Probleemoplossing voor ontkoppeling van access point van controller

Inhoud

Inleiding

Dit document beschrijft gebruikscases om de reden te begrijpen voor de tunnelonderbreking van het Control and Provisioning of Wireless Access points (CAPWAP)/Lichtgewicht Access Point Protocol (LWAP) tussen access points en de draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de configuratie van AP en controllers, samen met basiskennis van Routing en Switching.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Op controller gebaseerde AP-registratieproces

De AP's gaan door het genoemde proces om zich te registreren bij de controller:

1. CAPWAP detectiebericht verzoek aan WLC van AP.
2. Het bericht van de ontdekkingsreactie van WLC aan AP.
3. AP kiest de WLC om mee te doen op basis van de ontvangen CAPWAP-respons.
4. Doe mee aan Verzoek dat naar WLC van AP wordt verzonden.

5. De controller valideert het toegangspunt en verstuurt het antwoord.

Logbestanden die op AP zijn opgenomen wanneer geregistreerd met WLC:

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

Use Case 1

1. AP's worden losgekoppeld van WLC en wanneer geverifieerd van de switch, toont het aan dat AP geen IP heeft.

Logbestanden bij configuratie op het toegangspunt:

Oplossing:

Werk om de bereikbaarheidsproblemen te verhelpen met het IP-helperadres dat onder het VLAN is geconfigureerd als de DHCP-server op afstand is geïnstalleerd. Als de DHCP lokaal is geconfigureerd, zorg dan dat er geen DHCP-conflict is. Statische IP op het toegangspunt configureren:

Log in op het toegangspunt en typ deze opdrachten:

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

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

U kunt ook het IP-adres van de controller opgeven:

```
capwap ap controller ip address
```

2. Het bericht dat er APs met IP adressen zijn, maar het nalaten om met WLC te communiceren zou een resolutiemislukking kunnen zijn om IP te controleren.

Logbestanden vanaf AP met een probleem waarbij de DNS-resolutie (Domain Name System) is mislukt:

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

Not in Bound state.
```

Oplossing:

Controleer de interne bereikbaarheid van DNS-server, indien acceptabel, en zorg ervoor dat controller IP-adressen die via DHCP worden gedrukt bereikbaar zijn.

Break-fix: de controller handmatig configureren op het toegangspunt.

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

3. U ziet dat AP is geregistreerd op de controller en dat er nog steeds geen uitzending is van de vereiste Service Set Identifier (SSID).

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

Oplossing:
Voeg het draadloze LAN (WLAN) toe onder de AP-groep.

Use Case 2

Het bericht dat AP niet wordt gezien op de buur van Cisco Discovery Protocol (CDP) van de switch en dat de met AP verbonden switch zich in een staat bevindt die door een fout is uitgeschakeld.

Logbestanden die door de Switch zijn opgenomen:

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

Oplossing:
AP stuurt onder geen beding de Bridge Protocol Data Unit (BPDU) bewaker, dit is een probleem aan de kant van de switch. Verplaats de AP naar een andere vrije poort en repliceer de interfaceconfiguratie samen met de benodigde fysieke controles.

Use Case 3

Bij het instellen van externe kantoren, ziet u vaak dat de CAPWAP-tunneltraan willekeurig wordt neergehaald tussen AP's en controller en de belangrijkste te controleren parameter is opnieuw verzenden en opnieuw proberen interval.

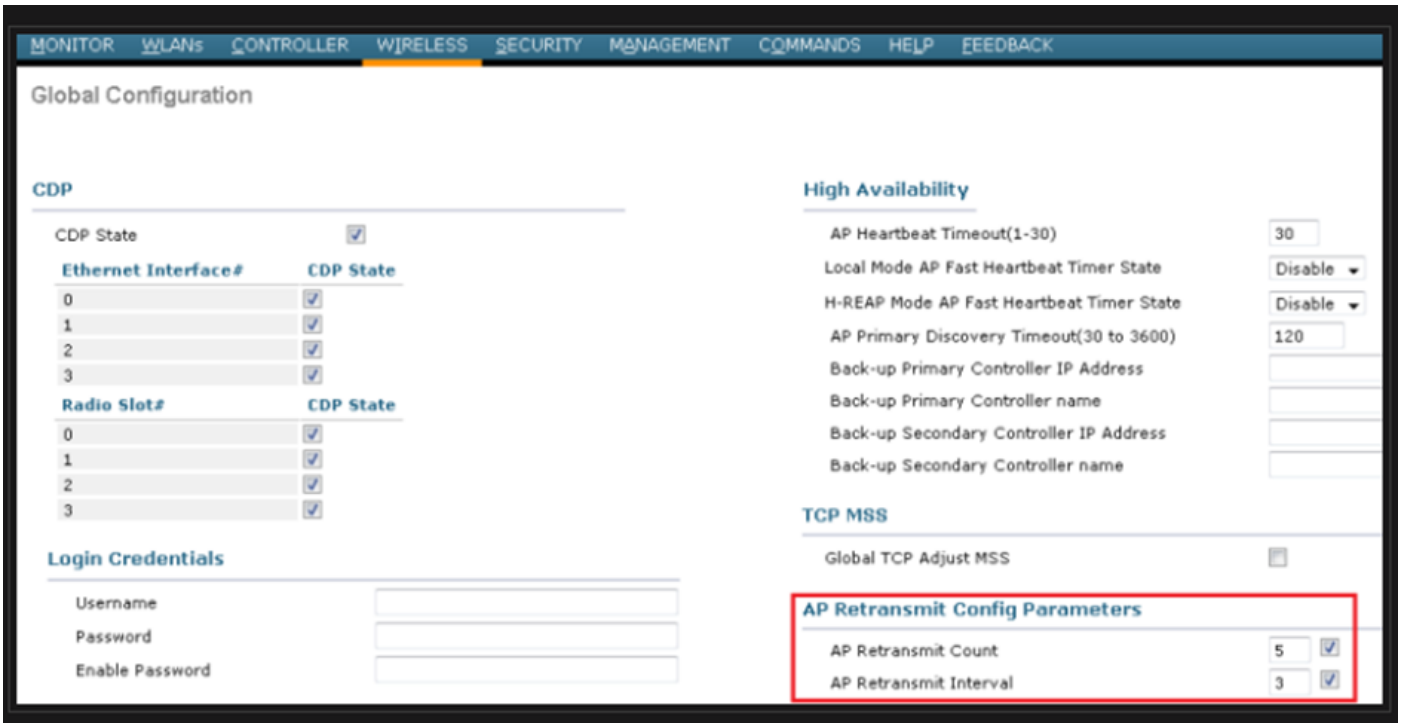
AP herzend interval en herprobeer interval kan worden geconfigureerd zowel op globaal niveau als op het AP niveau. Een globale configuratie past deze configuratieparameters op alle APs toe. Dat wil zeggen dat het interval voor de hertransmissie en de telling van de herhalingen voor alle AP's gelijk zijn.

Problematische logs van 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)

Oplossing: Als het probleem zich op alle sites voordoet, verhoog dan de **Retransmit count** en

Retransmit interval onder wereldwijde draadloze configuratie. Optie om de waarden te verhogen wanneer het probleem zich voordoet bij alle toegangspunten.



Optie om de parameters voor het opnieuw verzenden van AP te wijzigen onder Globale configuratie

Als het probleem specifiek is voor één externe site, neemt de **Retransmit count** en **Retransmit interval** op een bepaalde AP lost het probleem op.

Optie om AP opnieuw te verzenden configuratieparameter onder een specifieke APs te veranderen

Use Case 4

De AP wordt volledig losgekoppeld van de WLC en is niet in staat om de controller weer te verenigen, dit zou gerelateerd kunnen zijn aan de digitale certificaten.

Een aantal snelle feiten over apparaatcertificaten in termen van Cisco WLC's en AP's:

- Elk apparaat dat uit Cisco komt wordt standaard geleverd met een certificaat met een geldigheid van 10 jaar.
- Dit certificaat wordt gebruikt voor het uitvoeren van verificatie tussen Cisco WLC en AP.

- Met behulp van certificaten zetten AP en WLC een beveiligde Datagram Transport Layer Security (DTLS) tunnel op.

Er zijn twee soorten problemen met certificaten ondervonden:

Probleem 1: Oudere AP (wil niet toetreden tot WLC).

De console naar het toegangspunt helpt het probleem te bepalen en de logbestanden zien er als volgt uit:

*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: XXXXXXXXXXXXX) 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!

Probleem 2: Nieuwe AP wil niet toetreden tot een oudere WLC.
De console aan AP geeft een fout die als dit zou kunnen kijken:

[*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

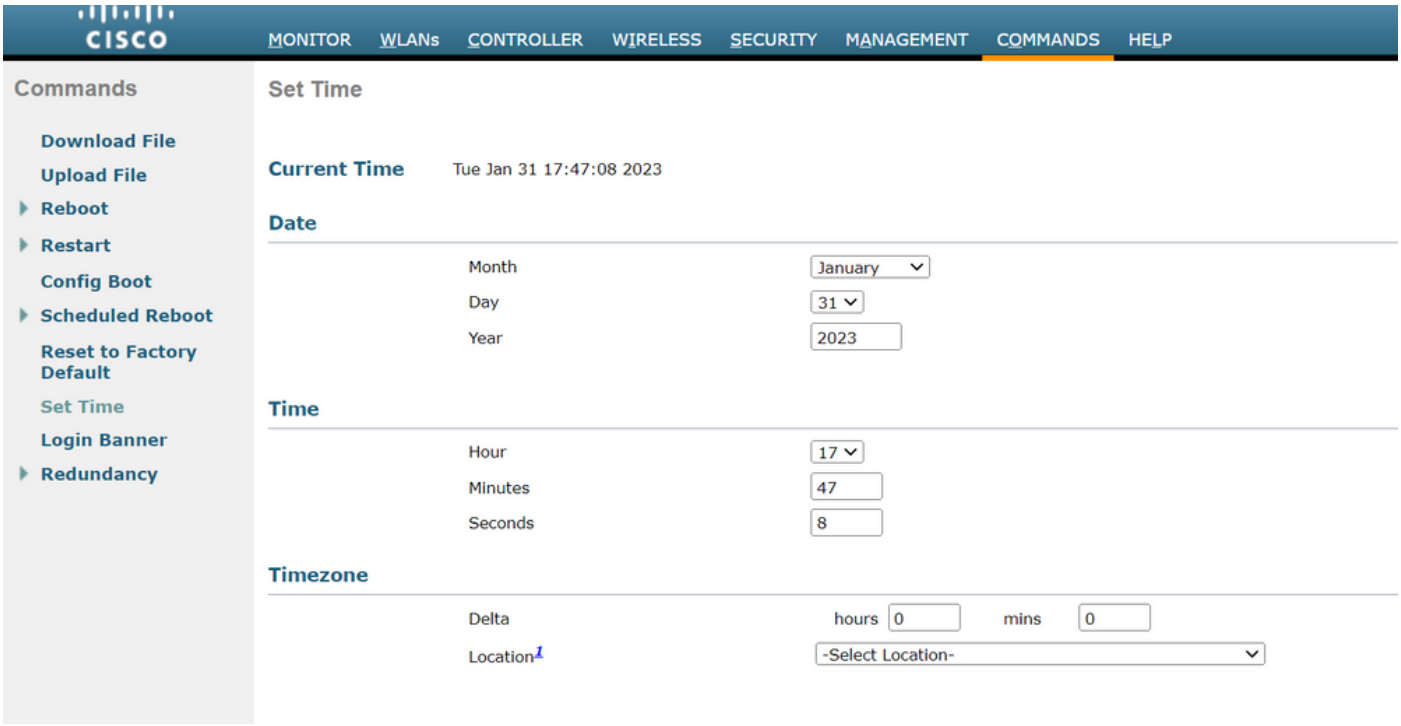
Oplossing:

1. NTP schakelt de tijd handmatig in en stelt deze in via CLI:

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

2. NTP schakelt de tijd handmatig uit en stelt deze in via GUI:

Naar navigeren **Controller > NTP > Server > Commands > Set Time** om de genoemde NTP-servers te verwijderen.



Plaats om tijd handmatig in te stellen op de GUI

2. Schakel het door de fabrikant geïnstalleerde certificaat (MIC) op de controller uit. Deze opdracht wordt alleen geaccepteerd op de nieuwste versies.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.