Lokale EAP-verificatie op Catalyst 9800 WLC configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram Belangrijkste lokale EAP-configuratie Stap 1. Lokaal EAP-profiel Stap 2. AAA-verificatiemethode Stap 3. Een AAA-autorisatiemethode configureren Stap 4. Lokale geavanceerde methoden configureren Stap 5. WLANâ€[™]s configureren Stap 6. Een of meer gebruikers maken Stap 7. Beleidsprofiel maken Beleidstag maken om dit WLAN-profiel toe te wijzen aan een beleidsprofiel Stap 8. Stel de beleidstag in op Access points. Verifiëren Problemen oplossen Voorbeeld van een client die geen verbinding kan maken vanwege een verkeerd wachtwoord Overtrekken van fouten

Inleiding

Dit document beschrijft de configuratie van Local EAP op Catalyst 9800 WLC's (draadloze LANcontrollers).

Voorwaarden

Vereisten

Dit document beschrijft de configuratie van Local EAP (Extensible Verification Protocol) op Catalyst 9800 WLC's; dat wil zeggen, de WLC presteert als RADIUS-verificatieserver voor de draadloze clients.

In dit document wordt ervan uitgegaan dat u bekend bent met de basisconfiguratie van een WLAN op de 9800 WLC en dat u zich alleen richt op de WLC die als Local EAP-server voor draadloze clients werkt.

Gebruikte componenten

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.

Catalyst 9800 op versie 16.12.1s

Configureren

Netwerkdiagram



Belangrijkste lokale EAP-configuratie

Stap 1. Lokaal EAP-profiel

Ga naar **Configuratie > Beveiliging > Lokaal EAP** in de 9800 web UI.

| Configuration - > | Security - > Local EAP |
|--------------------|------------------------|
| Local EAP Profiles | EAP-FAST Parameters |
| + Add | × Delete |

Selecteer Toevoegen

Voer een profielnaam in.

Het gebruik van LEAP wordt afgeraden vanwege de zwakke beveiliging. Om het even welke andere 3 methodes EAP vereist u om een trustpoint te vormen. Dit komt doordat de 9800, die als authenticator fungeert, een certificaat moet versturen voor de klant om het te vertrouwen.

Clients vertrouwen het WLC-standaardcertificaat niet, zodat u de validatie van servercertificaten aan de clientzijde zou moeten deactiveren (niet geadviseerd) of een certificaat trustpoint op de 9800 WLC installeren dat de client vertrouwt (of handmatig importeren in de client trust store).

| Create Local EAP Profiles | | × |
|---------------------------|------------|-----------------|
| Profile Name* | mylocaleap |] |
| LEAP | | |
| EAP-FAST | | |
| EAP-TLS | | |
| PEAP | | |
| Trustpoint Name | admincert | , |
| Cancel | | Apply to Device |
| | | |

```
CLI:
```

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

Stap 2. AAA-verificatiemethode

U moet een AAA dot1x-methode configureren die lokaal aanwijst om de lokale database van gebruikers te kunnen gebruiken (maar u kunt bijvoorbeeld externe LDAP-lookup gebruiken).

Ga naar **Configuration > Security > AAA** en ga naar het tabblad **AAA-methodelijst** voor **verificatie**. Selecteer **Toevoegen**.

Kies het type "dot1x" en het type lokale groep.

| AAA Witzend Servers / Groups AAA Method List AAA Method List Address Authoritation Authoritation | Configuration - > Security - > AAA | | | | | |
|---|------------------------------------|------------------|----------------|--------------------------------|----------|----------|
| Servers / Groups AAA Method List AAA Advanced Authonication Authorization + Add × Delete | + AAA Wizard | | | | | |
| Authorization + Add × Delete | Servers / Groups AAA Method Li | ist AAA Advanced | | | | |
| Authorization + Add × Delete | Authentication | | | | | |
| The second | Authorization | + Add × Delete | + Add X Delete | | | |
| Accounting Name v Type v Group Type v Group 1 v Group 2 | Accounting | Namo | v Type | Group Type | < Group1 | < Group2 |
| default dot1x local N/A N/A | | default | dot1x | local | N/A. | N/A |
| H < 1 > H 10 v Items per page | | H 4 1 H H 10 T | items per page | | | |



Ga naar het subtabblad **Autorisatie** en maak een nieuwe methode voor het **downloaden van referenties** en wijs het naar lokaal.

Doe hetzelfde voor het type netwerkautorisatie

CLI:

```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

Stap 4. Lokale geavanceerde methoden configureren

Ga naar het tabblad Geavanceerd van AAA.

Bepaal de lokale verificatie- en autorisatiemethode. Aangezien dit voorbeeld de "standaard" credentialdownload en "Default" dot1x methode gebruikte, moet u standaard instellen voor zowel lokale authenticatie en autorisatie drop-down boxen hier.

Als u benoemde methoden hebt gedefinieerd, kiest u "methodelijst" in de vervolgkeuzelijst en kunt u in een ander veld uw methodsnaam invoeren.

Configuration -> Security -> AAA + AAA Wizard Servers / Groups AAA Method List AAA Advanced **Global Config** Local Authentication **RADIUS Fallback** Local Authorization Attribute List Name Radius Server Load Balance **Device Authentication** Interim Update AP Policy Show Advanced Settings >>> Password Policy AAA Interface

Stap 5. WLAN's configureren

U kunt vervolgens uw WLAN voor 802.1x-beveiliging configureren met behulp van het lokale EAP-profiel en de AAA-verificatiemethode die in de vorige stap zijn gedefinieerd.

Ga naar Configuratie > Tags en profielen > WLANâ€TMs > + Add >

Geef SSID en profielnaam op.

Dot1x-beveiliging is standaard geselecteerd onder Layer 2.

Selecteer onder AAA lokale EAP-verificatie en kies in de vervolgkeuzelijst Local EAP-profiel en AAA-verificatielijst.

| Edit WLA | N | | | | |
|------------|-------------|-----------|-------------------|-----------------------|------------------|
| General | Security | Advanced | | | |
| Layer | Layer3 | AAA | | | |
| Layer 2 Se | curity Mode | | WPA + WPA2 🔻 | Fast Transition | Adaptive Enabled |
| MAC Filter | ing | | | Over the DS | |
| Protecte | d Manageme | ent Frame | | Reassociation Timeout | 20 |
| | | | Dischlard | MPSK Configuration | |
| PMF | | | Disabled v | MPSK | |
| WPA Par | ameters | | | | |
| | | | | | |
| WPA Polic | У | | | | |
| WPA2 Poli | су | | | | |
| WPA2 Enc | ryption | | AES(CCMP128) | | |
| | | | CCMP256 | | |
| | | | GCMP128 | | |
| | | | GCMP256 | | |
| Auth Key M | /lgmt | | ✓ 802.1x | | |
| | | | PSK | | |
| | | | CCKM | | |
| | | | FT + 802.1x | | |
| | | | FT + PSK | | |
| | | | 802.1x-SHA256 | | |
| | | | PSK-SHA256 | | |

16.12 en eerdere releases alleen TLS 1.0 ondersteunen voor lokale e-mailverificatie, wat problemen zou kunnen opleveren als uw client alleen TLS 1.2 ondersteunt, zoals steeds meer de norm is. Cisco IOS® XE 17.1 en hoger ondersteunen TLS 1.2 en TLS 1.0.

Gebruik RadioActive Tracing om problemen op te lossen bij een specifieke client die problemen heeft met het verbinden. Ga naar **Problemen oplossen > RadioActive Trace** en voeg het mac-adres van de client toe.

Selecteer Start om de overtrek voor die client in te schakelen.

| Troubleshooting - > Radioactive Trace | | | |
|---|---------------------------------|--|--|
| Conditional Debug Global State: Started | | | |
| + Add × Delete Start Start | | | |
| MAC/IP Address | Trace file | | |
| e836.171f.a162 | debugTrace_e836.171f.a162.txt 📥 | | |
| I I I I I I I I I I I I I I I I I I I | | | |

Nadat het probleem is gereproduceerd, kunt u de knop **Generate** selecteren om een bestand te maken dat de debugging-uitvoer bevat.

Voorbeeld van een client die geen verbinding kan maken vanwege een verkeerd wachtwoord

| 2019/10/30 | 14:54:00.781 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Ser</pre> |
|------------|--------------|-------------------|--|
| 2019/10/30 | 14:54:00.781 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF</pre> |
| 2019/10/30 | 14:54:00.784 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec |
| 2019/10/30 | 14:54:00.784 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.785 | {wncd_x_R0-0}{2}: | [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: |
| 2019/10/30 | 14:54:00.788 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Ser</pre> |
| 2019/10/30 | 14:54:00.788 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF</pre> |
| 2019/10/30 | 14:54:00.791 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec</pre> |
| 2019/10/30 | 14:54:00.791 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF</pre> |
| 2019/10/30 | 14:54:00.791 | {wncd_x_R0-0}{2}: | <pre>[caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG:</pre> |
| 2019/10/30 | 14:54:00.792 | {wncd_x_R0-0}{2}: | <pre>[dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Ser</pre> |
| 2019/10/30 | 14:54:00.792 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.795 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec |
| 2019/10/30 | 14:54:00.795 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.795 | {wncd_x_R0-0}{2}: | [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: |
| 2019/10/30 | 14:54:00.796 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Ser |
| 2019/10/30 | 14:54:00.796 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.804 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec |
| 2019/10/30 | 14:54:00.804 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.804 | {wncd_x_R0-0}{2}: | [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: |
| 2019/10/30 | 14:54:00.805 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Ser |
| 2019/10/30 | 14:54:00.805 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.808 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec |
| 2019/10/30 | 14:54:00.808 | {wncd_x_R0-0}{2}: | [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAF |
| 2019/10/30 | 14:54:00.808 | {wncd_x_R0-0}{2}: | [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: |
| | | | |

```
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAP\
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_9000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_9000004] Rece
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_9000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:6600006] DEBUG: m
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): FAIL for EAP method name: EAP-FAST
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rais
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [cerrmsg] [23294]: (info): [e836.171f.a162:capwap_90000004] Rais
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

Overtrekken van fouten

Het is mogelijk om de lijst van mislukkingsgebeurtenissen voor een bepaald mac-adres met de opdracht trace-on-failure te controleren, zelfs wanneer geen debugs zijn ingeschakeld.

In het volgende voorbeeld was de AAA-methode eerst afwezig (AAA-server down-gebeurtenis) en vervolgens gebruikte de client een paar minuten later verkeerde referenties.

De opdracht is **show logging trace-on-fail samenvatting** in release 16.12 en eerder en is **show logging profiel wireless (filter mac <mac>) trace-on-failure** in Cisco IOS® XE 17.1 en hoger. Er is geen technisch verschil, behalve dat 17.1 en later laat u filteren voor het client mac-adres.

Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds executing cmd on chassis 2 ... sending cmd to chassis 1 ... Collecting files on current[1] chassis. # of files collected = 30 Collecting files on current[2] chassis. # of files collected = 30 Collecting files from chassis 1. Time UUID Log

2019/10/3014:51:04.4380x0SANET_AUTHC_FAILURE - AAA Server Down username , audit session id (
e836.171f.a162CLIENT_STAGE_TIMEOUTState = AUTHENTICATING, WLAN provide

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.