Fehlerbehebung: Trennung des Access Points vom Controller

Inhalt

Einleitung

In diesem Dokument werden Anwendungsfälle beschrieben, die die Ursache für den Tunnelbruch bei Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) zwischen Access Points (APs) und dem Wireless LAN Controller (WLC) verdeutlichen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse der AP- und Controller-Konfiguration verfügen, zusammen mit Grundkenntnissen über Routing und Switching.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Controllerbasierter AP-Registrierungsprozess

Die APs führen den oben genannten Prozess für die Registrierung beim Controller aus:

1. CAPWAP-Erkennungsnachricht-Anfrage an WLC vom AP.
2. Die Erkennungsantwort vom WLC zum AP.
3. Der WAP wählt den WLC aus, dem er beitreten soll, basierend auf der empfangenen

CAPWAP-Antwort.
4. Beitrittsanfrage vom AP an WLC gesendet.
5. Der Controller validiert den Access Point und sendet die Join-Antwort.

Beim Registrieren beim WLC am AP erfasste Protokolle:

Press RETURN to get started! Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

Anwendungsfall 1

1. Die APs werden vom WLC getrennt, und die Switch-Verifizierung zeigt, dass der AP über keine IP-Adresse verfügt.

Protokolle bei Konsolenverbindung mit dem AP:

Lösung:

Beheben Sie die Erreichbarkeitsprobleme der IP-Hilfsadresse, die unter dem VLAN konfiguriert wurde, wenn sich der DHCP-Server entfernt befindet. Wenn DHCP lokal konfiguriert ist, stellen Sie sicher, dass kein DHCP-Konflikt auftritt. Konfigurieren Sie die statische IP auf dem AP:

Melden Sie sich beim AP an, und geben Sie die folgenden Befehle ein:

```
capwap ap ip address <ip> <mask>

capwap ap ip default-gateway <ip>
```

Sie können auch die IP-Adresse des Controllers angeben:

capwap ap controller ip address

2. Beachten Sie, dass es Access Points mit IP-Adressen gibt, dass jedoch bei einer fehlenden Kommunikation mit dem WLC die Behebung von Problemen mit der Controller-IP auftreten kann.

Protokolle vom Access Point mit einem Problem, bei dem die DNS-Auflösung (Domain Name System) fehlschlug:

```
<Date & time>  %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.local doamin

Not in Bound state.
```

Lösung:

Überprüfen Sie die Verfügbarkeit des internen DNS-Servers. Wenn möglich, stellen Sie sicher, dass die über DHCP per Push übermittelten Controller-IP-Adressen erreichbar sind.

Break-fix: Konfigurieren Sie den Controller manuell auf dem AP.

```
"capwap ap {primary-base | secondary-base | tertiary-base}controller-name controller-ip-address"
```

3. Der Access Point ist beim Controller registriert, und es wird immer noch keine Übertragung der

erforderlichen Service Set Identifier (SSID) angezeigt.

```
(4402-d) >config wlan apgroup interface-mapping add <ap group name> <wlandi> <interfacename>
```

Lösung:
Fügen Sie das Wireless LAN (WLAN) der AP-Gruppe hinzu.

Anwendungsfall 2

Beachten Sie, dass der Access Point nicht im benachbarten Cisco Discovery Protocol (CDP) des Switches zu sehen ist und dass sich der mit dem Access Point verbundene Switch in einem fehlerbehafteten Zustand befindet.

Vom Switch erfasste Protokolle:

Dec 9 08:42:35.836 UTC: RSTP(10): sending BPDU out Te3/0/47STP: pak->vlan_id: 10 Dec 9 08:42:35.836 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable stateSTP: pak->vlan_id: 1 Dec 9 09:47:32.651 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD Dec 9 09:47:33.651 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted Dec 9 09:47:53.545 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state Dec 9 09:48:10.955 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD Dec 9 09:48:11.955 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted Dec 9 09:48:32.114 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state

Lösung:
AP sendet unter keinen Umständen den Bridge Protocol Data Unit (BPDU) Guard, da es sich hierbei um ein Problem auf der Switch-Seite handelt. Verschieben Sie den AP auf einen anderen freien Port, und replizieren Sie die Schnittstellenkonfiguration zusammen mit den erforderlichen physischen Prüfungen.

Anwendungsfall 3

Bei der Einrichtung von Außenstellen werden CAPWAP-Tunnel zwischen APs und Controller häufig nach dem Zufallsprinzip zerlegt. Der wichtigste zu überprüfende Parameter sind das Intervall für Neuübertragungen und Wiederholungen.

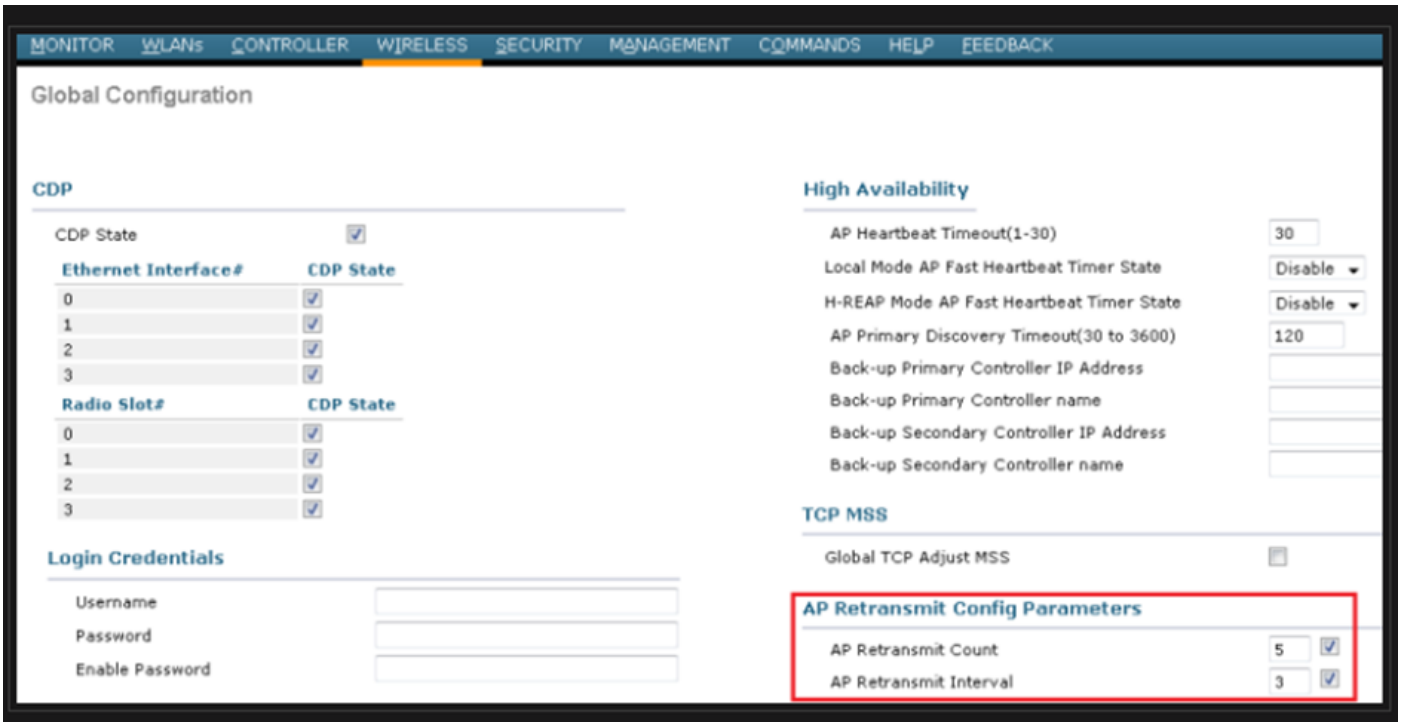
Das Intervall für die erneute Übertragung und das Wiederholungsintervall des Access Points können sowohl auf globaler als auch auf AP-Ebene konfiguriert werden. Eine globale Konfiguration wendet diese Konfigurationsparameter auf alle APs an. Das heißt, das Wiederholungsintervall und die Anzahl der Wiederholungen sind für alle APs gleich.

Problematische Protokolle vom WLC:

*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP Message Timeout. *spamApTask6: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1d:20) event (Capwap_configuration_update_request) and state (Capwap_dtls_teardown) combination -Traceback: 0xe69bba3a5f 0xe69b9b9446 0xe69bdc5e3b 0xe69b8f238c 0xe69bbaf33b 0xe69cc8041b 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d *spamReceiveTask: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1d:20) event (Capwap_configuration_update_request) and state (Capwap_dtls_teardown) combination -Traceback: 0xe69bba3a5f 0xe69b981950 0xe69b76dd5c 0xe69cc757c2 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d *spamApTask5: Jun 01 17:17:55.424: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7521 1c:d1:e0:43:1d:20: DTLS connection closed forAP 10:209:36:5 (5256), Controller: 10:176:92:53 (5246) AP Message Timeout *spamApTask5: Jun 01 17:17:55.423: %CAPWAP-3-

MAX_RETRANSMISSIONS_REACHED: capwap_ac_sm.c:8073 Max retransmissions reached on AP(1c:d1:e0:43:1d:20),message (CAPWAP_CONFIGURATION_UPDATE_REQUEST),number of pending messages(2)

Lösung: Wenn das Problem auf alle Standorte verteilt ist, erhöhen **Retransmit count** und **Retransmit interval** unter "Wireless Global Configuration". Option zum Erhöhen der Werte, wenn das Problem für alle APs vorliegt.



Option zum Ändern der Konfigurationsparameter für die AP-Neuübertragung unter der globalen Konfiguration

Wenn das Problem auf einen Remote-Standort zutrifft, erhöht sich **Retransmit count** und **Retransmit interval** auf einem bestimmten AP behebt das Problem.

Option zum Ändern des Konfigurationsparameters für die erneute Übertragung des Access Points unter einem bestimmten Access Point

Anwendungsfall 4

Der Access Point wird vollständig vom WLC getrennt und kann nicht wieder am Controller angeschlossen werden, da dies mit den digitalen Zertifikaten in Zusammenhang stehen könnte.

Hier einige kurze Fakten zu Gerätezertifikaten in Bezug auf Cisco WLCs und APs:

- Jedes Gerät von Cisco wird standardmäßig mit einem Zertifikat mit einer Gültigkeit von 10 Jahren ausgeliefert.
- Dieses Zertifikat wird für die Authentifizierung zwischen dem Cisco WLC und dem AP verwendet.
- Mithilfe der Zertifikate AP und WLC einen sicheren Datagram Transport Layer Security (DTLS) Tunnel einzurichten.

Es sind zwei Arten von Problemen im Zusammenhang mit Zertifikaten aufgetreten:

Ausgabe 1: Älterer AP (möchte nicht am WLC teilnehmen).

Die Konsole zum Access Point hilft bei der Problemermittlung, und die Protokolle sehen wie folgt aus:

*Sep 13 18:26:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.1 peer_port: 5246 *Sep 13 18:26:24.000: %CAPWAP-5-CHANGED: CAPWAP changed state to *Sep 13 18:26:24.099: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: XXXXXXXXXXXXXX) has expired. Validity period ended on 19:56:24 UTC Aug 12 2018 *Sep 13 18:26:24.099: %LWAPP-3-CLIENTERRORLOG: Peer certificate verification failed *Sep 13 18:26:24.099: %CAPWAP-3-ERRORLOG: Certificate verification failed!

Ausgabe 2: Neuere APs möchten keinem älteren WLC beitreten.
Die Konsole des AP zeigt einen Fehler an, der wie folgt aussehen könnte:

[*09/09/2019 04:55:26.3299] CAPWAP State: DTLS Teardown [*09/09/2019 04:55:30.9385] CAPWAP State: Discovery [*09/09/2019 04:55:30.9385] Did not get log server settings from DHCP. [*09/09/2019 04:55:41.0000] CAPWAP State: DTLS Setup [*09/09/2019 04:55:41.3399] Bad certificate alert received from peer. [*09/09/2019 04:55:41.3399] DTLS: Received packet caused DTLS to close connection

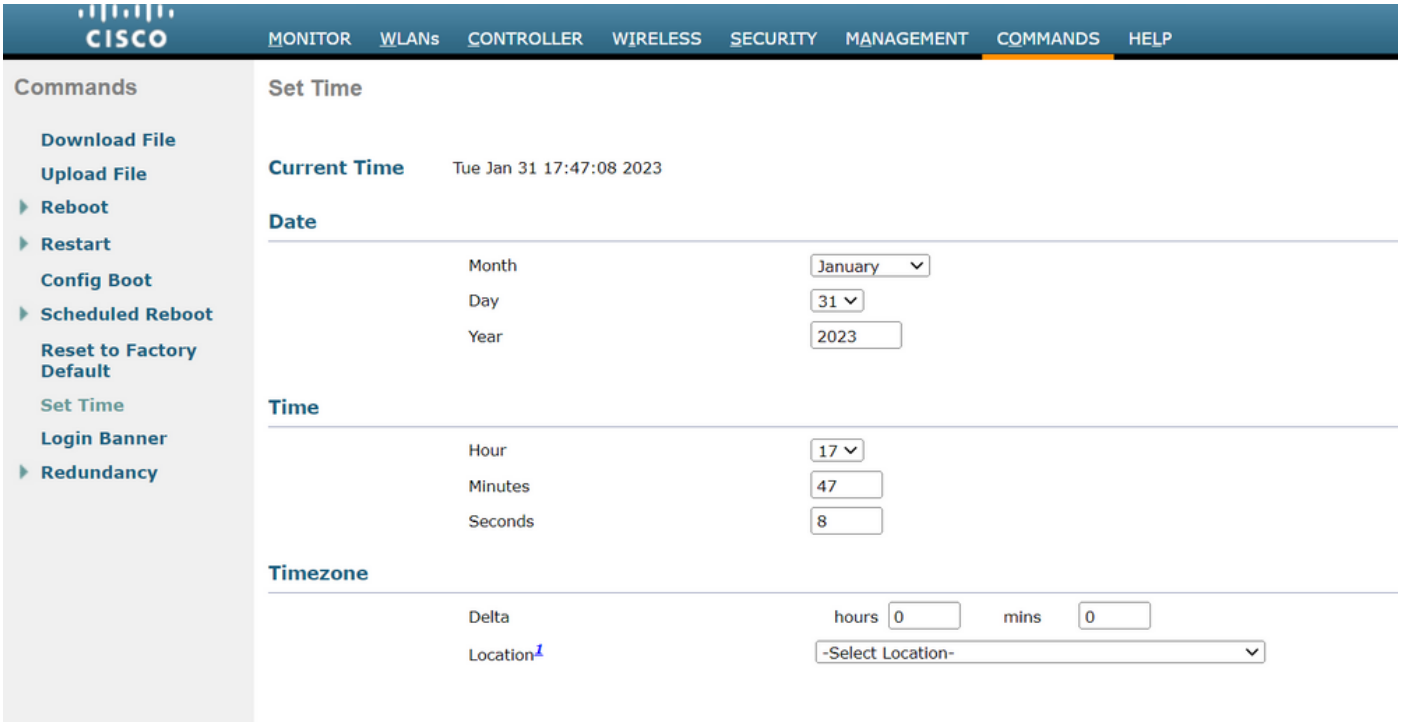
Lösung:

1. NTP deaktiviert die Uhrzeit und legt sie manuell über die CLI fest:

(Cisco Controller)> config time ntp delete 1 (Cisco Controller)> config time manual 09/30/18 11:30:00

2. NTP deaktiviert die Uhrzeit und legt sie manuell über die GUI fest:

Navigieren Sie zu **Controller > NTP > Server > Commands > Set Time** um die aufgelisteten NTP-Server zu entfernen.



Ort, an dem die Zeit manuell über die GUI eingestellt werden soll

2. Deaktivieren Sie das vom Hersteller installierte Zertifikat (MIC) auf dem Controller. Dieser Befehl wird nur für die neuesten Versionen akzeptiert.

```
(Cisco Controller)> config ap cert-expiry-ignore mic enable
```

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.