

Fehlerbehebung: Probleme beim Beitritt oder Trennen von Catalyst 9800 APs - Datenfluss

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Topologie](#)

[Generische Ausgänge zum Sammeln von WLC](#)

[Spezifische Ausgänge von WLC für konkrete AP](#)

[Fortschrittliche Protokolle vom WLC und AP für konkreten AP](#)

[Protokolle vom WLC:](#)

[Protokolle vom Access Point](#)

[Liste aller Befehle](#)

[Liste aller Befehle des WLC](#)

[Liste aller Befehle vom Access Point](#)

Einleitung

In diesem Dokument werden ein systematischer Ansatz und eine Liste von Befehlen beschrieben, die zur Fehlerbehebung bei Verbindungs-/Verbindungsproblemen mit 9800 APs gesammelt werden müssen:

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

Grundkenntnisse des Cisco WLC 9800

Grundkenntnisse der Cisco Wave2 und/oder 11AX APs

Topologie

Dieser Fehlerbehebungsablauf gilt für APs, die im lokalen Modus verbunden sind, oder APs, die im Flexconnect-Modus in einer Außenstelle verbunden sind.



Generische Ausgänge zum Sammeln von WLC

1.- Wir können nun überprüfen, ob die Anzahl der Access Points mit der erwarteten Anzahl der mit dem WLC verbundenen Access Points übereinstimmt. Überprüfen der WLC-Protokolle auf trennende APs

Identifizieren Sie, ob APs fehlen, und ob in den Protokollen zu beobachten ist, dass APs sich gleichzeitig trennen oder immer die gleichen APs sich verbinden/trennen.

show ap summary | i Anzahl der APs !!Überprüfen Sie, ob die Anzahl der APs mit der erwarteten Anzahl übereinstimmt

sh log | i AP-Ereignis: !!Überprüfen Sie, ob die APs gleichzeitig getrennt werden, oder ob ein Muster für die Verbindung bzw. Trennung der APs vorliegt.

2.- Wir können eine Liste aller APs abrufen und nach fehlenden APs suchen. Identifizieren von APs mit einer geringeren Betriebszeit und einer geringeren ASSOC-Betriebszeit, um festzustellen, ob APs wieder mit Capwap verbunden werden oder neu laden.

Wenn APs neu geladen werden, können wir nach APs mit ähnlicher Verfügbarkeit suchen und überprüfen, ob sich diese APs im gleichen Switch befinden. Wenn APs mit hoher Betriebszeit und niedrigerer Zuordnungszeit vorhanden sind, müssen wir prüfen, ob an diesen APs wurden Änderungen vorgenommen, die einen Neustart von CAPWAPs oder CAPWAPs aufgrund von Neuübertragungen verursachen könnten. Wir können auch überprüfen, ob AP-Abstürze vorliegen.

show ap Betriebszeit !! Check-Up-Zeit und Assoc-Up-Zeit. Nach Mustern suchen

show ap cdp nei !! Ermitteln Sie, ob sich alle APs mit ähnlicher Betriebszeit im selben Switch befinden.

show ap Absturz !! Überprüfen Sie, ob AP abstürzt.

Ordner all | i Absturz !! Suche nach AP-Abstürzen, die in WLC gespeichert sind.

3.- Wir können überprüfen, ob alle historischen Ereignisse oder Gründe für eine Verbindungstrennung beim AP vorliegen. Wir können herausfinden, ob der Grund für die Verbindungstrennung mit allen APs vergleichbar ist und in welcher Phase der Verbindung die Verbindung getrennt wurde.

Identifizieren Sie die wichtigsten Trennungsgründe und ob ein Zeitmuster für diese Trennungen vorliegt.

Wireless-Zustandsübersicht anzeigen !! Suchen nach Connect/Disconnect-Ereignissen, Zeit für diese Ereignisse, Grund und Anzahl der Trennungen

Anzeige der Wireless-Zustandszuordnung !! Suchanfragen, die vom WLC empfangen wurden, und Zeit für diese Suchanfragen

Zusammenfassung der Wireless-Zuordnungsstatistik anzeigen !! Ermitteln Sie den Status des Access Points, den Grund für die letzte Verbindungstrennung und die Phase, in der die Verbindung getrennt wurde.

4.- Falls die Fehler in der DTLS-Phase erkannt werden, können wir überprüfen, welcher Zertifikattyp und welche Chiffren für den AP DTLS-Handshake verwendet werden.

Wireless-Zertifizierungskonfiguration anzeigen !! DTLS-Version und -Verschlüsselungssuite prüfen

Wireless Management TrustPoint anzeigen !! Art des verwendeten Zertifikats

Wireless-dtls-Verbindungen anzeigen !! Zeigt an, ob DTLS für verwendete CAPWAP-Steuerungs-/Daten-Ports eingerichtet ist.

Spezifische Ausgänge von WLC für konkrete AP

5.- Jetzt können wir uns auf einige konkrete APs konzentrieren, die Probleme haben. Zuerst müssen wir die Ethernet- und Funk-MACs für diesen AP finden. Verlauf dieses Access Points überprüfen und fortlaufend nachverfolgen

Verwenden Sie die Befehle show, um eine Zusammenfassung der Ereignisse mit Zeitreferenz, verschiedenen Phasen der AP-Zuordnung zu erhalten, bei denen Ausfälle, Grund für einen Neustart oder die Trennung beobachtet werden können.

Wir können herausfinden, ob WLC den AP aufgrund eines Image-Upgrades neu gestartet hat. Oder wenn die Verbindung des Access Points aufgrund eines Keepalive-Fehlers getrennt wurde.

Verwenden Sie dann "Always-on-Tracing", um weitere Details zu den Ereignissen am Access Point zu erhalten, die eine Ereignissequenz anzeigen. Mit show command time reference können wir uns auf die Ereignisse konzentrieren, die zu dieser Zeit auftreten.

Sammeln Show Tech Wireless für konkrete AP bietet uns Konfigurationsdetails, Tag-Zuweisung, Informationen über Modell, Radios Kanäle, ...

show wireless stats ap history mac-address Ethernet_MAC@ !!Ermitteln Sie den Typ des Ereignisses und die Uhrzeit, und ermitteln Sie den Grund und die Anzahl der Verbindungstrennungen für den jeweiligen Access Point.

show wireless stats ap mac Radio_MAC@ discovery detail !!Überprüfen Sie die Anzahl der Ermittlungsanfragen/-antworten, Erkennungsfehler und den Typ für die letzte funktionierende Erkennung und die nicht funktionierende Erkennung.

show wireless stats ap mac Radio_MAC@ join detailliert !!Zähler für verschiedene Phasen Erkennung, dtls, join, config, data dtls. Zeigt auch den letzten Neustarttyp und Grund an. Verbindungstyp und Grund trennen.

show logging profile wireless start last X days filter mac <radio-or-ethernet-AP-mac> !!Always-on-tracing für diesen AP zeigt detailliertere Ereignisfehler an, die in der WLC-Ablaufverfolgungsdatenbank gespeichert sind. Konfigurationsänderungen, Funk-Ereignisse, Zuordnungs-/Trennungseignisse.

show tech wireless ap name <ap-name> !! Konfigurationsdetails, Tag, Radio Info Channels/txpower, SSIDs, ...

6.- Wenn wir feststellen, dass mehrere APs, die sich nicht im selben Switch befinden, ungefähr zur gleichen Zeit getrennt werden, können wir bestätigen, ob alle trennenden APs sich im selben Wld befinden.

Wenn dies der Fall ist, können wir die wncd-CPU-Auslastung überprüfen, um festzustellen, ob die Verbindung aufgrund der hohen wncd-CPU-Auslastung getrennt werden konnte und WLC nicht in der Lage war, Pakete zu verarbeiten, die von APs empfangen wurden.

show wireless loadbalance ap affinity mac Ethernet_MAC@ !!Überprüfen Sie wncd zugewiesen zu konkreten AP mac-Adresse, können wir auch wncd für konkrete Site-Tag erhalten

show wireless loadbalance ap affinity wncd <0-7> !!Eine weitere Option besteht darin, alle APs zu überprüfen, die einem konkreten wncd zugewiesen sind.

sh proc cpu-Plattform | i wncd !! CPU-Auslastung pro WLD prüfen

Fortschrittliche Protokolle vom WLC und AP für konkreten AP

7.- Wenn wir mit den vorherigen Informationen nicht in der Lage sind, den Grund für AP-Joins zu identifizieren, müssen wir ra-Traces und Paketerfassungen sowie AP-Debugs erfassen, falls wir für das nächste Ereignis auf den AP zugreifen können.

Auf diese Weise werden Paketaufzeichnungen vom Access Point und ausführliche Ablaufverfolgungen bereitgestellt, um die Gründe für die Verbindungstrennung des Access Points zu identifizieren. Muss vor dem nächsten Ereignis Traces und Captures aktivieren, um die Daten zu erfassen.

Falls der Zugriff auf den Access Point über SSH möglich ist, können wir Debug-Meldungen im Access Point aktivieren, der den Access Point im Hinblick auf Verbindungsabbrüche anzeigt.

Die Paketerfassung im WLC- und AP-Switch-Port kann wie folgt erfolgen:

hilfreich, um festzustellen, ob Verbindungen aufgrund von Paketverlusten im Netzwerk getrennt werden.

Protokolle vom WLC:

!! Aktivieren Sie ra-trace für AP mit der Standardüberwachungszeit von 1800 s, und erhöhen Sie sie auf max., falls Sie nicht wissen, wann die AP-Verbindung getrennt wird.

debug wireless mac <AP_Radio_MAC> internal monitor-time 2085978494 !!Verwenden der AP-Funk-MAC zum Erfassen von Ablaufverfolgungen mit ausführlicher Ebene vom WLC. Mit der Einstellzeit können wir Traces für bis zu 24 Tage aktivieren

!!Oder

debug wireless ip <AP_IP> internal monitor-time 2085978494 !!Verwenden der AP-IP-Adresse zum Erfassen von Ablaufverfolgungen mit ausführlicher WLC-Ebene Mit der Einstellzeit können wir Traces für bis zu 24 Tage aktivieren

!!Vervielfältigen

Kein Debuggen Wireless MAC <AP_Radio_MAC|AP_IP> interne Überwachungszeit 2085978494

!!WLC generiert eine ra_trace-Datei mit dem Befehl AP_info, um zu überprüfen, ob eine ra_trace-Datei generiert wurde.

dir bootflash: | i ra_trace

!! Eingebettete Erfassungen, gefiltert nach AP-IP-Adressen-ACL. Die Paketerfassung für die AP-IP-Adresse wird in beide Richtungen gefiltert. Der Puffer ist kreisförmig, um

sicherzustellen, dass bei einem Puffer von mehr als 100 Mio. die neuesten Ergebnisse erfasst werden.

!!ACL erstellen

```
ip access-list extended CAP-FILTER
permit ip host <AP_IP> any
permit ip any host <AP_IP>
```

!!Paketerfassung erstellen

MYCAP klar erfassen

MYCAP-Schnittstelle Po1 überwachen, beide

MYCAP-Puffer mit kreisförmiger Größe 100 erfassen

MYCAP-Übereinstimmung mit allen

MYCAP-Zugriffsliste CAP-FILTER für Überwachungserfassung

MYCAP Start überwachen

!!Vervielfältigen

MYCAP-Stopp überwachen

```
monitor capture export flash:|tftp:|http:.../filename.pcap
```

Protokolle vom Access Point

Technologie anzeigen !! Sammeln Sie Show-Tech, um alle Konfigurationsdetails und Funkstatistiken für den Access Point zu erhalten.

dtls-Verbindung anzeigen !! Zertifikate, Ports und Chiffren, Versionen für DTLS prüfen

Laufzeit

!!Grundlegend

debuggen capwap-Clientereignisse

```
debug capwap client error
```

!! Erweitert

```
debug capwap client pmtu
```

```
debuggen capwap client keepalive
```

```
debug capwap client payload
```

Debug Capwap-Clientdetails

```
debug capwap client info
```

Liste aller Befehle

Liste aller Befehle des WLC

```
show ap summary | i Number of APs
sh log | i AP Event:
show ap uptime
show ap cdp nei
show ap crash
dir all | i crash
show wireless stats ap history
show wireless stats ap discovery
show wireless stats ap join summary
show wireless certification config
show wireless management trustpoint
```

```
show wireless dtls connections
show wireless stats ap history mac-address Ethernet_MAC@
show wireless stats ap mac Radio_MAC@ discovery detailed
show wireless stats ap mac Radio_MAC@ join detailed
show logging profile wireless start last X days filter mac <radio-or-ethernet-AP-mac>
show tech wireless ap name <ap-name>
show wireless loadbalance ap affinity mac Ethernet_MAC@
show wireless loadbalance ap affinity wncd <0-7>
sh proc cpu platform | i wncd
debug wireless mac <AP_Radio_MAC> internal monitor-time 2085978494
```

Liste aller Befehle vom Access Point

```
show tech
show dtls connection
term mon
debug capwap client events
debug capwap client error
debug capwap client pmtu
debug capwap client keepalive
debug capwap client payload
debug capwap client details
debug capwap client info
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.