9800 WLCでのLWAに関する一般的な問題のト ラブルシューティング

内容
<u>はじめに</u>
前提条件
要件
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>9800 WLCでの放射性(RA)トレース</u>
<u>予想されるフロー</u>
<u>クライアント側から見たクライアントのステージ</u>
<u>WLCの観点からクライアントが受けるステージ</u>
<u>一般的なトラブルシューティングのシナリオ</u>
Authentication failures
<u>ポータルはユーザには表示されないが、クライアントは接続されているように見える</u>
ポータルがユーザに表示されず、クライアントが接続しない
<u>エンドクライアントがIPアドレスを取得していない</u>
<u>カスタマイズされたポータルがエンドクライアントに表示されない</u>
<u>カスタマイズされたポータルがエンドクライアントに正しく表示されない</u>
ポータルに「Your connection is not secure/verify signature failed」と表示される
<u>関連情報</u>

はじめに

このドキュメントでは、ローカルWeb認証(LWA)を使用してWLANに接続するクライアントに関する一般的な問題について説明します。

前提条件

要件

次の項目に関する基本的な知識があることが推奨されます。

- ・ Cisco Wireless LAN Controller(WLC)9800シリーズ
- ・ ローカルWeb認証(LWA)とその設定に関する一般的な知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 9800-CL WLC
- ・ Ciscoアクセスポイント9120AXI
- ・ 9800 WLC Cisco IOS® XEバージョン17.9.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

LWAは、接続を試みるエンドクライアントがリストからWLANを選択した後、ユーザにポータル を提供するWLCで設定できるWLAN認証のタイプです。このポータルでは、ユーザは(選択した 設定に応じて)ユーザ名とパスワードを入力して、WLANへの接続を終了できます。

9800 WLCでLWAを設定する方法の詳細については、『<u>ローカルWeb認証の設定</u>』設定ガイドを 参照してください。

9800 WLCでの放射性(RA)トレース

放射性トレースは、WLCおよびクライアント接続に関するさまざまな問題のトラブルシューティ ングを行う際に使用できる、優れたトラブルシューティングツールです。RAトレースを収集する には、次の手順を実行します。

GUIで次の手順を実行します。

- 1. Troubleshooting > Radioactive Traceの順に進みます。
- 2. Startをクリックして、Conditional Debug Global Stateを有効にします。
- 3. +追加をクリックします。ポップアップウィンドウが開きます。クライアントのMACアドレ スを入力します。任意のMACアドレス形式(aabb.ccdd.eeff、AABB.CCDD.EEEE、 aa:bb:cc:dd:ee:ff、またはAA:BB:CC:DD:EE:FF)を使用できます。次に、Apply to Deviceを クリックします。
- 4. クライアントに問題を3回または4回再現させます。
- 5. 問題が再現されたら、Generateをクリックします。
- 6. 新しいポップアップウィンドウが開きます。過去10分間のログを生成します。(この場合 、内部ログを有効にする必要はありません)。Apply to Deviceをクリックし、ファイルが処 理されるまで待ちます。
- 7. ファイルが生成されたら、Downloadアイコンをクリックします。

Troubleshooting * > Radioactive Trace	
Conditional Debug Global State Started	
+ Add X Delete Start Stor	
MAC/IP Address T Trace file	
H 4 0 > H 10 ¥	No items to display

条件付きデバッグの有効化

Troublesh	ooting * > Radioactiv	e Trace			
Conditio	nal Debug Global State	: Started			
+ Add	× Delete	🛩 Start 🛛 🔳 Stop	Add MAC/IP Address		×
	MAC/IP Address	Trace	file MAC/IP Address*	Enter a MAC/IP Address every newline	
H H	0 ⇒ ∺ 10 •			3333.3353.3553	
			D Cancel		Apply to Device

クライアントのMACアドレスを追加する

Conditional Debug Global State: Started Enter time interval	ж
Add X Delute V Start Stop Enable Internal Logs Generate logs for last (a) 10 minutes MAC/P Address Trace fee	
assa assa assa O minutes	
N 1 of 1 tems 0 1 hour	
⊖ since last boot	
O 4294967295	seconds v
Cancel	Apply to Device

過去10分間のログの生成

Troublesho	ooting * > Radioactive Trace				
Condition	nal Debug Global State: Started				
+ Add	X Delete	Stop		Status ()	
	MAC/IP Address	Trace file		State	Logs generation in progress
0	8888.8888.8888	\diamondsuit Logs are being generated. Please wait till it completes	► Generate	MAC/IP Address	8888.8888.8888
14	1 > ≥ 10 ¥		1 - 1 of 1 items	Start Time	04/12/2024 17:46:16
				End Time	

Condition	nal Debug Global State: Started				
+ Add	× Delete 🗸 Start	Stop		Last Run Result	
	MAC/IP Address	Trace file		✓ State	Successful
0	3333.3333.3333	debugTrace_aaaa.aaaa.aaaa.txt 📥 🎦	► Generate		See Details
$H \rightarrow 0$	1 F H 10 V		1 - 1 of 1 items	MAC/IP Address	8888.8888.8888
				Start Time	04/12/2024 17:46:16
				End Time	04/12/2024 17:46:17
				Trace file	debugTrace_aaaa.aaaa.aaaa.txt 📥

生成されるのを待つファイルをダウンロードする

CLIから、

Troubleshooting * > Radioactive Trace

<#root>

WLC# debug wireless mac

<mac-address>

monitor-time 600

ブートフラッシュにra_trace_MAC_<macaddress>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.logという名前の新しいファイル が生成されます。

<#root>

WLC# more bootflash:

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

分析のためにファイルを外部サーバにコピーする

<#root>

WLC# copy bootflash:

ra_trace_MAC_<mac-address>_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

ftp://username:password@<ftp-server-ip>/path/RATRACE_FILENAME.txt

放射性トレースの詳細については、<u>このリンク</u>を参照してください<u>。</u>

予想されるフロー

LWAの動作シナリオについては、この情報を参照してください。

クライアント側から見たクライアントのステージ

- 1. エンドクライアントがWLANに関連付けられます。
- 2. クライアントがIPアドレスを割り当てられる。
- 3. ポータルがエンドクライアントに表示されます。
- 4. エンドクライアントがログインクレデンシャルを入力します。
- 5. エンドクライアントが認証されます。
- 6. エンドクライアントがインターネットをブラウズできる。

WLCの観点からクライアントが受けるステージ



注意:わかりやすくするために、無線アクティブ(RA)トレースの多くのログが省略されています。

エンドクライアントがWLANに関連付けられている

<#root>

MAC: aaaa.bbbb.cccc

Association received

. BSSID d4e8.801a.3063, WLAN LWA-SSID, Slot 0 AP d4e8.801a.3060, APD4E8.8019.608C, old BSSID d4e8.801a. MAC: aaaa.bbbb.cccc Received Dot11 association request. Processing started,SSID: LWA-SSID, Policy profi MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS MAC: aaaa.bbbb.cccc Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type MAC: aaaa.bbbb.cccc WiFi direct: Dot11 validate P2P IE. P2P IE not present. MAC: aaaa.bbbb.cccc dot11 send association response. Framing association response with resp_status_code MAC: aaaa.bbbb.cccc Dot11 Capability info byte1 1, byte2: 14 MAC: aaaa.bbbb.cccc WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled MAC: aaaa.bbbb.cccc Clearing old call info. MAC: aaaa.bbbb.cccc dot11 send association response. Sending assoc response of length: 161 with resp_st MAC: aaaa.bbbb.cccc

Association success.

AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False MAC: aaaa.bbbb.cccc DOT11 state transition: S_DOT11_ASSOCIATED -> S_DOT11_ASSOCIATED

L2認証

<#root>

MAC: aaaa.bbbb.cccc Starting L2 authentication. Bssid in state machine:d4e8.801a.3063 Bssid in request MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_L2_AUTH_IN_PROGRESS MAC: aaaa.bbbb.cccc L2 Authentication initiated. method WEBAUTH, Policy VLAN 0, AAA override = 1 [aaaa.bbbb.cccc:capwap_90400002] -

authc_list: forwebauth

[aaaa.bbbb.cccc:capwap_90400002] - authz_list: Not present under wlan configuration MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUT MAC: aaaa.bbbb.cccc

L2 Authentication of station is successful.

, L3 Authentication : 1

クライアントがIPアドレスを割り当てられる

<#root>

MAC: aaaa.bbbb.cccc Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE -> S_IPLEARN_COMPLETE MAC: aaaa.bbbb.cccc

Received ip learn response. method: IPLEARN_METHOD_DHCP

L3認証

<#root>

MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS MAC: aaaa.bbbb.cccc

L3 Authentication initiated. LWA

MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH

クライアントがIPアドレスを取得する

<#root>

RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.fff s TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.fff s RX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y TX: DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y MAC: aaaa.bbbb.cccc IP-learn state transition: S_IPLEARN_COMPLETE ->

S_IPLEARN_COMPLETE

ポータル処理

<#root>

[aaaa.bbbb.cccc] [X.X.X.X] capwap_90400002

HTTP GET request

[aaaa.bbbb.cccc] [X.X.X.X] capwap_90400002

Parse GET, src [X.X.X.X] dst [Z.Z.Z.Z] url [http://connectivitycheck.gstatic.com/generate_204]

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 8 [aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map [aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

State GET_REDIRECT -> GET_REDIRECT

[...]

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

GET rcvd when in GET_REDIRECT state

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
HTTP GET request
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
Parse GET, src [X.X.X.X] dst [192.0.2.1] url [https://<virtual-ip-address>:443/login.html?redirect=http:
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 10
```

[aaaa.bbbb.cccc] [X.X.X.X] capwap_90400002

Param-map used: lwa-parameter_map

[aaaa.bbbb.cccc] [X.X.X.X] capwap_90400002

State GET_REDIRECT -> LOGIN

[aaaa.bbbb.cccc] [X.X.X.X] capwap_90400002

Sending Webauth login form

, len 8076
[...]
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

POST rcvd when in LOGIN state

```
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 get url: /login.html
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Read complete: parse_request return 4
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 45876/176 IO state READING -> AUTHENTICATING
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map
[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002
```

```
State AUTHENTICATING -> AUTHC_SUCCESS
```

WLCが接続エンドクライアントに適用される情報を処理する

<#root>

[aaaa.bbbb.cccc:capwap_90400002]

Authc success from WebAuth, Auth event success

[aaaa.bbbb.cccc:capwap_90400002] Raised event

APPLY_USER_PROFILE

(14)

```
[aaaa.bbbb.cccc:capwap_90400002] Raised event RX_METHOD_AUTHC_SUCCESS (3)
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
[aaaa.bbbb.cccc:capwap_90400002] SM will not send event Template Deactivated to PRE for 0xAE000012
```

Authentication Success.

Resolved Policy bitmap:4 for client aaaa.bbbb.cccc

```
Applying Attribute :
username 0 "cisco"
Applying Attribute : aaa-author-type 0 1 (0x1)
Applying Attribute : aaa-author-service 0 16 (0x10)
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : addr 0 0xac104206
Applying Attribute : addrv6 0 "p€"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : addrv6 0 " ?Ì??"
Applying Attribute : target-scope 0 0 [client]
Applying Attribute : audit-session-id 0 "1A4210AC0000001C5B12A51C"
Applying Attribute : aaa-unique-id 0 28 (0x1c)
Applying Attribute : client-iif-id 0 4261415483 (0xfe000a3b)
Applying Attribute :
vlan-id 0 100 (0xa63)
Applying Attribute : session-linksec-secured 0 False
Applying Attribute : nas-ip-address 0 0x0
Applying Attribute : nas-ipv6-Address 0 ""
Applying Attribute : interface 0 ""
Applying Attribute : port-type 0 19 [802.11 wireless]
Applying Attribute : nas-port 0 10014 (0x40eba)
Applying Attribute :
cisco-wlan-ssid 0 "LWA-SSID"
Applying Attribute :
wlan-profile-name 0 "LWA-SSID"
Applying Attribute : dnis 0 "d4-e8-80-1a-30-60:LWA-SSID"
Applying Attribute : formatted-clid 0 "3a-e6-3b-9a-fc-4a"
Applying Attribute : bsn-wlan-id 0 16 (0x10)
Applying Attribute : nas-identifier-wireless 0 "LWA-SSID"
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute : priv-lvl 0 1 (0x1)
Applying Attribute : timeout 0 86400 (0x15180)
Applying Attribute :
method 0 1 [webauth]
Applying Attribute : clid-mac-addr 0 3a e6 3b 9a fc 4a
Applying Attribute : intf-id 0 2420113410 (0x90400002)
[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr username(45
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute
Add/Update username cisco
[aaaa.bbbb.cccc:capwap_90400002]
```

Received User-Name cisco for client aaaa.bbbb.cccc

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr auth-domain [aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Success' [aaaa.bbbb.cccc:capwap_90400002] Context changing state from 'Running' to 'Authc Success' [aaaa.bbbb.cccc:capwap_90400002]

Username cisco received

[aaaa.bbbb.cccc:capwap_90400002]

WLAN ID 16 received

WLCが接続されたエンドクライアントにユーザプロファイルを適用する

<#root>

```
Applied User Profile: aaa-author-type 0 1 (0x1)
Applied User Profile: aaa-author-service 0 16 (0x10)
Applied User Profile: clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: target-scope 0 0 [client]
Applied User Profile: aaa-unique-id 0 28 (0x1c)
Applied User Profile: client-iif-id 0 4261415483 (0xfe000a3b)
Applied User Profile: vlan-id 0 100 (0xa63)
Applied User Profile:session-linksec-secured 0 False
Applied User Profile: nas-ip-address 0 0x0
Applied User Profile: nas-ipv6-Address 0 ""
Applied User Profile: interface 0 ""
Applied User Profile: port-type 0 19 [802.11 wireless]
Applied User Profile: nas-port 0 10014 (0x40eba)
Applied User Profile:
cisco-wlan-ssid 0 "LWA-SSID"
Applied User Profile:
wlan-profile-name 0 "LWA-SSID"
Applied User Profile:nas-identifier-wireless 0 "LWA-SSID"
Applied User Profile: priv-lvl 0 1 (0x1)
Applied User Profile: method 0 1 [webauth]
Applied User Profile:
clid-mac-addr 0 3a e6 3b 9a fc 4a
Applied User Profile: intf-id 0 2420113410 (0x90400002)
Applied User Profile:
username 0 "cisco"
Applied User Profile: bsn-wlan-id 0 16 (0x10)
Applied User Profile: timeout 0 86400 (0x15180)
Applied User Profile: timeout 0 86400 (0x15180)
MAC: aaaa.bbbb.cccc Link-local bridging not enabled for this client, not checking VLAN validity
[aaaa.bbbb.cccc:capwap_90400002]
User Profile applied successfully - REPLACE
```

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr method(757)

[aaaa.bbbb.cccc:capwap_90400002]
Raised event AUTHZ_SUCCESS (11)
[aaaa.bbbb.cccc:capwap_90400002]
Context changing state from 'Authc Success' to 'Authz Success'

Web認証が完了しました

<#root>

MAC: aaaa.bbbb.cccc

L3 Authentication Successful.

```
ACL:[]
MAC: aaaa.bbbb.cccc Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING ->
```

S_AUTHIF_WEBAUTH_DONE

エンドクライアントに適用されるAAA属性

<#root>

```
[ Applied attribute : username 0 "
```

cisco

```
" ]
[ Applied attribute : bsn-wlan-id 0 16 (0x10) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute : timeout 0 86400 (0x15180) ]
[ Applied attribute :bsn-vlan-interface-name 0 "
```

myvlan

"]

エンドクライアントがRun状態になる

<#root>

Managed client RUN state notification: aaaa.bbbb.cccc MAC: aaaa.bbbb.cccc Client state transition: S_CO_L3_AUTH_IN_PROGRESS ->

S_CO_RUN

一般的なトラブルシューティングのシナリオ

Authentication failures

考慮事項

- 表示されているポータルで、正しいクレデンシャルを入力すると「Authentication Failed」 と表示される。
- WLCに「Web Auth Pending」状態のクライアントが表示されています。
- 最初のスプラッシュページが再びユーザに表示されます。

WLC RAトレース

<#root>

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 Param-map used: lwa-parameter_map [aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State LOGIN -> AUTHENTICATING [aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 40828/176 IO state READING -> AUTHENTICATING [aaaa.bbbb.cccc][X.X.X.X]capwap_90400002

Param-map used: lwa-parameter_map

[aaaa.bbbb.cccc][X.X.X.X]capwap_90400002 State AUTHENTICATING ->

AUTHC_FAIL [INVALID CREDENTIALS]

```
[aaaa.bbbb.cccc:capwap_90400002] Authc failure from WebAuth, Auth event fail
[aaaa.bbbb.cccc:capwap_90400002] (Re)try failed method WebAuth - aaaa.bbbb.cccc
[aaaa.bbbb.cccc:capwap_90400002] Method webauth changing state from 'Running' to 'Authc Failed'
```

推奨ソリューション

ネットワーク認証用のデフォルトのAAA方式リストがWLC設定に存在することを確認します。

GUI で次の手順を実行します。

- 1. Configuration > Security > AAA > AAA Method List > Authorizationの順に選択します。 + Addをクリックします。
- 2. 次のように設定します。
 - 1. 方式リスト名:デフォルト
 - 2. タイプ: network
 - 3. グループタイプ: ローカル
- 3. Apply to Deviceをクリックします。

Method List Name* default Type* network Group Type local Authenticated I Available Server Groups Assigned Server Groups	
Type* Group Type local Authenticated Available Server Groups Image: Server Groups	
Group Type Authenticated Available Server Groups Assigned Server Groups	
Authenticated Image: Comparison of the server Groups Available Server Groups Assigned Server Groups	
Available Server Groups Assigned Server Groups	
radius	
Idap >	
Cancel	
Configuration * > Security * > AAA show Me How > * AAA Wizard Servers / Groups AAA Method List AAA Advanced	
Authentication	
Authorization + Add × Delete	
Accounting	1
Operature network local N/A N/A N/A H ≪ 1 H [10 •] 1 - 1 of 1 items 1 - 1 of 1 items	

CLIから、

<#root>

WLC# configure terminal
WLC(config)# aaa authorization default network local

ポータルはユーザには表示されないが、クライアントは接続されているように見え る

エンドクライアントから発生する可能性のある動作

• エンドクライアントはデバイスを「接続済み」として認識します。

- エンドクライアントにポータルが表示されない。
- エンドクライアントはクレデンシャルを入力しません。
- エンドクライアントにIPアドレスが割り当てられている。
- WLCに「Run」状態のクライアントが表示されます。

WLC RAトレース

クライアントは割り当てられたIPアドレスを取得し、WLC上ですぐに「Run」状態に移行します 。ユーザ属性は、エンドクライアントに割り当てられたVLANのみを表示します。

<#root>

MAC: aaaa.bbbb.cccc

Client IP learn successful. Method: DHCP IP: X.X.X.X

[aaaa.bbbb.cccc:capwap_90400002] auth mgr attr add/change notification is received for attr addr(8)
[aaaa.bbbb.cccc:capwap_90400002] SM Notified attribute Add/Update addr X.X.X.X
MAC: aaaa.bbbb.cccc IP-learn state transition:

S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

MAC: aaaa.bbbb.cccc Received ip learn response. method: IPLEARN_METHOD_DHCP [Applied attribute :bsn-vlan-interface-name 0 "

myvlan

"]

[Applied attribute : timeout 0 1800 (0x708)]
MAC: aaaa.bbbb.cccc Client QoS run state handler
Managed client RUN state notification: aaaa.bbbb.cccc
MAC: aaaa.bbbb.cccc Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

推奨ソリューション

WebポリシーがWLANで有効になっていることを確認します。

GUIで次の手順を実行します。

- 1. Configuration > Tags & Profiles > WLANsの順に選択します。
- 2. LWA WLANを選択します。
- 3. Security > Layer 3の順に選択します。
- 4. Web Policyチェックボックスが有効になっていることを確認します。

Config	uration * > Tags & Profi	les" > WLANs		Edit WLAN *
+ /	Add X Delete	Clone Enable W	LAN Disable WLAN	Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
Selection	dd x Delete d WLANS : 0 Status Y Name ↑ C LWA-SSID 4 1 ▷ H 10 √	Clone Enable W	AN Disable WLAN	Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it. General Security Advanced Add To Policy Tags Layer2 Layer3 AAA Show Advanced Settings >>> Web Policy Image: Show Advanced Settings >>> Web Auth Parameter Map Image: Im
				Cancel

Webポリシーを有効にする必要がある

CLIから、

<#root>

WLC# configure terminal

WLC(config)# wlan

<wlan>

WLC(config-wlan)# shutdown WLC(config-wlan)# security webauth WLC(config-wlan)# no shutdown

ポータルがユーザに表示されず、クライアントが接続しない

エンドクライアントから発生する可能性のある動作

- エンドクライアントは、デバイスが絶えず接続を試みていることを認識します。
- エンドクライアントにポータルが表示されない。
- エンドクライアントにIPアドレスが割り当てられていない
- WLCに「Webauth Pending」状態のクライアントが表示されます。

推奨ソリューション

必要なHTTP/HTTPSサーバを有効にします。ネットワークのニーズに完全に対応するために、ど

のHTTP/HTTPSサーバを有効にする必要があるのかをより細かく制御できるようになりました。 HTTPの組み合わせがいくつかサポートされているため、Web認証のHTTPおよびHTTPS要求の設 定の詳細については、<u>このリンク</u>を参照してください。たとえば、HTTPはwebadminにのみ使用 でき、HTTPはwebauthに使用できます。

HTTPアクセスとHTTPSアクセスの両方で管理デバイス管理とWeb認証を許可するには、CLIから 次の手順を実行します。

WLC# configure terminal WLC(config)# ip http server WLC(config)# ip http secure-server



注意:これらのサーバの両方を無効にしても、WLCのグラフィカルユーザインターフェ イス(GUI)にアクセスできません。 エンドクライアントがIPアドレスを取得していない

エンドクライアントから発生する可能性のある動作

- エンドクライアントは、デバイスがIPアドレスの取得を継続的に試みていることを認識します。
- WLCに「IPラーニング」状態のクライアントが表示されます。

WLC RAトレース

オファーなしのディスカバリ要求。

RX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s TX: DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff s

推奨ソリューション

最初:ポリシープロファイルに正しいVLANが割り当てられていることを確認します。

GUIで次の手順を実行します。

- 1. Configuration > Tags & Profiles > Policyの順に選択します。
- 2. 使用するポリシープロファイルを選択します。
- 3. Access Policiesに移動します。
- 4. 適切なVLANを選択します。

Conf	guration * >	Tags & Profiles	* > Policy	Edit Policy Profile					×
+	Add	C Delete	1) Clone	A Disabling a Policy of	r configuring it in 'Enabled' state,	will result in loss of connectiv	vity for clients ass	sociated with this Policy profi	le.
	Admin Y Status	Associated 0 Y Policy Tags	Policy Profile Name	General Access Policies	QOS and AVC Mobilit	ty Advanced			
	٢	•	lwa-policy_profile	RADIUS Profiling	0		WI AN ACI		
	 < 	н 10 🔻	default-policy-profile	HTTP TLV Caching	0		IPv4 ACL	Search or Select] 🛛
				DHCP TLV Caching	D		IPv6 ACL	Search or Select] 🛛
				WLAN Local Profiling			URL Filters	(i)
				Global State of Device Classification	Enabled (i)				
				Local Subscriber Policy Name	Search or Select	▼ Ø	Pre Auth	Search or Select	່ງຍ
				VLAN			Post Auth	Search or Select	
				VLAN/VLAN Group	100	•			
				Multicast VLAN	Enter Multicast V	LAN			
				Cancel				Update & Apply to	Device

CLIから、

<#root>

WLC# show wireless profile policy detailed

<policy-profile>

Policy Profile Name :

<policy-profile>

Description :

<policy-profile>

Status : ENABLED VLAN :

VLAN-selected

[...]

WLC# configure terminal
WLC(config)# wireless profile policy

<policy-profile>

WLC(config-wireless-policy)#

vlan <correct-vlan>

2番目:ユーザが使用できるDHCPプールが存在することを確認します。その設定と到達可能性を 確認します。RAトレースは、どのVLAN DHCP DORAプロセスが実行されているかを示します。 このVLANが正しいVLANであることを確認します。

DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y, DHCPv4 from interface capwap_90400002 on vlan 100 Src MAC: aaaa.bbbb.cccc Dst MAC: ffff.ffff.ffff src_i DHCPv4 from interface Gi2 on vlan 100 Src MAC: cccc.bbbb.aaaa Dst MAC: aaaa.bbbb.cccc src_ip: Y.Y.Y,

カスタマイズされたポータルがエンドクライアントに表示されない

エンドクライアントから発生する可能性のある動作

• WLCのデフォルトポータルが表示されます。

推奨ソリューション

最初:カスタマイズされたWeb認証パラメータマップをWLANが使用していることを確認します 。

GUI で次の手順を実行します。

- 1. Configuration > Tags & Profiles > WLANsの順に選択します。
- 2. リストからWLANを選択します。
- 3. Security > Layer 3の順に選択します。

4. カスタマイズされたWeb認証パラメータマップを選択します。

Edit WLAN	×
Changing WLAN parameters while it is enabled will result in loss of connectivity for clients con	innected to it.
Configuration * > Tags & Profiles * > WLANs	Edit WLAN *
+ Add X Delete	Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
Selected WLANs : 0	General Security Advanced Add To Policy Tans
Status Y Name Y ID	
LWA-SSID	Show Advanced Settings >>>
	Web Policy
	Web Auth Parameter Map Iwa-parameter V
	Authentication List forwebauth 🗸 🖉
	For Local Login Method List to work, please make sure the configuration 'asa authorization network default local'
	exists on the bevice
	1

カスタムパラメータマップが選択されました

CLIから、

<#root>

WLC# show wlan name LWA-SSID WLAN Profile Name : LWA-SSID

[...]

Security: Webauth Parameter Map :

<parameter-map>

WLC# configure terminal WLC(config)# wlan

<wlan>

WLC(config-wlan)# security web-auth parameter-map

<parameter-map>

2つ目:<u>Cisco.com</u> Webポータルからダウンロードするカスタマイズされたダウンロードは、非常 に堅牢で複雑なプログラミングインターフェイスでは動作しないことに注意してください。一般 に、変更はCSSレベルだけを行い、イメージの追加や削除を行うことをお勧めします。アプレッ ト、PHP、変数の変更、React.jsなどはサポートされていません。カスタマイズされたポータル がクライアントに表示されない場合は、デフォルトのWLCページを使用して、問題が再現される かどうかを確認してください。ポータルが正常に表示された場合、使用することになっているカ スタマイズされたページでサポートされていないものがあります。

3:EWC(<u>組み込みワイヤレスコントローラ</u>)を使用する場合は、カスタマイズされたページが正し く表示されるように、CLIを使用してカスタマイズされたページを追加することをお勧めします。

<#root>

EWC# configure terminal
EWC(config)# parameter-map type

<parameter-map>

EWC(config-params-parameter-map)# custom-page login device flash:loginsantosh.html EWC(config-params-parameter-map)# custom-page login expired device flash:loginexpire.html EWC(config-params-parameter-map)# custom-page failure device flash:loginfail.html EWC(config-params-parameter-map)# custom-page success device flash:loginsucess.html EWC(config-params-parameter-map)# end

カスタマイズされたポータルがエンドクライアントに正しく表示されない

エンドクライアントから発生する可能性のある動作

カスタマイズされたポータルが正しくレンダリングされない(つまり、イメージが表示されない)。

推奨ソリューション

グローバルパラメータマップに仮想IPアドレスが割り当てられていることを確認します。

GUIで次の手順を実行します。

- 1. Configuration > Security > Web Authの順に選択します。
- 2. リストからグローバルパラメータマップを選択します。
- 3. ルーティングできない仮想IPアドレスを追加します。



グローバルパラメータマップの仮想IPアドレスをルーティング不能IPアドレスに設定

CLIから、

<#root>

```
WLC# show parameter-map type webauth global
Parameter Map Name : global
[...]
Virtual-ipv4 :
```

<urr>display="block-in-color: series block-in-color: block-in-color: series block-in-color: series block-in-color: block-in-color: series block-in-color: series

[...]

```
WLC# configure terminal
WLC(config)# parameter-map type webauth global
WLC(config-params-parameter-map)# virtual-ip ipv4
```

<unroutable-ip>



ヒント:仮想IPアドレスは、Web認証ログインページのリダイレクトアドレスとして機能します。ネットワーク上の他のデバイスは同じIPを持つことはできず、物理ポートにマッピングすることも、ルーティングテーブルに存在することもできません。したがって、仮想IPはルーティング不能IPアドレスとして設定することを推奨します。<u>RFC5737</u>に記載されているものだけを使用できます。

ポータルに「Your connection is not secure/verify signature failed」と表示される

エンドクライアントから発生する可能性のある動作

- ポータルを開くと、接続が安全でないことを示すエラーがクライアントに表示されます。
- ポータルは証明書を使用することが想定されています。

ポータルがHTTPSの下に表示されることが予想される場合は、SSL(Secure Socket Layer)証明書 を使用する必要があることを意味します。この証明書は、ドメインが実際に存在することを検証 するために、サードパーティの認証局(CA)によって発行される必要があります。エンドクライア ントがクレデンシャルを入力したり、ポータルを表示したりするときに、信頼を提供します。 WLCに証明書をアップロードするには、<u>このドキュメント</u>を参照してください。

推奨ソリューション

最初に、必要なHTTP/HTTPSサービスを再起動します。ネットワークのニーズに完全に対応する ために、どのHTTP/HTTPSサーバを有効にする必要があるのかをより細かく制御できるようにな りました。Web認証用のHTTPおよびHTTPS要求の設定の詳細については、<u>このリンク</u>を参照し てください。

CLIから、

WLC# configure terminal WLC(config)# no ip http server WLC(config)# no ip http secure-server WLC(config)# ip http server WLC(config)# ip http secure-server

2番目:証明書がWLCに正しくアップロードされていること、およびその有効期間の日付が正し いことを確認します。

GUIで次の手順を実行します。

- 1. Configuration > Security > PKI Managementの順に選択します。
- 2. リストでトラストポイントを検索します
- 3. 詳細を確認する

Configura	ion * > Security * > PKI Management				
Trustpoint	s CA Server Key Pair Generation Add Certi	ficate Trustpool			
+ A4	d X Delete				
	Trustpoint Name	T Certificate Requests	Key Generated	T Issuing CA Authenticated	Y Used By
0	SLA-TrustPoint	None	No	Yes	
0	TP-self-signed-2473901665	Yes	Yes	Yes	
0	WLC_CA	None	Yes	Yes	
0	<trustpoint-name></trustpoint-name>	Yes	Yes	Yes	Web Admin 💋
H 4	1 > H 10 ¥				1 - 4 of 4 items

トラストポイントの存在の確認トラストポイントの

Configurat	ion*> Security*> PKI Management						
Trustpoints	CA Server Key Pair Generation	Add Certificate Tr	rustpool				
+ Ad	d × Dolote						
	Trustpoint Name	T Certifi	fcate Requests	Key Generated T	Issuing CA Authenticated	▼ Used By	
0	SLA-TrustPoint	None	B	No	Yes		
0	TP-self-signed-2473901665	Yes	B	Yes	Yes		
0	WLC_CA	None	D.	Yes	Yes		
0	<trustpoint-name></trustpoint-name>	Yes	B	Yes	Yes	Web Admin 🛃	
14 - 4	1 > H 10 v					1 - 4 of 4 items	
		Certificates		×	Certificates		,

CA Certificate Device Certificate	CA Certificate Device Certificate
CA Certificate	Certificate
Status: Available	Status: Available
Certificate Serial Number (hex): 01	Certificate Serial Number (hex): 02
Certificate Usage: Signature	Certificate Usage: General Purpose
Issuer:	Issuer:
O [±] <organizational-unit> Cn[±] <common-name></common-name></organizational-unit>	o= <organizational-unit> cn= <common-name></common-name></organizational-unit>
Subject:	Subject:
o= <organizational-unit></organizational-unit>	Name:
cn= <common-name></common-name>	Serial Number: 9217PVKUQ2B
Validity Date:	serialNumber=9217PVKUQ2B+hostname=standalone
start date: 15:55:18 UTC Mar 14 2024	o= <organizational-unit></organizational-unit>
end date: 15:55:18 UTC Mar 14 2034	cn= <common-name></common-name>
Associated Trustpoints: <trustpoint></trustpoint>	Validity Date:
Storage: nvram:CiscoVirtual#1CA.cer	start date: 15:55:23 UTC Mar 14 2024
	end date: 15:55:18 UTC Mar 14 2034
	Associated Trustpoints: <trustpoint></trustpoint>

詳細の確認トラストポイントの 有効性の確認

CLIから、

<#root>

WLC# show crypto pki certificate

```
[<certificate>]
```

CA Certificate Status: Available Certificate Serial Number (hex): 01 Certificate Usage: Signature Issuer: cn=<Common Name> o=<Organizational Unit> Subject: cn=<Common Name> o=<Organizational Unit> Validity Date:

start date: <start-date>

end date: <end-date>

Associated Trustpoints: <trustpoint>

IPv4ホスト名が証明書内の共通名(CN)と一致することを確認します。

GUIで次の手順を実行します。

- 1. Configuration > Security > Web Authの順に選択します。
- 2. 使用するパラメータマップをリストから選択します。
- 3. トラストポイントと仮想IPv4ホスト名が正しいことを確認します。

Configuration * > Security * > Web Auth	Edit Web Auth Parameter *				
+ Add × Delete	General Advanced				
	Parameter-map Name	global	Virtual IPv4 Address	<urr>alignment</urr>	
Parameter Map Name	Maximum HTTP connections	100	Trustpoint	<trustpoint> +</trustpoint>	
	Init-State Timeout(secs)	120	Virtual IPv4 Hostname	<certificate-cn></certificate-cn>	
	Туре	webauth 🔻	Virtual IPv6 Address	XXXXXX	
	Captive Bypass Portal	0	Web Auth intercept HTTPs	0	
	Disable Success Window	0	Enable HTTP server for Web Auth	0	
	Disable Logout Window	0	Disable HTTP secure server	o	
	Disable Cisco Logo	0	for Web Auth	_	
	Sleeping Client Status	0	Banner Configuration		
	Sleeping Client Timeout (minutes)	720	Banner Title		
			Banner Type None	O Banner Text	
			O Read	From File	
	X Cancel			update & Apply	

トラストポイントと仮想IPv4ホスト名の確認

CLIから、

<#root>

WLC# show run | section paramter-map type

<type> <name>

parameter-map type

<type> <name>

[...]
virtual-ip ipv4

<unroutable-ip> <certificate-common-name>

trustpoint

<trustpoint>

関連情報

- <u>ローカルWeb認証の設定</u>
- <u>Webベース認証(EWC)</u>
- <u>Catalyst 9800 WLCでのWeb認証ポータルのカスタマイズ</u>
- <u>Catalyst 9800 WLCでのCSR証明書の生成とダウンロード</u>
- 仮想インターフェイスの設定

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。