為Aruba WLAN管理員部署Umbrella DNS

目錄

簡介

本文檔介紹如何為Aruba WLAN管理員部署Umbrella DNS服務。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

Aruba Networks針對不同的市場細分市場和部署方案提供以下三個無線LAN(WLAN)產品線和作業系統：

- ArubaOS：適用於大型組織和高密度部署
- Aruba Instant / InstantOS：適用於中小型企業和分散式企業

- Aruba Instant開啟： 適用於家庭和小型辦公室使用者

本文為Aruba WLAN管理員採用和部署Umbrella DNS服務提供了指南。

部署方法

部署方法取決於您的Aruba作業系統以及您計畫如何使用Umbrella。

如果運行上述三個作業系統中的任何一個，可以參考Umbrella使用手冊開始部署Umbrella DNS。影片教程也可用。

如果運行Aruba Instant，您還有另一個選擇，可使用InstantOS中提供的Umbrella網路裝置整合。但是請注意，如果您選擇此選項，則在Umbrella報告(如Activity Search報告)中，您將看不到WLAN上無線客戶端的內部/私有IP地址。來自客戶端的DNS查詢對映到Umbrella中即時AP群集的網路裝置標識，並且有關各個客戶端的資訊不可用。從Umbrella雲的角度來看，DNS查詢可能來自即時AP集群，而不是Wi-Fi客戶端。

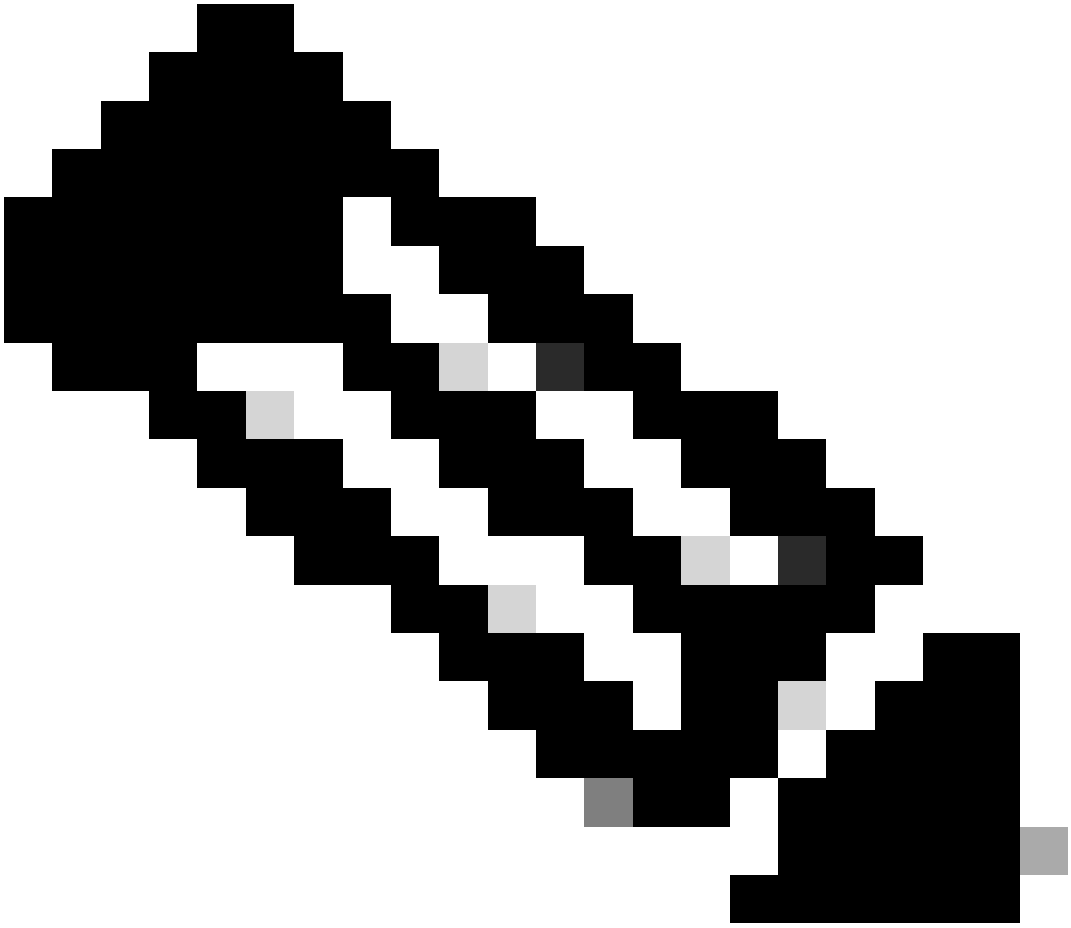
因此，如果您需要跟蹤單個客戶端的DNS查詢或為WLAN上的單個客戶端定製DNS策略，可以通過Umbrella DNS使用手冊中介紹的標準方法部署Umbrella（無需通過Aruba Instant使用網路裝置整合），並考慮將Umbrella虛擬裝置納入部署計劃。

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

4403300507924

Aruba即時整合

Aruba Instant的Umbrella(OpenDNS)網路裝置整合在這樣的環境中非常有用：連線到即時AP群集的所有Wi-Fi客戶端都受制於單一的Umbrella DNS策略，而且無需在Umbrella報告中檢視單個客戶端的DNS查詢。本節介紹如何設定整合。



附註：該整合使用Umbrella網路裝置API的舊版本。舊版不要求客戶從其Umbrella控制面板生成API令牌，但新版需要。

Umbrella傳統API已於2023-09-01停止使用，此後不再提供整合支援。如果您在2023-09-01年後遇到任何整合問題，請完成部署指南中的「入門」部分，以在不使用整合的情況下部署Umbrella。

使用整合需要滿足以下要求：

- AP需要運行InstantOS版本8.10.0.1或更高版本（截至2022年5月）。
- 用於整合的Umbrella儀表板帳戶需要具有Full Admin角色。
- 該帳戶的電子郵件地址不能與多個Umbrella儀表板關聯。如果您不確定該電子郵件地址是否只與單個控制面板關聯，可以聯系思科保護傘支持進行驗證。
- 無法為帳戶啟用單一登入(SSO)和雙因素身份驗證(2FA)。
- 如果AP和Internet之間存在網路安全裝置（如防火牆），則裝置需要允許到208.67.220.220、208.67.222.222、67.215.92.210和146.112.255.152/29(.152 ~ .159)進行未經過濾和未經檢查的連線。

組態

在高級別上，啟用整合需要四個配置步驟：

1.設定AP群集的名稱

2.輸入帳戶憑據

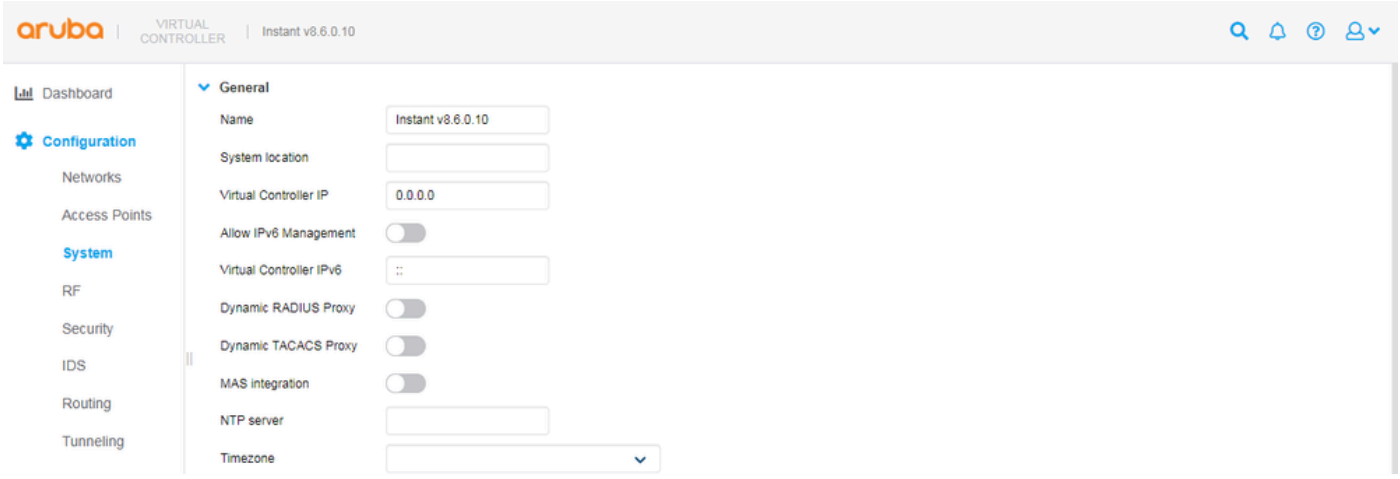
3.攔截DNS查詢

4.應用DNS策略

設定AP群集的名稱

當即時群集首次成功將自身註冊到Umbrella儀表板時，網路裝置條目將新增到部署>網路裝置下的Umbrella儀表板中。新條目的裝置名稱來自在群集的虛擬控制器上配置的系統名稱。

要在即時虛擬控制器上設定系統名稱，請導航到Configuration > System。



4404011628308

請注意，在初始註冊期間，僅複製一次名稱值。如果系統/裝置名稱隨後在Instant或Umbrella端發生更改，則必須手動更新另一端的名稱。

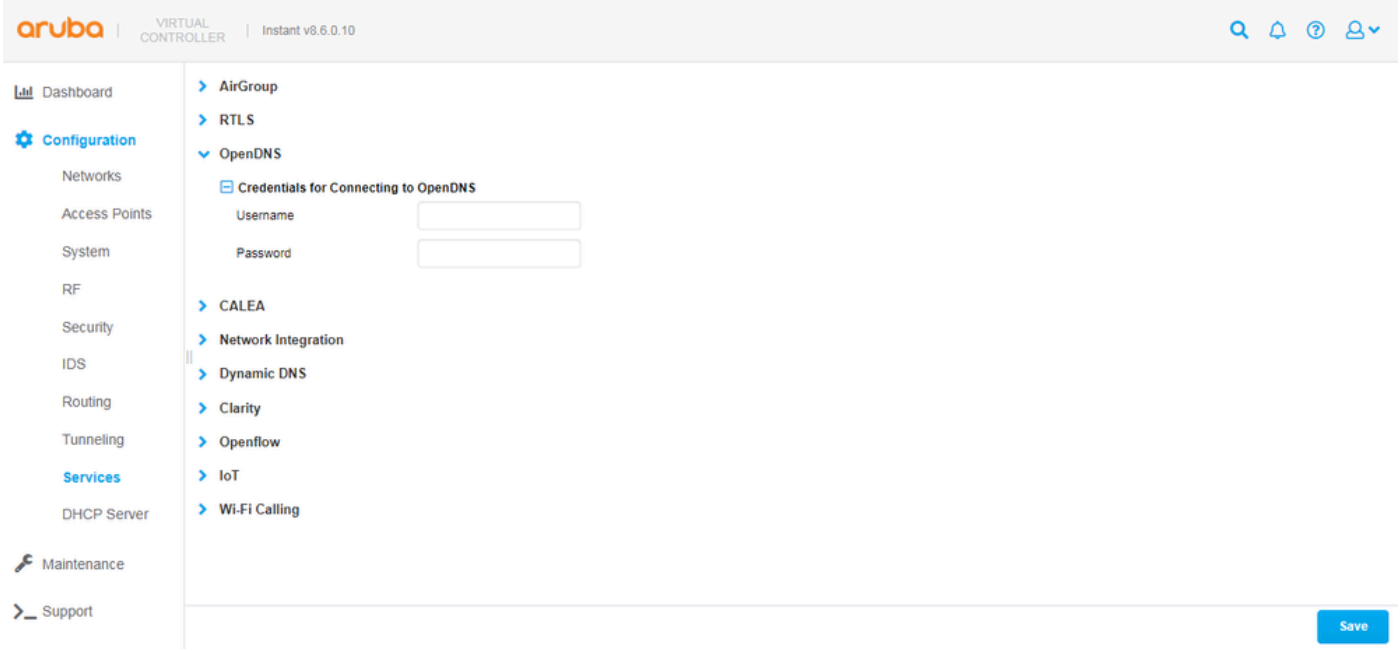
輸入帳戶憑據

如果滿足必要條件部分中列出的要求，則可以將即時群集作為網路裝置新增到Umbrella控制面板中。要從群集的虛擬控制器執行以下操作：

1.導覽至Configuration > Services > OpenDNS。

2.輸入Umbrella帳戶的登入憑據。

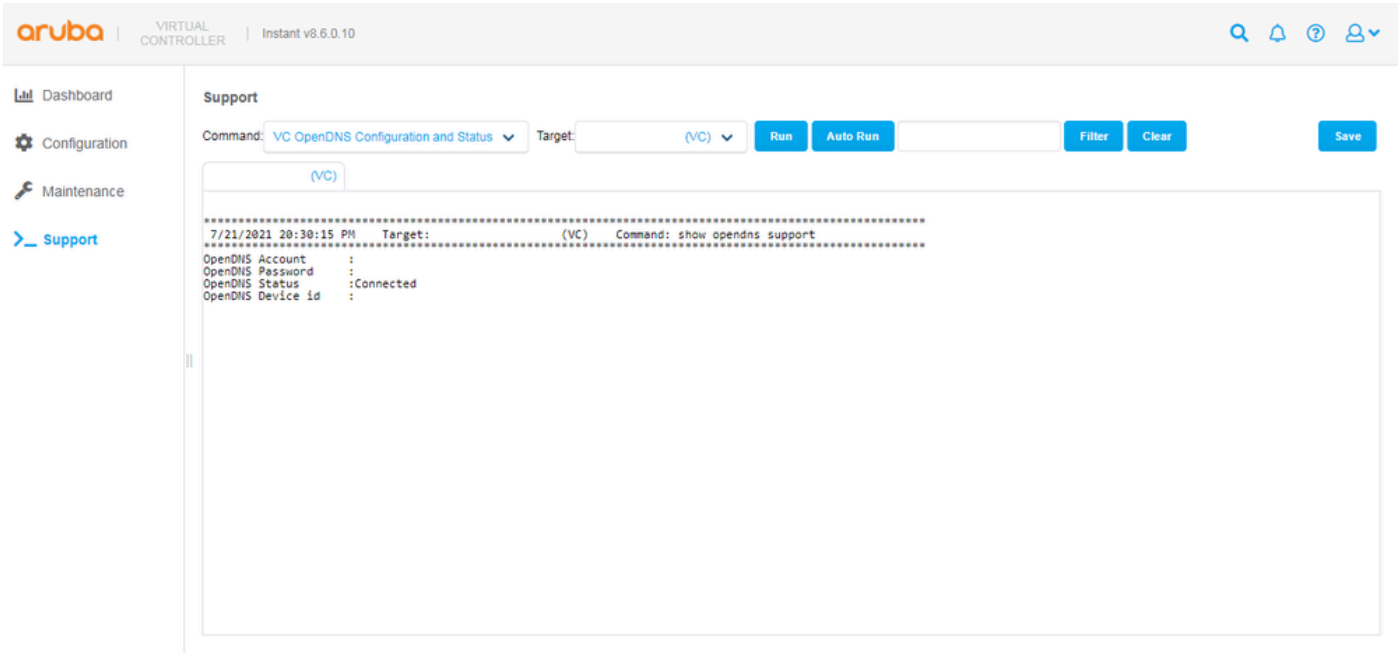
3.選擇儲存。



4404019266196

如果虛擬控制器(VC)成功連線到Umbrella，則當您導航到Support並運行「VC OpenDNS Configuration and Status」(`show opendns support`)命令時，可以看到一個Connected狀態。

您還可以看到裝置ID，該裝置ID由Umbrella在建立新網路裝置並將其儲存到即時VC配置中時生成。後一部分是重要的。由於每個即時群集都需要具有唯一的Umbrella網路裝置ID，因此不能將裝置ID從一個群集的配置複製到另一個群集。有效的裝置ID通常有16位數。

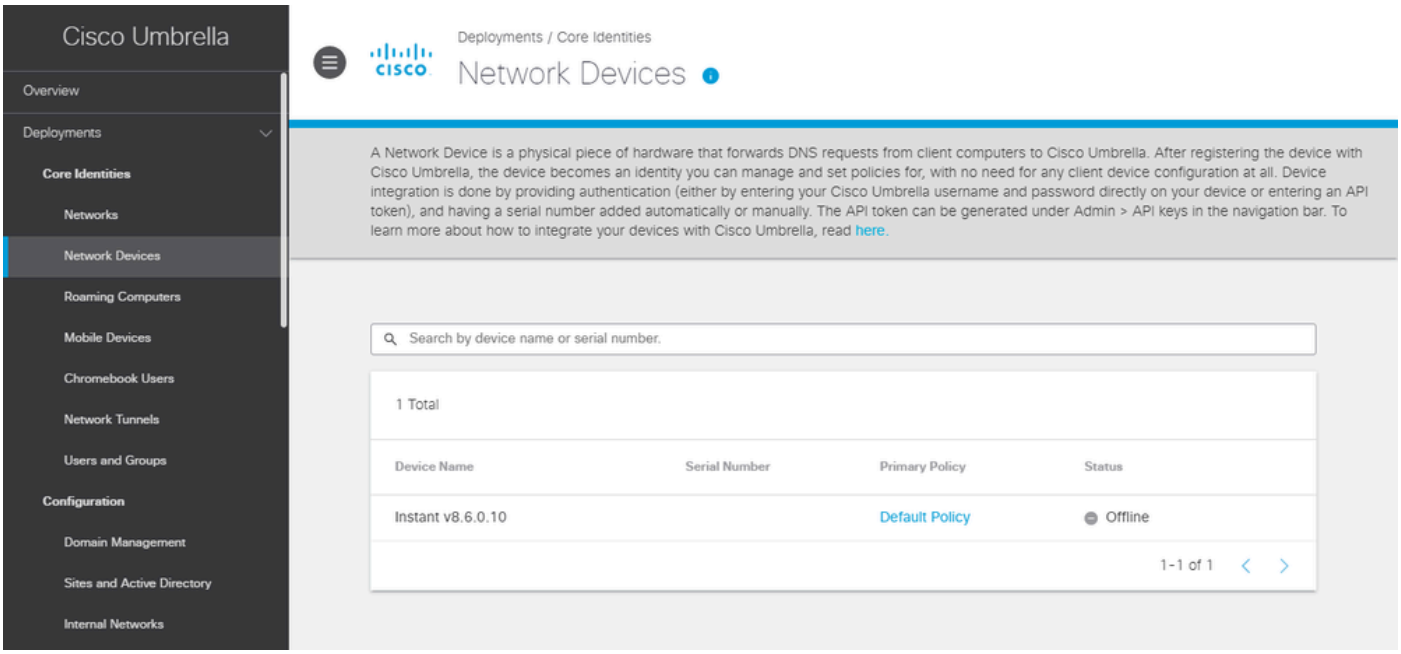


4404019268116

如果命令輸出顯示Not connected狀態，您可以嘗試通過運行「AP技術支援轉儲」(`show tech-support`)和「AP技術支援轉儲補充」(`show tech-support supplemental`)命令，然後搜尋日誌中的「opendns」來找出原因。也可與Aruba TAC共用命令輸出以進行故障排除。

如果一切正常，您可以在Umbrella控制面板中的部署>網路裝置下看到一個新條目，您可以在該條目

中按名稱搜尋即時AP集群，或者刪除現有條目（如果您希望生成新的裝置ID）。



4404011658516

攔截DNS查詢

確認已將群集作為網路裝置成功新增到Umbrella控制面板後，可以將群集設定為開始攔截從無線客戶端（連線到群集中的AP）傳送的DNS查詢。 設定後，無論無線客戶端的NIC上配置了哪些DNS伺服器IP地址，客戶端的DNS查詢都會被群集擷取，並轉發到Umbrella的任播解析器208.67.220.220和208.67.222.222。

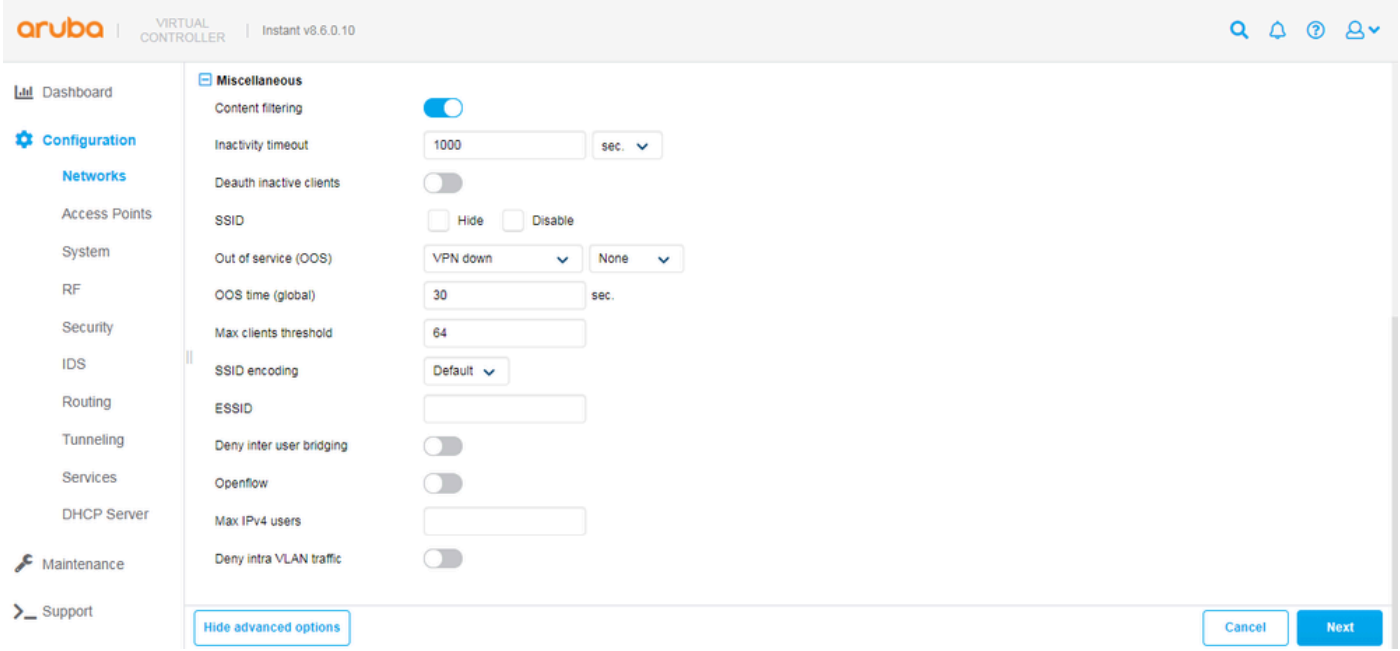
要攔截DNS查詢，請執行以下操作：

1.在Configuration > Networks下導航到群集的虛擬控制器。

2.選擇無線網路。

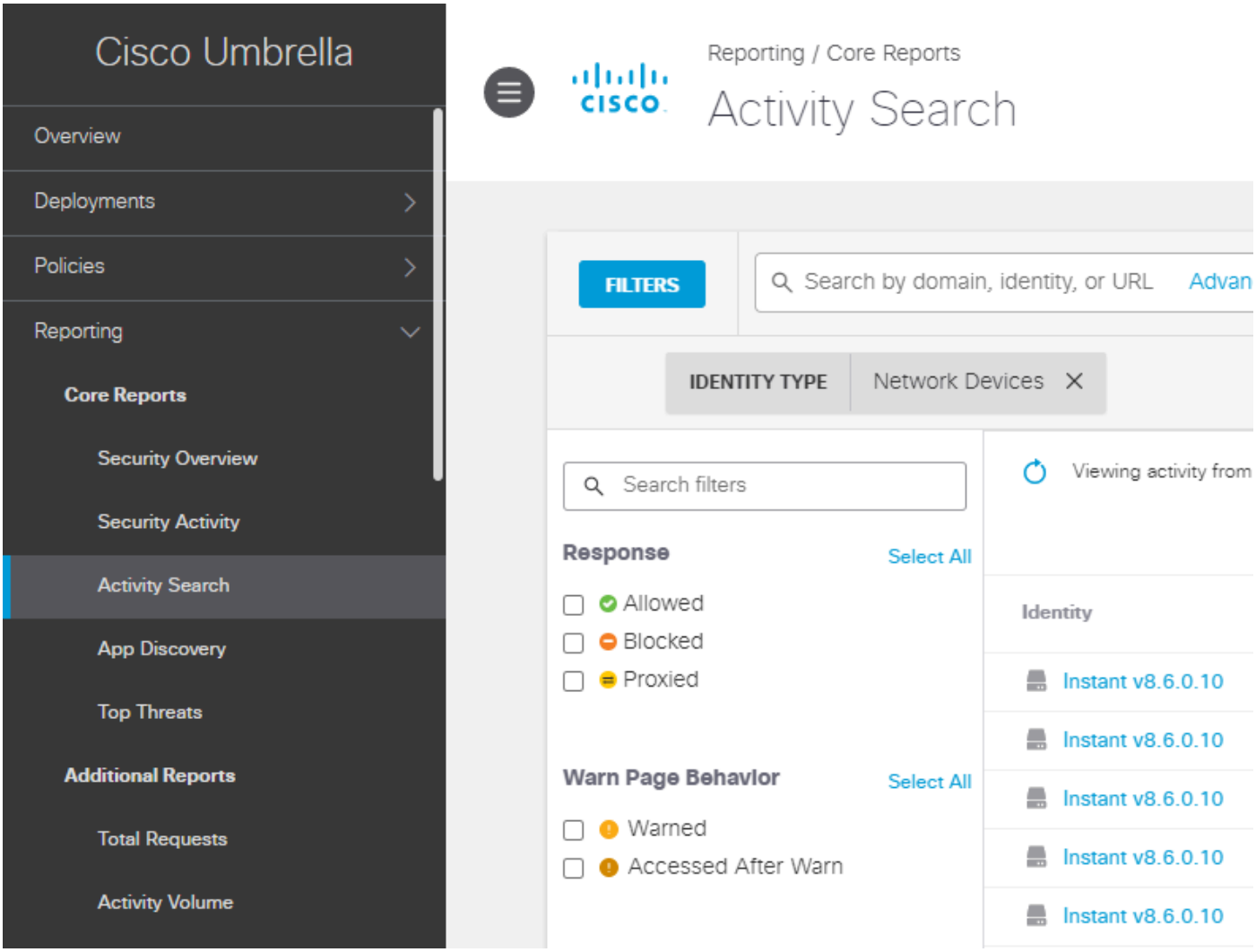
3.編輯網路，選擇Show advanced options，然後滾動到Miscellaneous部分。

4.啟用內容過濾選項，並繼續選擇下一步，直到可以選擇完成按鈕來儲存更改。



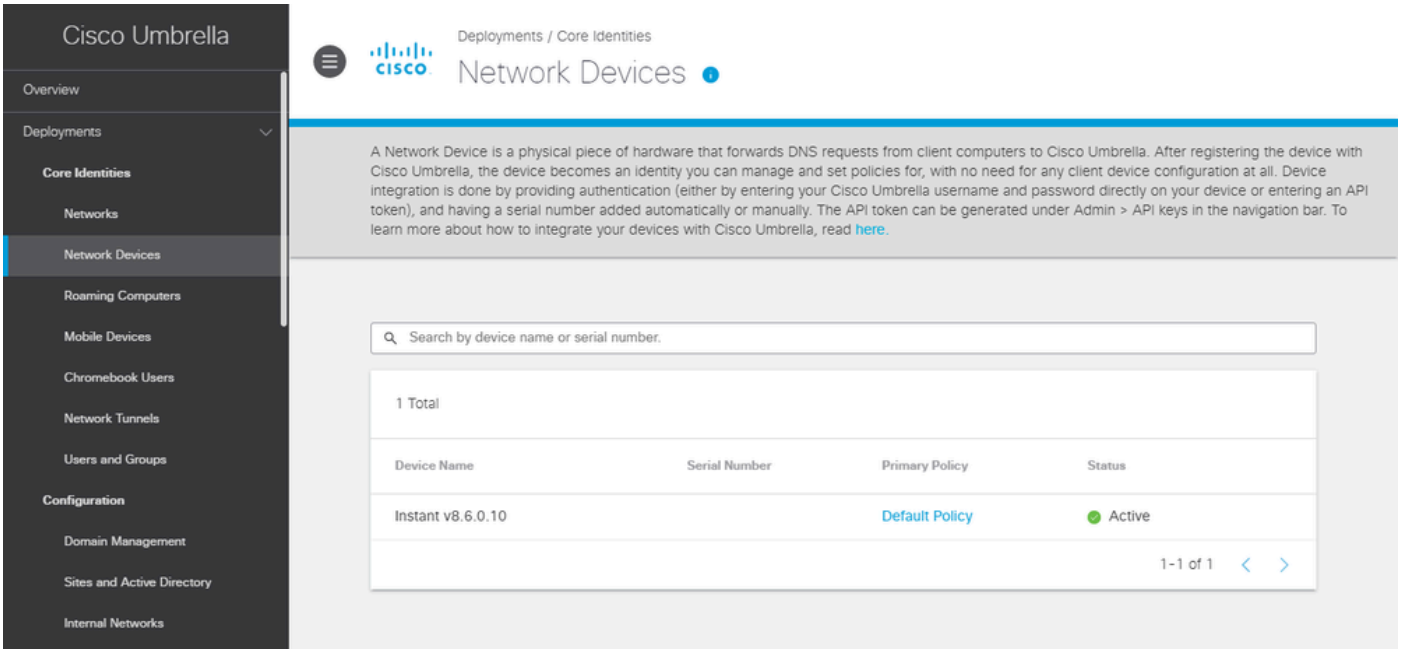
4404011668500

啟用該選項後，您可以在Umbrella控制面板中的Reporting > Activity Search下檢視DNS查詢。查詢的標識可以對映到網路裝置名稱，通常是AP群集虛擬控制器上配置的系統名稱。請注意，可能需要一些時間（大約15分鐘）才能在控制面板GUI中處理和顯示查詢。



4404011721620

在Deployments > Network Devices下的Umbrella控制面板中，裝置最多可能需要24小時才能更改為活動/聯機狀態。網路裝置的狀態僅表示DNS查詢是否被裝置截獲並在之前的24小時內轉發到Umbrella，並不影響裝置與Umbrella的通訊方式。離線/非活動狀態可能僅僅意味著過去24小時內沒有無線客戶端連線到AP群集，並且無法阻止群集使用Umbrella服務。

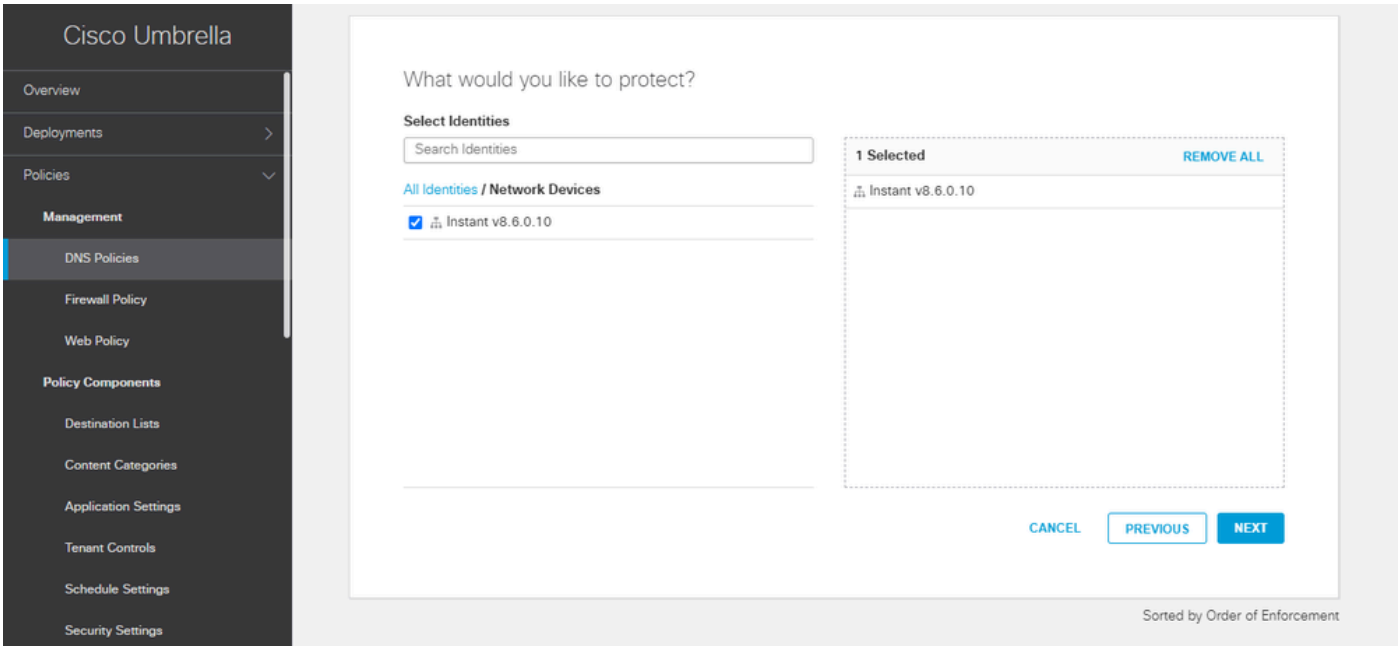


4404011756308

應用DNS策略

在Umbrella中，「Default Policy」（預設策略）自動包括新增到儀表板的所有標識（如網路裝置）。如果部署中的所有AP群集都受同一策略約束，則無需建立其他DNS策略。如果屬於這種情況，請跳至下一節。

或者，如果您希望將自定義策略應用於特定網路裝置，則需要在Policies > All Policies(DNS Policies)下的Umbrella控制面板中新增新策略，然後在策略中選擇網路設備。



4404011773588

當DNS Policies(All Policies)頁面上有多個策略時，這些策略將自上而下按第一個匹配項進行評估。有關更多資訊，請參閱策略優先文檔和定義策略文檔的最佳實踐。

內部DNS

在存在內部DNS伺服器，並且要將特定（內部）域的DNS查詢轉發到內部DNS伺服器的環境中，可以在即時中使用Enterprise Domains功能。

啟用此功能後，AP群集可以繼續攔截DNS查詢，但指定域的查詢無法再轉發到Umbrella。相反，它們可以轉發到最初在無線客戶端的NIC上配置的DNS伺服器IP地址（如通過DHCP）。 此功能類似於標準Umbrella部署方法(使用虛擬裝置)中提供的Internal Domains功能，其中不使用Aruba Instant整合。

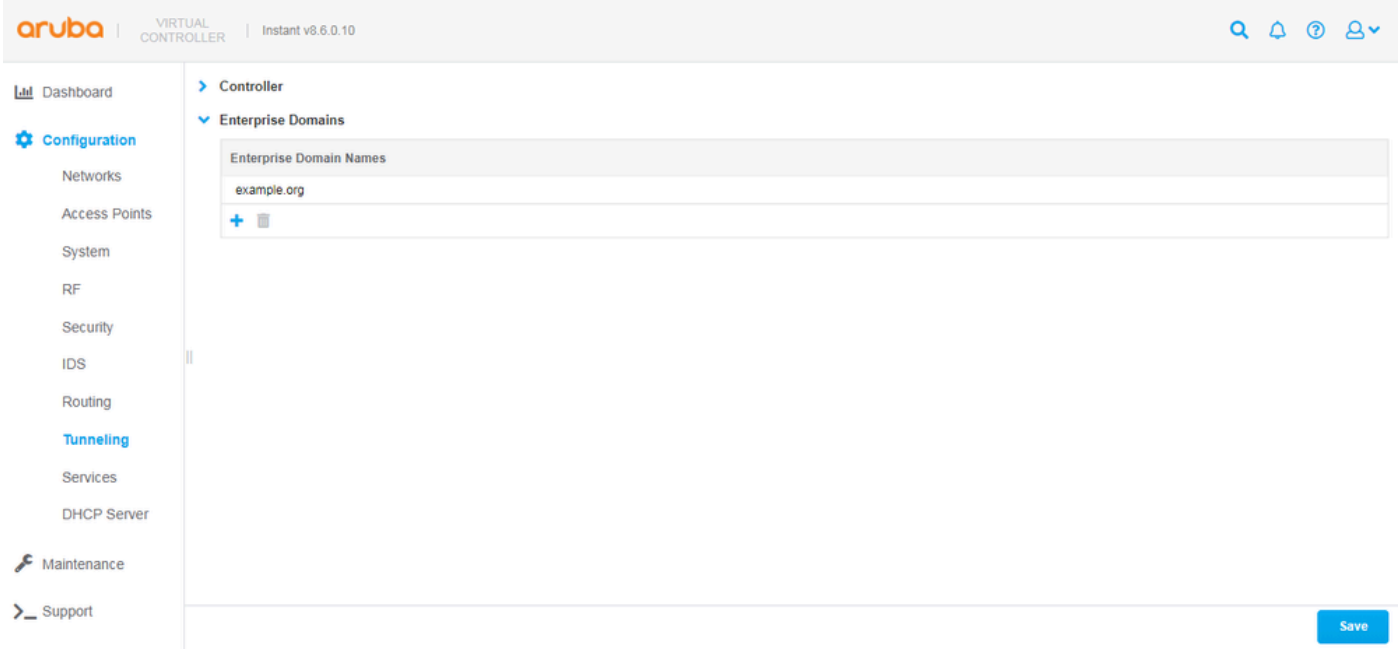
要在即時虛擬控制器上配置功能，請執行以下操作：

1.導覽至Configuration > Tunneling > Enterprise Domains。

2.向「企業域名」清單新增域或從「企業域名」列表中刪除域。

3.選擇儲存。

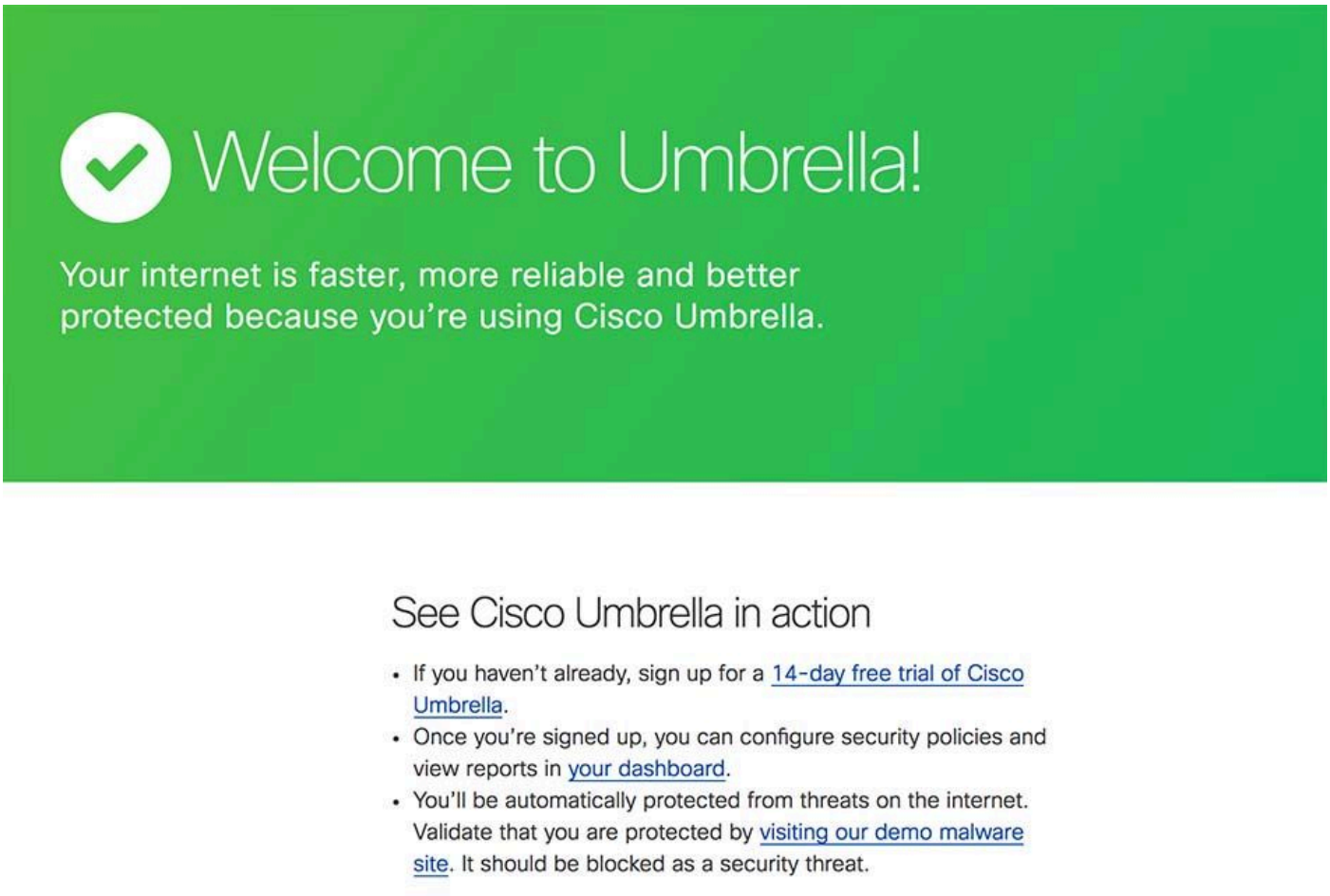
對於新增到清單中的任何域，都有一個隱式萬用字元，因此example.org表示*.example.org。



4404238114452

驗證

無論您是使用本指南的「部署概述」部分中提到的標準方法在WLAN上部署Umbrella，還是使用「Aruba即時整合」部分中描述的整合，您都可以通過從其中一個客戶端瀏覽到 https://welcome.umbrella.com/來驗證無線客戶端是否正在使用Umbrella DNS。然後，您會看到一個與Umbrella文檔中顯示的螢幕截圖類似的綠色勾選。



4404011960212

或者，您也可以在無線客戶端的命令提示符下運行此命令來驗證這一點。

```
nslookup -type=txt debug.opendns.com.
```

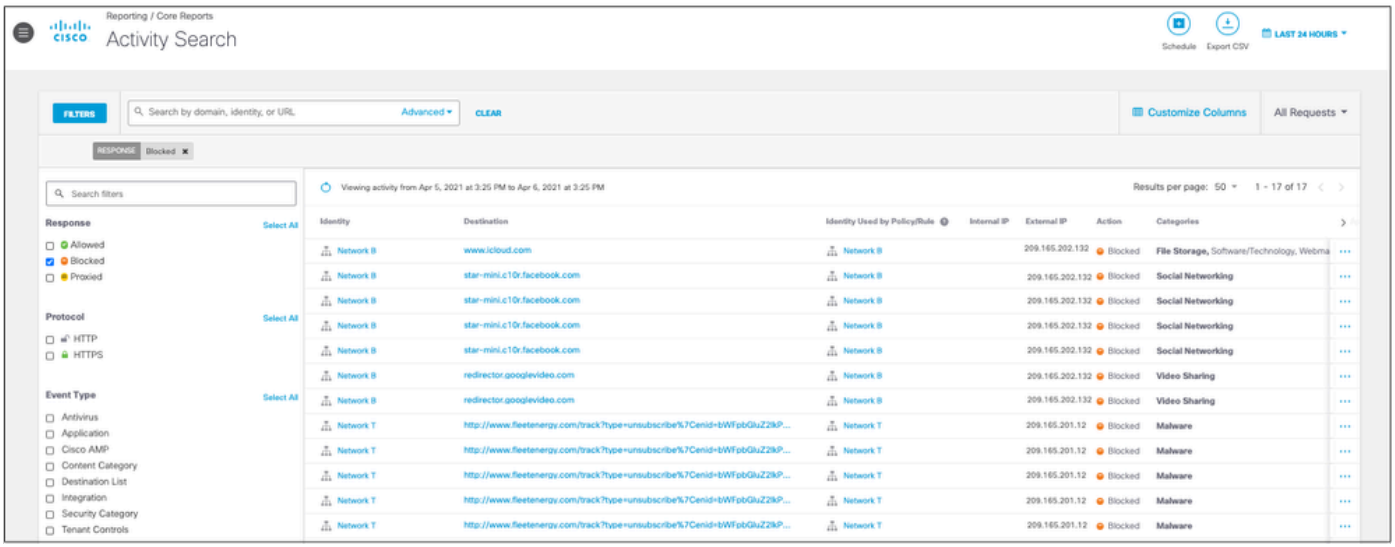
您可以看到包含大量文本行的輸出，類似於以下螢幕截圖：

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

從命令輸出中，您可以在「orgid」或「organization id」行中看到Umbrella控制面板的組織ID，如果使用即時整合，則可以看到包含裝置ID的額外「裝置」行。

要檢視Umbrella控制面板中的DNS查詢，請導航至Reporting > Activity Search。請注意，可能需要一些時間（約15分鐘）才能在儀表板GUI中顯示查詢。Umbrella文檔中提供了有關如何使用Activity Search的說明。



4404019393044

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）。