'expiration de session ou la connexion stable au même AP.

5. Une fois que le problème est limité au même point d'accès, suivez ces étapes pour collecter les débogages sur les points d'accès 3800/2800/4800, ainsi que la capture de paquets sur le commutateur connecté au point d'accès et les captures de paquets en direct.

Étape 1. Assurez-vous que le trafic utilisé pour reproduire le problème imite réellement le problème.

Étape 2. La capture de paquets par liaison radio doit être configurée du côté du client où le test a été effectué.

```
Instructions for collecting over-the-air packet captures:

Here you find the guide how to set up an Over-The-Air packet capture, you can use a windows client mach
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200527-Fundamentals-of-802-11-Wirele

There are few things we need to consider:
+Use an Open L2/L3 security SSID to avoid encryption on the packets through the air.
+Set client-serving-AP and sniffer AP on the same channel.
+Sniffer AP should be close enough to capture what serving-client-AP is receiving or sending.

SPAN session should be taken at the same time than OTA pcap for a proper analysis, how to configure a S

Nexus switches:
https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/113038-span-nexus-config
IOS switches:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/network_management/
```

Étape 3 : débogage du client à partir du WLC et capture de paquets à partir du commutateur où le point d'accès est connecté Les captures EPC du commutateur peuvent être utilisées pour capturer ces journaux.

Étape 4. Débogages de la session ssh/telnet du point d’accès 3800

```
Logs to be collected from 3800 AP:

A) Run following commands once before starting the test. [Once all commands are tested, copy all comman

Step A
Devshell commands on AP - Use SSH.
-------------------------------------------------
1) To Get wired0 input packet count

date
cd /click/fromdev_wired0/
cat icounts ocounts calls

2) Fabric gateway and clients

cat /click/client_ip_table/cli_fabric_clients
cd /click/fabric_tunnel/
cat show_fabric_gw

3) Tunnel Decap stats

cd /click/tunnel_decap/
cat icounts ocounts tunnel_decap_stats tunnel_decap_no_match decap_vxlan_stats
cat tunnel_decap_list

4) Tunnel Encap stats

cd /click/tunnel_encap/
cat icounts ocounts tunnel_encap_stats encap_vxlan_stats tunnel_encap_discard
cat get_mtu eogre_encap_list


5) Wireless client stats
```

Remarque : vous devez exécuter ces dernières commandes sur la combinaison radio vap appropriée. Par exemple, si le client est sur la radio 1, vap 1 : cat /click/client_ip_table/list = À partir du résultat, Vérifiez le port/l'interface client connecté aprXvY, utilisez la même valeur pour obtenir le résultat ci-dessous. cd /click/fromdev_apr1v3/ cat icounts counts calls cd /click/todev_apr1v3/ cat icounts counts calls Étapes B - E B) Démarrage de l'OTA entre AP. Client. Et démarrez le PCAP filaire (port Spanning AP où le client est connecté). (Pcap filaire et sans fil requis pour l'analyse.) C) Utilisez un WLAN Open-Auth (aucune sécurité pour analyser Pcap OTA). Commencez le test iperf et continuez-le pendant 10 à 15 minutes, en continu. D) Répétez l'étape A toutes les deux minutes à l'aide de la commande date. Effectuez au moins 5 itérations. E) Une fois le test terminé - Collectez show tech à partir du point d'accès.

Intégration AP

Méthode/étapes traditionnelles :

Il est considéré que l'étendue du VLAN AP a l'option 43 ou l'option 60 pointant vers le WLC.

1. Sélectionnez Authentification comme Aucune authentification.

2. Configurez Infra_VN avec le pool IP AP et Default_VN avec le pool IP client sans fil.

3. Configurez les ports d'interface de périphérie où les points d'accès sont connectés à Infra_VN.

4. Une fois qu'AP obtient l'IP et rejoint le WLC, il est découvert dans l'inventaire des périphériques.

5. Sélectionnez le point d'accès et affectez-le à un site spécifique et approvisionnez le point d'accès.

6. Une fois provisionné, le point d'accès est attribué au groupe de points d'accès créé lors de l'ajout du WLC au fabric.

Mise en service Plug-and-Play/point d'accès sans intervention

Il est considéré que AP Vlan Scope a l'option 43 pointant vers Cisco DNA Center. Suivez le guide DNAC pour configurer AP PNP

Côté périphérie du fabric :

Activez ces débogages.

- debug ip dhcp snooping packet
- debug ip dhcp snooping event

Informations connexes

- Guides de configuration sans fil pour chaque version
- Guide de déploiement sans fil SD
- Guide des meilleures pratiques sans fil
- Documents de référence technique pour les réseaux sans fil
- Matrice de compatibilité pour SDA
- Guides d'utilisation de Cisco DNA Center pour chaque version

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.