

# 瞭解Catalyst 9800無線LAN控制器上的AVC

## 目錄

---

[簡介](#)

[必備條件](#)

[有關應用可視性與可控性\(AVC\)的資訊](#)

[AVC的工作原理](#)

[網路型應用程式辨識\(NBAR\)](#)

[在策略配置檔案上啟用NBAR協定](#)

[升級9800 WLC上的NBAR](#)

[Netflow](#)

[Flexible Netflow](#)

[流量監控器](#)

[AVC支援的存取點](#)

[支援不同的9800部署模式](#)

[在9800上實施AVC時的限制](#)

[網路拓撲](#)

[本地模式下的AP](#)

[處於flex模式的AP](#)

[9800 WLC上的AVC配置](#)

[本地導出器](#)

[外部NetFlow收集器](#)

[使用Cisco Catalyst Center在9800 WLC上配置AVC](#)

[驗證AVC](#)

[在9800](#)

[在DNAC上](#)

[在外部NetFlow收集器上](#)

[示例1：Cisco Prime as Netflow Collector](#)

[示例2：第三方NetFlow收集器](#)

[流量控制](#)

[疑難排解](#)

[日誌收集](#)

[WLC日誌](#)

[AP日誌](#)

[相關資訊](#)

---

## 簡介

本檔案介紹Cisco Catalyst 9800 WLC上的應用可視性與可控性(AVC)，其可實現應用流量的精確管理。

## 必備條件

思科建議您瞭解以下主題：

- Cisco WLC 9800的基本知識。
- 本地和Flex連線模式AP的基本知識。
- 存取點必須具備AVC功能。（不適用於本地模式AP）
- 要使AVC (QoS)的控制部分正常工作，必須配置帶FNF的應用可視性功能。

## 有關應用可視性與可控性(AVC)的資訊

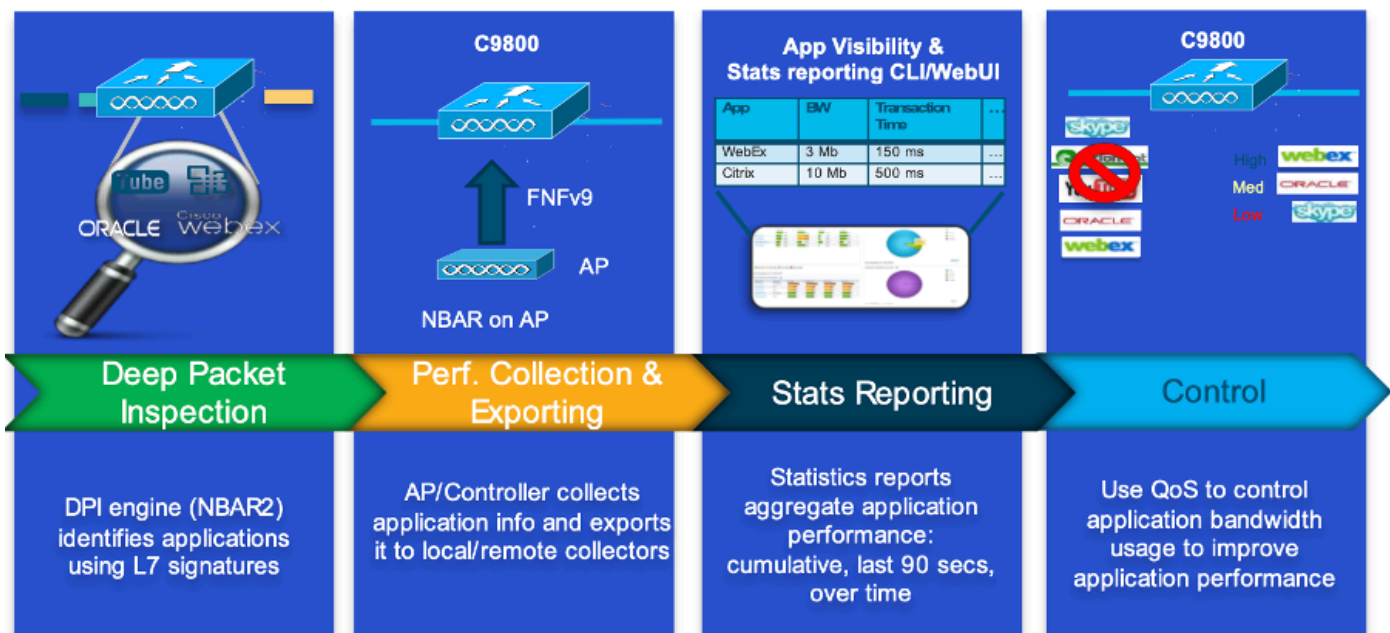
應用可視性與可控性(AVC)是思科在無線和有線網路中用於深度資料包檢測(DPI)技術的領先方法。使用AVC，您可以執行即時分析和建立策略來有效減少網路擁塞、最大限度地減少成本高昂的網路鏈路使用，並避免不必要的基礎設施升級。簡而言之，AVC使使用者能夠透過基於網路的應用辨識(NBAR)實現全新級別的流量辨識和整形。在9800 WLC上運行的NBAR軟體套件用於DPI，並且使用Flexible NetFlow (FNF)報告結果。

除了可視性之外，AVC還能夠區分不同型別流量的優先順序、阻止或限制。例如，管理員可以建立優先安排語音和影片應用的策略，以確保服務品質(QoS)或限制非關鍵應用在高峰工作時間可用的頻寬。它還可以與其他思科技術整合，例如用於基於身份的應用策略的思科身份服務引擎(ISE)以及用於集中管理的Cisco Catalyst Center。

### AVC的工作原理

AVC利用FNF和NBAR2引擎等先進技術實現DPI。透過使用NBAR2引擎分析和辨識流量流，特定流量會使用可辨識的協定或應用進行標籤。控制器會收集所有報告，並透過show命令、Web UI或其他NetFlow導出消息將其顯示給外部NetFlow收集器（如Prime）。

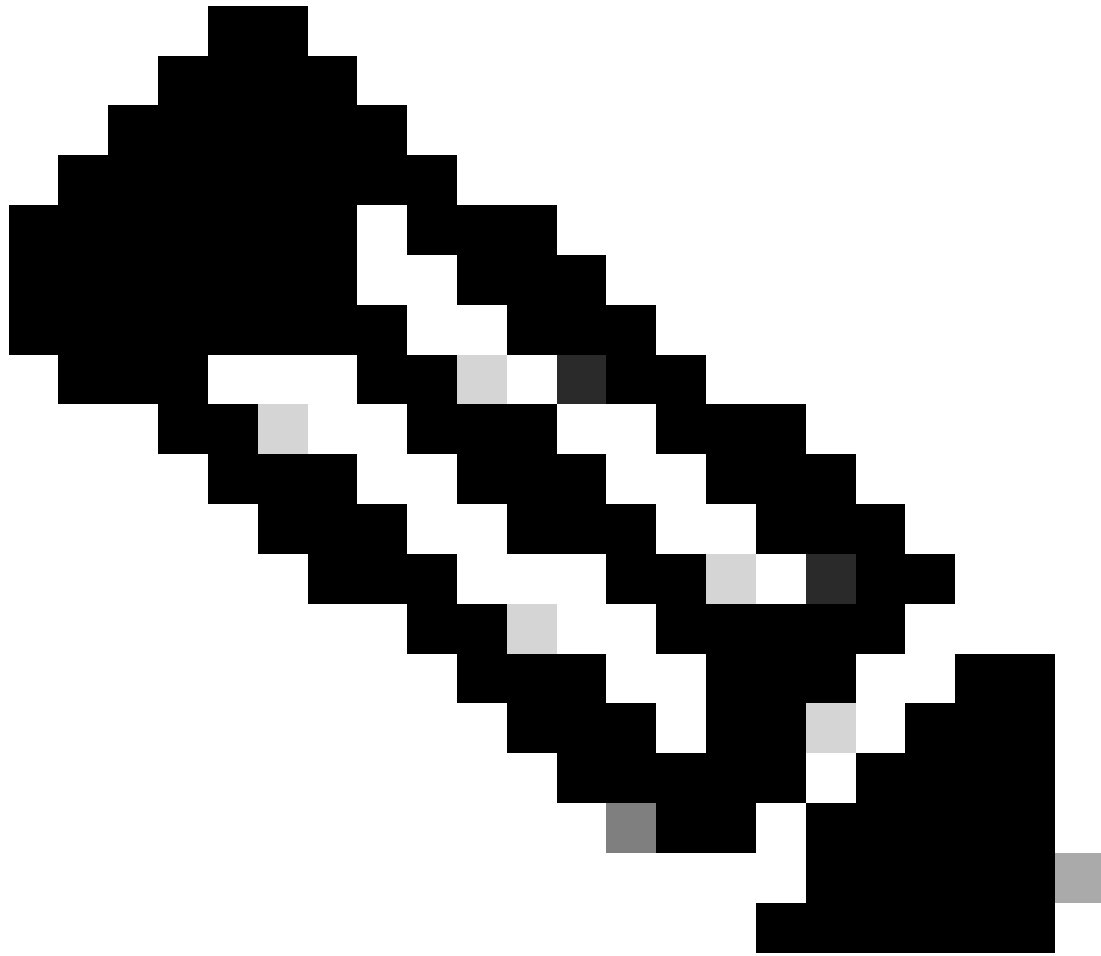
一旦建立了應用可視性，使用者就可以透過配置服務品質(QoS)，為客戶端建立具有策略機制的控制規則。



AVC的工作機制

## 網路型應用程式辨識(NBAR)

NBAR是整合在9800 WLC上的一種機制，用於執行DPI，以辨識和分類網路上運行的各種應用程式。它可以辨識和分類大量應用，包括加密和動態埠對映應用，這些應用通常對傳統資料包檢測技術不可見。



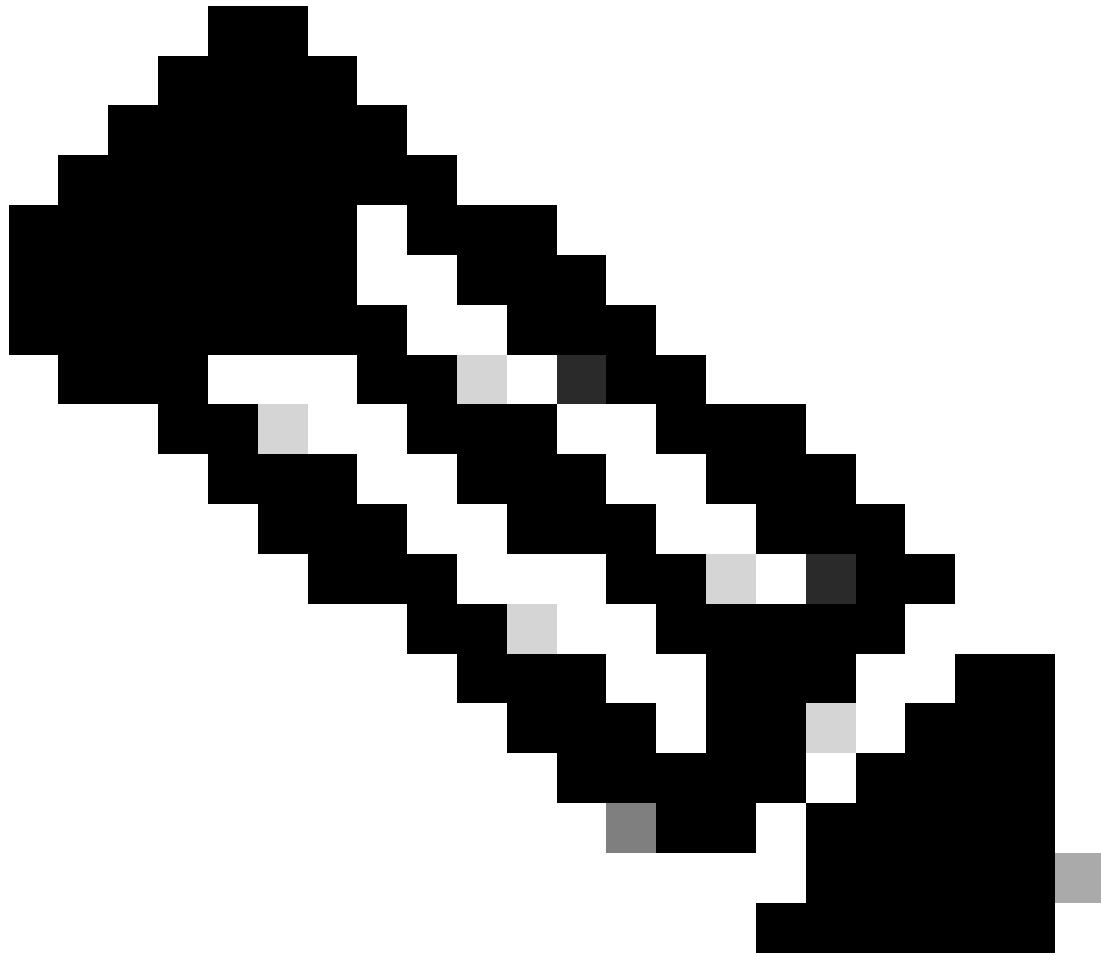
注意：要利用Catalyst 9800 WLC上的NBAR，需要經常結合特定AVC配置檔案來啟用和正確配置它，這些AVC配置檔案會根據流量的分類定義要採取的相應操作。

NBAR會持續定期更新，因此，請務必使WLC軟體保持最新，以確保NBAR功能集保持最新和有效。

有關最新版本中支援的協定的完整清單，請訪問[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_nbar/prot\\_lib/config\\_library/nbar-prot-pack-library.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html)

在策略配置檔案上啟用NBAR協定

```
9800WLC#configure terminal
9800WLC(config)#wireless profile policy AVC_testing
9800WLC(config-wireless-policy)#ip nbar protocol-discovery
9800WLC(config-wireless-policy)#end
```



注意：在執行此操作之前，需要停用%策略配置檔案。

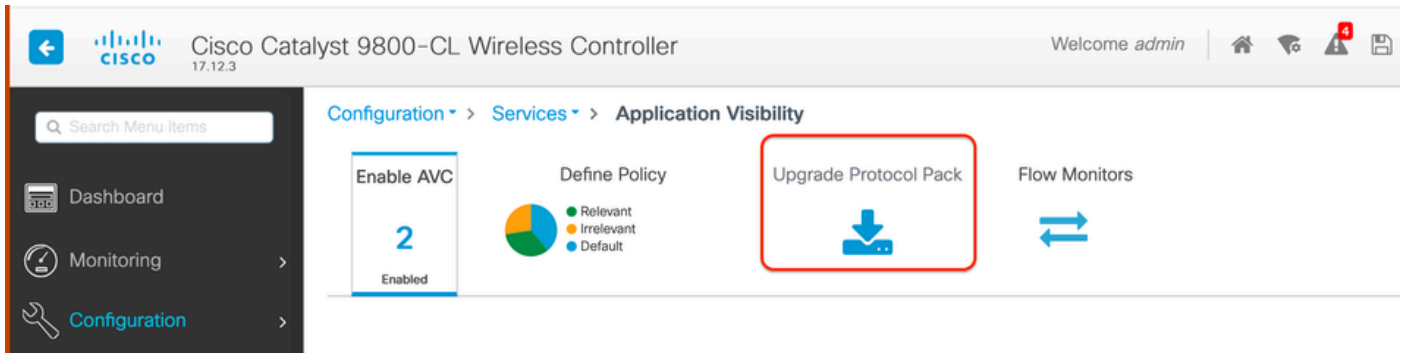
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR  
NBAR Protocol Discovery : Enabled
```

### 升級9800 WLC上的NBAR

9800 WLC已擁有約1500個可辨識的應用。在新應用發佈的情況下，將在需要從特定9800型號的軟體下載頁面下載的最新NBAR中更新其協定。

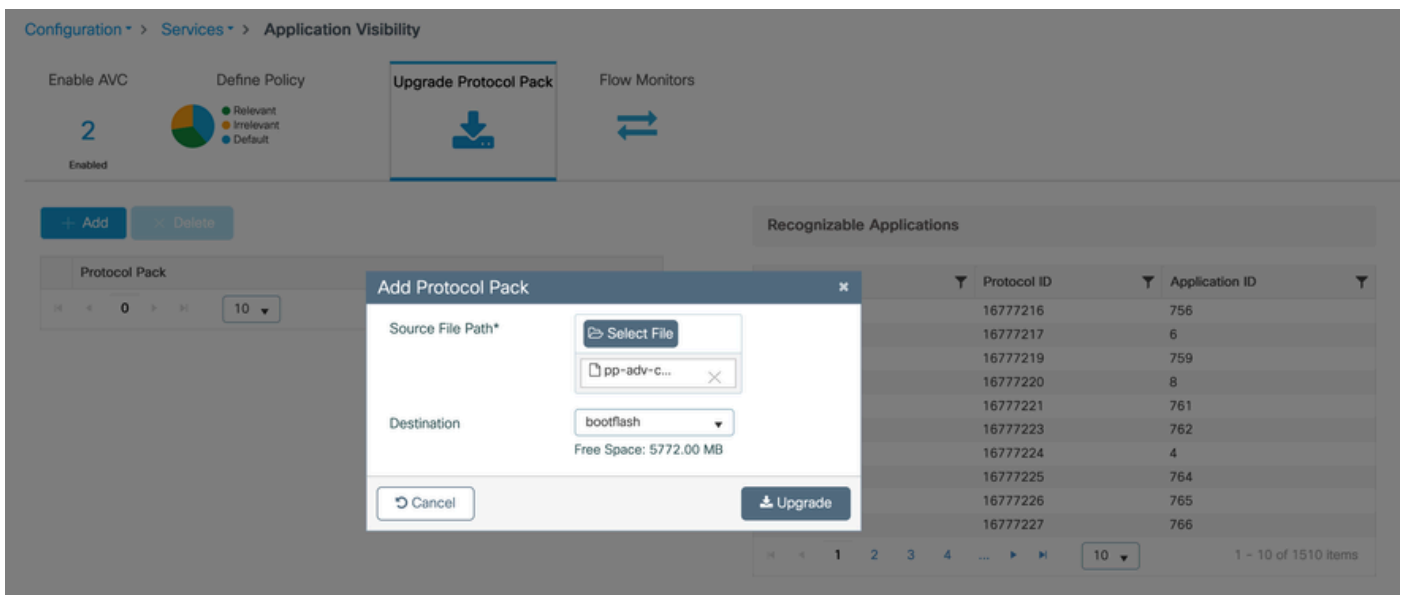
### 透過GUI

導航到配置>服務>應用可視性。按一下Upgrade Protocol Pack。



9800 WLC中的上傳協定部分

按一下Add，然後選擇要下載的協定包，然後按一下Upgrade（如果您使用Telnet會話）。



增加NBAR協定

升級完成後，您會看到協定包已增加。

Enable AVC Define Policy Upgrade Protocol Pack Flow Monitors

2

Enabled

+ Add × Delete

Protocol Pack	
<input type="checkbox"/>	bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack

Navigation: ⏪ ⏩ 1 10 ▼ 1 - 1 of 1 items

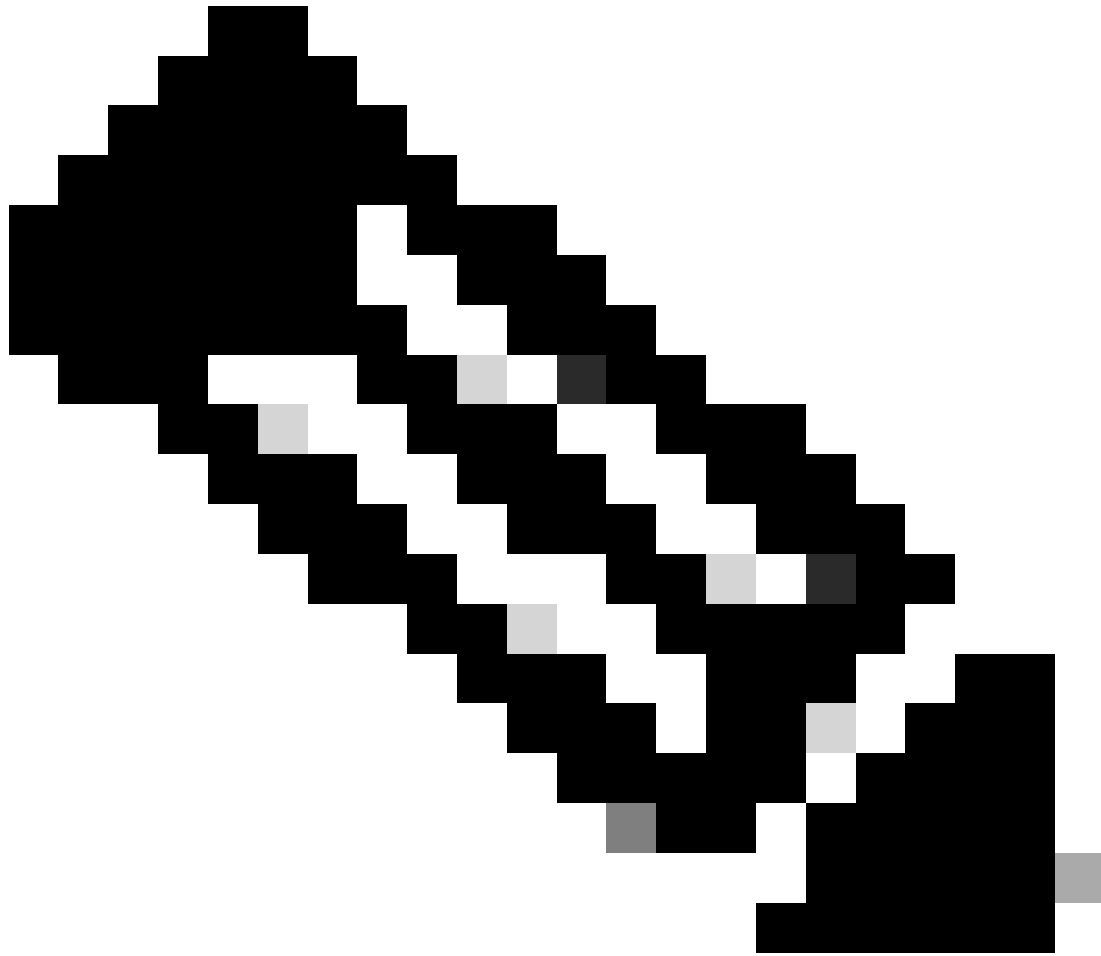
驗證通訊協定套件

### 透過CLI

```
9800WLC#copy tftp://10.10.10.1/pp-adv-c9800-1712.1-49-70.0.0.pack bootflash:  
9800WLC#configure terminal  
9800WLC(config)#ip nbar protocol-pack bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
```

To verify NBAR protocol pack version

```
9800WLC#show ip nbar protocol-pack active  
Active Protocol Pack:  
Name: Advanced Protocol Pack  
Version: 70.0  
Publisher: Cisco Systems Inc.  
NBAR Engine Version: 49  
Creation time: Tue Jun 4 10:18:09 UTC 2024  
File: bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack  
State: Active
```



注意：在NBAR協定包的升級過程中不會中斷服務。

## Netflow

NetFlow是用於收集IP流量資訊和監控網路流量資料的網路協定。它主要用於網路流量分析和頻寬監控。以下概述NetFlow如何在Cisco Catalyst 9800系列控制器上運行：

- 資料收集：9800 WLC收集流經它們的IP流量的資料。此資料包括源和目標IP地址、源和目標埠、使用的協定、服務類別以及流終止的原因等資訊。
- 流程記錄：收集的資料會組織成流程記錄。流被定義為共用一組通用屬性（如相同的源/目標IP、源/目標埠和協定型別）的單向資料包序列。
- 導出資料：流記錄會定期從啟用了NetFlow的裝置導出到NetFlow收集器。收集器可以是本地WLC，也可以是接收、儲存和處理流資料的專用伺服器或軟體應用程式。
- 分析：您可以使用NetFlow收集器和分析工具來檢視流量模式、辨識頻寬、檢測指示安全漏洞的不尋常流量流、最佳化網路效能以及規劃網路擴展。
- 無線特定資訊：在無線控制器的環境中，NetFlow可以包含特定於無線網路的其他資訊，如



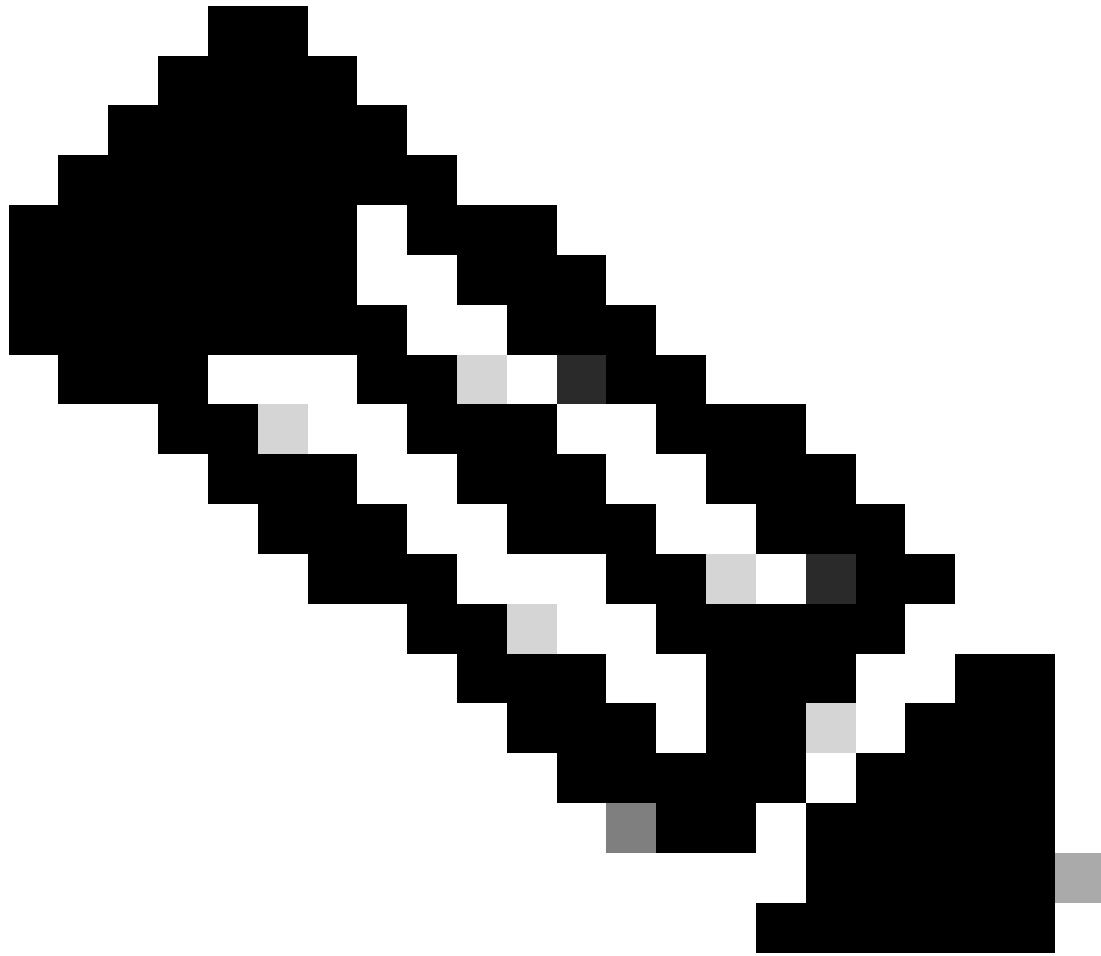
SSID、AP名稱、客戶端MAC地址以及與Wi-Fi流量相關的其他詳細資訊。

## Flexible Netflow

Flexible NetFlow (FNF)是傳統NetFlow的進階版本，受Cisco Catalyst 9800系列無線區域網控制器(WLC)支援。它為跟蹤、監控和分析網路流量模式提供了更多自定義選項。Catalyst 9800 WLC上的Flexible NetFlow的主要功能包括：

- 自定義：FNF允許使用者定義要從網路流量收集哪些資訊。這包括各種流量屬性，如IP地址、埠號、時間戳、資料包和位元組計數、應用型別等。
- 增強的可視性：透過利用FNF，管理員可以詳細瞭解流經網路的流量型別，這對於容量規劃、基於使用的網路計費、網路分析和安全監控至關重要。
- 協定獨立性：FNF具有足夠的靈活性，可支援IP以外的各種協定，因此能夠適應不同型別的網路環境。

在Catalyst 9800 WLC上，可以配置FNF以將流記錄導出到外部NetFlow收集器或分析應用程式。這些資料可用於故障排除、網路規劃和安全分析。FNF配置包括定義流記錄（要收集的內容）、流導出器（傳送資料的位置），以及將流監控器（繫結記錄和導出器）附加到適當的介面。



注意：FNF可以向外部第三方Netflow收集器傳送17條不同的資料記錄（如RFC 3954中所定義），例如Stealthwatch、Solarwinds等，包括：應用標籤、客戶端Mac地址、AP Mac地址、WlanIP id、源IP、目標IP、源埠、目標埠、協定、流開始時間、流結束時間、方向、資料包輸出、位元組計數、VLAN ID（本地模式）-管理/客戶端和TOS - DSCP值

## 流量監控器

流監控器是與Flexible NetFlow (FNF)結合使用的元件，用於捕獲和分析網路流量資料。它在監控和瞭解流量模式以實現網路管理、安全和故障排除方面起著至關重要的作用。流監控器基本上是FNF的一個應用例項，它根據定義的標準收集和跟蹤流資料。它與三個主要元素相關聯：

- 流記錄：定義流監控器必須從網路流量收集的資料。它指定流資料中將包含的金鑰（如源和目標IP地址、埠、協定型別）和非金鑰欄位（如資料包和位元組計數器、時間戳）。
- 流導出器：用於指定必須傳送收集的流資料的目標。它包括NetFlow收集器的IP地址、傳輸協定（通常為UDP）以及收集器偵聽的目標埠號等詳細資訊。
- 流監控器：流監控器自身將流記錄和流導出器繫結在一起，並將它們應用於介面或WLAN，以實際啟動監控進程。它根據流記錄中的條件集和流導出器中的目標集，確定如何收集和導出流

資料。

## AVC支援的存取點

只有以下存取點支援AVC：

- Cisco Catalyst 9100系列存取器
- Cisco Aironet 2800系列存取點
- Cisco Aironet 3800 系列存取點
- Cisco Aironet 4800 系列存取器

## 支援不同的9800部署模式

部署模式	9800 WLC	第1波存取點	Wave 2存取點	Wifi 6存取點
本地模式 (集中交換)	IPV4流量： 支援AVC 支援FNF  IPV6流量： 支援AVC 支援FNF	在WLC級別進行處理	在WLC級別進行處理	在WLC級別進行處理
Flex模式 (集中交換)	IPV4流量： 支援AVC 支援FNF  IPV6流量： 支援AVC 支援FNF	在WLC級別進行處理	在WLC級別進行處理	在WLC級別進行處理
Flex模式 (本地交換)	在AP層級處理	IPV4流量： 支援AVC 支援FNF  IPV6流量： 支援AVC 不支援FNF	IPV4流量： 支援AVC 支援FNF  IPV6流量： 支援AVC 支援FNF	IPV4流量： 支援AVC 支援FNF  IPV6流量： 支援AVC 支援FNF
本地模式 (交換矩陣)	在AP層級處理	IPV4流量： 不支援AVC	IPV4流量： 支援AVC	IPV4流量： 支援AVC

		不支援FNF  IPV6流量： 不支援AVC 不支援FNF	支援FNF  IPV6流量： 支援AVC 支援FNF	支援FNF  IPV6流量： 支援AVC 支援FNF
--	--	---	--	--

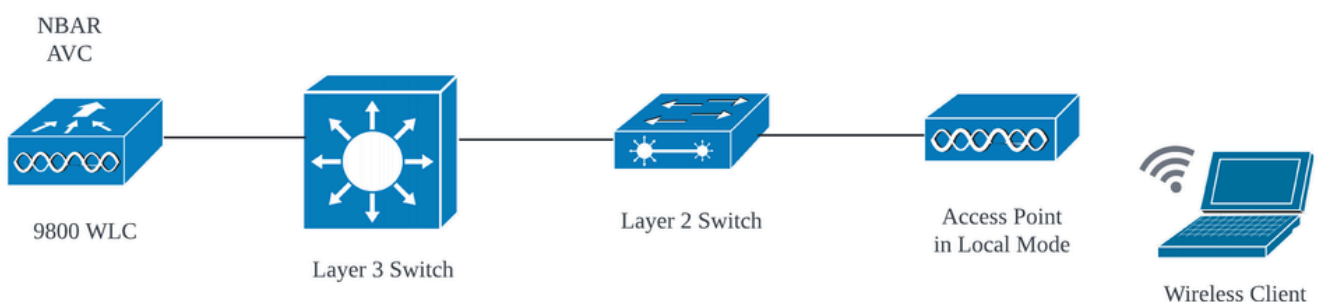
## 在9800上實施AVC時的限制

應用可視性與可控性(AVC)和Flexible NetFlow (FNF)是Cisco Catalyst 9800系列無線區域網控制器的強大功能，可增強網路可視性和可控性。但是，在使用這些功能時，請記住一些限制和注意事項：

- 不支援跨控制器第2層漫遊。
- 不支援組播流量。
- 只有透過應用可視性辨識的應用才能用於應用QoS控制。
- AVC中的NetFlow欄位不支援資料鏈路。
- 不能將同一個WLAN配置檔案對映到未啟用AVC的策略配置檔案和啟用AVC的策略配置檔案。
- 您不能將具有不同交換機制的策略配置檔案用於同一WLAN以實現AVC。
- 管理埠(Gig 0/0)不支援AVC。
- 僅允許在有線物理埠上配置基於NBAR的QoS策略。虛擬介面（例如VLAN、埠通道和其他邏輯介面）不支援策略配置。
- 啟用AVC時，AVC配置檔案僅支援最多23條規則，其中包括預設DSCP規則。如果規則超過23，AVC策略將不會向下推送到AP。

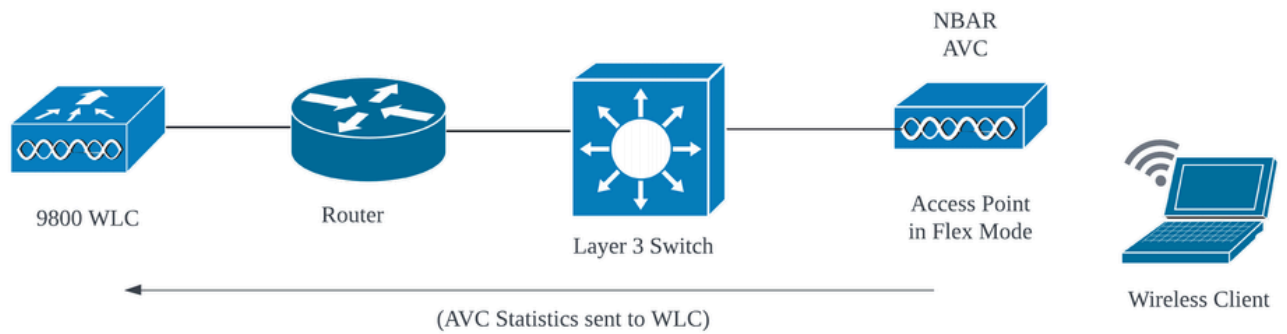
## 網路拓撲

### 本地模式下的AP



本地模式AP中的AVC (集中交換)

### 處於flex模式的AP



Flex模式下的AVC AP

## 9800 WLC上的AVC配置

在9800 WLC上配置AVC時，您可以將其用作NetFlow收集器，也可以將NetFlow資料輸出到外部NetFlow收集器。

### 本地導出器

在Cisco Catalyst 9800無線LAN控制器(WLC)上，本機NetFlow收集器是指WLC中的嵌入式功能，允許其收集並本機儲存NetFlow資料。此功能使WLC能夠執行基本NetFlow資料分析，而無需將流記錄輸出到外部NetFlow收集器。

### 透過GUI

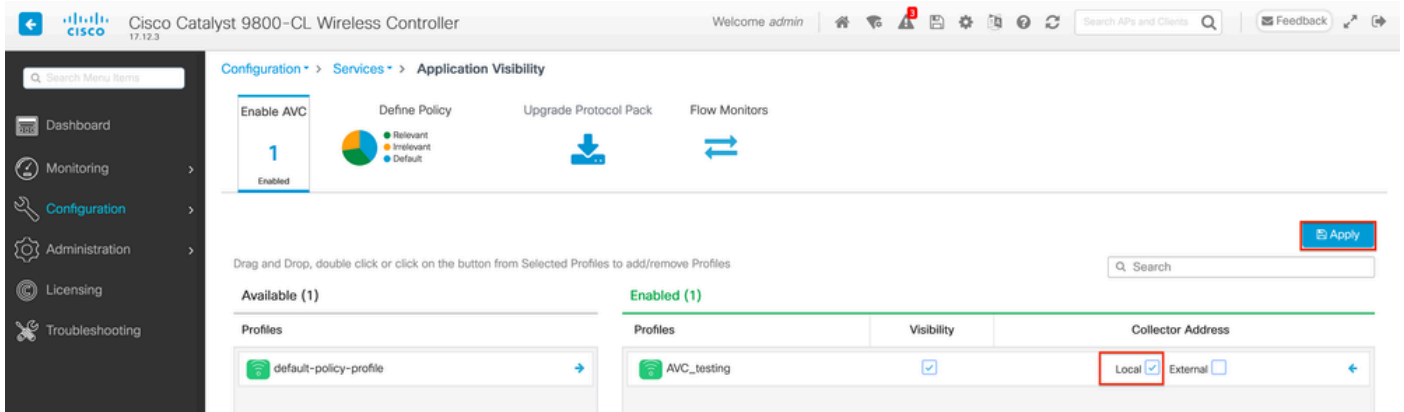
第1步：要在特定SSID上啟用AVC，請導航到配置>服務>應用可視性。選擇要為其啟用AVC的特定策略配置檔案。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is 'Configuration > Services > Application Visibility'. The 'Enable AVC' toggle is set to 'Enabled'. Below this, there are sections for 'Available (2)' and 'Enabled (0)'. The 'Available' section contains a table with two profiles: 'AVC\_testing' and 'default-policy-profile'. The 'AVC\_testing' profile has a red box around its right-pointing arrow button, indicating it is the selected profile to be enabled.

Profiles	Visibility	Collector Address
AVC_testing		
default-policy-profile		

在策略配置檔案上啟用AVC

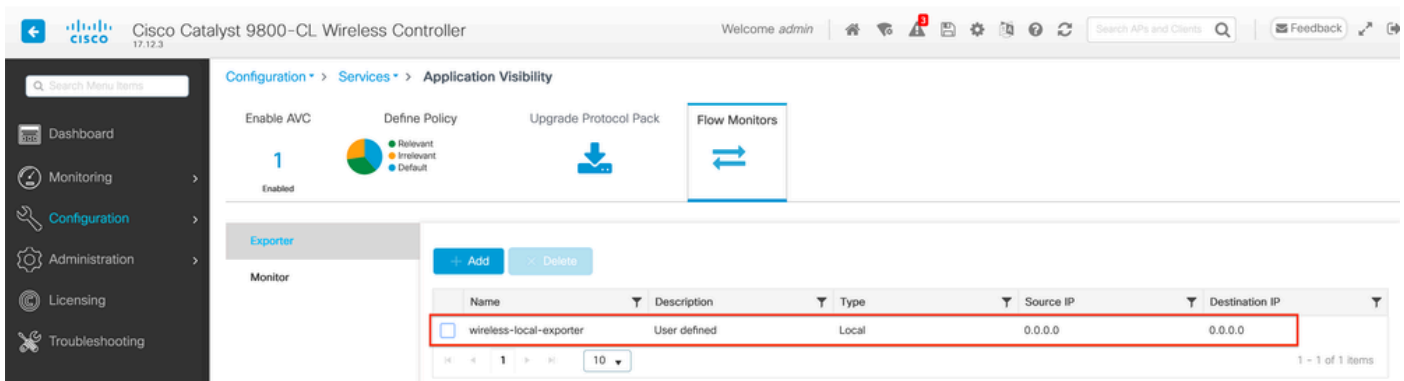
第2步：選擇本地作為Netflow收集器，然後按一下應用。



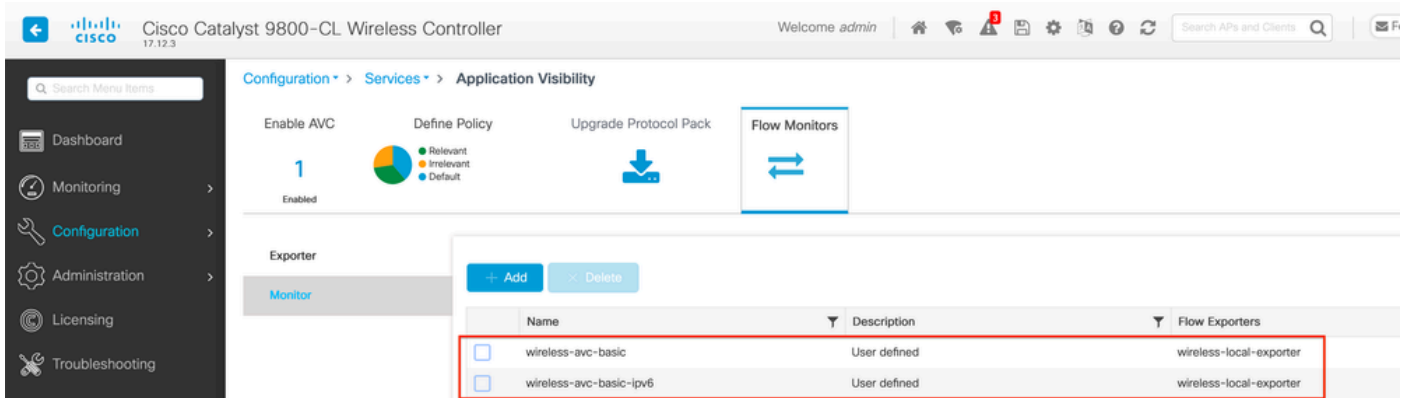
選擇本地NetFlow收集器

請注意，應用AVC配置後，NetFlow導出器和NetFlow設定已根據指定的首選項自動配置。

您可以導航到Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor進行驗證。

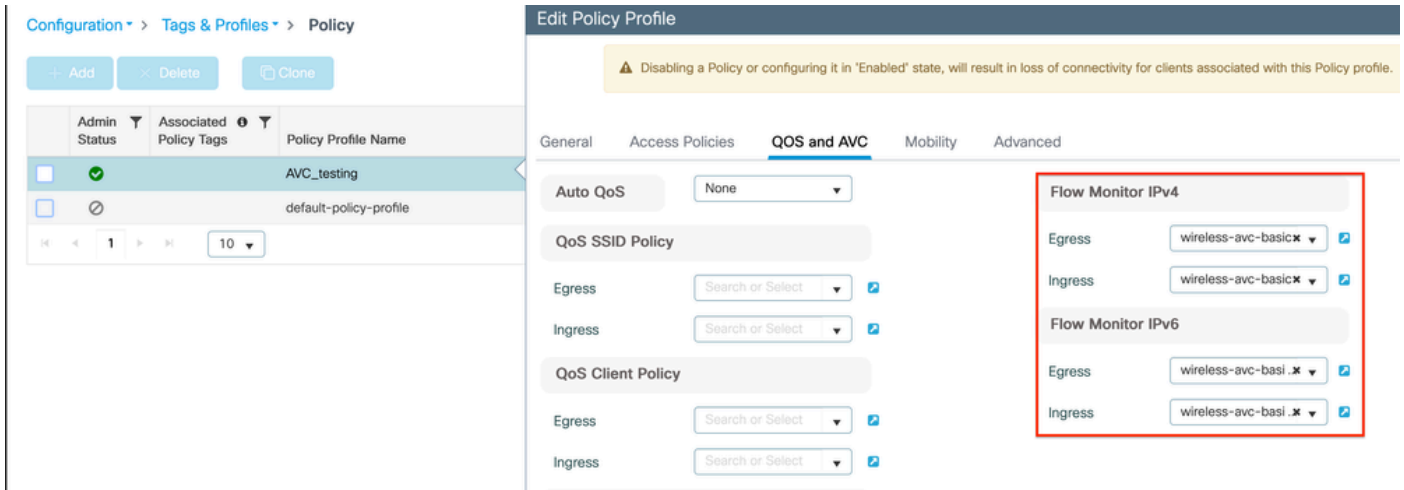


9800 WLC上的本機流量收集器組態



使用本地NetFlow收集器的流監控器配置

IPv4和IPv6 AVC流監控器將自動與策略配置檔案關聯。導航到配置>標籤和配置檔案>策略。按一下Policy Profile > AVC和QOS (AVC和QOS)。



策略配置檔案中的流監控器配置

## 透過CLI

第1步：將9800 WLC配置為本地導出器。

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter wireless-local-exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

第2步：配置IPv4和IPv6網路流監控器以使用本地(WLC)作為Netflow導出器。

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter wireless-local-exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor wireless-avc-basic-ipv6
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

第3步：在策略配置檔案中對映入口和出口流量的IPv4和IPv6流監控器。

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
```

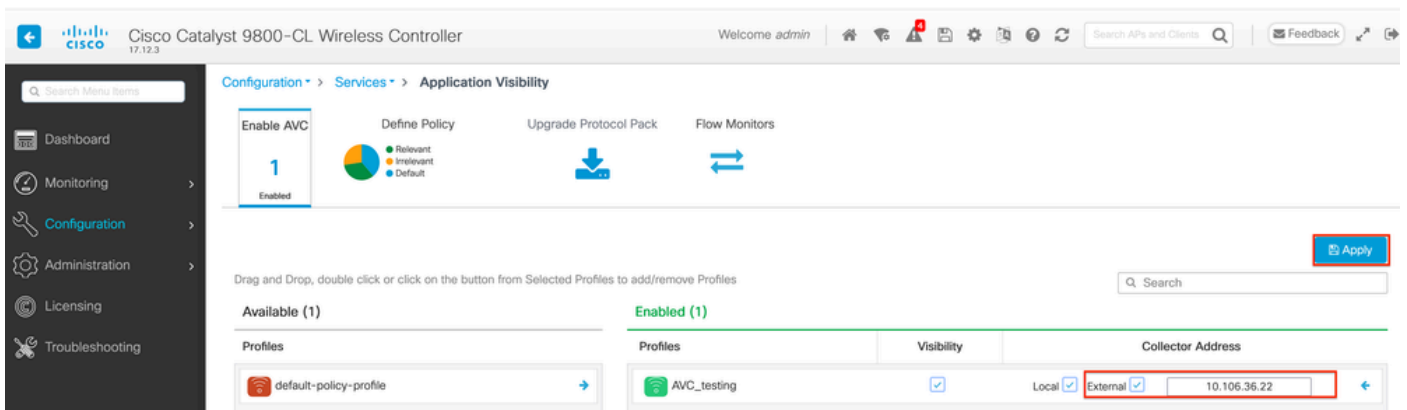
```
9800-CL-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 input
9800-CL-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 output
9800-CL-VM(config-wireless-policy)#no shutdown
9800-CL-VM(config-wireless-policy)#exit
```

## 外部NetFlow收集器

外部NetFlow收集器在Cisco Catalyst 9800無線LAN控制器(WLC)上的應用可視性與控制性(AVC)環境中使用時，是接收、聚合和分析從WLC導出的NetFlow資料的專用系統或服務。您可以僅配置外部NetFlow收集器以監控應用可視性，也可以將其與本地收集器一起使用。

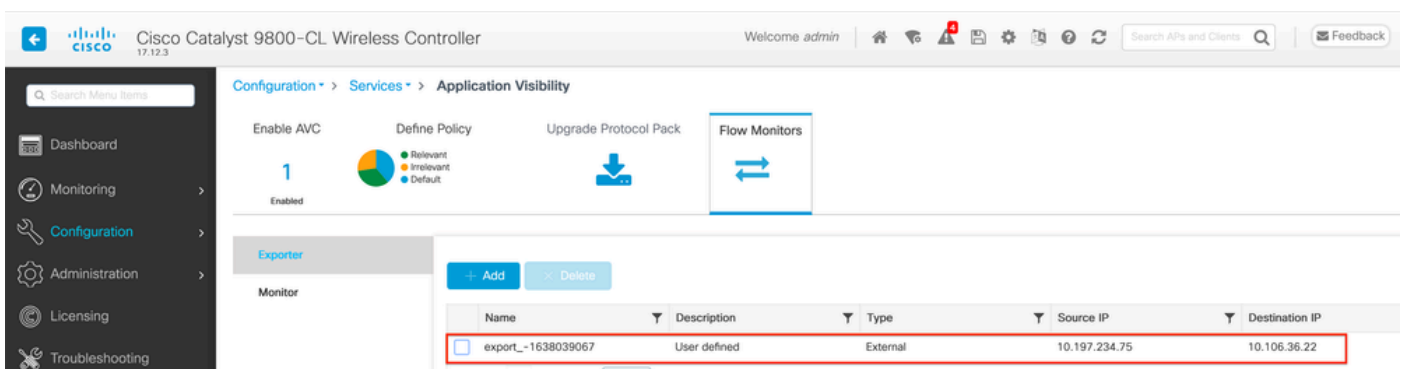
### 透過GUI

第1步：要在特定SSID上啟用AVC，請導航到配置>服務>應用可視性。選擇要為其啟用AVC的特定策略配置檔案。選擇Collector作為External，並配置NetFlow收集器（如Cisco Prime、SolarWind、StealthWatch）的IP地址，然後按一下Apply。



外部NetFlow收集器的AVC配置

請注意，應用AVC配置後，NetFlow導出器和NetFlow設定已自動配置，將NetFlow收集器IP地址用作導出器，將導出器地址配置為9800 WLC，同時使用預設超時設定和UDP埠9995。您可以導航到Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor進行驗證。



9800 WLC上的外部NetFlow收集器配置



Cisco Catalyst 9800-CL Wireless Controller 17.12.3

Welcome admin

Search APs and Clients

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

Exporter: Monitor

Name	Description	Flow Exporters
dwavc_-1638039067	User defined	export_-1638039067
dwavc_ipv6_-1638039067	User defined	export_-1638039067

使用外部NetFlow收集器的流監控器配置

導航到Configuration > Services > NetFlow，您可以檢查自動生成的NetFlow監控器的埠配置。

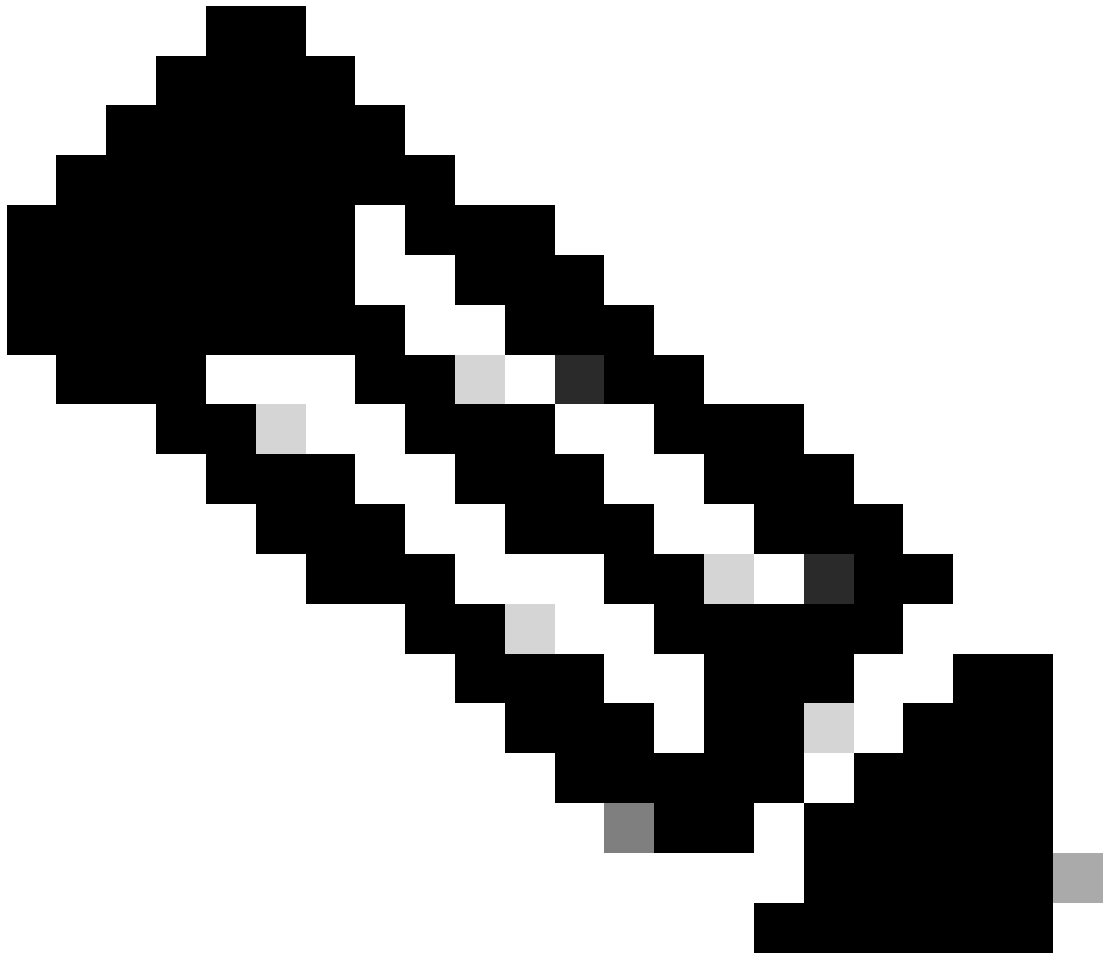
Cisco Catalyst 9800-CL Wireless Controller 17.12.3

Welcome admin

Search APs and Clients

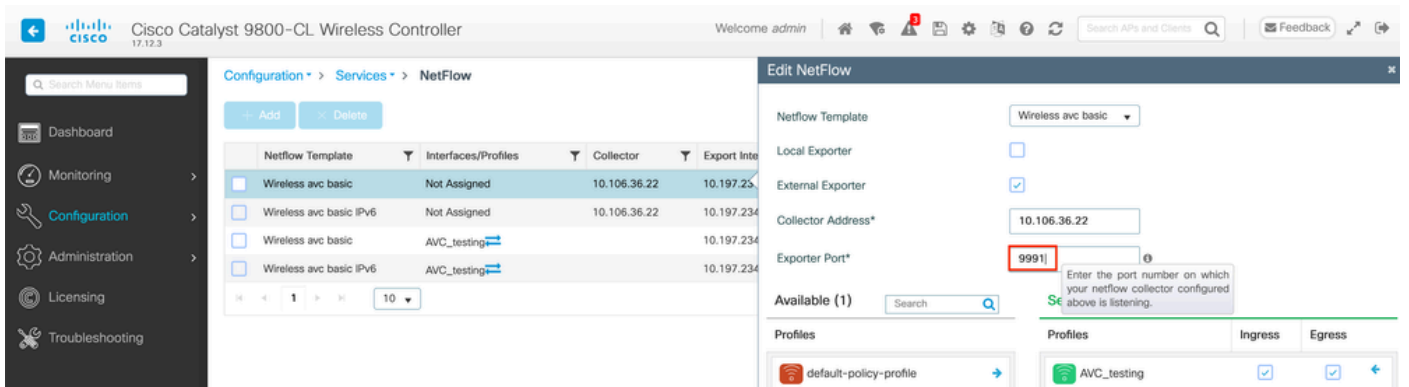
Configuration > Services > NetFlow

Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



注意：如果透過GUI配置AVC，則自動生成的NetFlow導出器將配置為使用UDP 9995埠。請確保驗證NetFlow收集器正在使用的埠號。

例如：如果您使用Cisco Prime作為NetFlow收集器，必須將導出器埠設定為9991，因為這是Cisco Prime監聽NetFlow流量的埠。您可以在NetFlow配置中手動更改導出器埠。



在NetFlow配置中更改導出器埠號

## 透過CLI

第1步：使用源介面配置外部NetFlow收集器的IP地址。

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter External_Exporter
9800-C1-VM(config-flow-exporter)#destination 10.106.36.22
9800-C1-VM(config-flow-exporter)#source $Source_Interface
9800-C1-VM(config-flow-exporter)#transport udp $Port_Numbet
9800-C1-VM(config-flow-exporter)#exit
```

第2步：配置IPv4和IPv6網路流監控器以使用本地(WLC)作為Netflow導出器。

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

第3步：在策略配置檔案中對映入口和出口流量的IPv4和IPv6流監控器。

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

## 使用Cisco Catalyst Center在9800 WLC上配置AVC

在透過Cisco Catalyst Center在Cisco Catalyst 9800無線LAN控制器(WLC)上繼續配置應用可視性與控制(AVC)之前，必須驗證WLC和Cisco Catalyst Center之間的遙測通訊是否已成功建立。確保WLC在Cisco Catalyst Center介面內顯示為託管狀態，並且其運行狀況處於主動更新狀態。此外，為了有效監控健康狀態，請務必將WLC和存取點(AP)正確指派給Cisco Catalyst Center中各自的

網站。

```
9800WLC#show telemetry connection all
Telemetry connections
```

Index	Peer Address	Port	VRF	Source Address	State	State Description
170	10.78.8.84	25103	0	10.105.193.156	Active	Connection up

9800 WLC上的遙測連線驗證

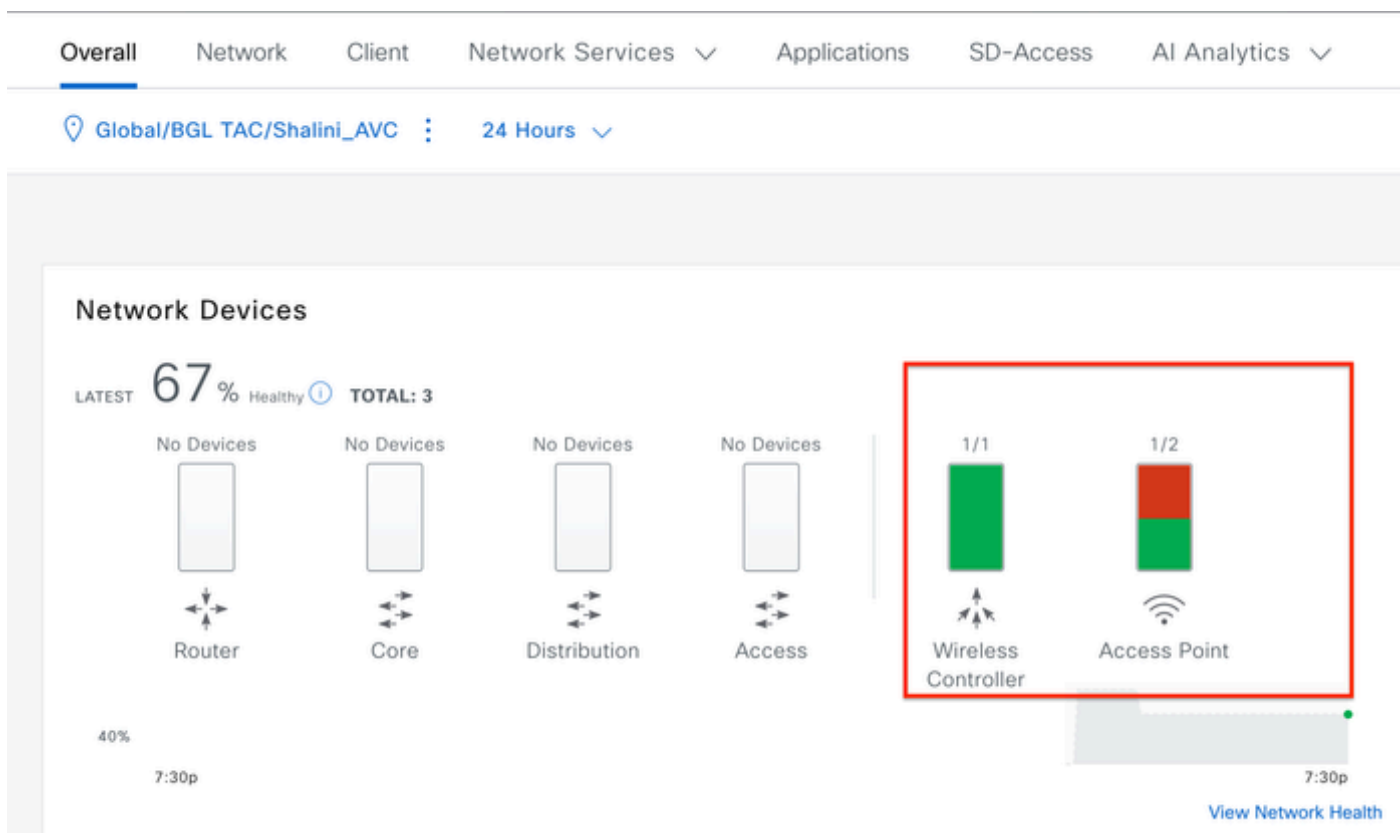
Devices (5) Focus: Inventory

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Tag Add Device Edit Device Delete Device Actions

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability
	9800WLC.cisco.com	10.105.193.156	Cisco	Reachable	Not Scanned	Managed
	CW9164I-ROW1	10.105.193.152	NA	Reachable	Not Scanned	Managed
	CW9164I-ROW2	10.105.60.35	NA	Reachable	Not Scanned	Managed

WLC和AP處於託管狀態



Cisco Catalyst Center上WLC和AP的運行狀態

第1步：將Cisco Catalyst Center配置為NetFlow收集器並在全局設定中啟用無線遙測。導航到設計

>網路設定>遙測，然後啟用所需的配置（如圖所示）。

Catalyst Center Telemetry configuration page. The page is titled "Design / Network Settings" and has tabs for Servers, Device Credentials, IP Address Pools, Wireless, Telemetry, and Security and Trust. The Telemetry tab is active. The page content includes:

- Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.
- Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. [View details](#) on the metrics gathered and the frequency with which they are collected.
- Application Visibility**
  - Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment ⓘ
  - Enable by default on supported wired access devices**
  - Choose the destination collector for Netflow records sent from network devices.
    - Use Catalyst Center as the Netflow Collector**
    - Use Cisco Telemetry Broker (CTB) or UDP director
- Wired Endpoint Data Collection**
  - The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.
  - Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.
  - Enable Catalyst Center Wired Endpoint Data Collection At This Site
  - Disable Catalyst Center Wired Endpoint Data Collection At This Site** ⓘ
- Wireless Controller, Access Point and Wireless Clients Health**
  - Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.
  - Enable Wireless Telemetry**

無線遙測和AVC配置

第2步：在所需的9800 WLC上啟用應用遙測，以在9800 WLC上推送AVC配置。為此，請導航到調配>網路裝置>資產。選擇要在其上啟用應用程式遙測的9800 WLC，然後導航到操作>遙測>啟用應用程式遙測。

Catalyst Center Provision / Inventory page. The page is titled "Provision / Inventory" and has tabs for All, Routers, Switches, Wireless Controllers, Access Points, and Sensors. The Wireless Controllers tab is active. The page content includes:

- Global
- DEVICES (5) Focus: Inventory
- Click here to apply basic or advanced filters or view recently applied filters
- 1 Selected Tag Add Device Edit Device Delete Device Actions ⓘ
- Table with columns: Tags, Device Name, IP Address, Actions, EoX Status, Manageability
- Table rows:
  - 9800WLC.cisco.com (10.105.193.156) - Telemetry menu open, showing "Enable Application Telemetry" highlighted.
  - CW9164I-ROW1 (10.105.193.152)
  - CW9164I-ROW2 (10.105.60.35)
  - SDA\_WLC.cisco.com (10.106.38.185)

第3步：根據需要選擇部署模式。

本地：在本地策略配置檔案中啟用AVC（集中交換）

Flex/Fabric：在Flex策略配置檔案（本地交換）或基於交換矩陣的SSID中啟用AVC。

### Enable Application Telemetry

You have chosen to enable Netflow with application telemetry on 1 wireless controllers.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry. To override this default behavior, tag specific WLAN profile names with keyword "lan". Once specific WLANs are tagged, only those WLANs will be monitored.

For each wireless controller, select the AP modes where you would like to enable application telemetry.

- For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.
- For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

**⚠** Enabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.

**⚠** Note: In order to update application telemetry configuration on the WLC, disable application telemetry first and then re-enable it. To do so, please use the Disable/Enable Application Telemetry buttons in the Actions menu.

9800WLC.cisco.com

Local  Flex/Fabric

Include Guest SSIDs

Telemetry Source: **NetFlow**

Note: Devices require Catalyst Center Advantage license for this feature to be enabled.

Cisco Catalyst Center上的部署模式選擇

第4步：啟動啟用AVC設定的任務，相應的配置將應用於9800 WLC。您可以導航到活動>稽核日誌檢視狀態。

Jul 18, 2024 09:22 PM [↻](#)

3:37p

**Filter**

Time	Description
Today	
Jul 18, 2024 20:52 PM (IST)	Compliance run completed for device 10.105.193.156[9800WLC.cisco.com] and compliance status is NON_COMPLIANT
Jul 18, 2024 20:36 PM (IST)	Executing command config t wireless profile policy default-policy-profile no shutdown exit wireless profile policy testpsk no shutdown exit wireless profile policy BGL14-4_WLANID_12 no shutdown exit wireless profile po...
Jul 18, 2024 20:36 PM (IST)	Executing command config t flow exporter avc_exporter destination 10.78.8.84 source Vlan1 transport udp 6007 export-protocol ipfix option vrf-table timeout 300 option ssid-table timeout 300 option application-table tim...
Jul 18, 2024 20:36 PM (IST)	Request received to enable telemetry on device(s) : [10.105.193.156]

在9800 WLC上啟用遙測後的稽核日誌

Cisco Catalyst Center將部署流導出器和流監控器配置，包括指定的埠和其他設定，並在選擇的模式策略配置檔案內啟用它們，如下所示：

Configure Cisco Catalyst Center as Flow Exporter:

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_exporter
9800-C1-VM(config-flow-exporter)#destination 10.104.222.201
9800-C1-VM(config-flow-exporter)#source Vlan10
9800-C1-VM(config-flow-exporter)#transport udp 6007
9800-C1-VM(config-flow-exporter)#export-protocol ipfix
9800-C1-VM(config-flow-exporter)#option vrf-table timeout 300
9800-C1-VM(config-flow-exporter)#option ssid-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-attributes timeout 300
9800-C1-VM(config-flow-exporter)#exit
```

Configure 9800 WLC as Local Exporter

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_local_exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

Configure Network Flow Monitor to use both Local(WLC) and Cisco Catalyst Center as Netflow Exporter:

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance_rtp
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance_rtp
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
```

```
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

Mapping the IPv4 and IPv6 Flow Monitor in Policy Profile

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

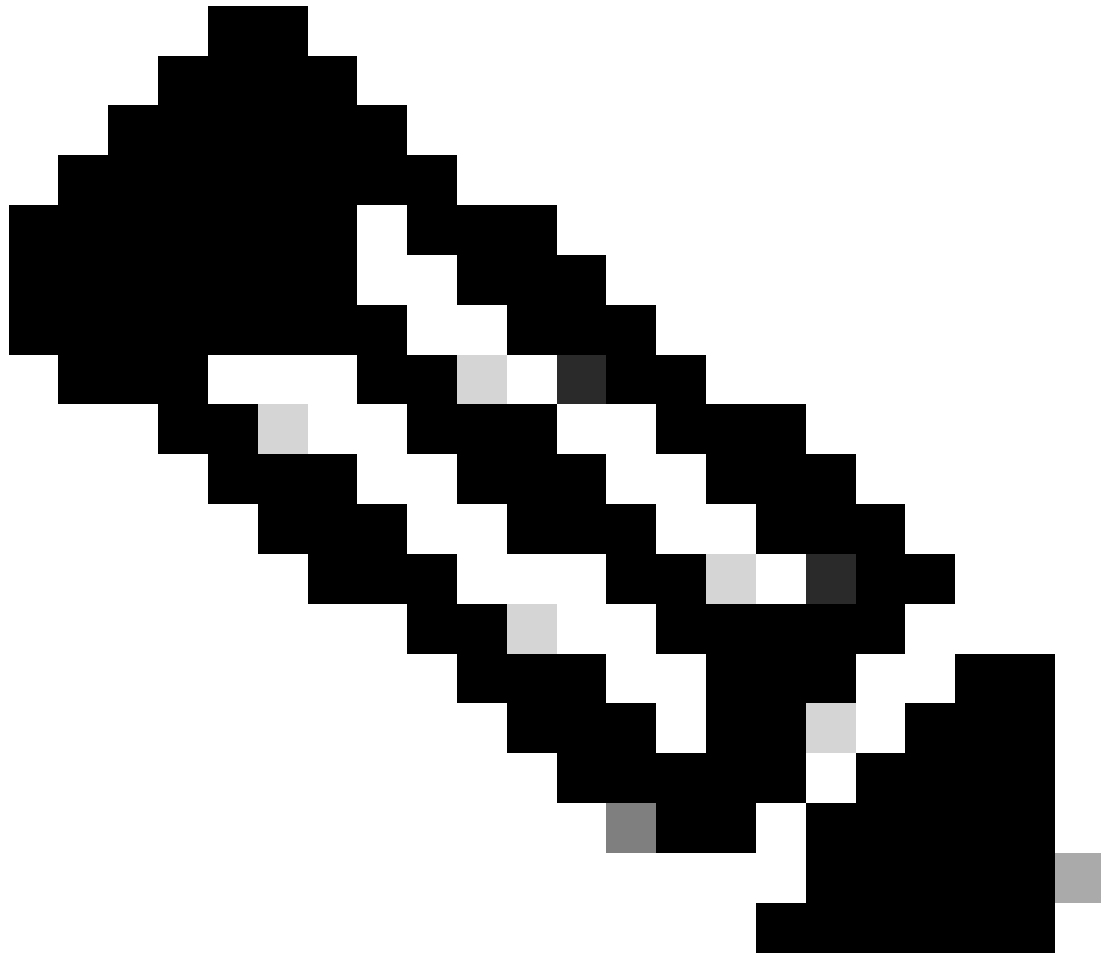
## 驗證AVC

在9800

將9800 WLC用作流導出器時，可以觀察以下AVC統計資訊：

- 跨所有SSID連線的客戶端的應用可視性。
- 每個客戶端的單獨應用程式使用情況。
- 每個SSID上的特定應用使用情況。





注意：您可以選擇按方向過濾資料，包括傳入（傳入）和傳出（傳出）流量，以及按時間間隔過濾資料，可以選擇最長48小時的時間範圍。

透過GUI

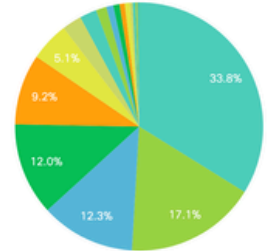
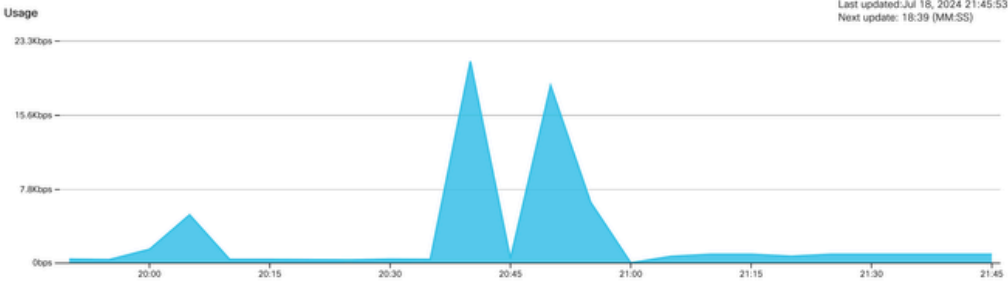
導航到監控>服務>應用可視性。

Clear AVC

NBAR Protocol Pack Version: 61.0  
NBAR Version: 46

Source type: SSID | SSID: AVC\_testing | Direction: Both | Interval: Last 2 hours

Clients
  Applications



Application	Usage(%)	Usage	Received	Sent
Unknown	33.83	796.0KB	300.0KB	496.0KB
Domain Name System	17.08	402.0KB	168.0KB	234.0KB
Ping	12.32	290.0KB	145.0KB	145.0KB
HyperText Transfer Protocol	12.03	283.0KB	117.0KB	166.0KB
ICMP for IPv6	9.22	217.0KB	169.0KB	48.0KB
Internet Control Message Protocol	5.10	120.0KB	84.0KB	36.0KB
Simple Service Discovery Protocol	2.55	60.0KB	47.0KB	13.0KB
Microsoft Services	2.21	52.0KB	44.0KB	8.0KB
mDNS	1.36	32.0KB	27.0KB	5.0KB
Binary over HTTP	0.93	22.0KB	9.0KB	13.0KB

連線到AVC\_testing SSID的使用者對入口和出口流量的應用可視性

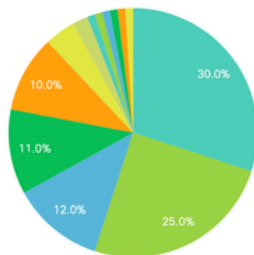
要檢視每個客戶端的應用可視性統計資訊，您可以按一下「客戶端」頁籤，選擇特定客戶端，然後按一下檢視應用詳細資訊。

Clear AVC

NBAR Protocol Pack Version: 61.0  
NBAR Version: 46

Source type: SSID | SSID: All | Direction: All | Interval: Last 90 seconds

Clients
  Applications



Total Clients: 1

View Application Details

Client MAC Address	AP Name	WLAN	State	Protocol
[Redacted]	CW9164I-ROW1	18	Run	11n(2,4)

特定客戶端的應用可視性- 1

[← Back to Client's](#)

Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ping	60	6662	29	390.4KB	195.2KB	195.2KB
unknown	693	572	29	387.2KB	122.4KB	264.8KB
dns	108	1511	12	160.4KB	23.3KB	137.1KB
ipv6-icmp	111	1313	10	142.6KB	115.4KB	27.2KB
http	300	427	9	125.4KB	52.1KB	73.3KB
icmp	147	333	4	47.8KB	44.1KB	3.7KB
ssdp	168	123	1	20.3KB	16.0KB	4.3KB
mdns	80	204	1	16.0KB	14.8KB	1.2KB
ms-services	64	231	1	14.6KB	10.9KB	3.7KB
llmnr	81	159	1	12.6KB	6.9KB	5.7KB

1 - 10 of 17 items

特定客戶端的應用可視性- 2

## 透過CLI

### 驗證AVC狀態

```
9800WLC#show avc status wlan AVC_testing
WLAN profile name: AVC_testing
```

-----

AVC configuration complete: YES

### 來自NetFlow ( FNF快取 ) 的統計資訊

```
9800WLC#show flow monitor $Flow_Monitor_Name cache format table
```

```
9800WLC#show flow monitor wireless-avc-basic cache format table
Cache type: Normal (Platform cache)
Cache size: 200000
Current entries: 102
High Watermark: 102

Flows added: 102
Flows aged: 0
```

IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	FLOW DIRN	WIRELESS SSID	IP PROT	APP NAME	bytes long
wireless client mac addr	mac addr							
10.105.193.170	10.105.193.195	5355	61746	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.129	10.105.193.195	5355	61746	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.2	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.195	10.105.193.114	0	771	Input	AVC_testing	1	prot icmp	120
10.105.193.4	10.105.193.195	5355	64147	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.169	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.52	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.59	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120

在9800 CLI上驗證AVC

要單獨檢查每個WLAN及其連線的客戶端的排名靠前的應用使用情況，請執行以下操作：

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
where n = <1-30> Enter the number of applications
```

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
where n = <1-10> Enter the number of clients
```

驗證傳送到控制平面(CP)的FNFv9資料包計數和解碼狀態

```
9800WLC#show platform software wlavc status decoder
```

```
9800WLC#show platform software wlavc status decoder
AVC FNFv9 Decoder status:
```

Pkt Count	Pkt Decoded	Pkt Errors	Data Records	Last decoded time	Last error time
25703	25703	0	132480	07/20/2024 14:10:46	01/01/1970 05:30:00

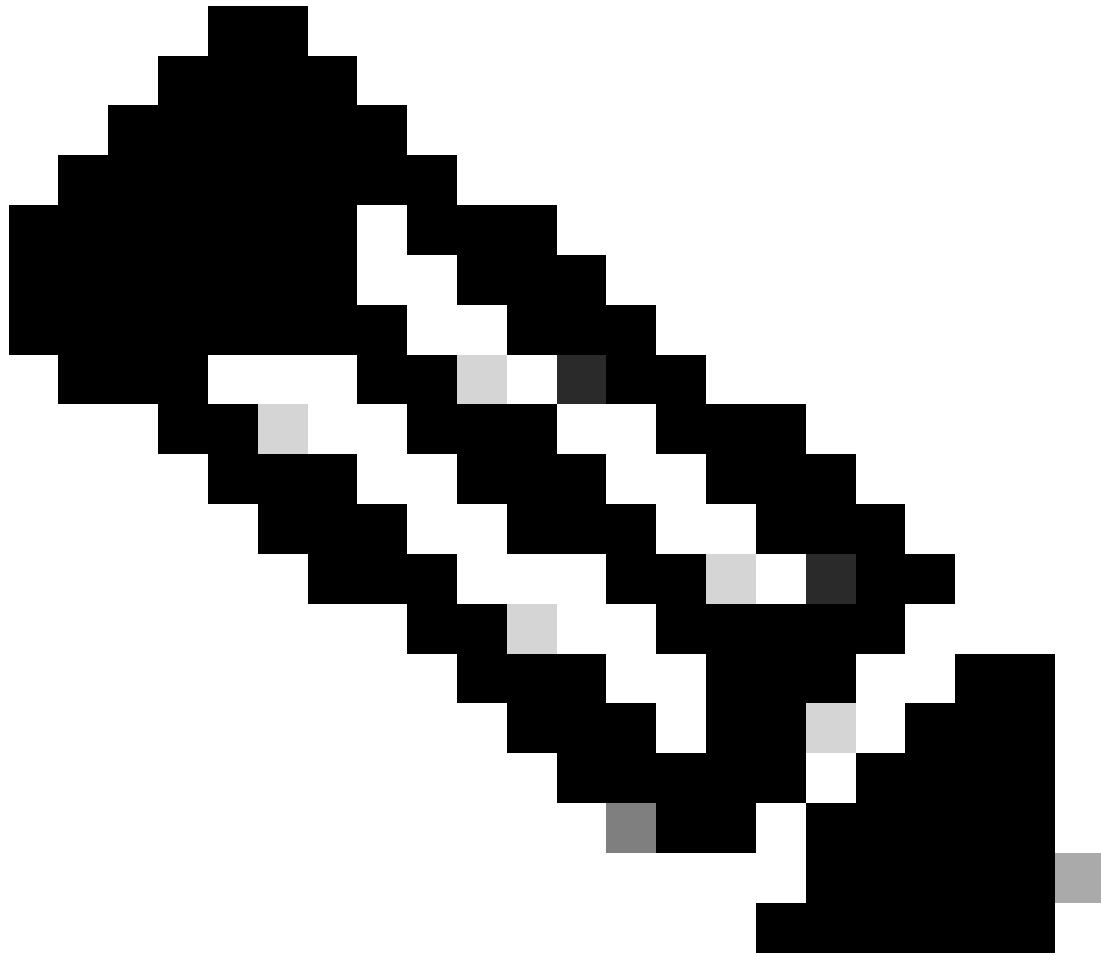
FNFv9資料包記錄

您還可以直接檢查nbar統計資訊。

```
9800WLC#show ip nbar protocol-discovery
```

在Fabric和Flex模式下，您可以透過以下方式從AP獲取NBAR統計資訊：

```
AP#show avc nbar statistics
Works on both IOS and ClickOS APs
```



注意：在外來錨點設定中，錨點WLC充當客戶端的第3層存在，而外來WLC在第2層運行。由於應用可視性與可控性(AVC)在第3層運行，因此只能在錨點WLC上檢視相關資料。

## 在DNAC上

從9800 WLC上捕獲的資料包中，我們可以驗證它是否持續向Cisco Catalyst中心傳送有關應用和網路流量的資料。

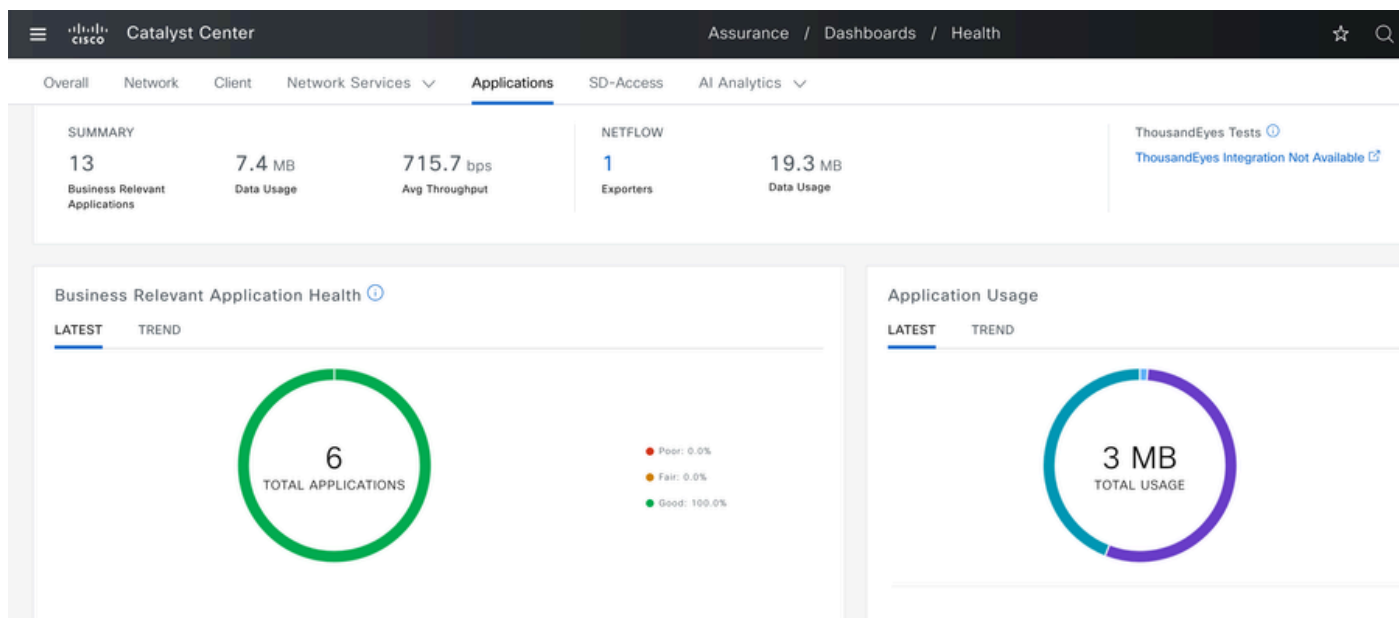
ip.addr == 10.78.8.84 and udp.port == 6007

No.	Time	Source	Destination	Protocol	Length	Info
74227	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
74228	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76582	15:06:41.012984	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76879	15:06:45.016997	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
79686	15:07:01.032987	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
85872	15:07:17.047986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
93095	15:07:37.066982	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
94989	15:07:43.073986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
98292	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98293	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98294	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98295	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98296	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98297	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98298	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98299	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98300	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98301	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98302	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98303	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98304	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98305	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98306	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98307	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310

> Frame 1332: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)  
 > Ethernet II, Src: [REDACTED]  
 > Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.78.8.84  
 > User Datagram Protocol, Src Port: 55148, Dst Port: 6007  
 > Data (136 bytes)  
 Data [truncated]: 000a00886698e17a00001fa700000100011800780a69c150080808080411003501242fd0daa7da00000002000000120d000309005  
 [Length: 136]

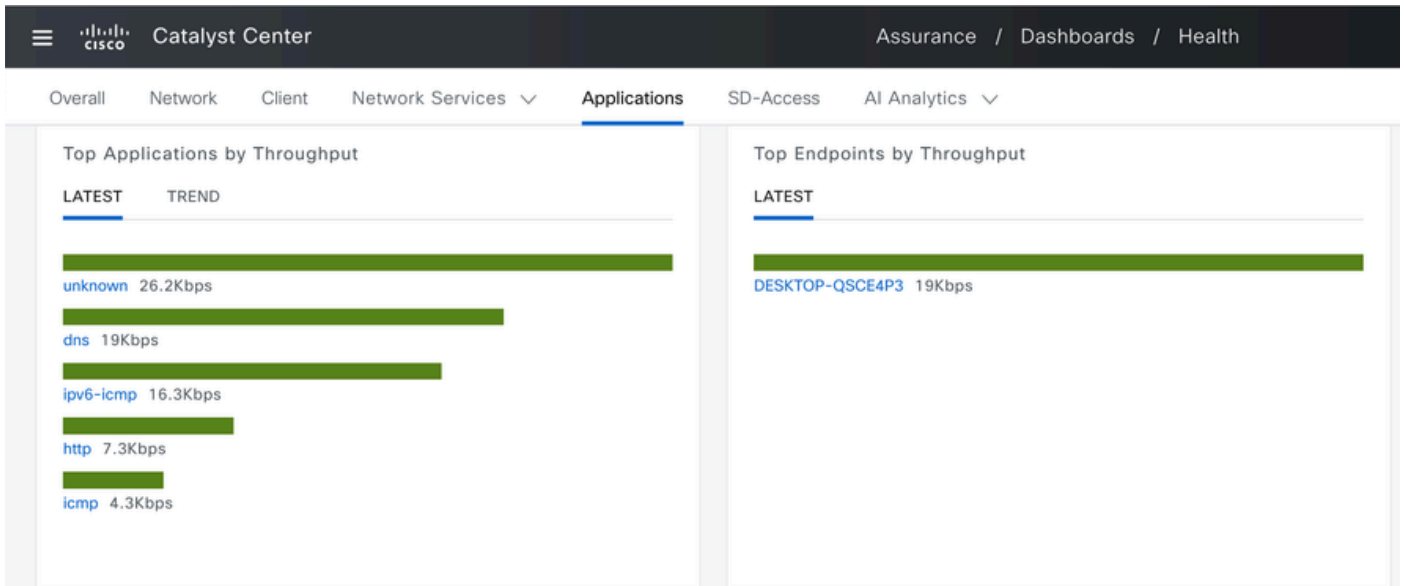
9800 WLC上的資料包捕獲

要檢視連線到Cisco Catalyst Center上特定WLC的客戶端的應用程式資料，請導航到保證>控制台>運行狀況>應用程式。



Cisco Catalyst Center上的AVC監控

我們可以跟蹤客戶最常使用的應用程式，並確定最高的資料使用者，如圖所示。



排名靠前的應用和排名靠前的頻寬使用者統計資訊

您可以為特定SSID設定過濾器，從而監控與該SSID關聯的客戶端的整體吞吐量和應用使用情況。

此功能可讓您辨識網路中的常用應用程式和最高頻寬消耗的使用者。

此外，您還可以利用時間過濾器功能檢查此資料以前的時間段，提供對網路使用情況的歷史見解。

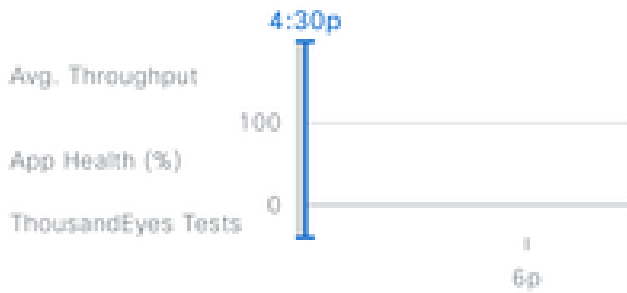
Global/BGL TAC/Shalini\_AVC

24 Hours

Filter (1)



By default, hourly data is shown



Time Range

3 Hours 24 Hours 7 Days

Start Date

7 / 17 / 2024

4:23 PM

End Date

7 / 18 / 2024

4:23 PM

SSID: AVC\_testing

SUMMARY

13

Business Relevant Applications

7.4 M

Data Usage

Cancel

Apply

用於顯示AVC統計資訊的時間過濾器

o



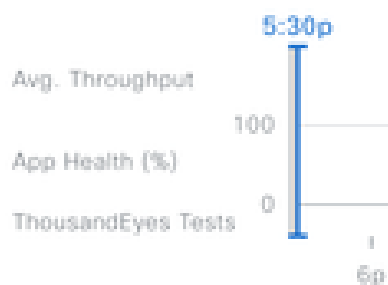


By default, hourly data is shown

SSID (1/14)

Clear Filter

- CWA-test-321
- Session\_timeout
- LM-INTERNAL
- AVC\_testing
- testvritti
- CWA-test-2
- renjith
- Start-Stop
- testmohant...



SSID: AVC\_testing

Cancel

Apply

用於顯示AVC統計資訊的SSID過濾器

## 在外部NetFlow收集器上

### 示例1：Cisco Prime as Netflow Collector

使用Cisco Prime作為Netflow收集器時，您可以看到9800 WLC作為傳送Netflow資料的資料來源，並且系統將根據9800 WLC傳送的資料自動建立NetFlow模板。

從9800 WLC捕獲的資料包中，我們可以驗證它是否持續向Cisco Prime傳送有關應用和網路流量的資料。

ip.addr == 10.106.36.22 && udp.port == 9991

No.	Time	Source	Destination	Protocol	Length	Info
87	20:50:23.855943	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1453	20:50:24.775945	10.105.193.156	10.106.36.22	UDP	458	51154 → 9991 Len=416
1465	20:50:24.856950	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1583	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1584	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1082	51154 → 9991 Len=1040
1596	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1597	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1598	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	474	51154 → 9991 Len=432
1779	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1780	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1158	51154 → 9991 Len=1116
1857	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1858	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1859	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1860	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	270	51154 → 9991 Len=228
1861	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1862	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	678	51154 → 9991 Len=636
2086	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2087	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2088	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	534	51154 → 9991 Len=492
2113	20:50:27.859940	10.105.193.156	10.106.36.22	UDP	578	51154 → 9991 Len=536
2287	20:50:28.779958	10.105.193.156	10.106.36.22	UDP	378	51154 → 9991 Len=336
2295	20:50:28.859940	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2296	20:50:28.859940	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128

> Frame 87: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)

> Ethernet II, Src: [REDACTED]

> Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.106.36.22

> User Datagram Protocol, Src Port: 51154, Dst Port: 9991

> Data (128 bytes)

Data [truncated]: 0009000120eb01e9669932b70000000400000400014f006c000000000000000000000000000000ff0200000000000000000011  
[Length: 128]

在9800 WLC上進行的資料包捕獲

Cisco Prime Infrastructure

Services / Application Visibility & Control / Data Sources

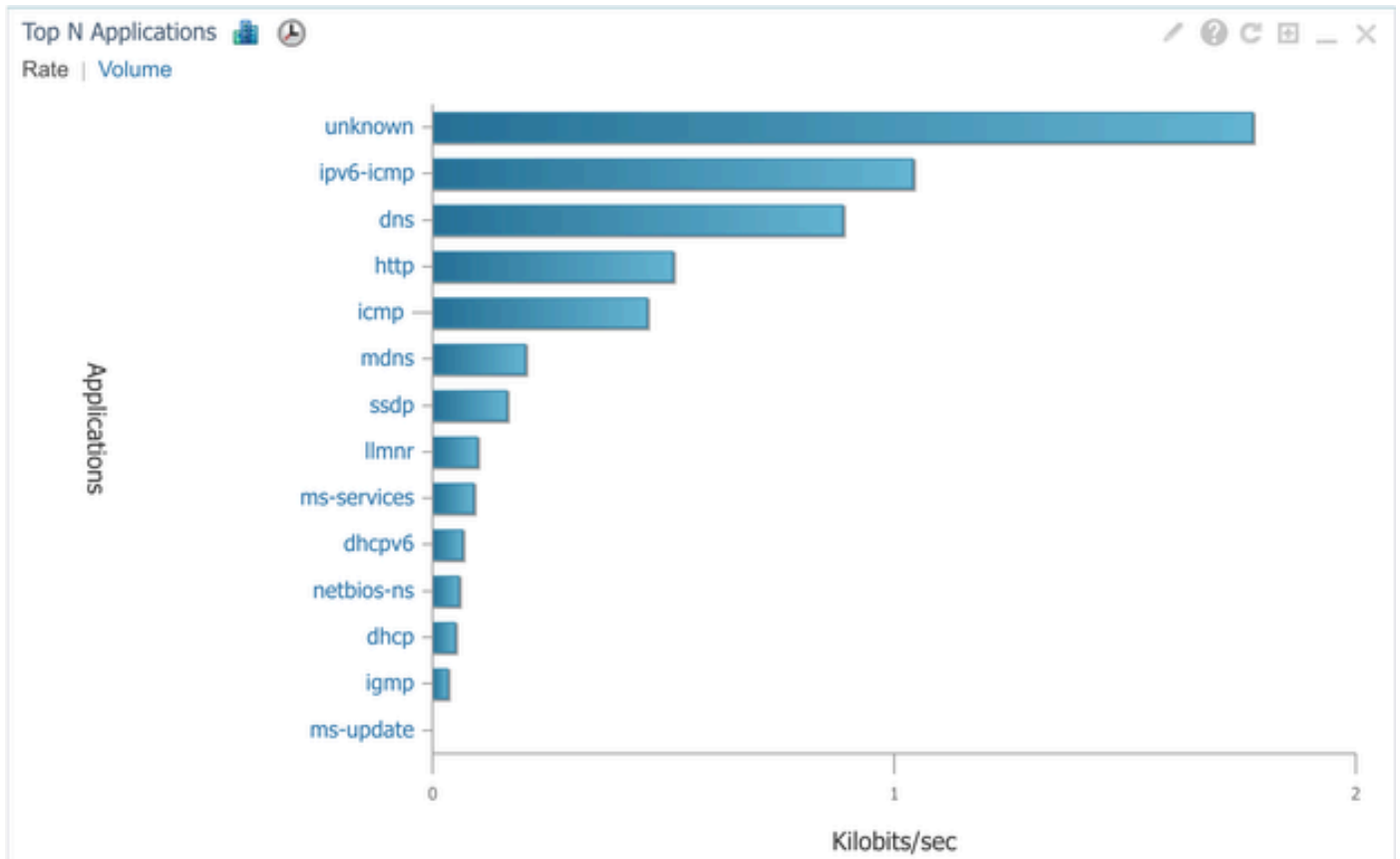
Device Data Sources

Device Name	Data Source	Type	Exporting Device	Last 5 min Flow Record Rate	Last Active Time
<input type="checkbox"/> 9800WLC.cisco.com	10.105.193.156	NETFLOW	10.105.193.156	2	Friday, July 19 2024 at 04:50:18 AM India Stand...

Cisco Prime Detecting 9800 WLC作為Netflow資料來源

您可以使用IP地址，根據應用、服務（甚至按客戶端）設定過濾器，以進行更有針對性的資料分析

o

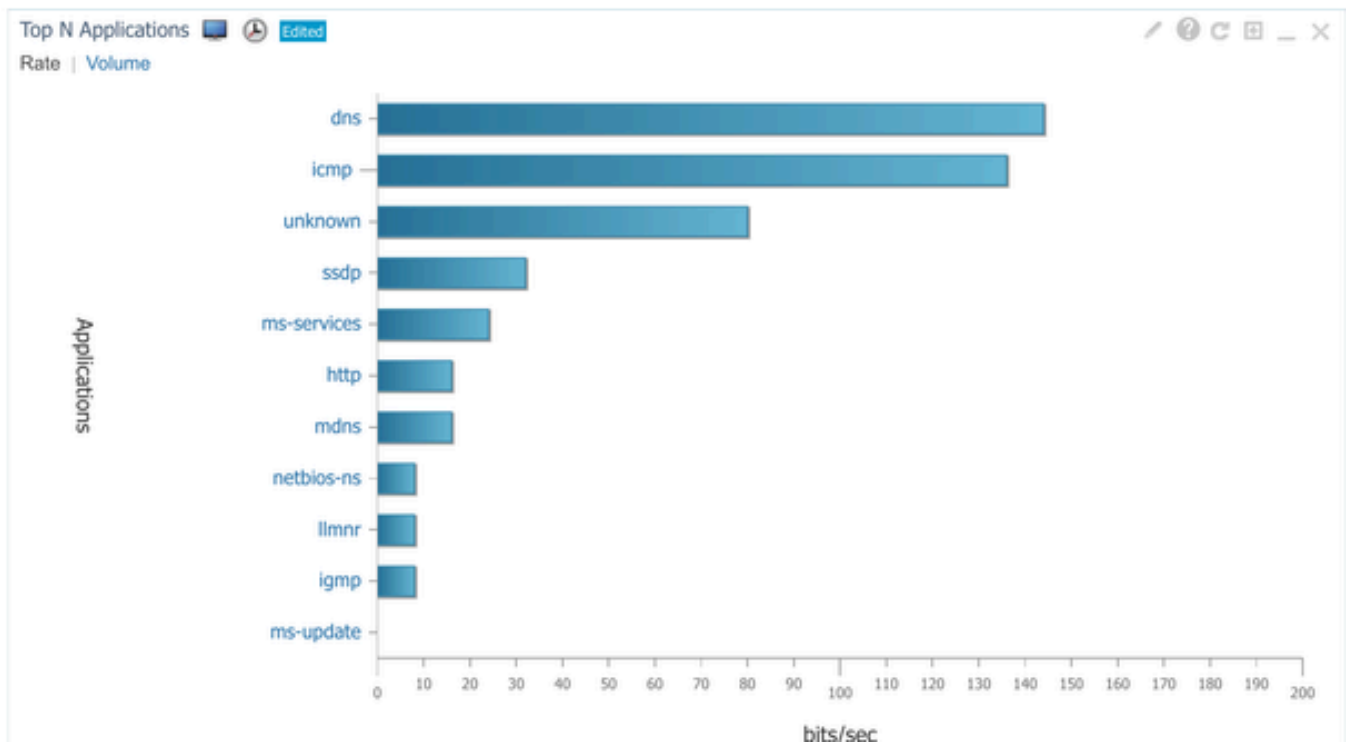


所有客戶端的應用可視性

## Dashboard / Performance

[Site](#) | 
 [Device](#) | 
 [Access Point](#) | 
 [Interface](#) | 
 [Application](#) | 
 [Voice/Video](#) | 
 **[End User Experience](#)**

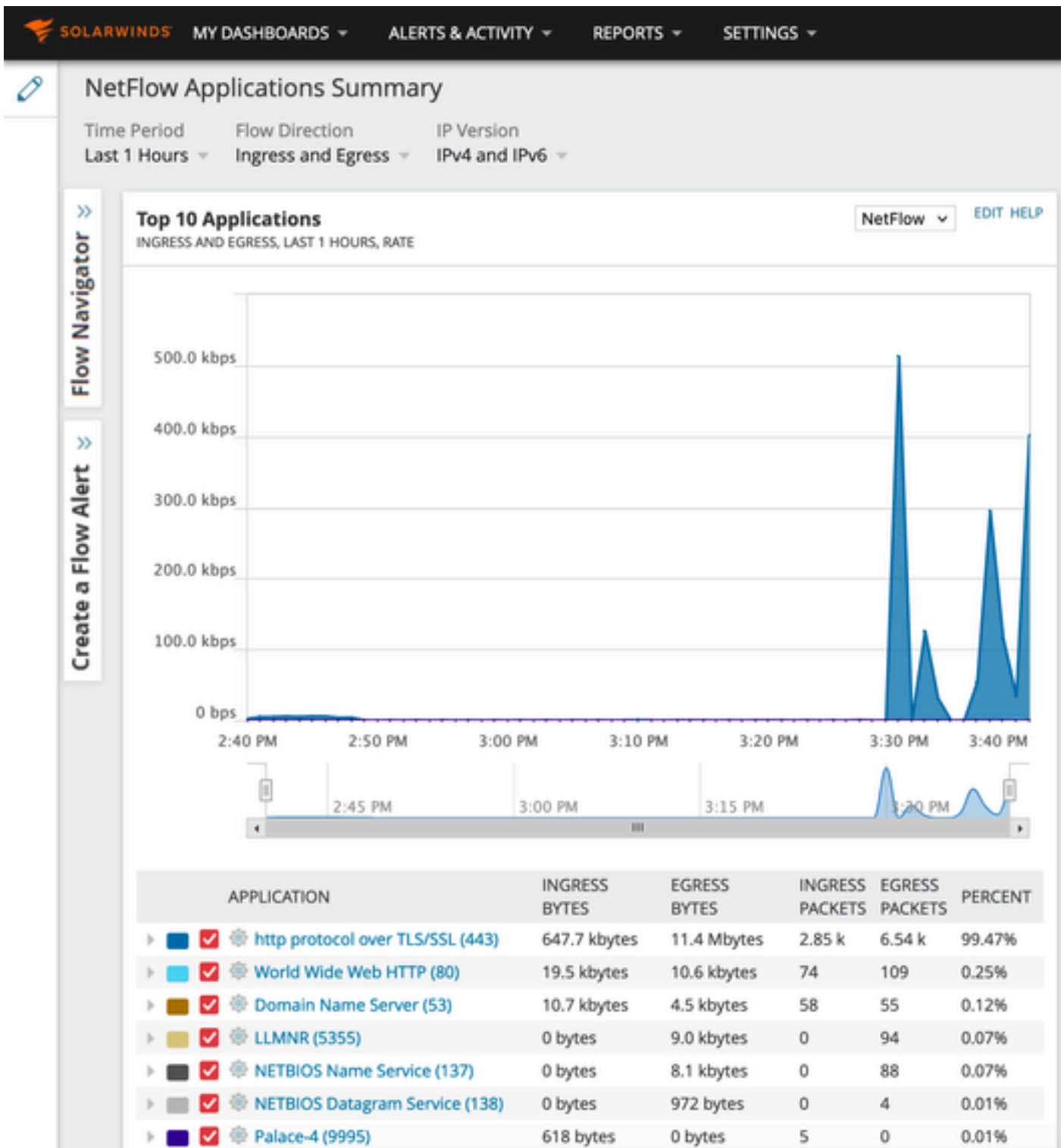
Filters: \*Client: 10.105.193.80,Una... | 
 \*Time Frame: Past 1 Hour | 
 Application: All | 
 Network Aware



使用IP地址的特定客戶端的應用

## 示例2：第三方NetFlow收集器

在本示例中，使用第三方NetFlow收集器[SolarWinds]來收集應用統計資訊。9800 WLC使用Flexible NetFlow (FNF)傳輸有關應用和網路流量的綜合資料，然後由SolarWinds收集。



Netflow在SolarWind中的應用統計

## 流量控制

流量控制是指用於管理和調控網路流量流的一組功能和機制。流量管制或速率限制是無線控制器中

用於控制從客戶端傳輸的流量量的機制。它會監控網路流量的資料速率，並在超過預先定義的速率限制時立即採取行動。當流量超過指定的速率時，速率限制可能會捨棄多餘的封包，或藉由變更其 Class of Service (CoS)或Differentiated Services Code Point (DSCP)值將其降級。這可以透過在 9800 WLC中配置QOS來實現，可以參閱 <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html>以獲取有關這些元件如何工作以及如何配置它們以實現不同結果的概述。

## 疑難排解

排除AVC故障涉及辨識和解決可能影響AVC準確辨識、分類和管理無線網路上應用流量的能力的問題。常見問題可能包括流量分類、策略實施或報告方面的問題。以下是在Catalyst 9800 WLC上排除AVC故障時的一些步驟和注意事項：

- 驗證AVC配置：確保AVC在WLC上配置正確，並與正確的WLAN和配置檔案關聯。
- 當透過GUI設定AVC時，它將自動將埠9995指定為預設值。但是，如果使用外部收集器，請驗證它配置為偵聽哪個埠的NetFlow流量。正確配置此埠號以符合收集器的設定非常重要。
- 驗證AP型號和部署模式支援。
- 在無線網路中實施AVC時，請參閱對9800 WLC的限制。

## 日誌收集

### WLC日誌

1. 啟用時間戳記，以取得所有命令的時間參照。

```
9800WLC#term exec prompt timestamp
```

2. 複查組態

```
9800WLC#show tech-support wireless
```

3. 您可以驗證avc狀態和netflow統計資訊。

檢查AVC配置狀態。

```
9800WLC#show avc status wlan <wlan_name>
```

檢查傳送到控制平面(CP)的FNFv9資料包計數和解碼狀態。

```
9800WLC#show platform software wlavc status decoder
```

檢查來自NetFlow ( FNF快取 ) 的統計資訊。

```
9800WLC#show flow monitor <Flow_Monitor_Name>
```

檢查每個wlan的前n個應用使用情況，其中n = <1-30>輸入應用數。

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
```

檢查每個客戶端的前n個應用程式使用情況，其中n = <1-30>輸入應用程式數。

```
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
```

使用特定應用檢查連線到特定wlan的前n個客戶端，其中n=<1-10>輸入客戶端數。

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
```

檢查nbar統計資訊。

```
9800WLC#show ip nbar protocol-discovery
```

4. 將記錄層次設定為「除錯/詳細」。

```
9800WLC#set platform software trace all debug/verbose
```

!! To View the collected logs

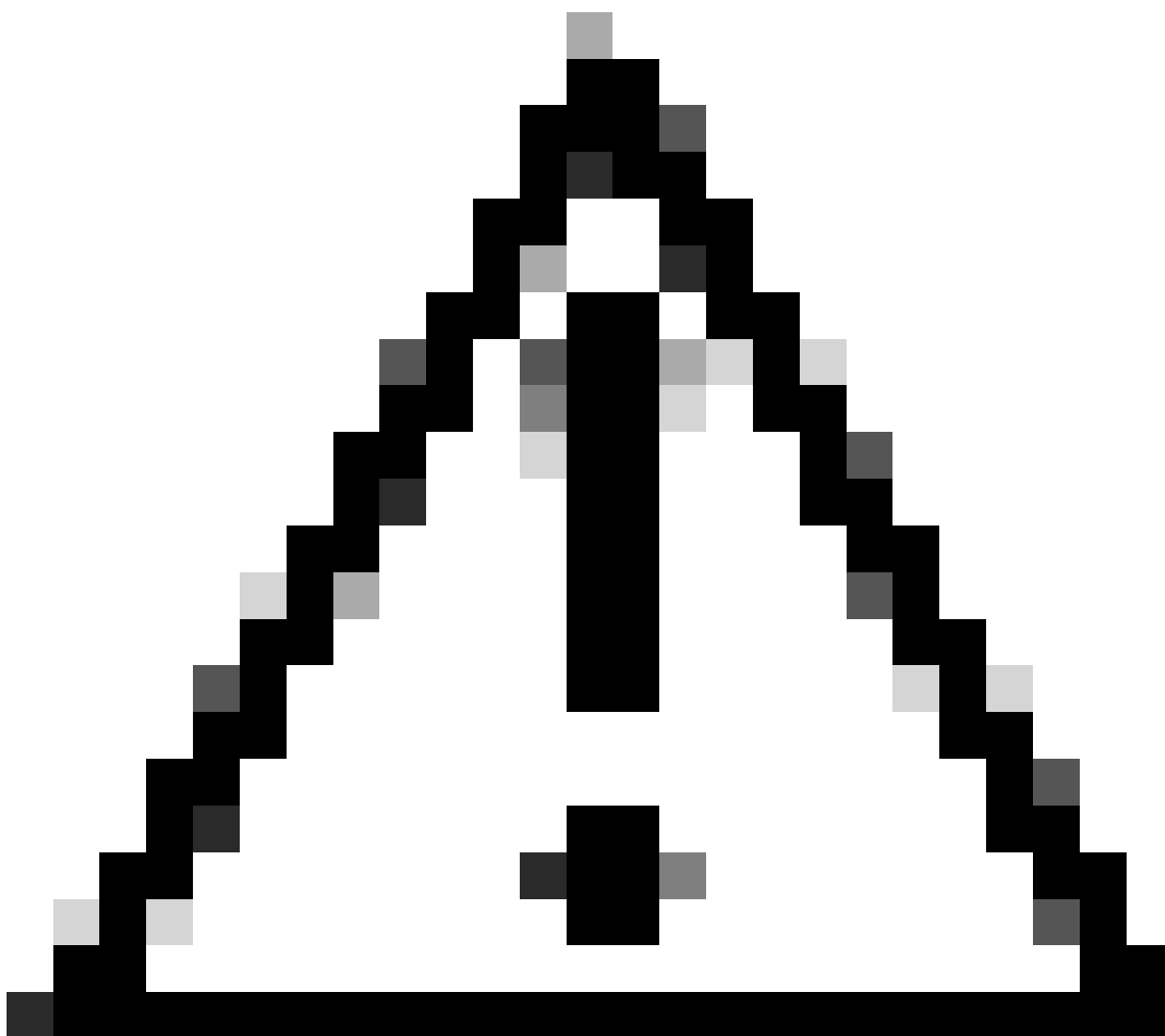
```
9800WLC#show logging profile wireless internal start last clear to-file bootflash:<File_Name>
```

!!Set logging level back to notice post troubleshooting

```
9800WLC#set platform software trace wireless all debug/verbose
```

5. 為客戶端MAC地址啟用放射性(RA)跟蹤以驗證AVC統計資訊。  
透過CLI

```
9800WLLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti
9800WLC#no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
9800WLC#dir bootflash: | i debug
```



注意：條件調試會啟用調試級別日誌記錄，從而增加生成的日誌量。保持此運行狀態可減少從檢視日誌的時間間隔。因此，建議在故障排除會話結束時始終停用調試。

```
# clear platform condition all
# undebug all
```

## 透過GUI

步驟 1. 導航至 Troubleshooting ( 故障排除 ) > Radiative Trace ( 放射性跟蹤 )。

步驟 2. 按一下 Add 並輸入要排除故障的客戶端 Mac 地址。您可以增加多個 Mac 地址進行跟蹤。

步驟 3. 當您準備好開始放射性追蹤時，請按一下「開始」。啟動後，調試日誌記錄將寫入磁碟，記錄與跟蹤的 MAC 地址相關的任何控制層面處理情況。

步驟 4. 當您重現要排除故障的問題時，按一下 Stop。

步驟 5. 對於已調試的每個 mac 地址，您可以透過按一下 Generate 來生成一個日誌檔案，整理屬於該 mac 地址的所有日誌。

步驟 6. 選擇您要經過分頁的日誌檔案保留多長時間，然後按一下 Apply to Device。

步驟 7. 現在您可以按一下檔案名稱旁邊的小圖示來下載檔案。此檔案存在於控制器的開機快閃磁碟機中，也可以透過 CLI 從包裝箱中複製。

以下是 RA 跟蹤中的 AVC 調試簡介

```
2024/07/20 20:15:24.514842337 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514865665 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514875837 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:40.530177442 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
```

6. 按客戶端 MAC 地址雙向過濾的嵌入式捕獲，客戶端內部 MAC 過濾器在 17.1 之後可用。

在使用外部收集器時，它特別有用，因為它有助於確認 WLC 是否按照預期將 NetFlow 資料傳輸到預期埠。

## 透過CLI

```
monitor capture MYCAP clear
monitor capture MYCAP interface <Interface> both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!! Initiate different application traffic from user
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:../filename.pcap
```

## 透過GUI

步驟 1. 導航到故障排除 > 資料包捕獲 > + 增加。



步驟 2. 定義資料包捕獲的名稱。最多允許8個字元。

步驟 3. 定義篩選條件 ( 如果有 )。

步驟 4. 如果希望看到流量被傳送至系統CPU並注入資料平面中，請選中此框以監控控制流量。

步驟 5. 定義緩衝區大小。最多允許100 MB。

步驟 6. 根據需要定義允許範圍1 - 1000000秒的期限或允許範圍1 - 100000個資料包的資料包數量。

步驟 7. 從左側列中的介面清單中選擇介面，並選擇箭頭將其移動到右側列。

步驟 8. 按一下Apply to Device。

步驟 9. 要啟動捕獲，請選擇開始。

步驟 10. 您可以讓擷取執行到定義的限制。要手動停止捕獲，請選擇停止。

步驟 11. 一旦停止，就可以使用Export按鈕和選項進行按一下，以透過HTTP或TFTP伺服器、FTP伺服器、本地系統硬碟或快閃記憶體將捕獲檔案(.pcap)下載到本地案頭。

## AP日誌

在交換矩陣和Flex模式下

1. show tech顯示AP的所有配置詳細資訊和客戶端統計資訊。

2. 顯示來自無線存取點的avc nbar統計資訊nbar統計資訊

3. AVC調試

```
AP#term mon
AP#debug capwap client avc <all/detail/error/event>
AP#debug capwap client avc netflow <all/detail/error/event/packet>
```

## 相關資訊

[AVC配置指南](#)

[9800 WLC上的速率限制](#)

## 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）。