Risoluzione dei problemi di accesso wireless definito dal software su Cisco DNA Center

Sommario

Introduzione

Questo documento descrive le domande frequenti (FAQ) sul wireless e come risolvere i problemi relativi all'accesso definito dal software su Cisco DNA Center.

Scheda di comandi per Fabric

Di seguito vengono riportati i comandi cheat sheet per fabric su Control Node, Edge Node, Wireless Lan Controller (WLC) e Access Point (AP).

Nodo di controllo:

- show lisp instance-id <ID istanza ap L2> ethernet server - Mapping MAC - EID (Endpoint Identification)
- show lisp instance-id <ID istanza ap L3> server ipv4 - Mapping da IP a EID

- show lisp instance-id 8188 ethernet server address-resolution - Mapping da MAC a IP per un ID istanza specifico
- mostra sito lisp
- show tech-support
- show tech-support lisp

Edge Node:

- show lisp instance-id <ID istanza ap L2> ethernet database wlc
- show lisp instance-id <ID istanza client L2> ethernet database wlc
- show access-tunnel summary
- show platform software fed switch active ifm interfaces tunnel di accesso
- show platform software access-tunnel switch attivo R0
- show platform software access-tunnel switch attivo R0 statistiche
- show platform software access-tunnel switch attivo F0
- show platform software access-tunnel switch attivo F0 statistiche
- show platform software object-manager switch attivo F0 statistics
- show platform software object-manager switch attivo F0 in sospeso-problema-aggiornamento
- show platform software object-manager switch attivo F0 in attesa di aggiornamento
- show platform software object-manager switch attivo F0 error-object
- show tech-support
- show tech-support lisp

WLC (AireOS):

- mostra riepilogo ap infrastruttura
- mostra riepilogo fabric
- mostra riepilogo server mappa fabric
- show run-config
- comandi show run-config
- show tech

WLC (IOS-XE)

- mostra riepilogo app
- mostra riepilogo ap infrastruttura
- mostra riepilogo infrastruttura wireless
- mostra riepilogo client wireless
- show tech-support wireless
- show tech-support wireless fabric
- show tech-support lisp (se il fabric è in una scatola o wireless integrato in esecuzione su 9300/9400/9500)
- mostra supporto tecnico (se il fabric è in una scatola o wireless integrato in esecuzione su 9300/9400/9500)

Access Point:

- show ip tunnel fabric
- show tech-support

Push della configurazione WLC di AireOS da Cisco DNA Center

In questo esempio viene mostrato il push della configurazione WLC di AireOS da Cisco DNA Center dopo il provisioning (nota: utilizzo di Reference come 3504 WLC).

mostra riepilogo raggio dopo il provisioning 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
```

Il Push della configurazione WLAN è visualizzato in show wlan summary.

```
(sdawlc3504) >show wlan summary

Number of WLANs..... 7

WLAN ID  WLAN Profile Name / SSID                                                    Status    Interface N
-------  -------------------------------------------------------------------------  --------  ----------
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 della configurazione WLC da Cisco DNA Center

In questo esempio viene mostrato il push della configurazione WLC da Cisco DNA Center dopo l'aggiunta del WLC al fabric.

Verifica della raggiungibilità di Map-Server

mostra riepilogo server mappa fabric dopo l'aggiunta del WLC all'infrastruttura.

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

MS-IP     Connection status

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

192.168.4.45    UP

192.168.4.66    UP
```

Debug connettività server mappa infrastruttura

La connettività del Control Plane (CP) può interrompersi o rimanere inattiva per vari motivi.

- Se il PC andasse giù. (che non è questo il caso)
- I nodi intermedi che si interrompono e che connettono il WLC al PC, ad esempio il router di fusione.
- Se la connettività TCP al WLC è stata interrotta a causa di un collegamento non attivo. Può essere un WLC per un vicino immediato o un CP per un vicino immediato verso il WLC.

mostra informazioni dettagliate su server mappa fabric

show fabric TCP creation-history <IP server mappe>

Debug che possono fornire ulteriori informazioni

debug fabric lisp map-server tcp enable

debug fabric lisp map-server all enable

Come verificare se l'infrastruttura è abilitata e qual è l'output previsto?

mostra il riepilogo dell'infrastruttura dopo l'aggiunta del WLC all'infrastruttura.

```
(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_
```

Push della configurazione WLAN da Cisco DNA Center

Il push della configurazione WLAN da Cisco DNA Center viene visualizzato in show fabric wlan

summary dopo l'aggiunta del WLC al fabric e l'assegnazione del pool IP del client alla WLAN (Fabric Wireless LAN) in Provisioning > Fabric > Host Onboarding.

mostra riepilogo wlan infrastruttura dopo il provisioning 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_
```

Debug dei problemi wireless

Debug aggiunta punto di accesso/Debug della formazione del tunnel di accesso

1. Verificare se il punto di accesso ha ricevuto l'indirizzo IP.

show ip dhcp snooping binding → On Fabric Edge

Se non viene visualizzato un indirizzo IP per l'interfaccia AP collegata, abilitare i debug sullo switch e verificare se il punto di accesso sta ricevendo l'indirizzo IP o meno.

debug ip dhcp snooping packet

debug ip dhcp snooping event

File di log di esempio allegato di seguito →

Esempio:

```
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 ha
```

2. Verificare se l'access point si unisce al WLC.

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

Se l'AP non è mai stato aggiunto al WLC, abilitare questi debug sul WLC.

- debug capwap events enable

- debug capwap errors enable

3. Se l'access point forma il protocollo CAPWAP ma non sono stati formati tunnel di accesso tra l'access point e lo switch, eseguire questi controlli

Passaggio 1. Verificare se gli access point nel WLC dispongono o meno di IP RLOC. In caso contrario, controllare qui il punto 1.

1. Per rendere il protocollo del control plane dell'infrastruttura più resiliente, è importante che nella tabella di routing globale di ciascun nodo dell'infrastruttura sia presente un percorso specifico verso il WLC. Il percorso all'indirizzo IP del WLC deve essere ridistribuito nel protocollo IGP sottostante al bordo o configurato staticamente su ciascun nodo. In altre parole, il WLC non deve essere raggiungibile tramite la route predefinita.

Passaggio 2. Se gli access point nel WLC mostrano RLOC corretti e in show fabric summary mostra RLOC richiesto con RLOC ricevuto corretto, controllare questi passaggi

2. Controllare il nodo Control Plane, show lisp instance-id <ID istanza ap L2> server ethernet→ Deve contenere Base Radio MAC per AP.

Controllare sul nodo Fabric Edge, show lisp instance-id <L2 ap instance id> ethernet database wlc → Deve contenere Base Radio MAC per AP e non il MAC ethernet di AP.

Se i 2 comandi precedenti non mostrano il MAC della radio base dell'access point e i tunnel di accesso non si stanno formando. Abilitare debug lisp control-plane all sul Control Plane e cercare Base Radio MAC nel log.

Nota: debug lisp control-plane all on Control Plane is very chatty. Disabilitare la registrazione sulla console prima di attivare i debug.

Se viene visualizzato un errore di autenticazione come mostrato di seguito, controllare la chiave di autenticazione tra il nodo WLC e il nodo 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
```

Come controllare la chiave di autenticazione sulla configurazione dell'infrastruttura tra WLC e CP.

Sul WLC, controllare la GUI in Controller > Fabric Configuration > Control Plane > (chiave già condivisa)

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)

Nota: In genere, Cisco DNA Center preme questa chiave in modo da non modificarla a meno che non sia necessario e da sapere cosa è configurato su CP/WLC]

---

4. Controlli generali e comandi show per i tunnel di accesso.

- 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 tunnel di accesso

```
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#
```

Se i tunnel di accesso di cui al comando b) sono superiori a a), si tratta di un problema. Qui le voci Fed non sono state cancellate correttamente da Fabric Edge e quindi ci sono più voci access-tunnel in Fed rispetto a IOS. Confrontare l'indirizzo IP distinto dopo aver eseguito il comando

mostrato di seguito. Se più tunnel di accesso condividono lo stesso IP di destinazione, il problema è proprio la programmazione.

- show platform software fed switch ifm attivo if-id <Ogni AP IF-ID>

Nota: Ciascun IF-ID può essere recuperato dal comando precedente.

```
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 attivo 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 attivo R0 statistiche

```
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 attivo 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 attivo F0 statistiche

```
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 attivo f0 in sospeso-problema-aggiornamento
- show platform software object-manager switch attivo f0 in attesa di aggiornamento
- show platform software object-manager switch active f0 error-object

5. Tracce e debug da raccogliere.

Passaggio 1. Raccogliere i log di archivio prima di abilitare le tracce e i debug

richiesta flash di destinazione dell'archivio di traccia software della piattaforma:<Nomefile>

```
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]
```

Passaggio 2. Aumentare il buffer di registrazione e disattivare la console.

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

Passaggio 3. Impostazione delle tracce.

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

Passaggio 4. Abilitazione dei debug.

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

Passaggio 5. porta dell'interfaccia di chiusura/non chiusura a cui è collegato il punto di accesso.

Passaggio 6. Raccogliere i log di archivio come nel Passaggio 1. con un nome file diverso.

Passaggio 7. Reindirizza il file di registrazione a flash.

Floor_Edge-6#show logging | redirect flash:<Nomefile>

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

Debug del client

Debug dei problemi del client wireless su SDA POCHI possono diventare difficili.

Segui questo flusso di lavoro per eliminare un dispositivo alla volta.

1. WLC

2. Fabric Edge

3. Access Point (se il debug su Fabric Edge punta a AP)

4. Nodo intermedio/di confine. (se si verifica un problema con il percorso dei dati)

5. Nodo del piano di controllo. (Se si verifica un problema relativo al percorso di controllo)

Debug WLC

Per i problemi di connettività del client, iniziare il debug raccogliendo informazioni sul WLC, che includono comandi show e debug.

Comandi show AireOS WLC:

- show run-config
- show tech
- show wlan summary
- show wlan <id> —> Raccoglie questo output per tutti gli SSID, almeno 1 per i sistemi operativi e non
- mostra riepilogo fabric
- mostra riepilogo server mappa fabric
- show client summary
- show client detail <mac_id>

Comandi di debug AireOS WLC:

- debug client <mac1> —> Associazione client, roaming, debug.
- debug fabric client detail enable —> Fornisce i messaggi di registrazione dell'infrastruttura delle informazioni

Debug di Fabric Edge

Una volta eseguito il debug su WLC e osservato che non vi sono problemi relativi al percorso del control plane per il client. Il client passa da Assoc, Autenticazione ed esegue lo stato con il tagging SGT o i parametri AAA corretti; passare a questo passaggio per isolare ulteriormente il problema.

Un'altra cosa da verificare è che la programmazione del tunnel di accesso sia corretta, come descritto nella precedente sezione sul debug AP.

show commands to verify:

Trova ID istanza lisp L2 da (mostra dettagli client <mac_id> dall'alto)

<#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 s

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

Comandi di debug su Fabric Edge

È necessario raccogliere le tracce Fed in caso di problemi nella programmazione della voce client su Fabric Edge. Dopo aver abilitato i debug, è possibile procedere in due modi.

I debug e i comandi set devono essere abilitati indipendentemente dal metodo.

- set platform software trace fed switch active tutti i moduli di emergenza
- set platform software trace fed switch active l2_fib_entry verbose
- set platform software trace fed switch active l2_fib_adj verbose
- set platform software trace fed switch active inject verbose
- set platform software trace fed switch active matm verbose

debug (disabilitare la registrazione nella console e aumentare il buffer di registrazione)

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

Metodo 1. Dopo l'abilitazione dei debug, raccogliere i log di traccia radio attivi per un client specifico.

 Nota: se si verifica un problema con DHCP, non utilizzare questo metodo]

Attendere che il problema si riproduca

- debug platform condition mac <mac-id> control-plane
- avvio condizione piattaforma di debug
- arresto condizione piattaforma di debug
- mac contesto wireless binario filtro traccia soft request plat <mac-id>

Reindirizzare i log della console in modo che lampeggino una volta riprodotto il problema.

Metodo 2. Raccolta dei log di traccia dell'archivio dopo l'abilitazione dei debug.

Attendere che il problema si riproduca

richiedi archivio di traccia software piattaforma

Raccogliere il file decodificare i log e analizzare i log fed, ios, fman per il client mac.

Reindirizzare i log della console in modo che lampeggino una volta riprodotto il problema.

Debug del punto di accesso

Debug sui modelli AP 2800/3800/1562:

Per i problemi del lato AP, assicurarsi di raccogliere tutti i comandi show del WLC e i log prima di raccogliere i log del lato AP e collegarli alla SR.

Seguire questi passaggi per eseguire il debug dei problemi relativi ai dati sul lato client.

1. Comandi Collect AP show: (2-3 volte, prima e dopo il completamento delle prove)

- show clock
- termine len 0
- mon
- show tech
- show logging (visualizza registri)
- show controllers nss stats show controllers nss status
- show ip tunnel fabric

In caso di problemi CWA, oltre ai comandi superiori raccogliere anche i log riportati di seguito. I comandi seguenti devono essere raccolti una volta prima e dopo il completamento del 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
- mostra supporto tecnico

2. Debug AP (filtro per indirizzo MAC)

Problemi relativi al percorso dati del client:

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

Tracce punto di accesso client:

- config ap indirizzo traccia client add <mac>
- config ap client-trace output console-log enable
- abilita tutti i filtri di traccia client dell'access point di configurazione

- probe del filtro di traccia client dell'access point di configurazione disabilitato
- avvio traccia client ap di configurazione
- mon
- exec-timeout 0 0

Problemi CWA:

- debug capwap client avc all
- acl client debug capwap
- debug client <client mac>
- debug dot11 indirizzo info a livello client <mac>
- debug dot11 indirizzo eventi a livello client <mac>
- debug flexconnect pmk

Debug Use Case

Debug CWA client

Note importanti:

- Quando si distribuisce CWA in SDA, utilizzare sempre DNAC per distribuire la configurazione.
- Una volta implementato utilizzando DNAC, anche il criterio di autorizzazione, il criterio di autenticazione e il profilo di autorizzazione verranno implementati in ISE da DNAC.
- Le identità per l'autenticazione devono essere configurate manualmente come per Dot1x

Verificare in quale fase si trova il problema.

Passaggio 1. Il client riceve un indirizzo IP e passa a Webauth in sospeso?

1. In caso affermativo, passare al passaggio successivo.
2. In caso negativo, il problema si trova nella fase iniziale di unione.
3. Controllare la configurazione su WLC e AP.
4. Controllo del push dell'ACL nell'access point e corrispondenza con il contenuto del WLC
5. Se il push dell'ACL non è corretto, ricaricare l'AP e verificare che si tratti di uno stato provvisorio in cui non viene eseguito il push della configurazione. Una volta confermato su 1 AP, accertarsi che il provisioning degli AP venga eseguito tramite DNAC.

Passaggio 2. Il client può caricare la pagina di reindirizzamento?

1. In caso affermativo, passare al passaggio successivo.
2. In caso negativo, il problema potrebbe presentarsi in più punti.
3. Controllare la configurazione su WLC e AP.
4. Controllo del push dell'ACL nell'access point e corrispondenza con il contenuto del WLC
5. Se il push dell'ACL non è corretto, ricaricare l'AP e verificare che si tratti di uno stato provvisorio in cui non viene eseguito il push della configurazione. Una volta confermato su 1 AP, accertarsi che il provisioning degli AP venga eseguito tramite DNAC.
6. Verificare la raggiungibilità dal WLC all'ISE e controllare lo switch a cui l'AP è collegato

all'ISE. Assicurarsi che non vi sia alcun firewall tra
7. Verificare che il DNS sia configurato correttamente.

Passaggio 3. Il client è in grado di visualizzare la pagina Web ma il problema è costituito dal login e dal passaggio al successo?

1. Verificare le configurazioni dei passi 1 e 2.
2. Verificare che il profilo di autorizzazione, i criteri di autenticazione e i criteri di autorizzazione siano corretti.
3. Controlla i log di ISE Live
4. Verificare che il nome utente e la password siano configurati correttamente nelle identità ISE.
5. Raccogliere i debug su WLC e AP come di seguito se tutto sembra buono.

1. Debug sul WLC:

- Di seguito sono riportati i comandi show rispettivamente per AireOS e Polaris:

AireOS:

- show run-config
- show wlan summary
- show wlan <id_for_Guest>
- mostra riepilogo acl flexconnect
- show flexconnect acl detail <ACl_from_PREVIOUS_command>

Polaris

- mostra in esecuzione
- show tech-support wireless
- show tech-support wireless fabric
- show wlan summary
- show wlan id <id_for_guest>
- show ap name <nome_AP> config general
- show running-config ACL | sec
- mostra riepilogo flessibilità profilo wireless
- show wireless profile flex detailed <nome_profilo_from_ABOVE>

- Abilitare questi debug su AireOS e Polaris.

AireOS:

- client di debug <mac_client>
- debug aaa all enable
- Riprodurre il problema
- Raccogli registri console/ssh/telnet

Polierie (9300/9400/9500):

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

Riprodurre il problema

show platform software trace messaggio wncd switch active R0 reverse | redirect flash:<nomefile>

richiedi archivio di traccia software piattaforma

Raccogli entrambi i file da flash

2. Debug su AP:

Raccogli informazioni sugli ACL:

show ip access-lists

Raccogli i debug seguenti dal punto di accesso:

- debug capwap client avc all
- acl client debug capwap
- debug client <client mac>
- debug dot11 indirizzo info a livello client <mac>
- debug dot11 indirizzo eventi a livello client <mac>
- debug flexconnect pmk

Debug DHCP client

È possibile eseguire il debug di alcuni problemi utilizzando questi debug.

1. Messaggi di individuazione DHCP non visualizzati sullo switch.

2. Il client wireless non riceve l'offerta DHCP. Il rilevamento DHCP viene eseguito nei log dei pacchetti di snooping ip dhcp di debug.

3. Raccogliere l'acquisizione dei pacchetti sulla porta collegata all'access point, la porta uplink e la porta connessa al server DHCP sul lato fusione.

Debug/Mostra comandi, che possono essere:

1. Verificare su Cisco DNA Center se l'SSID è assegnato al pool IP.

2. Verificare se la WLAN è abilitata sul WLC.

3. Verificare che le radio siano abilitate e che le reti 802.11a e 802.11b siano abilitate.

Debug delle prestazioni del client su AP

1. Limitare il problema ai sistemi cablati o wireless o a entrambi. Verificare lo stesso traffico su un

client connesso a una rete wireless sullo stesso VNID e verificare lo stesso traffico su reti cablate sullo stesso VNID.

2. Se i client cablati nella struttura sulla stessa VN non hanno problemi ma i client wireless lo sono, il problema è sul lato AP.

3. Per eseguire il debug sul lato AP in caso di problemi relativi alle prestazioni del client o al traffico, verificare innanzitutto che il problema non sia la connettività del client.

4. Verificare che l'uso del client di debug sul WLC faccia in modo che il client osservi una riduzione del livello durante il roaming, il timeout della sessione o la connessione stabile allo stesso access point.

5. Dopo aver individuato il problema sullo stesso access point, eseguire la procedura seguente per raccogliere i debug sugli access point serie 3800/2800/4800 e sull'acquisizione dei pacchetti sullo switch collegato all'access point e sulle acquisizioni dei pacchetti via etere.

Passaggio 1. Verificare che il traffico utilizzato per riprodurre il problema stia effettivamente imitando il problema.

Fase 2. L'acquisizione dei pacchetti via etere deve essere impostata dal cliente sul punto in cui è stato eseguito il test.

```
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/
```

Passaggio 3. Eseguire il debug del client dal WLC e dell'acquisizione dei pacchetti dallo switch a cui è connesso l'access point. Le acquisizioni EPC degli switch possono essere sfruttate per acquisire questi log.

Passaggio 4. Debug dalla sessione ssh/telnet del 3800 AP

```
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
```

Nota: è necessario usare questi ultimi comandi sulla combinazione corretta di radio vap. Ad esempio, se il client si trova su radio 1, vap 1: cat /click/client_ip_table/list = Dall'output, Check client connected port/interface aprXvY, utilizzare lo stesso per ottenere l'output riportato di seguito. cd /click/fromdev_ apr1v3/ cat icounts conteggi chiamate cd /click/todev_ apr1v3/ cat icounts conteggi chiamate Passaggi B - E B) Avviare OTA tra punti di accesso. Client. Avviare inoltre il protocollo PCAP (Spanning AP port dove è connesso il client) cablato. (Per l'analisi è necessario sia pcap cablato che wireless.) C) Utilizzare la WLAN di autenticazione aperta (nessuna protezione per analizzare pcap OTA). Avviare il test iperf e mantenerlo in esecuzione per 10-15 minuti, continuamente. D) Ripetere il passo A ogni due minuti utilizzando il comando date. Eseguire 5 o più iterazioni. E) Una volta completato il test - Raccogliere show tech da AP.

Onboarding AP

Metodo/Fasi tradizionali:

Si ritiene che l'ambito della Vlan dell'access point abbia l'opzione 43 o l'opzione 60 che punta al WLC.

1. Selezionare Autenticazione come Nessuna autenticazione.

2. Configurare Infra_VN con il pool IP AP e Default_VN con il pool IP del client wireless.

3. Configurare le porte dell'interfaccia perimetrale da cui i punti di accesso sono connessi con Infra_VN.

4. Una volta che AP ottiene l'IP e si unisce a WLC, viene rilevato nell'inventario dei dispositivi.

5. Selezionare l'access point e assegnarlo a un sito specifico ed eseguire il provisioning.

6. Una volta eseguito il provisioning, l'access point viene assegnato al gruppo AP creato durante l'aggiunta del WLC all'infrastruttura.

Plug and Play/Provisioning di punti di accesso zero-touch

Si ritiene che l'opzione 43 dell'ambito VLAN dell'access point faccia riferimento a Cisco DNA Center. Seguire la guida DNAC per configurare PNP AP

Lato Fabric Edge:

Abilitare questi debug.

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

Informazioni correlate

- Guide alla configurazione wireless per ciascuna release
- Guida all'installazione wireless SD
- Guida alle best practice wireless
- Documenti di riferimento tecnici per reti wireless
- Matrice di compatibilità per SDA
- Guide per l'utente di Cisco DNA Center per ciascuna release

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).