Problembehebung bei vermaschten Wi-Fi-Verbindungen des Catalyst 9800

Inhalt

Einleitung

In diesem Dokument werden verschiedene Methoden zur Fehlerbehebung in Mesh-Umgebungen der Serie 9800 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie sowohl über Kenntnisse des Wireless Controllers als auch über Kenntnisse der Mesh-Bereitstellung verfügen.

1. Geltungsbereich und Geltungsbereich

Gilt für: Diese Probleme sind für Seehafen und Bergbauumgebung aufgetreten.

* Catalyst Wireless LAN Controller 9800-L/9800-CL/9800-40

* Outdoor Mesh-Bereitstellungen (RAP-MAP)

* Dual-Band-WLANs (2,4 GHz/5 GHz)

* Umgebungen mit:

  * Langstrecken-Mesh-Verbindungen

  * Hochfrequenzrauschen / Industriegebiete (Häfen, Terminals, Yards)

2. Häufige, vom Kunden gemeldete Symptome

Mesh/AP-Symptome

1. Mesh AP zeigt Joined auf WLC, aber keine Client-Verbindungen

  * Kein Client- oder Upstream-Verkehr

  * Ping schlägt fehl, bis AP neu gestartet wird.

2. RAP-MAP-Link

* Klappt gelegentlich.

* MAP wechselt unerwartet zu einem anderen RAP/MAP.

* Der Mesh-AP trennt sich vom WLC und erfordert einen manuellen Neustart.

3. Symptome der Client-Verbindung

* Der Client befindet sich auf unbestimmte Zeit im Authentifizierungsstatus.

* Der Client durchläuft APs, bleibt aber nicht authentifiziert.

* Client stellt erst eine Verbindung her, nachdem:

* Erzwingung des Entfernens aus dem WLC- oder AP-Neustart

* Häufige Client-Verluste bei 2,4 GHz

3. Große Wahrscheinlichkeit, Ursache Eimer

Kategorie	Typische Probleme
RF/Design	Kanalüberdeckung, große Kanalbreite, Antennenversatz
Netzsteuerung	Instabilität bei übergeordneter Auswahl, schwacher Backhaul-SNR
Konfiguration	Gemischte Datenraten, mehrere BGNs, statische Stromversorgung
Software	wncd Prozess-Stalls, veralteter Client-Status
Skalierung/Auslastung	Übermäßige Authentifizierungsanrufe, EAPOL-Timer stimmen nicht überein

4. Erforderliches Design und Konfigurationsvalidierung

4.1 Mesh-Backhaul (kritisch)

Root-AP (RAP)

- Kanalbreite: nur 20 MHz
- Überlappungsfreie Kanäle über RAPs hinweg
- Derselbe Bridge-Gruppen-Name (BGN)
- Statische Kanalzuweisung
- Sichtverbindung zu MAP

Vermeiden

- Kombination von 20/40 MHz auf RAPs
- Auf allen RAPs derselbe Kanal
- Mehrere BGNs im gleichen Bereich

4.2 Antenne und Montage

- 5-GHz-Rundstrahlantenne:
- Senkrecht zum Boden montiert
- Dediziertes 5-GHz-Funkmodul für Mesh-Backhaul
- Richtantenne bevorzugt für MAPs mit großer Reichweite
- Beseitigung von Hindernissen (Metall, Kräne, Behälter)

5. Best Practices für RF und WLAN

5.1 Datenübertragungsraten (sehr empfehlenswert)

2.4 GHz)

Verpflichtend: 12 Mbit/s

Deaktivieren: 6, 9 Mbit/s

Sonstige: Unterstützt

5 GHz)

Verpflichtend: 12 Mbit/s

Deaktivieren: 6, 9 Mbit/s

Sonstige: Unterstützt

Auswirkungen:

- Weniger anfällige Clients
- Verbessert Roaming- und Authentifizierungsstabilität

5.2 Stromversorgung und RRM

- Vermeidung von statischem TX-Strom auf AP-Ebene
- Globales RRM verwenden
- Minimale TX-Leistung:
- 2,4 GHz: ≥ 12 dBm

Vermeidung aggressiver DCA-Änderungen in den Produktionszeiten

Beheben von Verbindungsproblemen beim Client

Problembeschreibung

In vernetzten Bereichen:

- Clients wurden erfolgreich mit MAPs verknüpft.
- Die Authentifizierung beginnt, wird aber nie abgeschlossen.
- Der Client verbleibt im Authentifizierungsstatus auf dem WLC.
- Der Client kann während der Authentifizierung zwischen APs wechseln.
- Die Authentifizierung ist nur erfolgreich nach: Der Client wird manuell aus dem WLC entfernt, oder MAP wird neu gestartet.

Dieses Verhalten tritt nur gelegentlich auf, ist bei Bedarf schwer nachzuvollziehen und gehört nicht zum normalen Authentifizierungsablauf.

Symptome beobachtet

- Eine Zusammenfassung der Wireless-Clients anzeigen zeigt Clients, die sich nicht authentifizieren konnten.
- Clients generieren wiederholte Authentifizierungsversuche.
- Es wurde kein expliziter Authentifizierungsfehler oder keine Ablehnung festgestellt.
- Der Client bleibt auch nach mehreren Roaming-Ereignissen hängen.
- Problem, das hauptsächlich bei der Verbindung von Clients über MAPs auftritt.
- Die Häufigkeit des Auftretens nimmt während der Auslastung zu.

Wichtigste Faktoren bei Mesh-Bereitstellungen für Probleme mit der Client-Verbindung

1. Instabilität durch Mesh-Backhaul

- Schwankende RSSI/SNR zwischen RAP und MAP.
- MAP wählt während der Authentifizierung das übergeordnete Element erneut aus.
- Netzwerklatenz verursacht EAP-Timeout oder -Neuübertragung.
- MAP leitet Datenverkehr vorübergehend weiter, jedoch nicht konsistent

Auswirkungen:

- Der Authentifizierungsstatuscomputer wurde nicht abgeschlossen.
- Der Client bleibt bei der Authentifizierung stecken.

2. Roaming während der Authentifizierung

- Clients roamen zwischen MAPs oder zwischen MAP und RAP.
- Der Authentifizierungskontext wird nicht vollständig übertragen.
- Client setzt Roaming fort, bleibt aber im Authentifizierungsstatus

Auswirkungen:

- Die Authentifizierung wird wiederholt neu gestartet.
- Der Client erreicht nie den RUN-Status.

3. Niedrige Datenübertragungsraten auf Client-Dienstfunk (2,4 GHz)

- 6 oder 9 Mbit/s erforderlich
- Übermäßige Wiederholungen und übermäßiger Sendezeitverbrauch
- Authentifizierungsframes wurden verzögert oder verworfen.

Auswirkungen:

- Der EAP-Austausch über das Mesh wird unzuverlässig.
- Die Authentifizierung scheint ohne expliziten Fehler hängen zu bleiben.

4. Mesh-Backhaul und Client-Datenverkehr, der dieselben RF-Einschränkungen nutzt

- Hohe Auslastung bei Mesh-Links.
- Der Client-Authentifizierungsverkehr steht im Wettbewerb mit:
- Datenverkehr
- Datenverkehr steuern
- Authentifizierungspakete sind klein, aber zeitkritisch.

Auswirkungen:

- Die Authentifizierung wird erst nach einem erneuten Versuch oder Zurücksetzen abgeschlossen.

Identifizieren des Trefferfalls (Mesh-Authentifizierung blockiert)

Das Problem gilt als behoben, wenn bei einer Mesh-Bereitstellung alle genannten Bedingungen gleichzeitig erfüllt werden:

Client-Verhaltensindikatoren

- Der Client bleibt für mehr als 60-120 Sekunden im Authentifizierungsstatus.
- Der Client wechselt nicht automatisch in den RUN-Status.
- Der Client stellt erst dann eine Verbindung her:
- Zwangsvolles Entfernen des Clients aus dem WLC
- Neustart des Mesh-AP
- Der Client kann zwischen MAPs oder RAPs wechseln und dabei den Authentifizierungsstatus beibehalten.

WLC-Anzeigen

Command:

Übersicht über Wireless-Clients anzeigen

Indikatoren:

- Dieselbe Client-MAC wird dauerhaft unter "Authentifizieren" aufgeführt.
- Der Client-Eintrag altert nicht automatisch.

Aktivieren Sie diesen Befehl, wenn der Client länger als 10 Minuten verbunden ist:

show wireless client mac <Client-mac>

Mesh-spezifische Indikatoren

Befehle:

Übergeordnetes Element für AP-Mesh anzeigen

Maschendraht anzeigen

Indikatoren:

- Übergeordnete Änderung oder Instabilität während der Client-Authentifizierung
- Schwankende RSSI/SNR-Werte
- Erhöhte Anzahl von Wiederholungen oder Paketverlust beim Mesh-Backhaul

Obligatorische Protokollerfassung (während des Fehlerfensters)

Protokolle müssen gesammelt werden, während sich der Client im Authentifizierungsstatus befindet.
Protokolle, die nach einem Neustart oder nach dem Löschen des Clients gesammelt werden, sind für die Ursache nicht hilfreich.

1. Controller-Baseline-Protokolle

Technologie-Wireless anzeigen

show clock

Zweck:

- Gesamten WLC-Status erfassen
- Zeitstempel protokollübergreifend korrelieren

2. Client-Status-Validierungsprotokolle

Übersicht über Wireless-Clients anzeigen

Übersicht über Wireless-Clients anzeigen | Authentifizierung einschließen

show wireless client mac <Client-mac>

3. Interne WNCD-Protokolle (kritisch)

Ausführliche Ablaufverfolgung aktivieren:

set plattform software trace wncd chassis active r0 all verbotsed

Protokolle sammeln (letzte 30 Minuten):

show logging process wncd internal last 30 minutes

Client-spezifische gefilterte Protokolle:

show logging process wncd start last 30 minutes filter mac <client-mac> to-file bootflash:wncd_client.log

4. Radio Active (RA)-Verfolgung - pro Client

Über GUI:

- Monitor > Wireless > Client > Fehlerbehebung
- Betroffene Client-MAC hinzufügen.
- RA Trace starten.
- Reproduzieren des Problems

5. Mesh-Backhaul-Validierungsprotokolle

Maschendraht anzeigen

Übergeordnetes Element für AP-Mesh anzeigen

ap Mesh Statistiken anzeigen

6. Optional (falls verfügbar) - Authentifizierungsserver-Protokolle

- RADIUS-Authentifizierungsprotokolle für den betroffenen Client
- Authentifizierungslatenz und Neuübertragungen

Fehlerbehebung: MAP-RAP-Verbindungsproblem

Problembeschreibung

Intermittierender und unvorhersehbarer Verlust der Mesh-Backhaul-Konnektivität über mehrere IW9167-MAPs, was zu AP-Disjoins, Mesh-Authentifizierungsfehlern, nicht erreichbaren APs und Blackholing des Client-Datenverkehrs führt. Die Wiederherstellung erforderte häufig einen AP-Neustart oder WLC-Eingriff.

Symptome

- MAP trennt sich vom übergeordneten RAP
- Zugeordneter MAP, aber kein Datenverkehr
- MAP nicht erreichbar vom WLC, RAP und Gateway
- Zugeordnete Clients, aber keine Upstream-Erreichbarkeit
- Kaskadieren von Ausfällen bei übergeordnetem MAP- oder RAP-Roaming

Fehlermeldungen/Anzeigen

FEHLER bei MeshSecurity: Zeitgeber abgelaufen

CRIT-MeshSicherheit: Fehler bei der Authentifizierung der Mesh-Sicherheit mit dem übergeordneten Element.

CRIT-MeshAwppAdj: Als übergeordnetes Element entfernen

mlme_ext_vap_down: VAP (Mon1) ist ausgefallen

ieee80211_ucfg_mesh_add_client(): Knoten nicht gefunden

DTLS - Warnungen schließen

CAPWAP-Heartbeat-Timeout

Identifizieren des Trefferproblems (RAP-MAP-Verbindungsproblem)

1. Mesh-Kontrollebene ist fehlerfrei

Die genannten Befehle können normal angezeigt werden und können nicht allein zur Validierung der Datenverkehrsweiterleitung verwendet werden:

show ap summary

Drahtlose Mesh-AP-Baumstruktur anzeigen

show capwap client rcb

Mit diesen Befehlen wird nur der Status der Kontrollebene bestätigt.

Identifizieren von Mesh-Datenebenenfehlern

MAP: Mesh-Status anzeigen

Dies ist der primäre Indikator für den Zustand der Mesh-Weiterleitung.

Fehlerfreie Ausgabe

MAC übergeordneter AP: 24:D7:9C:04:79:B1

Status der vermaschten Verbindung: UP

Weiterleitungsstatus: AKTIVIERT

Datenverkehr-Blackholing-Ausgabe

MAC übergeordneter AP: 24:D7:9C:04:79:B1

Status der vermaschten Verbindung: UP

Weiterleitungsstatus: DEAKTIVIERT

Dolmetschen:
Mesh-Adjacency ist vorhanden, aber der Access Point leitet den Datenverkehr nicht weiter.

2. MAP: Mesh-Verlauf anzeigen

Wiederholte übergeordnete Übergänge ohne AP-Neuladen weisen auf einen instabilen Weiterleitungsstatus hin:

CRIT-MeshAwppAdj: Als übergeordnetes Element entfernen

CRIT-MeshAwppAdj: Als übergeordnetes Element festlegen

CRIT-MeshAwppAdj: Als übergeordnetes Element entfernen

Durch dieses Muster befindet sich der Access Point häufig in einem nicht weiterleitenden Zustand.

3. MAP Syslog Symptome

Häufige Syslog-Meldungen, die bei Blackholing des Datenverkehrs beobachtet wurden:

ieee80211_ucfg_mesh_add_client(): Knoten nicht gefunden

CLSM: Schlüsselprogrammierung aufgrund von Nulltaste überspringen

Diese weisen darauf hin, dass der Mesh-Sicherheitskontext unvollständig ist und die Weiterleitung von verschlüsseltem Datenverkehr verhindert.

4. WLC-Mesh-Pfad "ap name <AP>" anzeigen

Dieser Befehl bestätigt die Ansicht des Datenpfads durch den Controller.

Gesund

Pfadstatus: Aktiv

Datenpfad: Abschließen

Blackholing von Datenverkehr

Pfadstatus: Aktiv

Datenpfad: Unvollständig

Auslegung:
Der Mesh-Pfad ist vorhanden, die Datenweiterleitung ist jedoch nicht eingerichtet.

5. ARP-bezogene Indikatoren

Bei Bereitstellungen, bei denen sich die VLAN-SVI auf dem WLC befindet:

- Für Clients und AP sind ARP-Einträge vorhanden.
- Client-Datenverkehr schlägt fehl.
- Beim Löschen des ARP wird die Verbindung sofort wiederhergestellt.

Dieses Verhalten bestätigt einen Fehler bei der Weiterleitung auf Datenebene und keine RF- oder CAPWAP-Instabilität.

Obligatorische Protokollerfassung (während des Fehlerfensters)

Phase 0 - Obligatorische Vorbereitung (vor der Veröffentlichung)

WICHTIG: Die nach dem Neustart gesammelten Protokolle sind für die Mesh-RCA nicht ausreichend.

Permanente Fehlersuche auf RAP und MAP aktivieren

Auf RAP

Anschlusslänge 0

Debuggen von Mesh-Ereignissen

debug mesh adjacency child

debug mesh adjacency packet

debug mesh adjacency channel

Debugging Mesh Security

Debug-Mesh-Weiterleitungspaket

debuggen capwap-Clientereignisse

debug capwap client error

Terminalmonitor

Auf KARTE

Anschlusslänge 0

Debuggen von Mesh-Ereignissen

debug mesh adjacency parent

debug mesh adjacency packet

debug mesh adjacency channel

Debugging Mesh Security

debuggen capwap-Clientereignisse

debug capwap client error

Terminalmonitor

Lassen Sie Debug aktiviert, bis sich das Problem reproduziert.

Phase 1 - Protokollerfassung während der Ausgabe (KRITISCH)

Starten Sie APs NICHT NEU, BEVOR Sie PROTOKOLLE SAMMELN

Protokolle von betroffenem MAP (sofort bei Auftreten des Problems)

show mesh status

Mesh-Historie älteste anzeigen

Mesh-Verlauf anzeigen

Flash-Syslogs anzeigen

Weitere Syslog-Informationen <Datum>

Protokolle von RAP (vorheriges und neues übergeordnetes Element)

Mesh-Historie älteste anzeigen

show mesh status

Protokolle von WLC (zur Fehlerzeit)

Drahtlose Mesh-AP-Baumstruktur anzeigen

Wireless Mesh-Nachbarn anzeigen

show ap name <AP-NAME> Mesh-Pfad

show ap name <AP-NAME> allgemeine Konfiguration

Show tech-support wireless

Optional (hoher Wert):

show logging process wncd start last 2 days level verbos

Client- und Datenverkehrskorrelation (empfohlen)

Durchgängige Ping-Befehle während des Fehlerfensters ausführen:

ping -t <Gateway-IP>

Phase 2 - Validierung von HF und Konfiguration (nach der Erfassung)

RF-Validierung (WLC)

show ap dot11 5ghz zusammenfassung

show ap dot11 24ghz zusammenfassung

show ap name <AP> config dot11 5 GHz

show ap name <AP> config dot11 24ghz

ARP-/Weiterleitungs-Validierung (bei Blackholing von Datenverkehr)

Bei auf WLC gehosteter SVI:

Löschen des ARP-Caches

Wenn der Datenverkehr wiederhergestellt wird → trägt die ARP-Verarbeitung dazu bei.

Phase 3 - Stabilisierungsmaßnahmen (validiert)

Mesh-Topologiesteuerung

- Aktivieren Sie ggf. Untergeordnete Elemente auf MAPs blockieren.
- Erzwingen Sie die Verbindung von MAPs mit dem nächsten RAP.
- Reduzierung der Mesh-Hop-Anzahl

RF-Optimierung

- Reduzieren Sie die RAP-Übertragungsleistung.
- Sperren von 5-GHz-Backhaul-Kanälen
- Standardisierung von 2,4-GHz-Kanälen (1/6/11)

Alle genannten Probleme treten bei der Mesh-Bereitstellung nur gelegentlich auf und sind schwer zu beheben. Daher kann die Bereitstellung von Quick Script zur Protokollerfassung die Lösung schneller beschleunigen.

Im Folgenden finden Sie ein EEM-Beispielskript, das auf dem WLC für Probleme bei der Client-Authentifizierung ausgeführt werden kann:

Vollständiges EEM-Skript (Anwendung über WLC CLI)

```
::cisco::eem::event_register_timer watchdog zeit 900 maxrun 240
Namespace-Import::cisco::eem::*
Namespace-Import ::cisco::lib::
# ----------------------------
# Prozess: WLC-Zeitzeichenfolge in Sekunden konvertieren
# Unterstützt: "X Tage Xh:Xm:Xs", "Xh:Xm:Xs", "Xm:Xs", "Xs"
# ----------------------------
proc time_to_seconds {time_str} {
Gesamtsumme festlegen 0
if {[regexp {([0-9]+)\s+days?\s+([0-9]+)\s+h:([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> d h m s]} {
set total [expr {$d*86400 + $h*3600 + $m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+h:([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> h m s]} {
set total [expr {$h*3600 + $m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+m:([0-9]+)\s+s} $time_str -> m s]} {
set total [expr {$m*60 + $s}]
} elseif {[regexp {([0-9]+)\s+s} $time_str -> s]} {
Gesamtbetrag $s
}
Rückerstattung $total
}
# ----------------------------
# Prozess: Protokollieren der gesamten Protokollsammlungsinstanzen (max. 2)
# ----------------------------
proc get_log_count {} {
if {[file exist /bootflash/auth_log_count.txt]} {
set fd [open /bootflash/auth_log_count.txt r]
set count [read $fd]
Geschlossen $fd
Rückgabe von $count
} else {
```

```
Rücklauf 0
}
}
proc set_log_count {count} {
set fd [open /bootflash/auth_log_count.txt w]
spart $fd $count
Geschlossen $fd
}
# ----------------------------
# EEM-Hauptausführung
# ----------------------------
if {[catch {cli_open} result]} {
Ausgang 1
}
array set cli $result
set fd $cli(fd)
cli_exec $fd "enable"
cli_exec $fd "Terminallänge 0"
cli_exec $fd "Klemmenbreite 0"
# Aktuelle Protokollsammlung abrufen
set log_count [get_log_count]
max_log_instance2 festlegen
# Alle Clients im Authentifizierungsstatus abrufen
set summary [cli_exec $fd] "Zusammenfassung des Wireless-Clients anzeigen | Authentifizierung
einschließen"]
set lines [split $summary "\n"]
foreach line $lines
# Übereinstimmung mit MAC-Format xxxx.xxxx.xxxx
if {[regexp {([0-9a-fA-F]{4}\.[0-9a-fA-F]{4}\.[0-9a-fA-F]{4})} $line -> mac]} {
set detail [cli_exec $fd "show wireless client mac-address $mac detail"]

# Zeitzeichenfolge "Connected For" extrahieren
if {[regexp {Connected For[:space:]]*:[:space:]]*(.+)} $detail -> conn_time]} {
Sekunden einstellen [time_to_seconds $conn_time]

# Prüfen, ob er >15 Minuten (900 Sekunden) stecken geblieben ist
if {$seconds > 900} {
action_syslog msg "EEM: Client $mac bei der Authentifizierung für $conn_time (>$seconds
seconds) festgehalten"

# Protokolle nur bei maximaler Instanzgrenze sammeln
if {$log_count < $max_log_instance} {
action_syslog msg "EEM: WLC- + Client-Protokolle werden gesammelt (Instanz [expr {$log_count
+ 1}]/$max_log_instance)"
set log_file "/bootflash/auth_stuck_eem.log"
```

```
set fd_log [open $log_file a]

Anzahl Protokolle pro Client
setzt $fd_log "\n=== [Uhrenformat [Uhrzeitsekunden]] | Client $mac | $conn_time ==="
setzt $fd_log "\n— Client Detail —"
setzt $fd_log $detail
setzt $fd_log "\n— Client-Zusammenfassung —"
put $fd_log [cli_exec $fd] "show wireless client summary | $mac einfügen"]

Anzahl WLC-weite Protokolle
put $fd_log "\n— WLC WNCD Logs (30m) —"
put $fd_log [cli_exec $fd "show logging process wncd start last 30 minutes"]
setzt $fd_log "\n— WLC Show Tech Wireless —"
put $fd_log [cli_exec $fd "show tech wireless"]

$fd_log schließen
set log_count [expr {$log_count + 1}]
set_log_count $log_count
} else {
action_syslog msg "EEM: Die maximale Anzahl an Protokollinstanzen ($max_log_instance) wurde erreicht. Protokollsammlung wird übersprungen."
}

# Immer festsitzenden Client deaktivieren
cli_exec $fd "MAC-Adresse des Wireless-Clients $mac deauthentifizieren"
action_syslog msg "EEM: Deauthentifizierter Client $mac"
}
}
}
}
cli_close $fd
Beenden 0
—
#### Hauptfunktionen des Skripts
1. **15-Minuten-Intervall**: Watchdog-Zeitgeber auf 900 Sekunden (15 Minuten) eingestellt, wie angefordert
2. **Schwellenwert**: Nur bei Clients, die > 15 Minuten (900 Sekunden) hängen geblieben sind
3. **Protokolllimit**: Erfasst WLC + Client-Protokolle für **max. 2 Instanzen** und überspringt anschließend die Protokollerfassung (deauthentifiziert noch Clients)
4. **WLC-Protokollsammlung**: Umfasst:
- Kundenspezifische Details/Zusammenfassung
- WNCD-Prozessprotokolle (30-Minuten-Fenster)
- Vollständige "Show tech wireless"
5. **Permanenter Zähler**: Nachverfolgung von Protokollinstanzen über "/bootflash/auth_log_count.txt" in EEM-Skriptausführungen
```

Bereitstellung und Überprüfung
1. Wendet das Skript auf WLC an:
WLC#-Konfigurationsterminal
WLC(config)# Ereignismanager-Applet AuthStuckHandler
WLC(config-applet)# Ereignis-Timer Überwachungszeit 900
WLC(config-applet)# action 1 cli-Befehl "sh bootflash:auth_stuck_eem.tcl"
WLC(config-applet)# Ende
(Oder fügen Sie das vollständige TCL-Skript direkt in die WLC EEM-Konfiguration ein.)

2. EEM-Registrierung überprüfen:
WLC# Show Event Manager-Richtlinie registriert

3. Sammelprotokolle abrufen:
WLC# copy bootflash:auth_stuck_eem.log ftp:
WLC# copy bootflash:auth_log_count.txt ftp:

4. Setzen Sie den Protokollzähler zurück, um die Erfassung erneut zu aktivieren (falls erforderlich):
WLC# delete bootflash:auth_log_count.txt

Schlussfolgerung

In diesem Dokument werden validierte TAC-Methoden und Fallstudien zusammengeführt, um die dringendsten Probleme mit Mesh-Wi-Fi beim Catalyst 9800 zu lösen: instabiles Backhaul, Clients bleiben im Authentifizierungszustand und der Datenverkehr wird nicht übertragen.

Ein wichtiger Punkt ist, dass 90 % der gemeldeten Netzausfälle nicht isolierte Hardware- oder Client-Fehler sind, sondern Symptome eines nicht übereinstimmenden Status auf Kontroll- und Datenebene, einer instabilen Mesh-Topologie oder eines suboptimalen HF-Designs.

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.