對使用無線Lan控制器(WLC)9800和身分識別服務引擎(ISE)的中央Web驗證(CWA)進行排解疑難

目錄

簡介

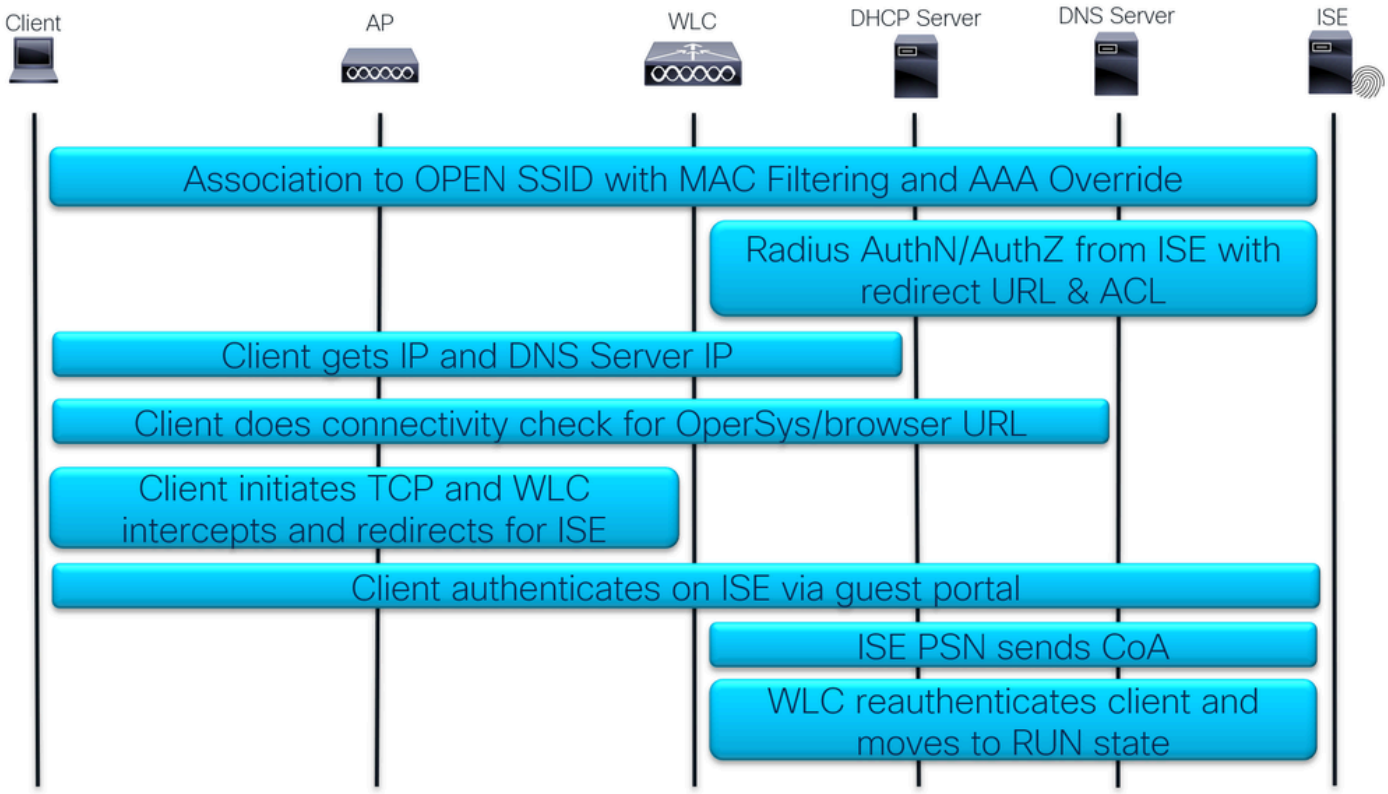
本檔案介紹如何對WLC 9800和ISE的中央Web驗證(CWA)進行疑難排解。

背景資訊

當前存在如此多的個人裝置，以致於尋求保護無線接入的網路管理員通常選擇使用CWA的無線網路。
在本文檔中，我們將重點介紹CWA的流程圖，它有助於排除影響我們的常見問題。
我們將檢視該過程的常見陷阱、如何收集與CWA相關的日誌、如何分析這些日誌，以及如何在WLC上收集嵌入式資料包捕獲以確認流量。

CWA是允許使用者使用個人裝置（也稱為BYOD）連線到公司網路的公司最常見的設定。
任何網路管理員都對在開啟TAC案例之前執行修復問題和故障排除步驟感興趣。

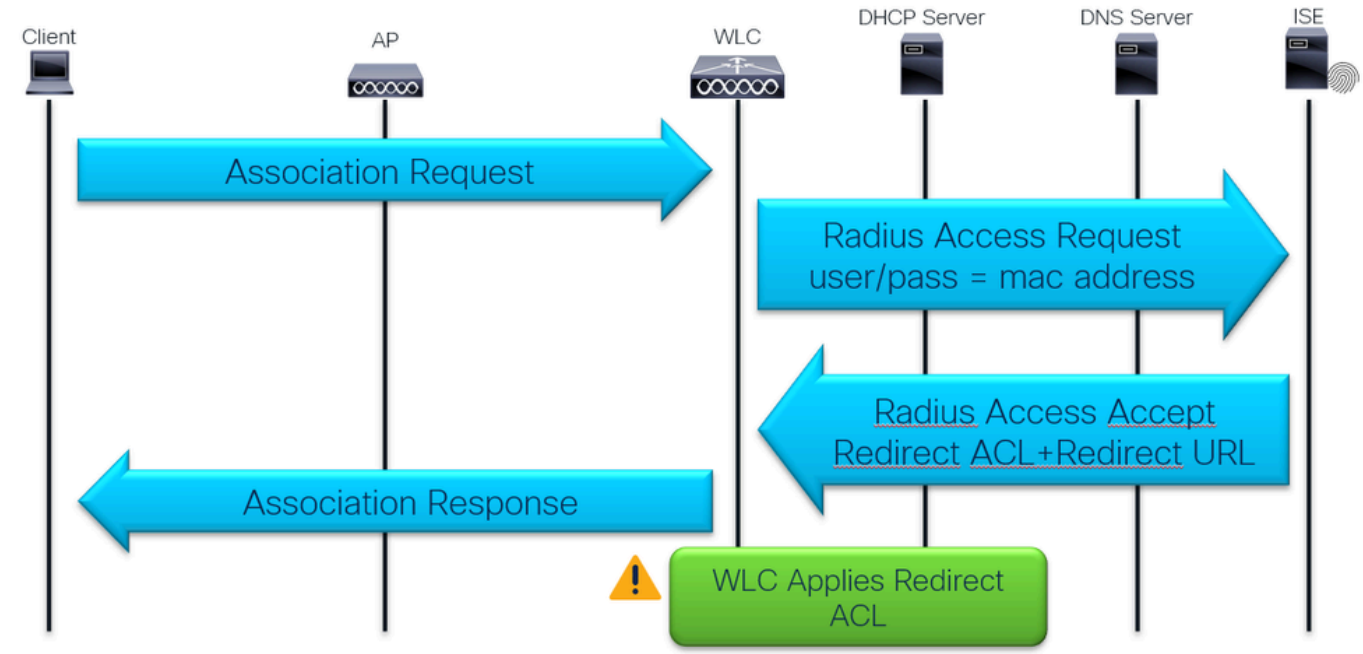
以下是CWA資料包流：



CWA封包流

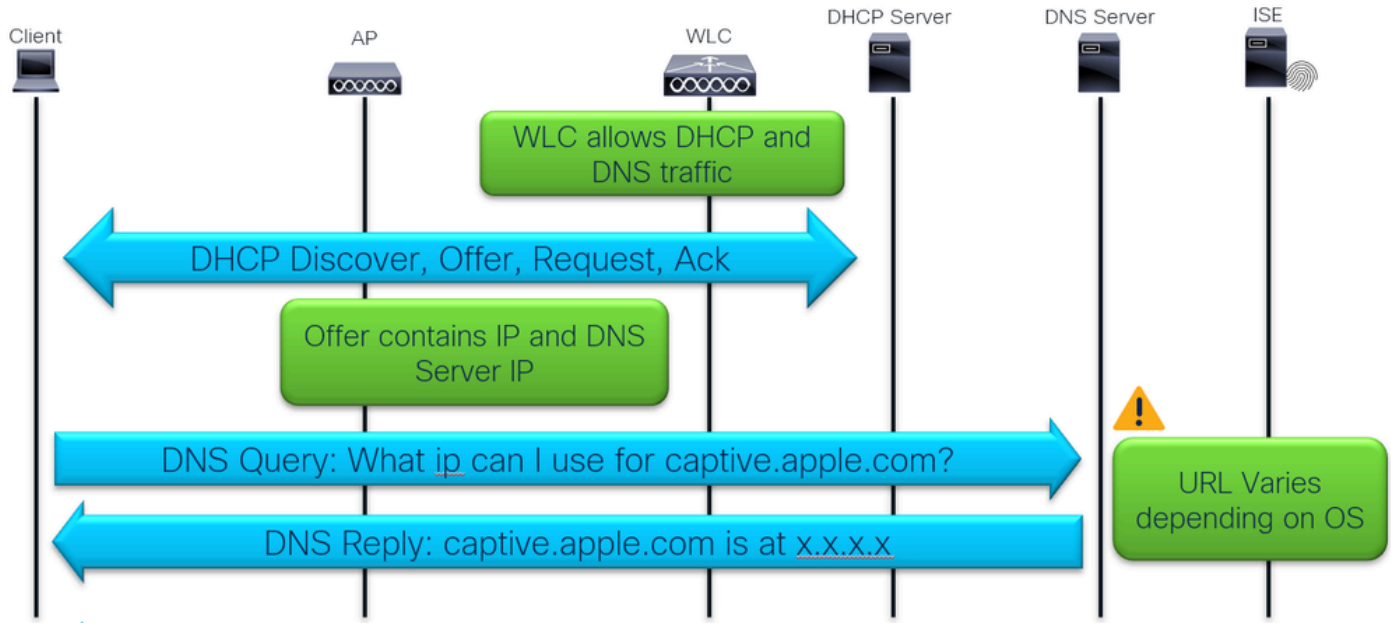
詳細流程

首次關聯和RADIUS身份驗證：



首次關聯和RADIUS身份驗證

DHCP、DNS和連線檢查：



DHCP、DNS和連線檢查

連線檢查由客戶端裝置作業系統或瀏覽器使用強制網路門戶檢測完成。

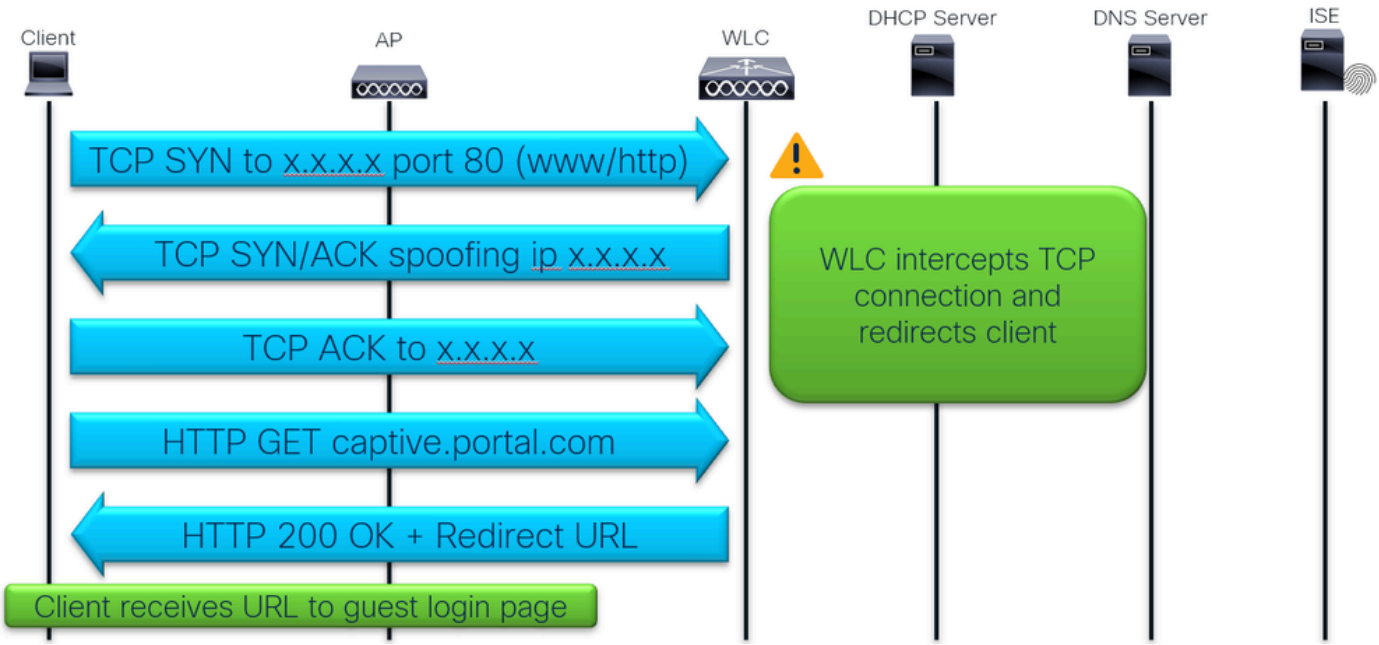
有預程式設計的裝置作業系統可針對特定域執行HTTP GET

- 蘋果= captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnectest.com

並且瀏覽器在開啟時也會執行此檢查：

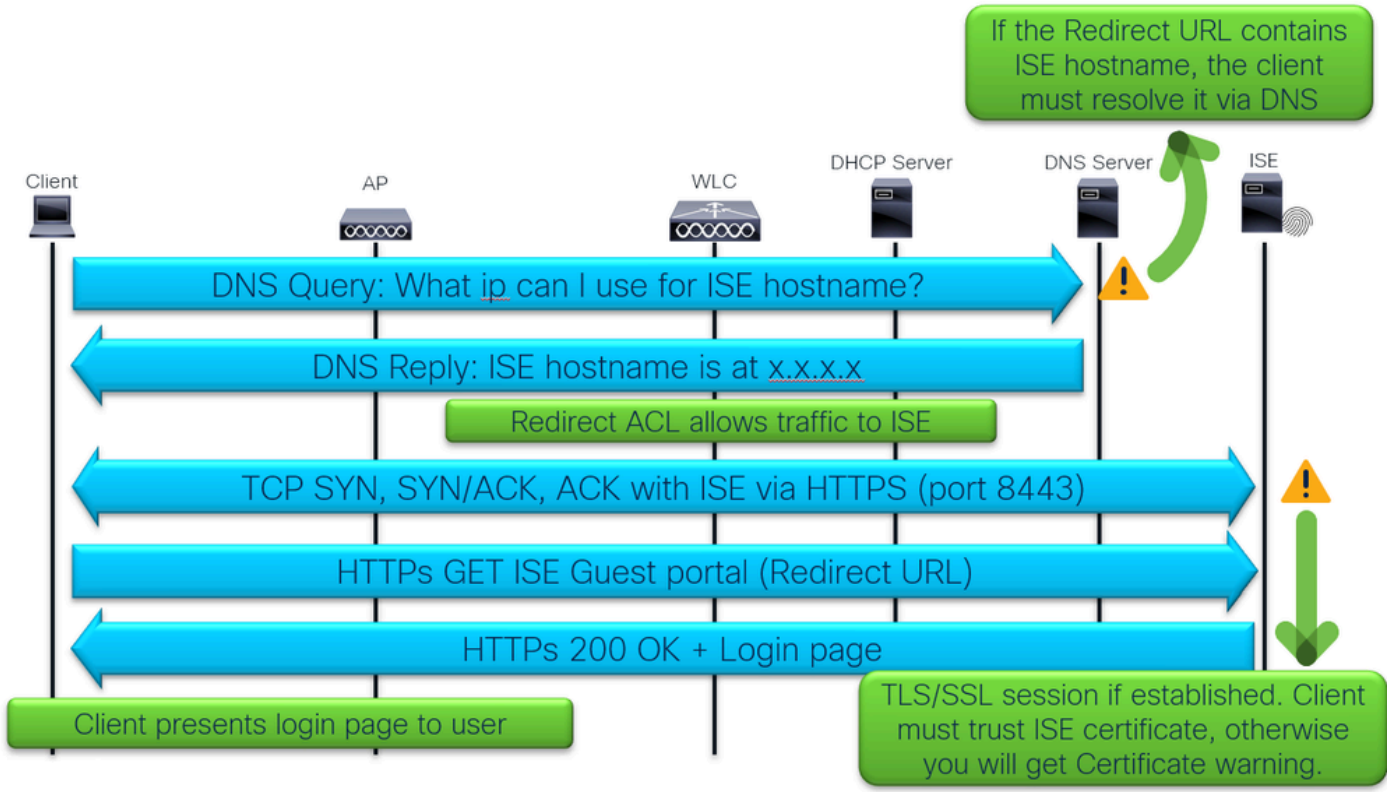
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

流量攔截和重定向：



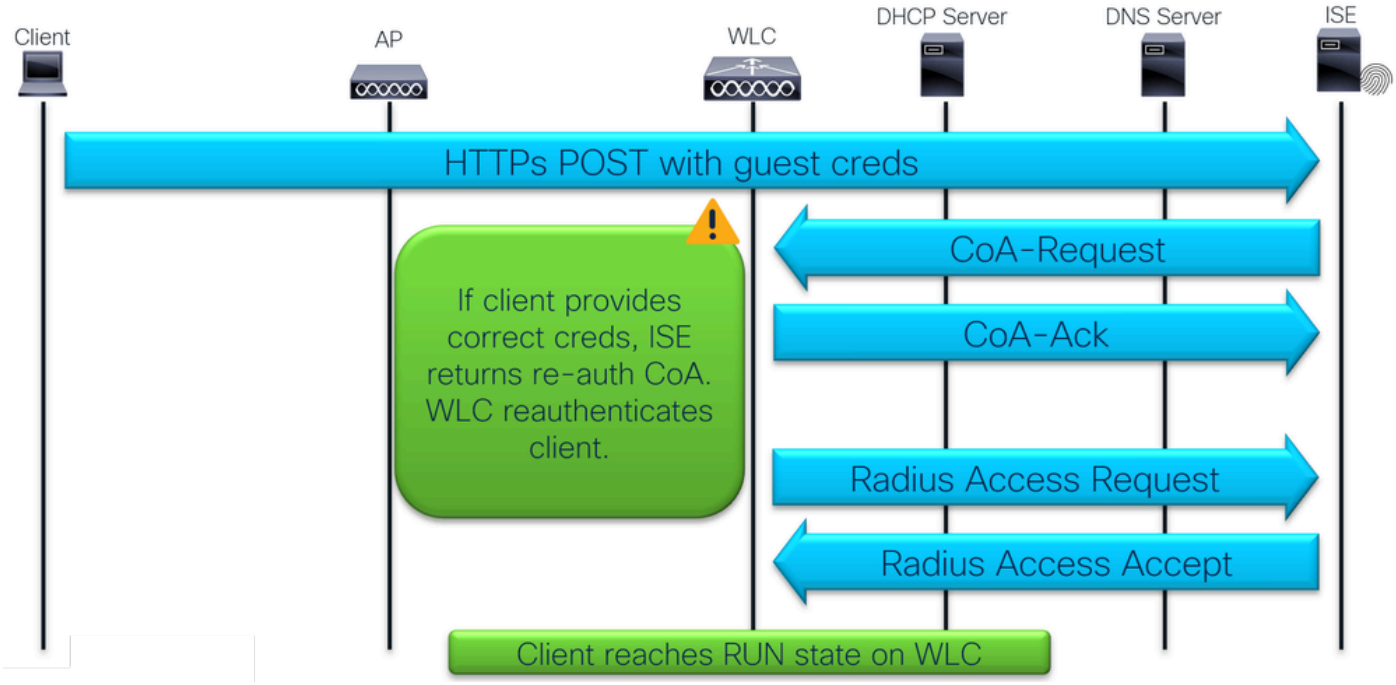
流量攔截和重定向

客戶端登入到ISE訪客登入門戶：



客戶端登入到ISE訪客登入門戶

客戶端登入和CoA:

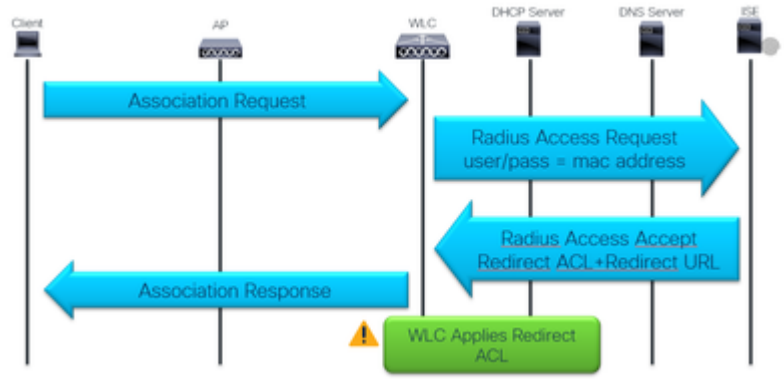


客戶端登入和CoA

疑難排解

常見症狀：使用者沒有重新導向至登入頁面。

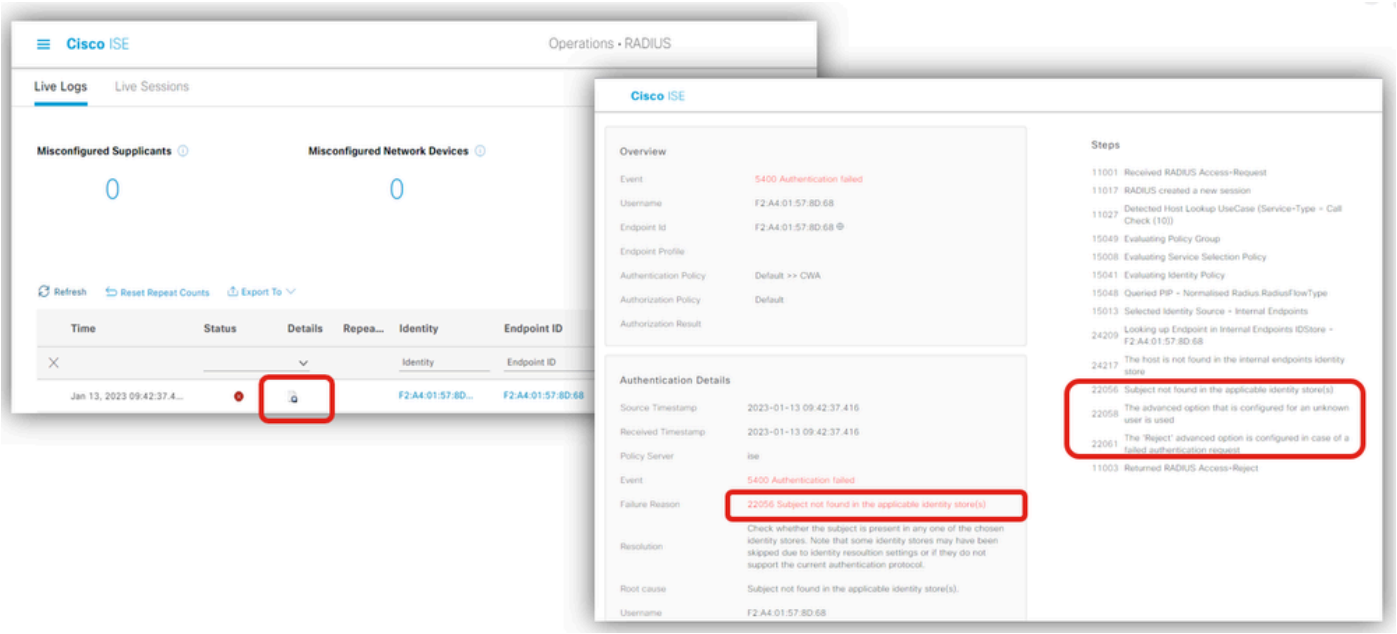
讓我們從流程的第一部分開始：



首次關聯和RADIUS身份驗證

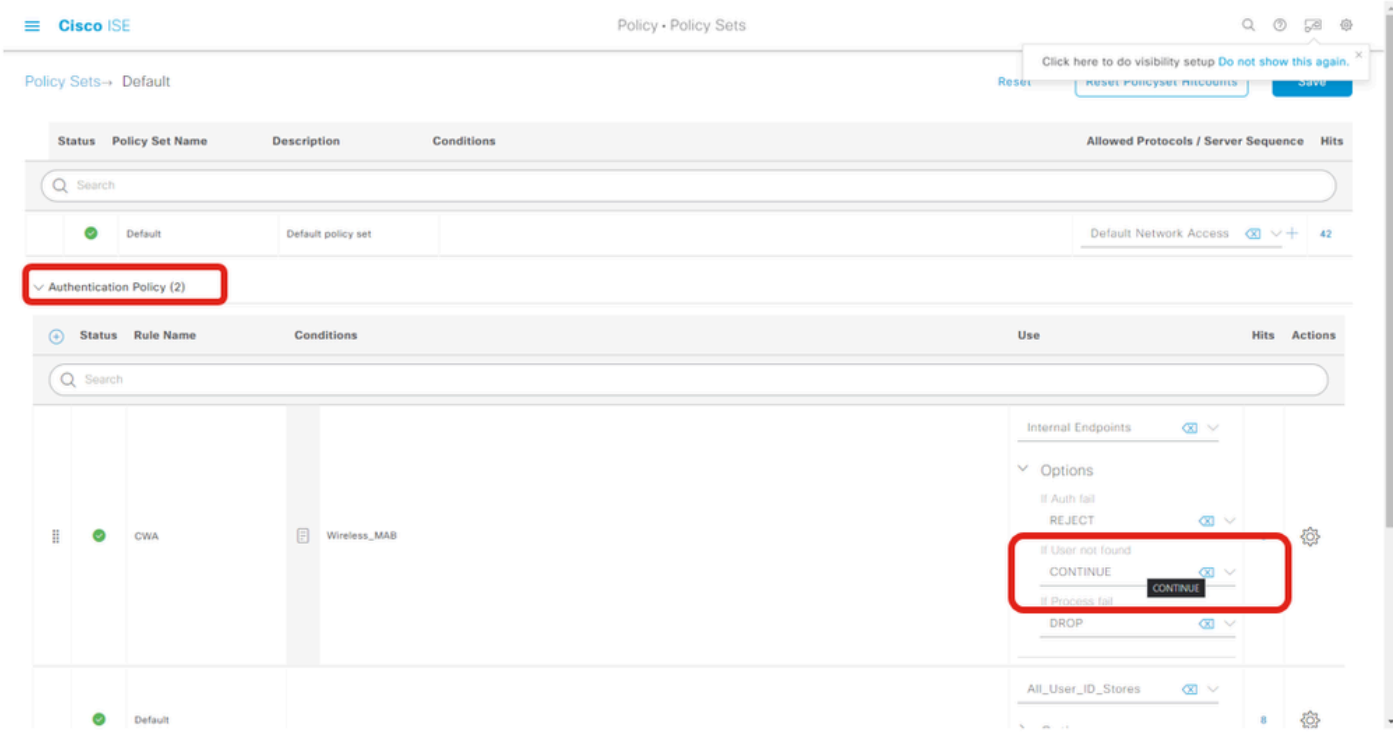
1 — 第一個RADIUS身份驗證是否成功？

檢查mac過濾驗證結果：



顯示mac過濾身份驗證結果的ISE Live日誌

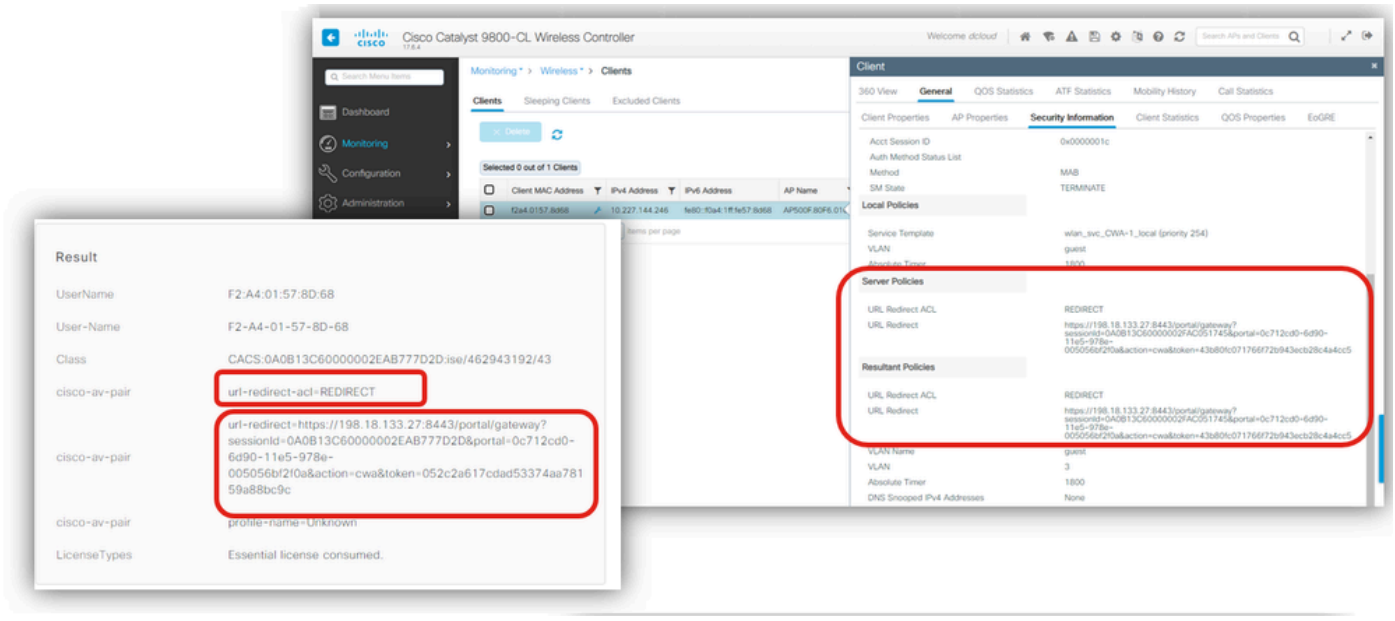
如果找不到使用者，請確保身份驗證的高級選項設定為「繼續」：



未找到使用者高級選項

2 - WLC收到重新導向URL和ACL?

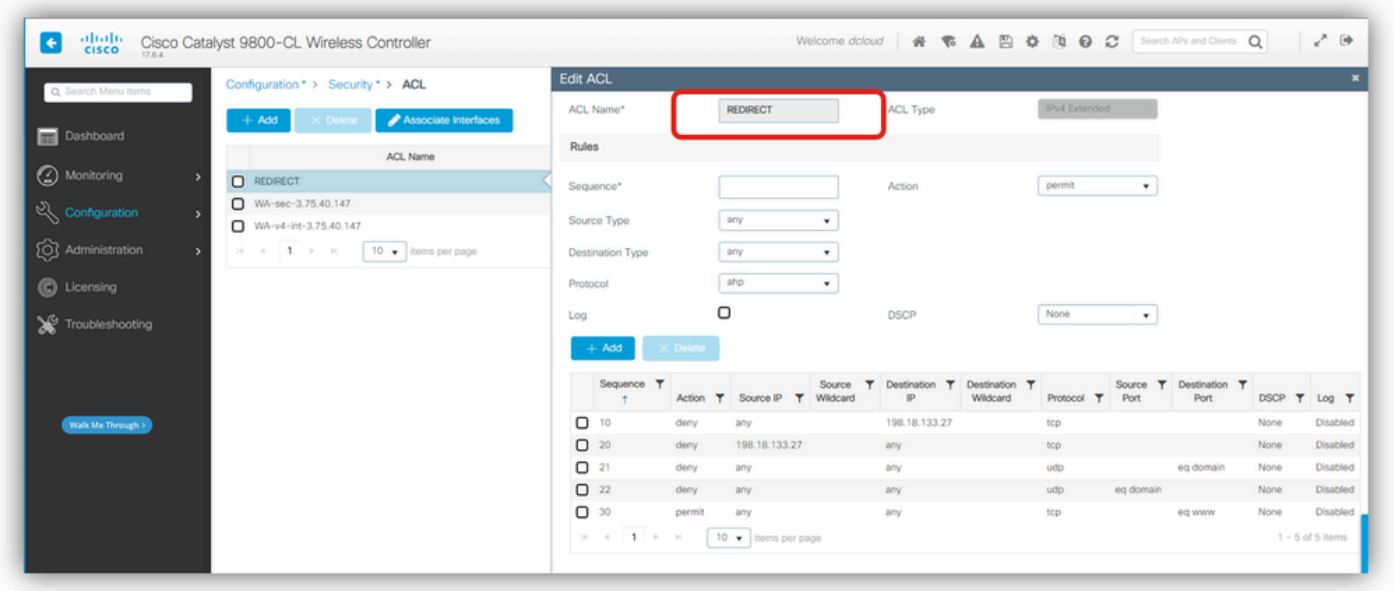
檢查Monitoring下的ISE即時日誌和WLC客戶端安全資訊驗證ISE在Access Accept中傳送Redirect URL和ACL，並且WLC會收到該資訊，並在客戶端詳細資訊中將其應用到客戶端：



重新導向ACL和URL

3 — 重定向ACL是否正確？

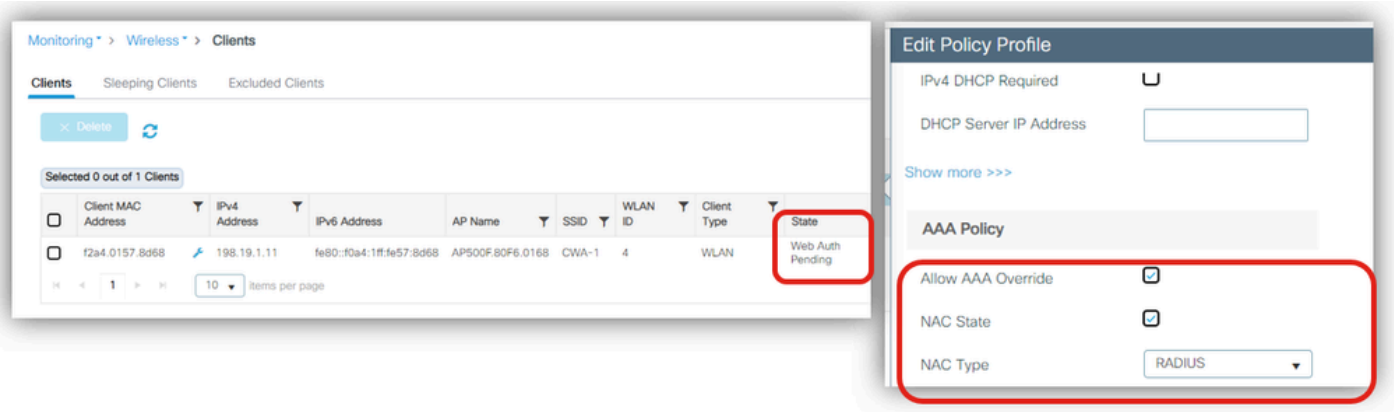
檢查ACL名稱中是否存在任何拼寫錯誤。確保它與ISE傳送的完全相同：



重新導向ACL驗證

4 — 是否將使用者端移至Web-Auth Pending?

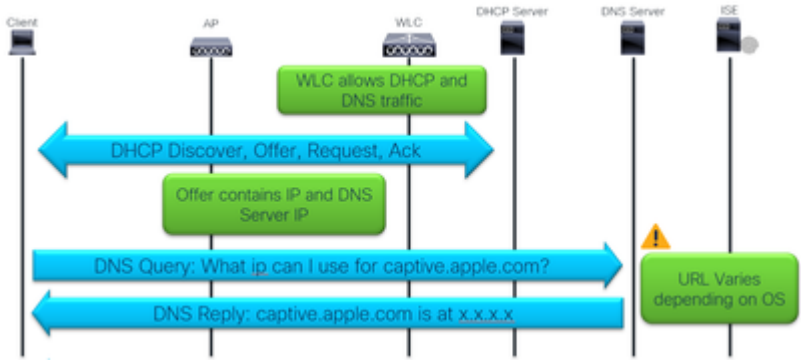
檢查使用者端詳細資訊，瞭解「Web Auth Pending」狀態。如果它未處於該狀態，則驗證是否已在策略配置檔案中啟用AAA覆蓋和Radius NAC:



客戶端詳細資訊、aaa覆蓋和RADIUS NAC

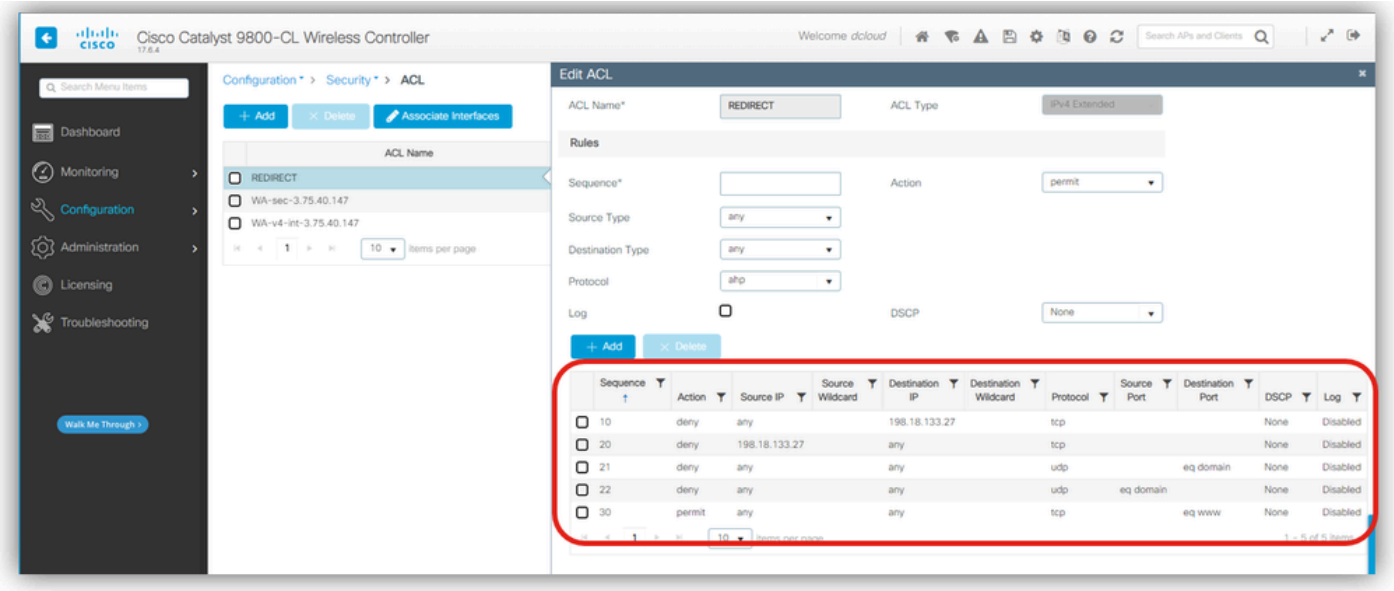
還是不工作？

讓我們重新審視一下流程……



5 - WLC是否允許DHCP和DNS流量？

驗證WLC中的重新導向ACL內容：



在WLC中重新導向ACL內容

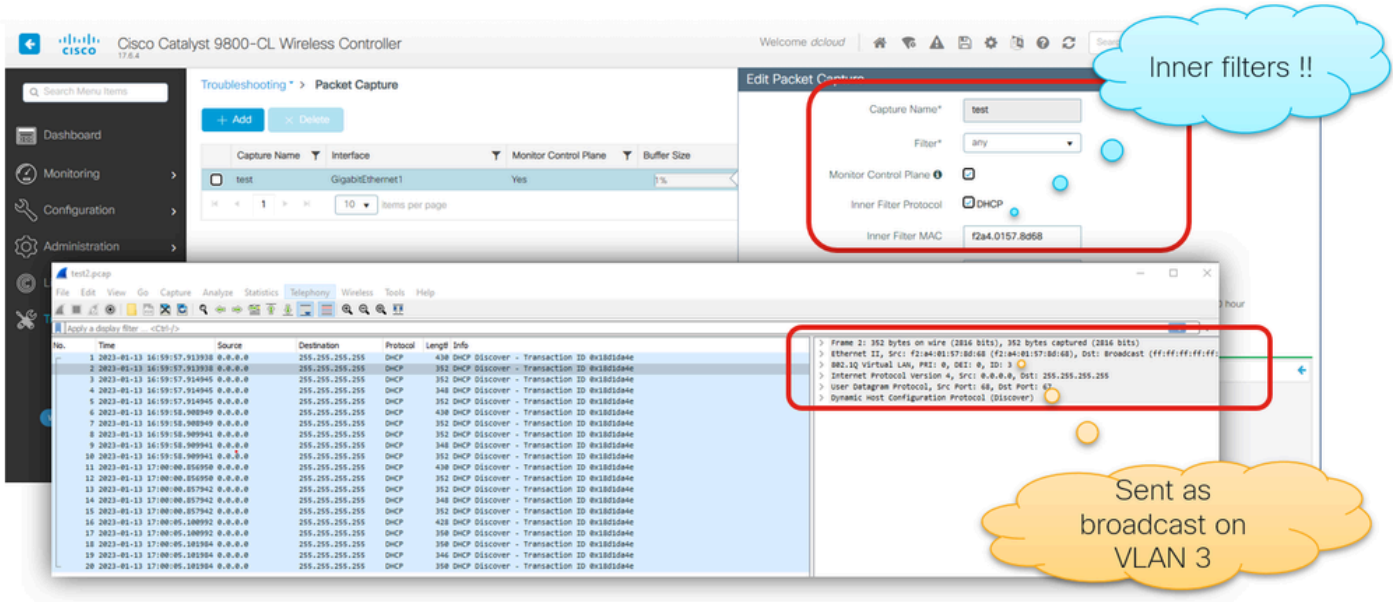
重定向ACL定義哪些流量被permit語句攔截和重定向，哪些流量被以deny語句從攔截和重定向中忽略。

在本例中，我們允許DNS和流量流入/流出ISE IP地址，並攔截埠80(www)上的任何tcp流量。

6 - DHCP伺服器是否接收DHCP發現/請求？

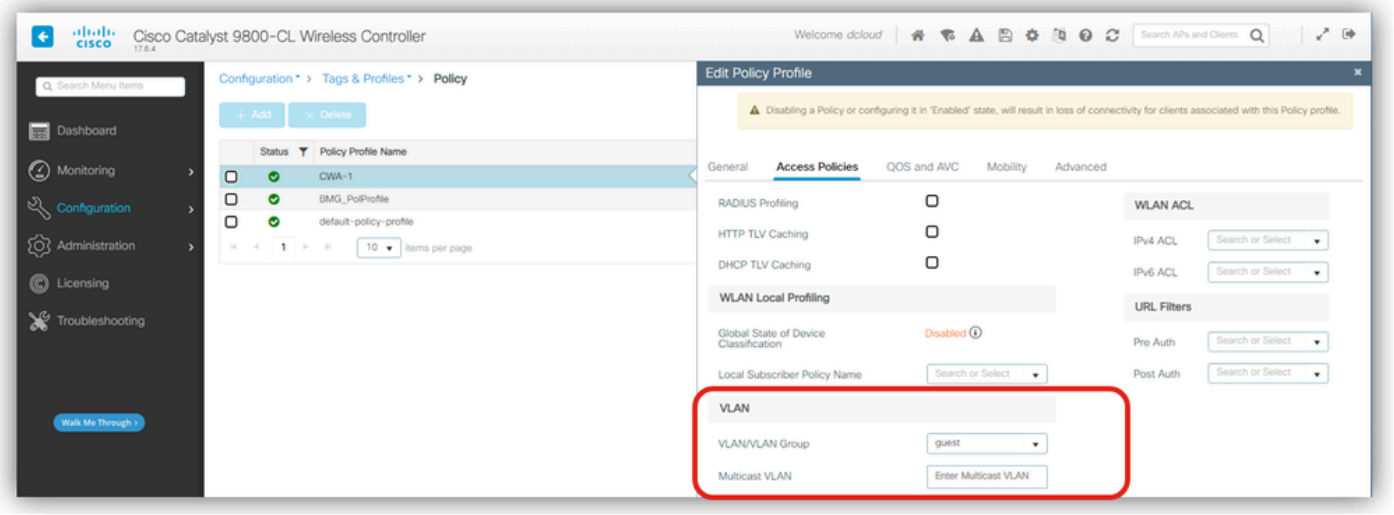
如果發生DHCP交換，請檢查EPC。EPC可以與內部過濾器（例如DHCP協定和/或內部過濾器MAC）一起使用，其中我們可以使用客戶端裝置MAC地址，並且我們只能在EPC中獲取由客戶端裝置MAC地址傳送或傳送到客戶端裝置MAC地址的DHCP資料包。

在本例中，我們可以看到VLAN 3上的DHCP發現資料包以廣播形式傳送：



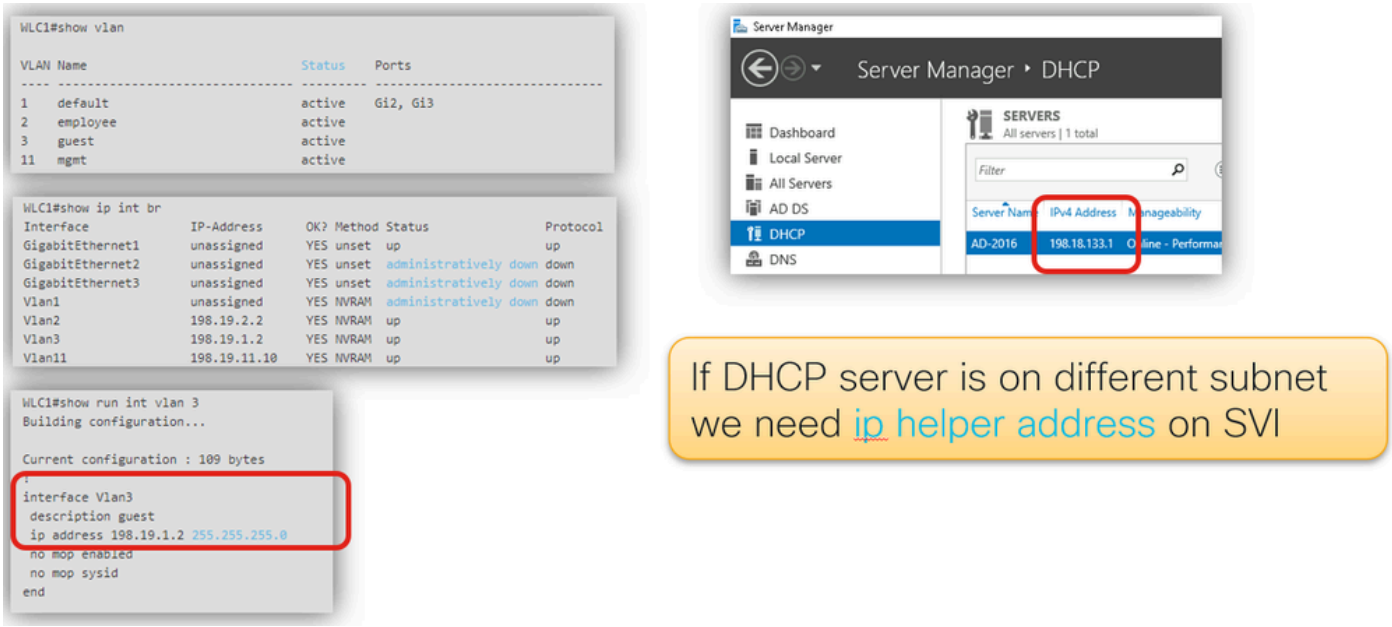
用於驗證DHCP的WLC EPC

確認策略配置檔案中預期的客戶端VLAN:



策略配置檔案中的VLAN

驗證WLC VLAN和switchport Trunk配置和DHCP子網：



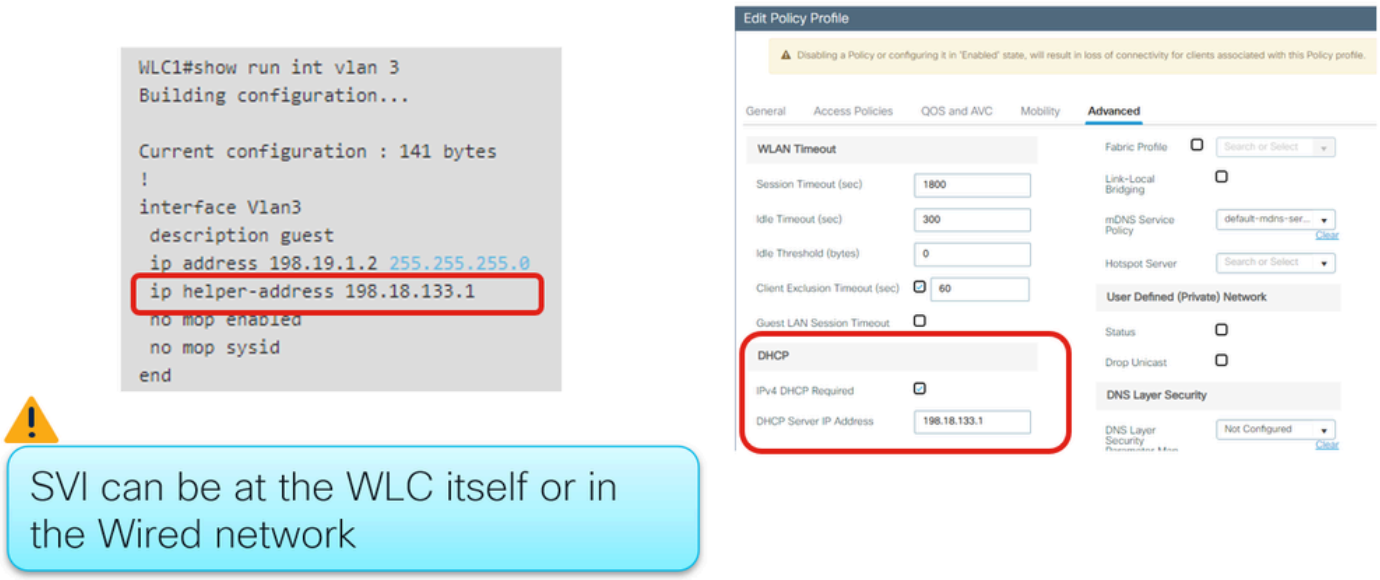
VLAN、switchport和DHCP子網

我們可以看到VLAN 3存在於WLC中，而且它也有用於VLAN 3的SVI，但是當我們驗證DHCP伺服器的IP地址時，它位於不同的子網中，因此我們需要在SVI上提供IP幫助地址。

最佳實踐要求在有線基礎架構中配置客戶端子網的SVI，並在WLC上避免配置。

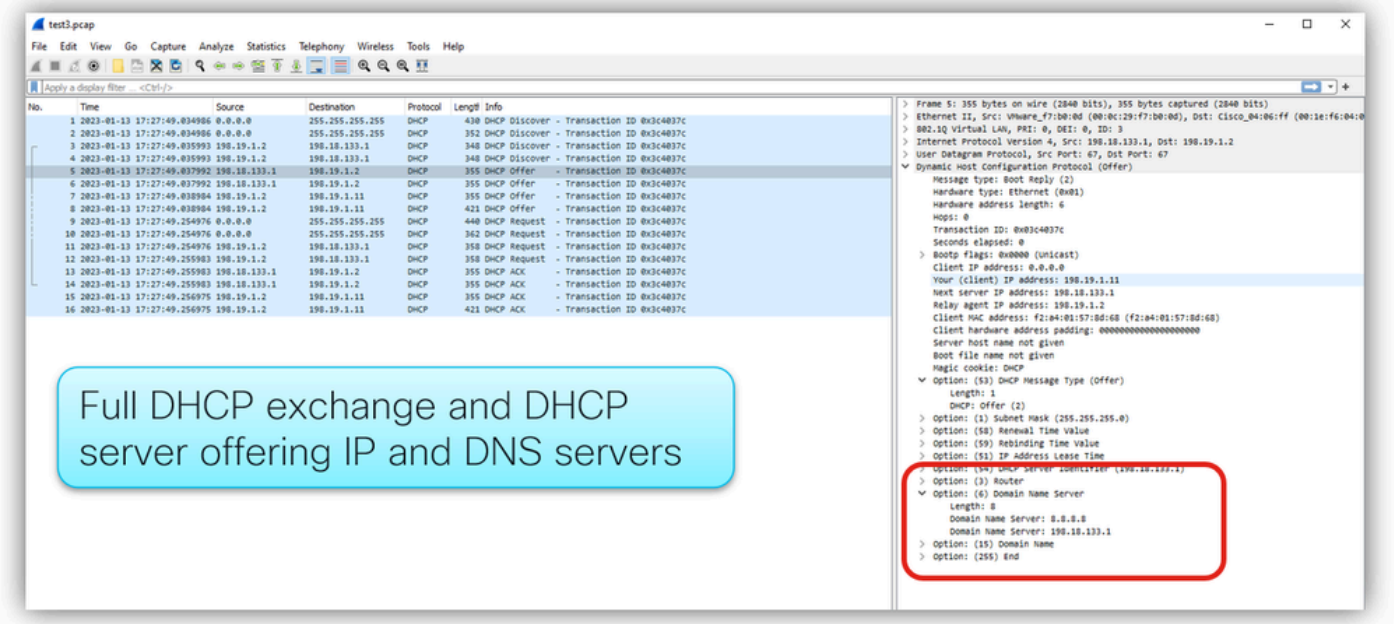
在任何情況下，都需要將ip helper-address命令新增到SVI，無論它位於何處。

另一種方法是在策略配置檔案中配置DHCP伺服器IP地址：



SVI或策略配置檔案的IP幫助程式地址

然後，您可以使用EPC驗證DHCP交換現在是否正常，以及DHCP伺服器是否提供DNS伺服器IP:



DNS伺服器IP的DHCP提供詳細資訊

7 — 是否發生自動重定向？

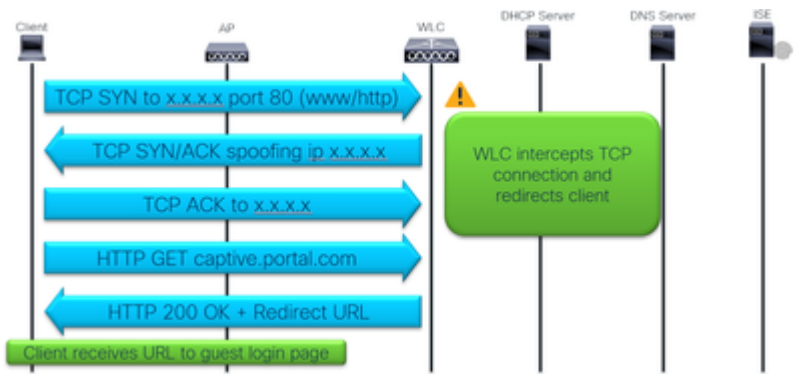
使用WLC EPC驗證DNS伺服器是否響應查詢：

DNS查詢和響應

- 如果重新導向不是自動的，請開啟瀏覽器並嘗試隨機的IP地址。例如10.0.0.1。
- 如果重新導向隨後生效，則可能會遇到DNS解析問題。

還是不工作？

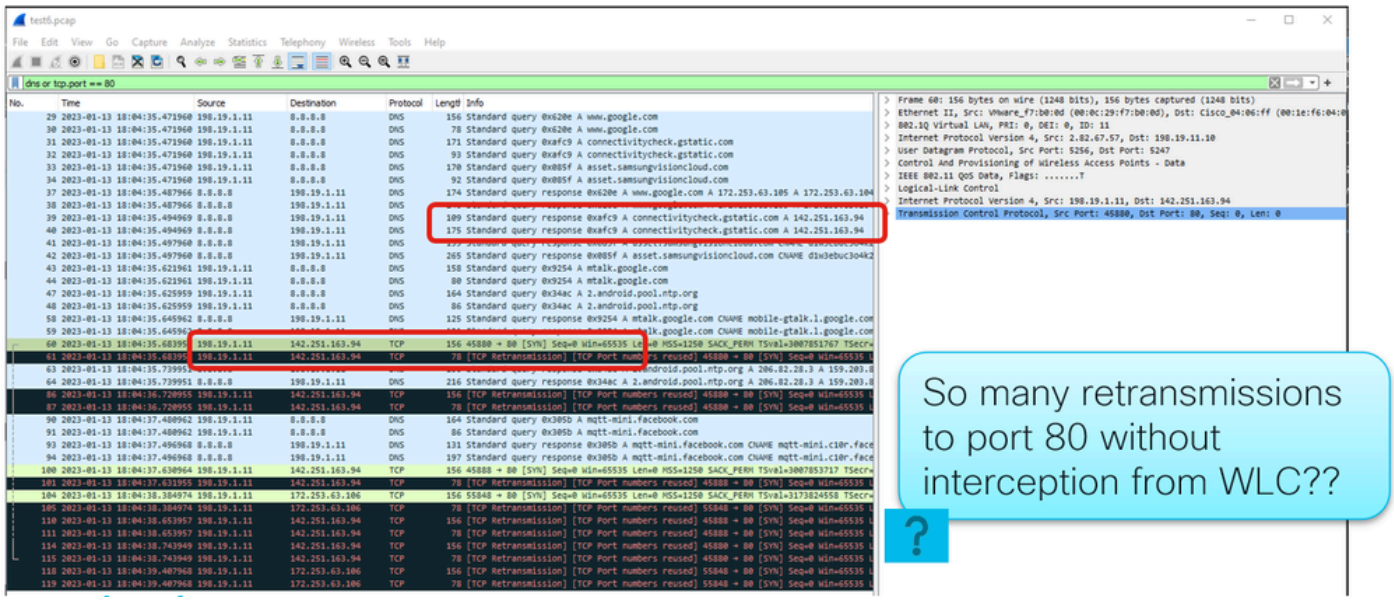
讓我們重新審視一下流程……



流量攔截和重定向

8 — 瀏覽器不顯示登入頁面？

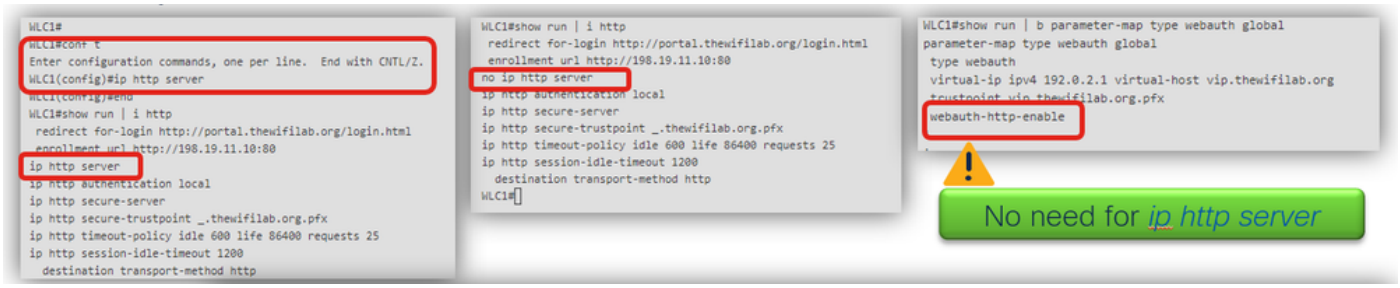
驗證使用者端是否將TCP SYN傳送到連線埠80，然後WLC攔截該連線埠：



TCP重新傳輸到埠80

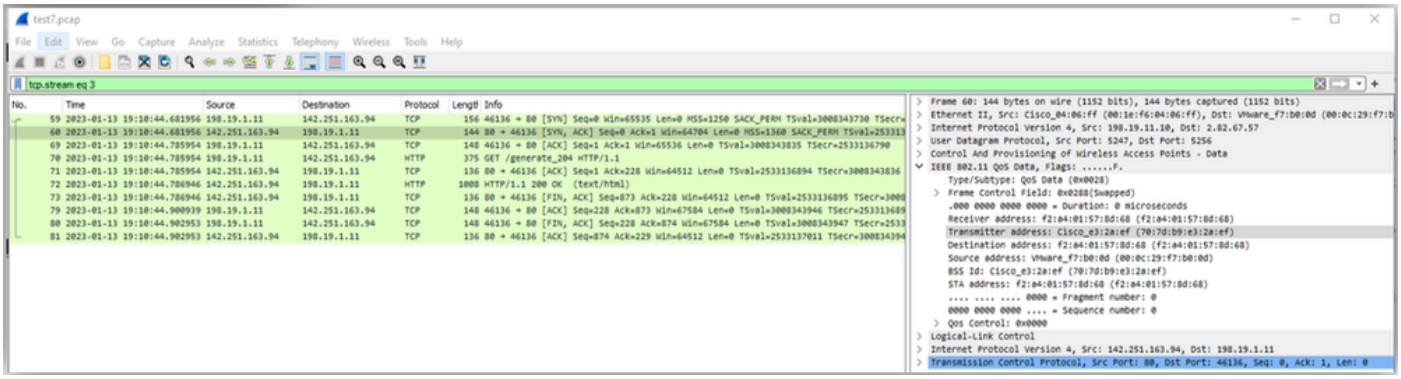
此處我們可以看到使用者端將TCP SYN封包傳送到連線埠80，但沒有取得任何回覆，而且會執行TCP重新傳輸。

確保在全域性配置中使用ip http server命令，或在引數對映全域性配置中使用webauth-http-enable:



http攔截命令

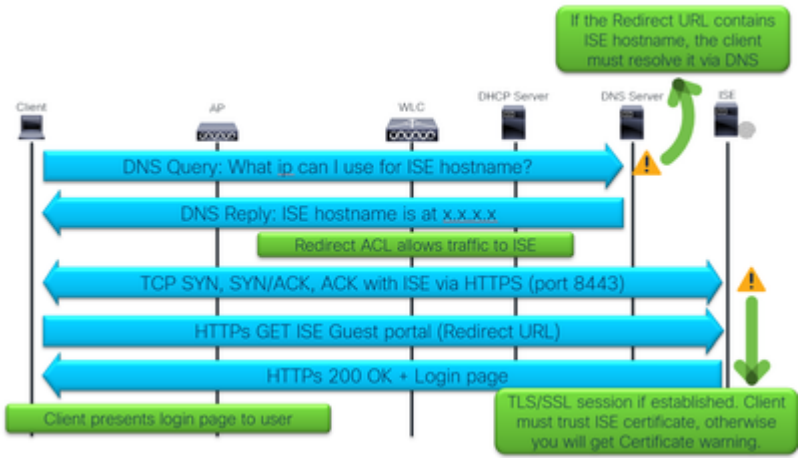
執行此命令後，WLC會攔截TCP並偽裝目的地IP位址，以回複使用者端並進行重新導向。



WLC的TCP攔截

還是不工作？

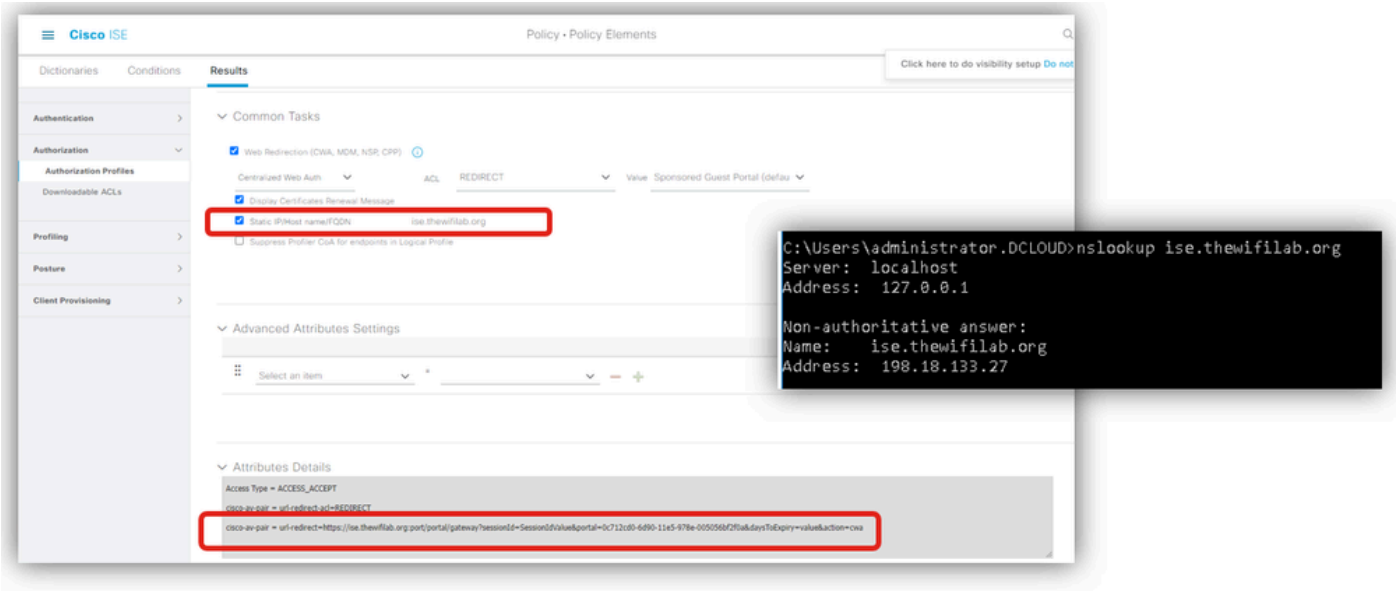
流程中有更多內容……



客戶端登入到ISE訪客登入門戶

9 — 客戶端是否可以解析ISE主機名？

驗證重定向URL是否使用IP或主機名，以及客戶端是否解析ISE主機名：

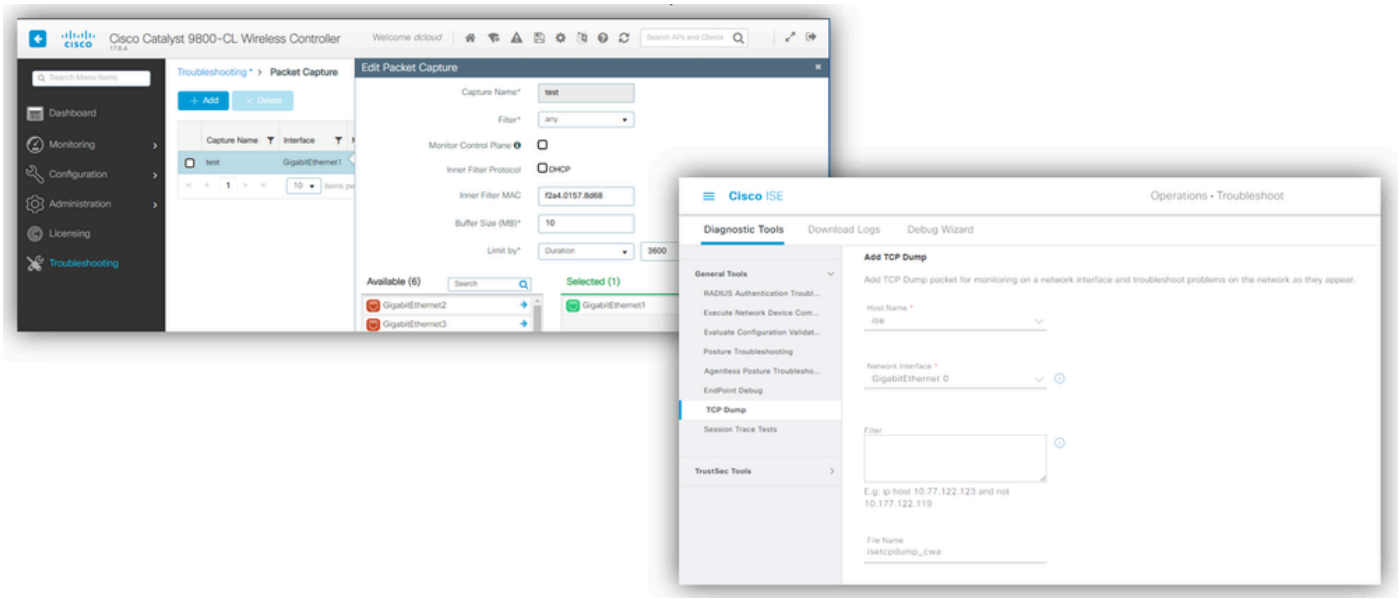


ISE主機名解析

當重定向URL包含ISE主機名時會出現一個常見問題，但客戶端裝置無法將該主機名解析為ISE IP地址。如果使用主機名，請確保可以通過DNS解析。

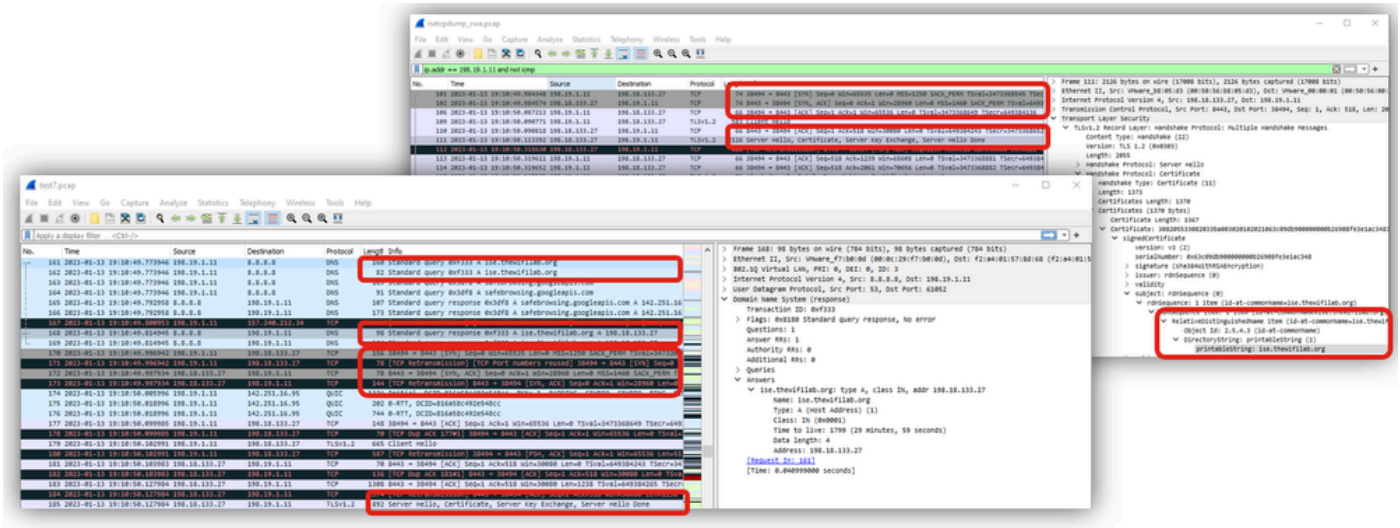
10 — 登入頁面仍無法載入？

如果客戶端流量達到ISE PSN，使用WLC EPC和ISE TCPdump進行驗證。在WLC和ISE上配置並啟動捕獲：



WLC EPC和ISE TCPDump

問題再現後，收集捕獲並關聯流量。在此我們可以看到ISE主機名已解析，然後客戶端和ISE在埠8443上通訊：



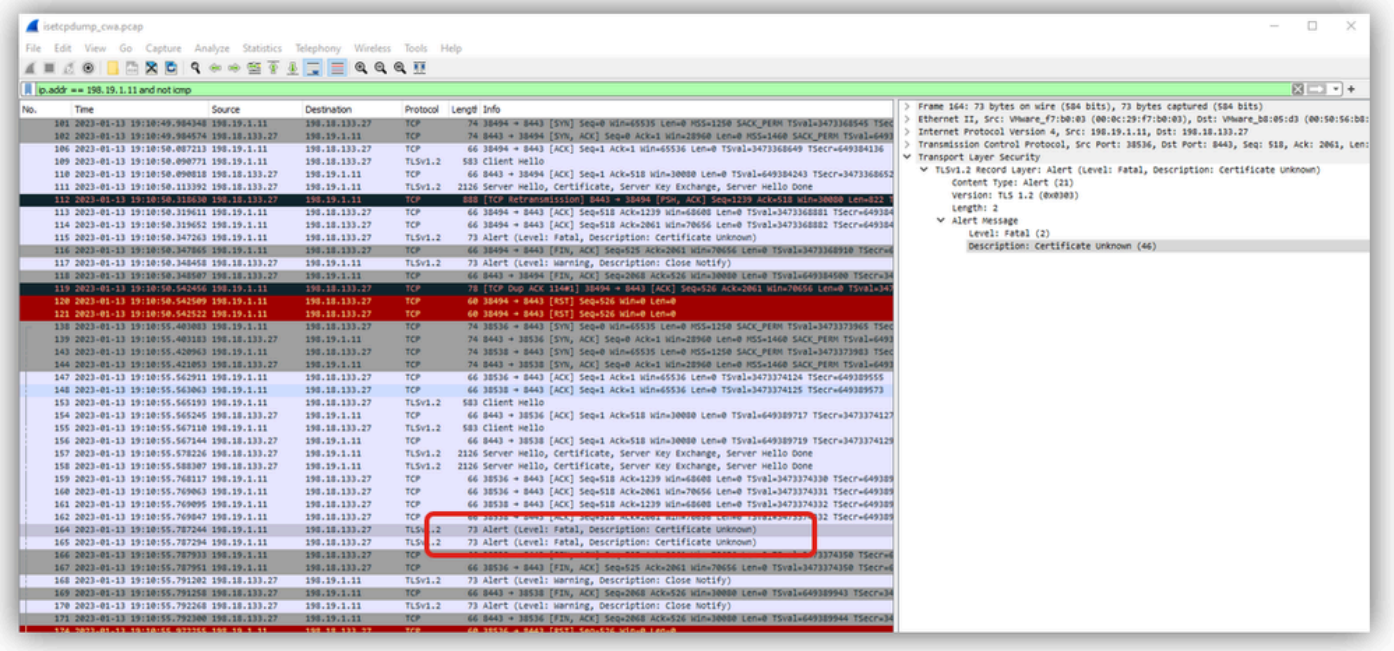
WLC和ISE流量

11 — 為什麼由於證書導致安全違規？

如果您在ISE上使用自簽名證書，則當客戶端嘗試顯示ISE門戶登入頁面時，客戶端會發出安全警告。

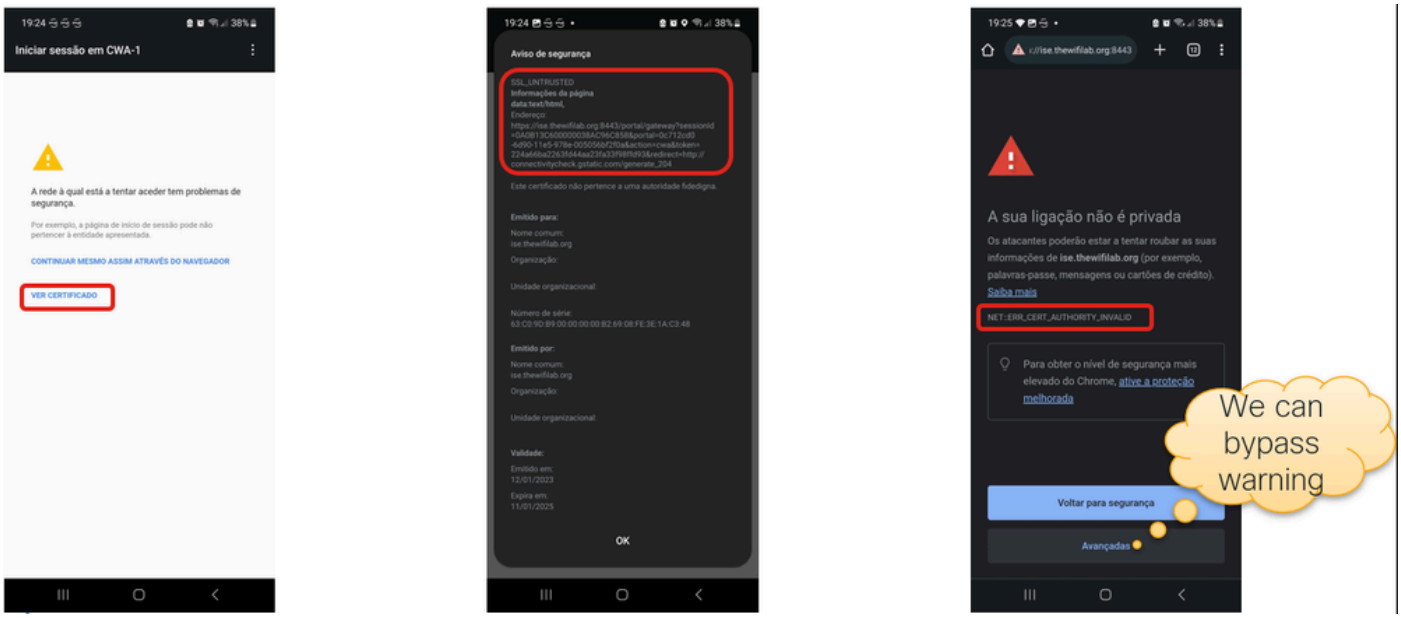
在WLC EPC或ISE TCPdump上，我們可以驗證ISE證書是否受信任。

在本例中，我們可以看到連線從客戶端關閉並發出警報(級別：致命，描述：certificate Unknown)，表示ISE證書未知（受信任）：



ISE不受信任的證書

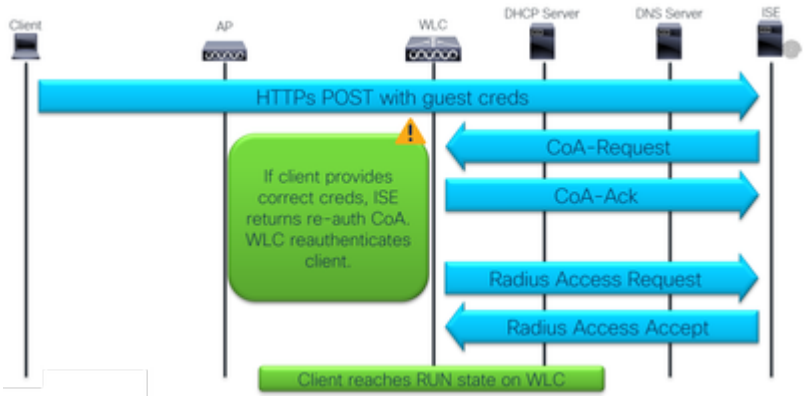
如果在客戶端進行檢查，則會看到以下示例輸出：



不信任ISE證書的客戶端裝置

最後，重定向正在起作用!!但登入失敗……

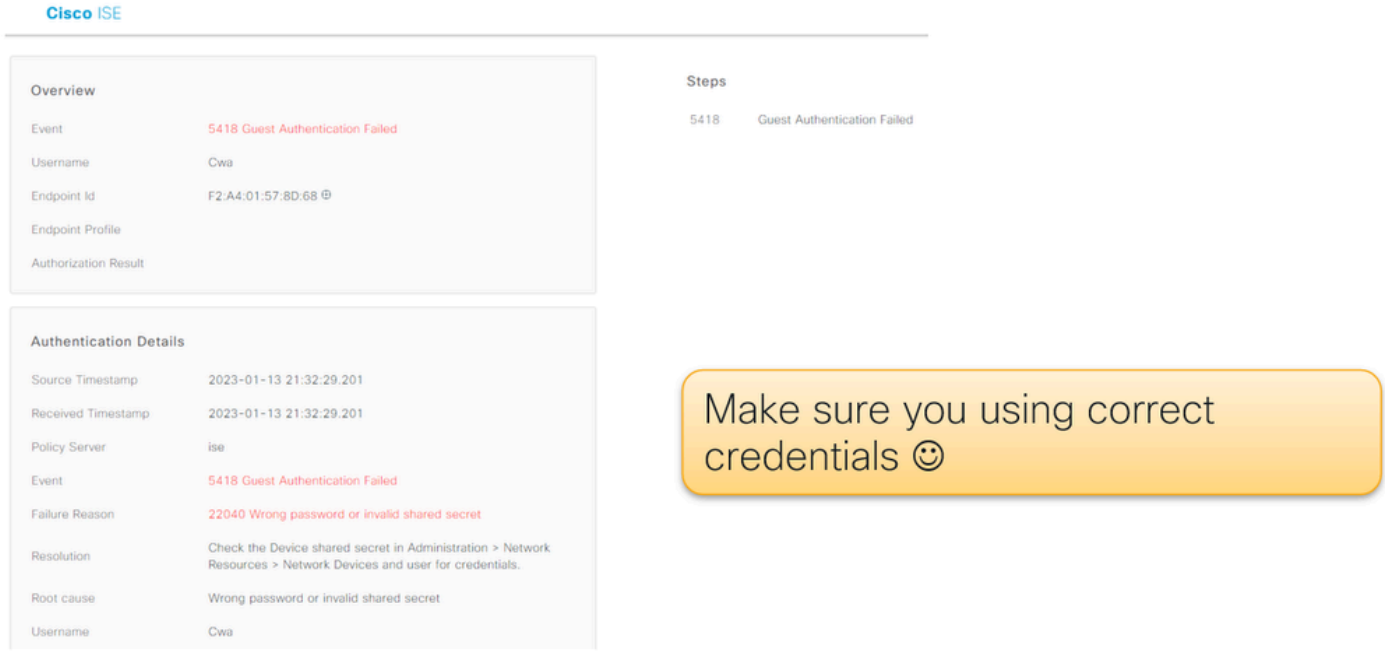
最後一次檢查流量……



客戶端登入和CoA

12 — 訪客登入失敗？

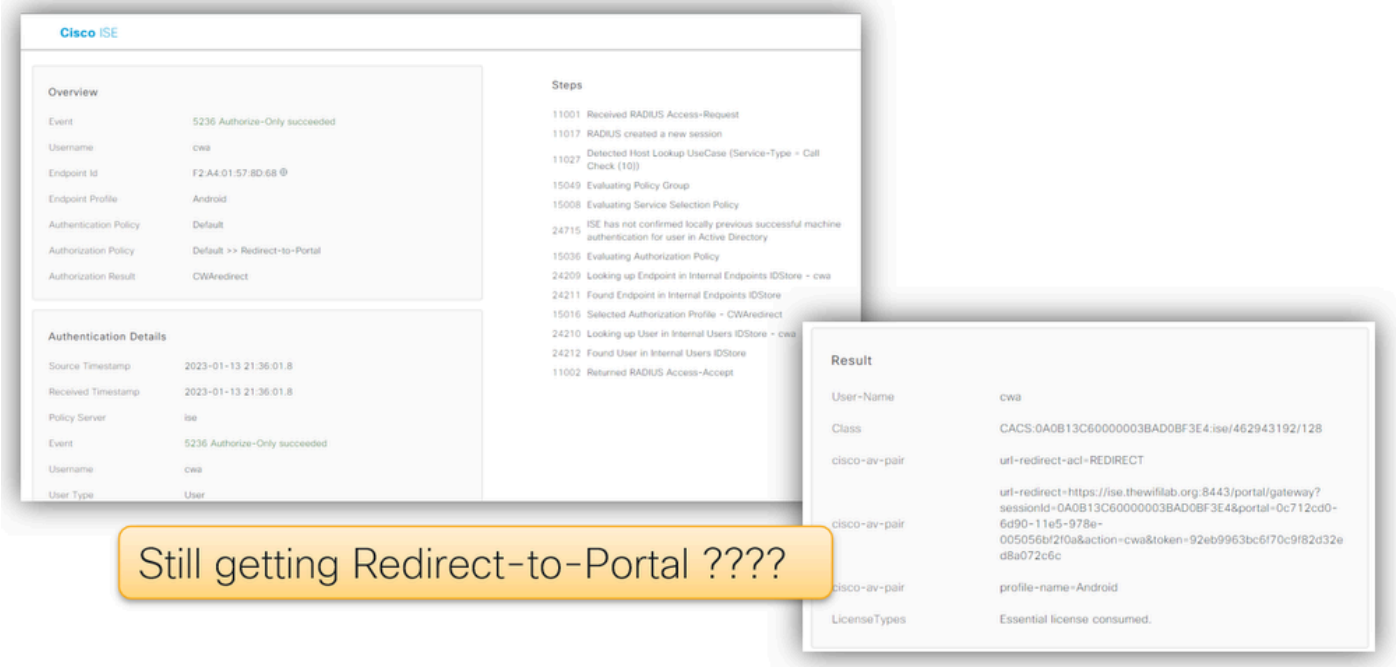
檢查ISE日誌以確認身份驗證失敗。確保憑據正確。



由於憑據錯誤，來賓身份驗證失敗

13 — 登入成功，但不移至RUN?

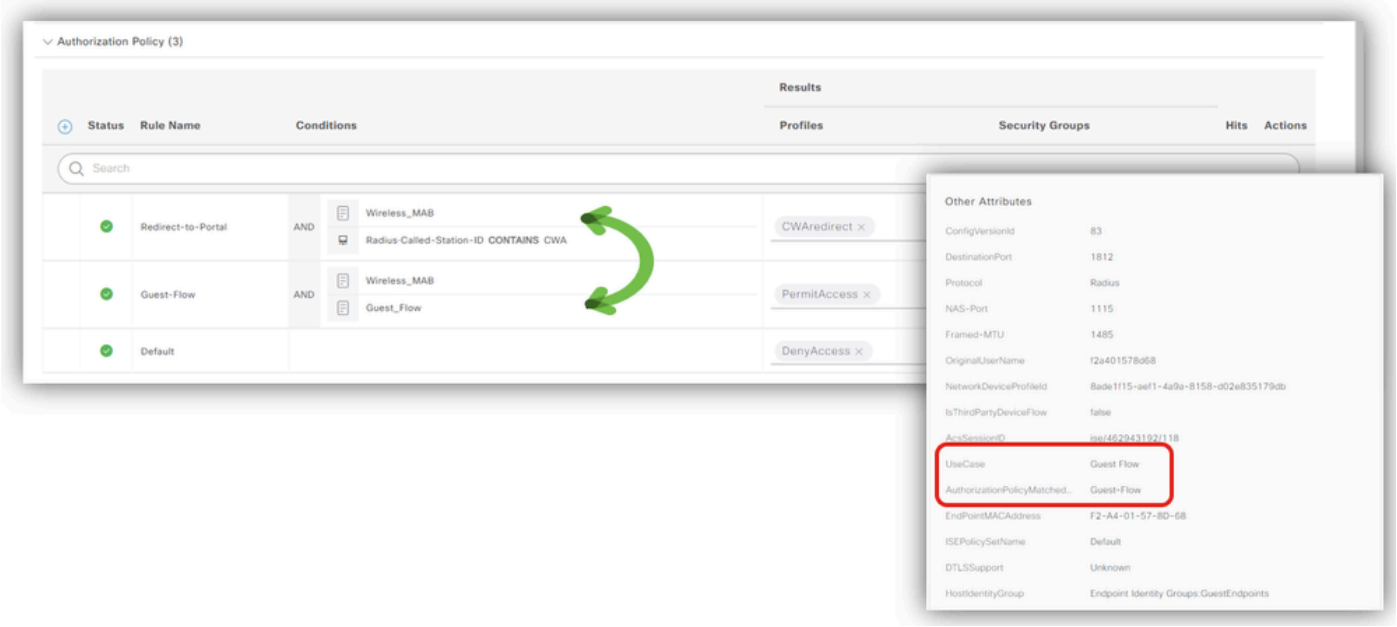
檢查ISE日誌，瞭解身份驗證詳細資訊和結果：



重新導向回圈

在此範例中，我們可以看到使用者端再次取得包含重新導向URL和重新導向ACL的授權設定檔。這會導致重新導向回圈。

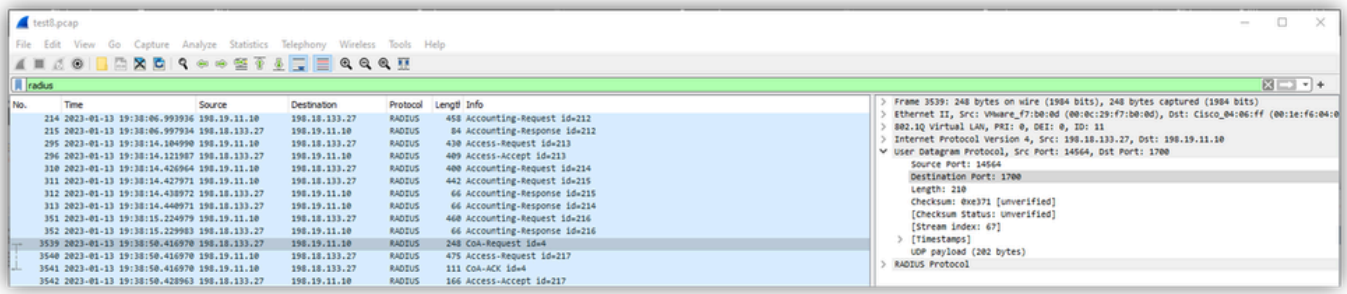
檢查策略集。在重定向之前必須檢查Guest_Flow:



Guest_Flow規則

14 - COA失敗？

使用EPC和ISE TCPDump，我們可以驗證CoA流量。驗證WLC和ISE之間的CoA埠(1700)是否開啟。確保共用金鑰匹配。



CoA流量

附註：在17.4.X及更高版本中，請確保在配置RADIUS伺服器時也配置CoA伺服器金鑰。使用與共用金鑰相同的金鑰（在ISE上預設使用相同的金鑰）。 其目的是為CoA配置一個不同於共用金鑰的金鑰（如果共用金鑰是RADIUS伺服器配置的金鑰）。在Cisco IOS® XE 17.3中，Web UI僅使用與CoA金鑰相同的共用金鑰。

自版本17.6.1起，此連線埠支援RADIUS（包括CoA）。如果要將服務連線埠用於RADIUS，則需要此組態：

<#root>

```
aaa server radius dynamic-author
 client 10.48.39.28
```

vrf

Mgmt-intf

```
 server-key cisco123

interface GigabitEthernet0
```

vrf

forwarding

Mgmt-intf

```
 ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
 server name nicoISE
```

ip

vrf

```
forwarding


Mgmt-intf


ip


radius


source

-interface GigabitEthernet0
```

結論

這是恢復的CWA核對表：

- 確保客戶端位於正確的VLAN上並獲得IP地址和DNS。
  - 在WLC上獲取客戶端詳細資訊並運行資料包捕獲以檢視DHCP交換。
- 驗證客戶端是否可通過DNS解析主機名。
  - 從cmd ping主機名。
- WLC必須在埠80上偵聽
  - 驗證全域命令ip http server或全域引數對映命令webauth-http-enable。
- 若要消除證書警告，請在ISE上安裝受信任證書。
  - 無需在CWA的WLC上安裝受信任憑證。
- ISE高級選項「Continue」處的身份驗證策略（如果未找到使用者）
  - 允許受贊助的訪客使用者連線並獲取URL重定向和ACL。

以及故障排除中使用的主要工具：

- WLC EPC
  - 內部篩選器：DHCP協定，mac地址。
- WLC監控器
  - 檢查客戶端安全詳細資訊。
- WLC RA追蹤
  - 在WLC端使用詳細資訊進行偵錯。
- ISE 即時記錄
  - 身份驗證詳細資訊。
- ISE TCPDump
  - 在ISE PSN介面收集資料包捕獲。

參考資料

[在Catalyst 9800 WLC和ISE上配置中央Web驗證(CWA)]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。