

Conoscenza di AVC sul controller LAN wireless Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisito](#)

[Informazioni su Visibilità e controllo delle applicazioni \(AVC\)](#)

[Funzionamento di AVC](#)

[Riconoscimento applicazioni basato su rete \(NBAR\)](#)

[Abilita protocollo NBAR sul profilo criteri](#)

[Aggiornamento di NBAR su 9800 WLC](#)

[NetFlow](#)

[Flexible NetFlow](#)

[Monitoraggio flusso](#)

[Access point supportati da AVC](#)

[Supporto per diverse modalità di installazione 9800](#)

[Restrizioni durante l'implementazione di AVC su 9800](#)

[Topologia della rete](#)

[AP In Modalità Locale](#)

[AP in modalità flex](#)

[Configurazione di AVC su 9800 WLC](#)

[Esportatore locale](#)

[External NetFlow Collector](#)

[Configurazione di AVC su 9800 WLC con Cisco Catalyst Center](#)

[Verifica dell'AVC](#)

[Su 9800](#)

[Su DNAC](#)

[In External NetFlow Collector](#)

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

[Esempio 2: agente di raccolta NetFlow di terze parti](#)

[Controllo del traffico](#)

[Risoluzione dei problemi](#)

[Raccolta log](#)

[Log WLC](#)

[Log AP](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive l'AVC (Application Visibility and Control) su un Cisco Catalyst 9800 WLC, che consente una gestione precisa del traffico delle applicazioni.

Prerequisito

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Cisco WLC 9800.
- Conoscenze base dei punti di accesso in modalità di connessione locale e flessibile.
- I punti di accesso devono essere compatibili con AVC. (Non applicabile con la modalità locale AP)
- Affinché la parte di controllo di AVC (QoS) funzioni, è necessario configurare la funzionalità di visibilità dell'applicazione con FNF.

Informazioni su Visibilità e controllo delle applicazioni (AVC)

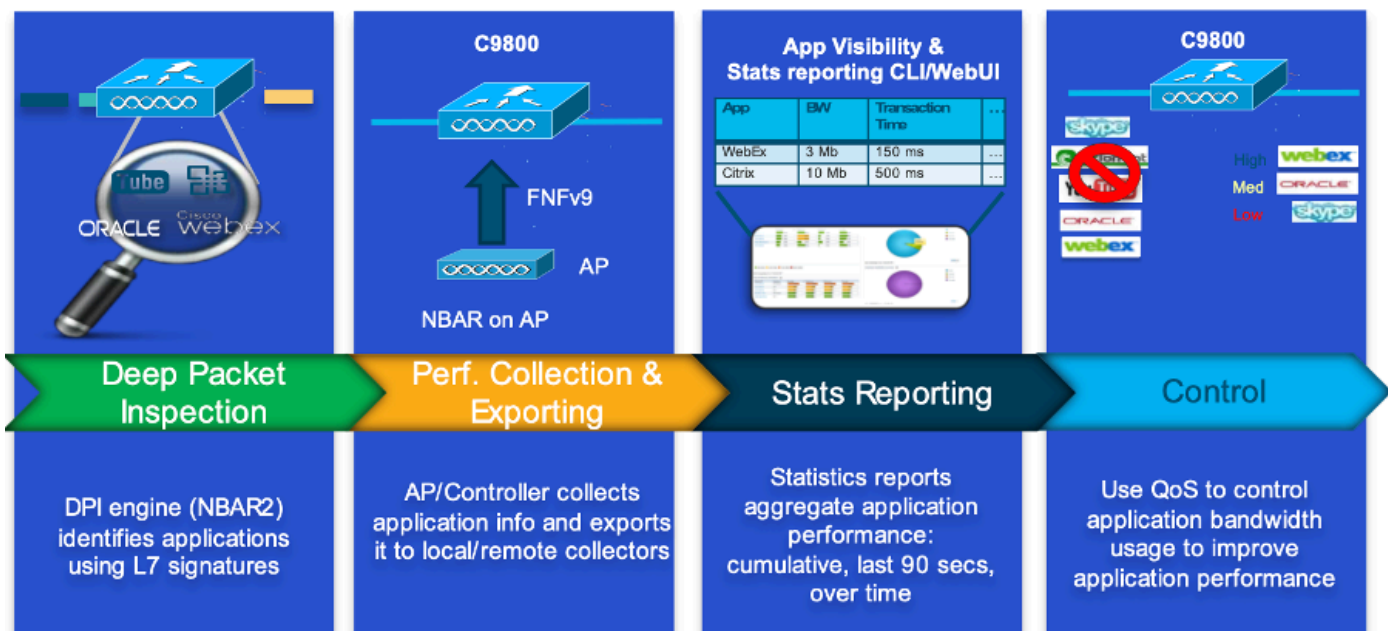
Application Visibility and Control (AVC) è l'approccio leader di Cisco per la tecnologia DPI (Deep-Packet Inspection) nelle reti wireless e cablate. Con AVC è possibile eseguire analisi in tempo reale e creare regole per ridurre efficacemente la congestione della rete, ridurre al minimo il costoso utilizzo dei collegamenti di rete ed evitare inutili aggiornamenti dell'infrastruttura. In breve, AVC consente agli utenti di raggiungere un livello completamente nuovo di riconoscimento e shaping del traffico tramite NBAR (Network Based Application Recognition). I pacchetti NBAR in esecuzione sul WLC 9800 vengono utilizzati per DPI e i risultati vengono riportati utilizzando Flexible NetFlow (FNF).

Oltre alla visibilità, AVC consente di assegnare priorità, bloccare o limitare diversi tipi di traffico. Ad esempio, gli amministratori possono creare policy che assegnano priorità alle applicazioni voce e video per garantire la qualità del servizio (QoS) o limitare la larghezza di banda disponibile per le applicazioni non essenziali durante le ore di punta. Può inoltre essere integrato con altre tecnologie Cisco, ad esempio Cisco Identity Services Engine (ISE) per le policy applicative basate sull'identità e Cisco Catalyst Center per la gestione centralizzata.

Funzionamento di AVC

AVC utilizza tecnologie avanzate, quali FNF e motore NBAR2 per DPI. Analizzando e identificando i flussi di traffico tramite il motore NBAR2, i flussi specifici vengono contrassegnati con il protocollo o l'applicazione riconosciuti. Il controller raccoglie tutti i report e li presenta tramite i comandi show, l'interfaccia utente Web o altri messaggi di esportazione NetFlow agli agenti di raccolta NetFlow esterni come Prime.

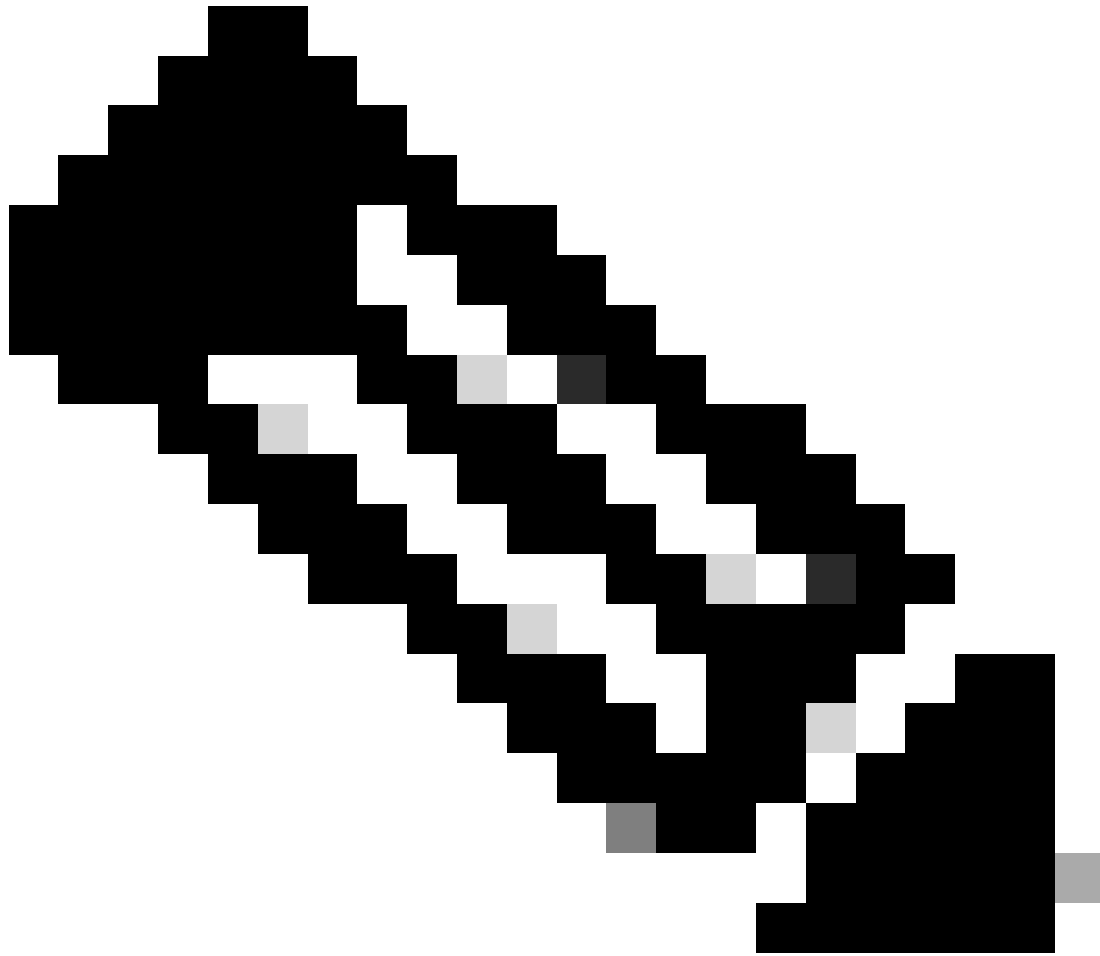
Una volta stabilita la visibilità dell'applicazione, gli utenti possono creare regole di controllo con meccanismi di controllo per i client configurando QoS (Quality of Service).



Meccanismo di lavoro dell'AVC

Riconoscimento applicazioni basato su rete (NBAR)

NBAR è un meccanismo integrato nel 9800 WLC, utilizzato per eseguire DPI per identificare e classificare un'ampia varietà di applicazioni in esecuzione su una rete. È in grado di riconoscere e classificare un vasto numero di applicazioni, incluse le applicazioni crittografate e quelle con mappatura dinamica delle porte, che sono spesso invisibili alle tradizionali tecnologie di ispezione dei pacchetti.



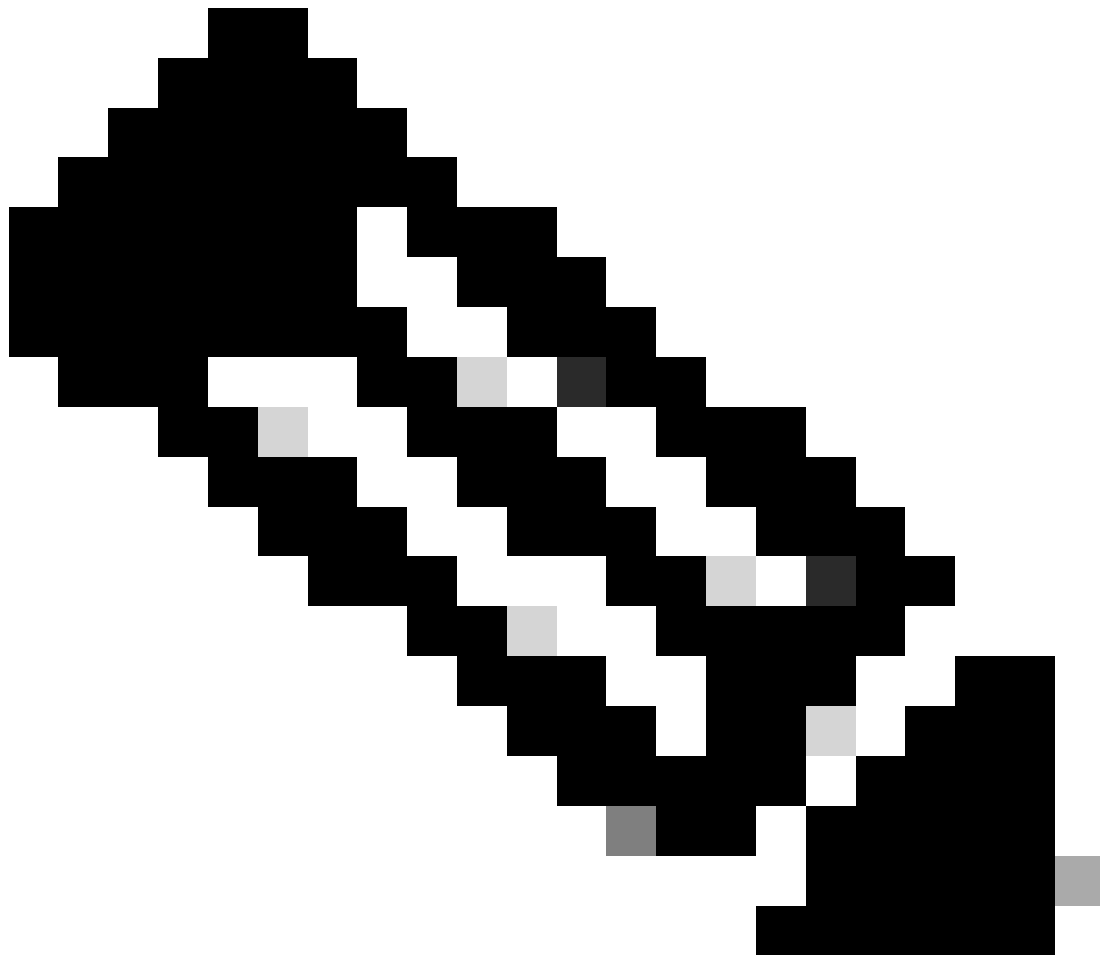
Nota: per utilizzare NBAR sul WLC di Catalyst 9800, è necessario abilitarlo e configurarlo correttamente, spesso in combinazione con profili AVC specifici che definiscono le azioni appropriate da intraprendere in base alla classificazione del traffico.

NBAR continua ad essere aggiornato periodicamente ed è importante mantenere aggiornato il software WLC per garantire che il set di funzionalità NBAR rimanga attuale ed efficace.

Un elenco completo dei protocolli supportati nelle ultime versioni è disponibile all'indirizzo https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Abilita protocollo NBAR sul profilo criteri

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



Nota: per eseguire questa operazione, è necessario disabilitare il profilo criteri %.

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

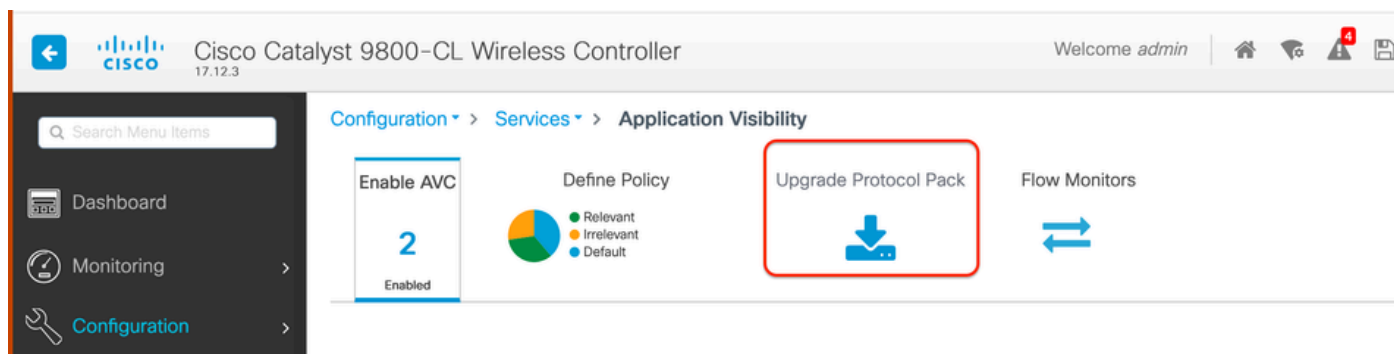
Aggiornamento di NBAR su 9800 WLC

9800 WLC dispone già di circa 1500 applicazioni riconoscibili. Nel caso in cui venga rilasciata una nuova applicazione, il protocollo corrispondente verrà aggiornato nell'ultima NBAR che sarà necessario scaricare dalla pagina di download del software per il modello 9800 specifico.

Tramite GUI

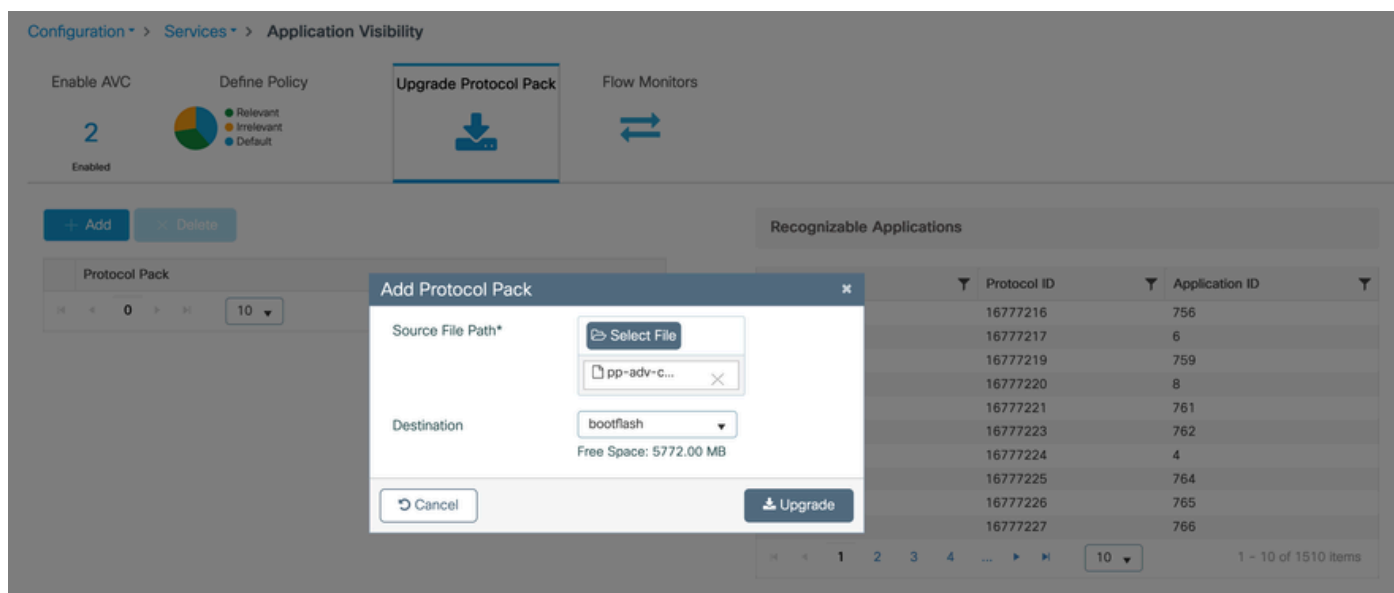
Passare a Configurazione > Servizi > Visibilità applicazione. Fare clic su Aggiorna pacchetto di

protocollo.



Caricamento della sezione del protocollo in 9800 WLC

Fare clic su Add, quindi scegliere il pacchetto del protocollo da scaricare e fare clic su Upgrade (Aggiorna).



Aggiunta del protocollo NBAR

Al termine dell'aggiornamento, verrà aggiunto il pacchetto del protocollo.

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

1 10 1 - 1 of 1 items

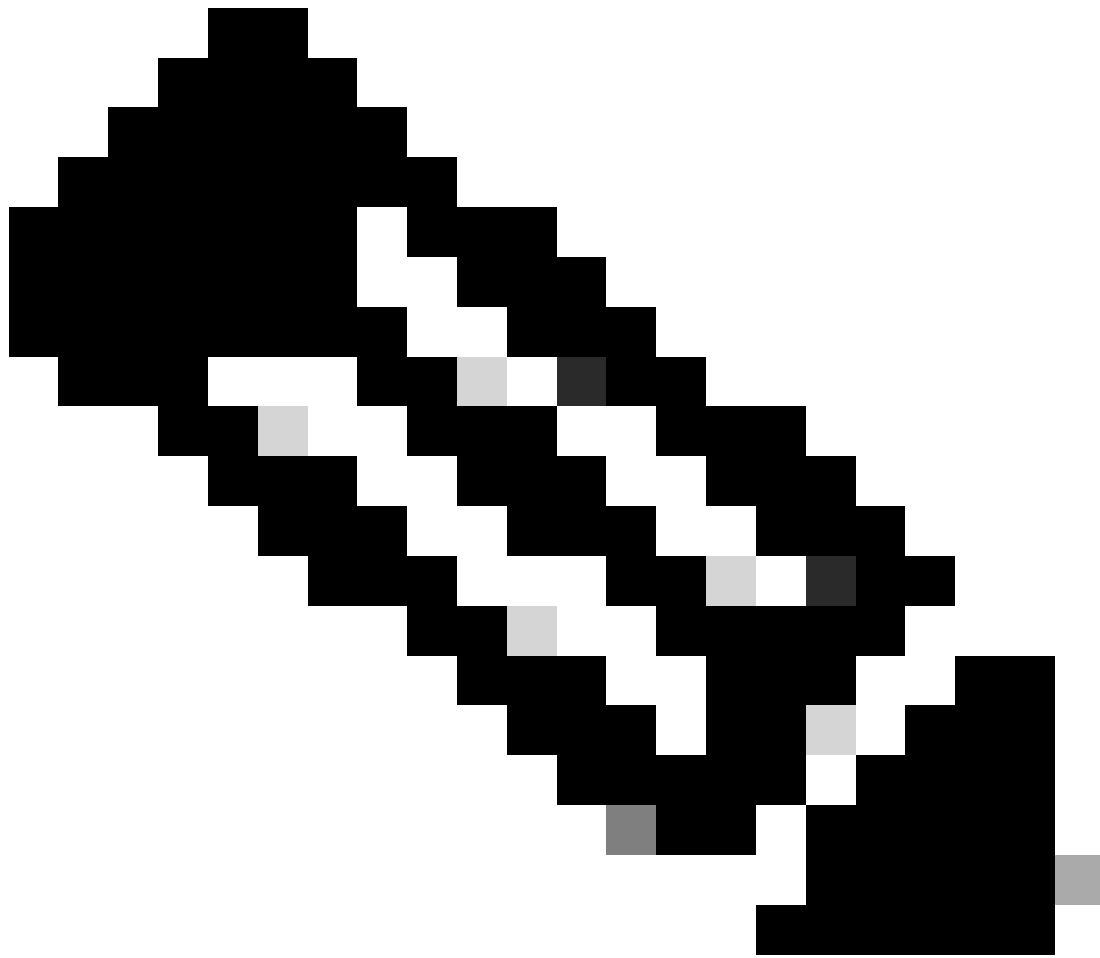
Verifica del Protocol Pack

Tramite 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
```



Nota: non si verificheranno interruzioni del servizio durante l'aggiornamento del pacchetto di protocollo NBAR.

NetFlow

NetFlow è un protocollo di rete utilizzato per raccogliere informazioni sul traffico IP e monitorare i dati del flusso di rete. Viene utilizzato principalmente per l'analisi del traffico di rete e il monitoraggio della larghezza di banda. Di seguito è riportata una panoramica del funzionamento di NetFlow sui controller Cisco Catalyst serie 9800:

- Raccolta dei dati: 9800 WLC raccoglie i dati sul traffico IP che vi passa attraverso. Questi dati includono informazioni quali gli indirizzi IP di origine e di destinazione, le porte di origine e di destinazione, i protocolli utilizzati, la classe di servizio e la causa della terminazione del flusso.
- Record di flusso: i dati raccolti sono organizzati in record di flusso. Un flusso è definito come una sequenza unidirezionale di pacchetti che condividono un insieme di attributi comuni, ad

esempio lo stesso IP di origine/destinazione, le stesse porte di origine/destinazione e lo stesso tipo di protocollo.

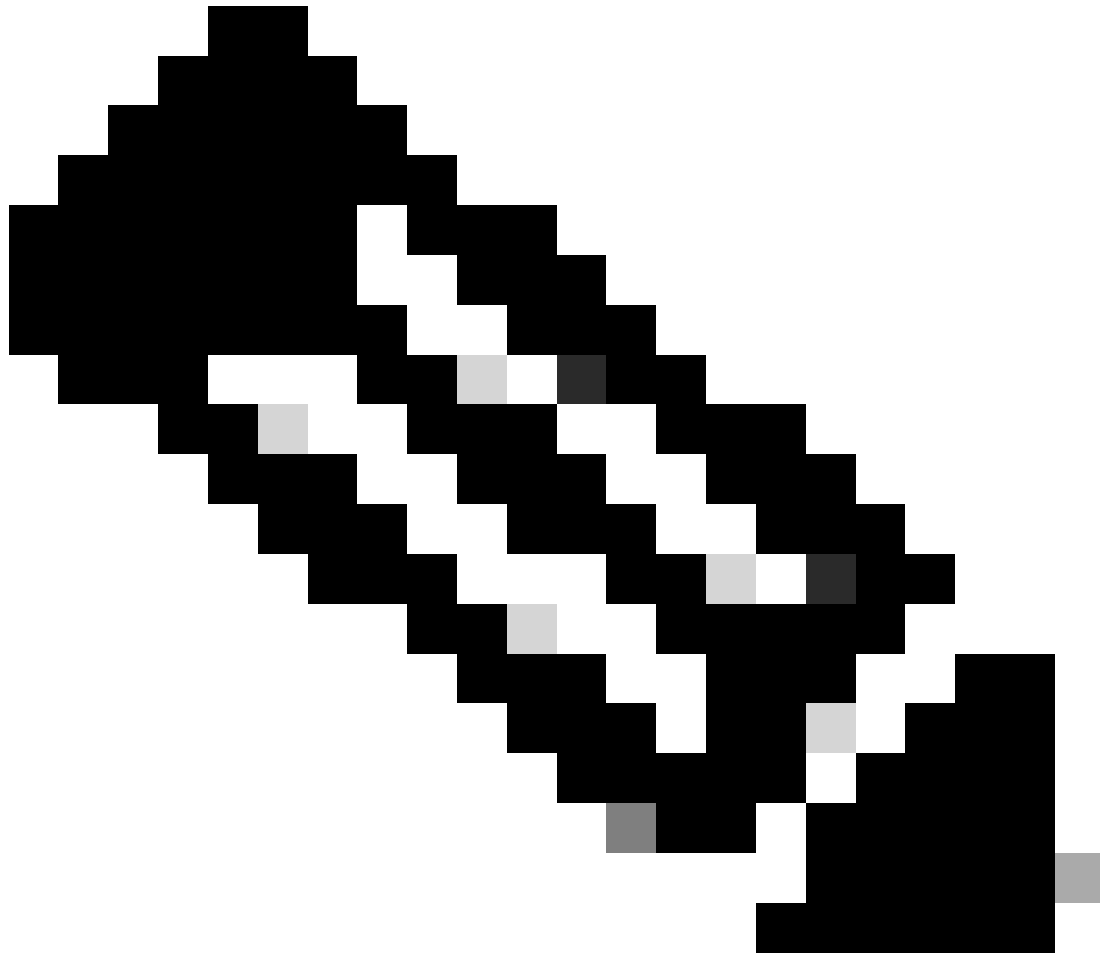
- Esportazione dei dati: i record di flusso vengono esportati periodicamente dal dispositivo abilitato per NetFlow a un raccogliatore NetFlow. L'agente di raccolta può essere un WLC locale o un server dedicato o un'applicazione software che riceve, archivia ed elabora i dati di flusso.
- Analisi: è possibile utilizzare gli agenti di raccolta e gli strumenti di analisi NetFlow per visualizzare i modelli di traffico, identificare la larghezza di banda, rilevare flussi di traffico insoliti che indicano violazioni della sicurezza, ottimizzare le prestazioni della rete e pianificare l'espansione della rete.
- Informazioni specifiche per la rete wireless: nel contesto dei controller wireless, NetFlow può includere informazioni aggiuntive specifiche per la rete wireless, quali il SSID, i nomi dei punti di accesso, gli indirizzi MAC dei client e altri dettagli relativi al traffico Wi-Fi.

Flexible NetFlow

Flexible NetFlow (FNF) è una versione avanzata di NetFlow tradizionale ed è supportata dai Cisco Catalyst serie 9800 Wireless LAN Controller (WLC). Offre un maggior numero di opzioni di personalizzazione per il monitoraggio, il monitoraggio e l'analisi dei modelli di traffico di rete. Le caratteristiche principali di Flexible NetFlow sul Catalyst 9800 WLC includono:

- Personalizzazione: FNF consente agli utenti di definire quali informazioni raccogliere dal traffico di rete. Tra queste, una vasta gamma di attributi del traffico, come indirizzi IP, numeri di porta, timestamp, conteggi di pacchetti e byte, tipi di applicazioni e altro ancora.
- Visibilità migliorata: sfruttando il FNF, gli amministratori ottengono una visibilità dettagliata dei tipi di traffico che passano attraverso la rete, essenziale per la pianificazione della capacità, la fatturazione della rete basata sull'uso, l'analisi della rete e il monitoraggio della sicurezza.
- Indipendenza dal protocollo: il protocollo FNF è sufficientemente flessibile da supportare diversi protocolli oltre l'IP, adattandosi ai diversi tipi di ambienti di rete.

Sul Catalyst 9800 WLC, è possibile configurare FNF per esportare i record di flusso in un'applicazione di raccolta o analisi NetFlow esterna. Questi dati possono quindi essere utilizzati per la risoluzione dei problemi, la pianificazione di rete e l'analisi della protezione. La configurazione FNF implica la definizione di un record di flusso (cosa raccogliere), un esportatore di flusso (dove inviare i dati) e l'associazione del monitor di flusso (che lega il record e l'esportatore) alle interfacce appropriate.



Nota: FNF è in grado di inviare 17 record di dati diversi (come definito nella RFC 3954) al programma di raccolta Netflow esterno di terze parti, ad esempio Stealthwatch, Solarwinds e altri che sono: codice di matricola, indirizzo Mac del client, indirizzo Mac del punto di accesso, WlanID, IP di origine, IP di destinazione, porta di origine, porta di destinazione, protocollo, ora di inizio del flusso, ora di fine del flusso, direzione, uscita pacchetto, conteggio byte, ID VLAN (modalità locale) - Mgmt/Client e TOS - valore DSCP

Monitoraggio flusso

Un monitor di flusso è un componente utilizzato in combinazione con Flexible NetFlow (FNF) per acquisire e analizzare i dati del traffico di rete. Svolge un ruolo cruciale nel monitoraggio e nella comprensione dei modelli di traffico per la gestione della rete, la sicurezza e la risoluzione dei problemi. Il monitor di flusso è essenzialmente un'istanza applicata di FNF che raccoglie e tiene traccia dei dati di flusso in base a criteri definiti. Esso è associato a tre elementi principali:

- Record di flusso: definisce i dati che il monitor di flusso deve raccogliere dal traffico di rete. Specifica le chiavi (ad esempio indirizzi IP di origine e di destinazione, porte, tipi di

protocollo) e i campi non chiave (ad esempio contatori di pacchetti e byte, timestamp) che verranno inclusi nei dati di flusso.

- Esportatore flusso: specifica la destinazione a cui devono essere inviati i dati di flusso raccolti. Include dettagli come l'indirizzo IP del collector NetFlow, il protocollo di trasporto (generalmente UDP) e il numero della porta di destinazione dove il collector è in ascolto.
- Monitor di flusso: il monitor di flusso stesso associa il record di flusso e l'utilità di esportazione e li applica a un'interfaccia o a una WLAN per avviare effettivamente il processo di monitoraggio. Determina il modo in cui i dati di flusso devono essere raccolti ed esportati in base ai criteri impostati nel record di flusso e alla destinazione impostata nell'utilità di esportazione flusso.

Access point supportati da AVC

AVC è supportato solo sui seguenti access point:

- Cisco Catalyst serie 9100 Access Point
- Cisco Aironet serie 2800 Access Point
- Cisco Aironet serie 3800 Access Point
- Cisco Aironet serie 4800 Access Point

Supporto per diverse modalità di installazione 9800

Modalità di distribuzione	9800 WLC	Access point Wave 1	Access point Wave 2	Access Point Wifi 6
Modalità locale (commutazione centrale)	Traffico IPV4: AVC supportato FNF supportato Traffico IPV6: AVC supportato FNF supportato	Elaborazione a livello WLC	Elaborazione a livello WLC	Elaborazione a livello WLC
Modalità Flex (commutazione centrale)	Traffico IPV4: AVC supportato FNF supportato Traffico IPV6: AVC supportato FNF supportato	Elaborazione a livello WLC	Elaborazione a livello WLC	Elaborazione a livello WLC
Modalità Flex (Switching locale)	Elaborazione a livello AP	Traffico IPV4: AVC supportato	Traffico IPV4: AVC supportato	Traffico IPV4: AVC supportato

		FNF supportato Traffico IPV6: AVC supportato FNF non supportato	FNF supportato Traffico IPV6: AVC supportato FNF supportato	FNF supportato Traffico IPV6: AVC supportato FNF supportato
Modalità locale (fabric)	Elaborazione a livello AP	Traffico IPV4: AVC non supportato FNF non supportato Traffico IPV6: AVC non supportato FNF non supportato	Traffico IPV4: AVC supportato FNF supportato Traffico IPV6: AVC supportato FNF supportato	Traffico IPV4: AVC supportato FNF supportato Traffico IPV6: AVC supportato FNF supportato

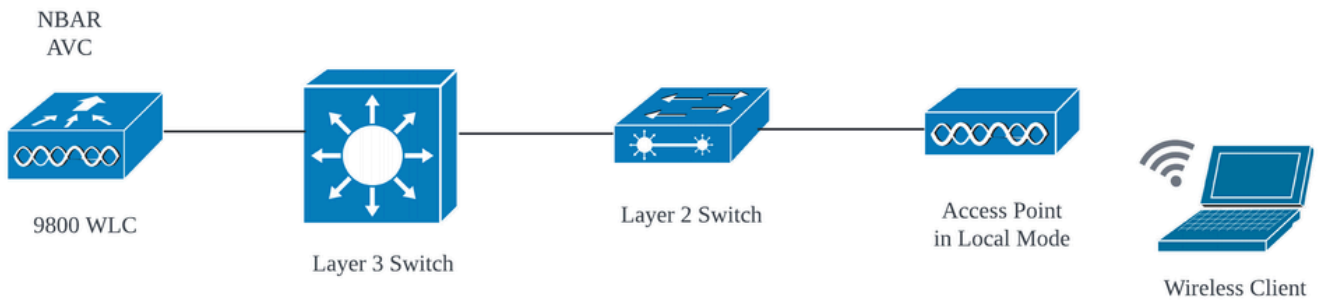
Restrizioni durante l'implementazione di AVC su 9800

Sia AVC (Application Visibility and Control) che FNF (Flexible NetFlow) sono potenti funzionalità dei Cisco Catalyst serie 9800 Wireless LAN Controller che migliorano la visibilità e il controllo della rete. È tuttavia necessario tenere presenti alcune limitazioni e considerazioni quando si utilizzano queste funzionalità:

- Il roaming di livello 2 non è supportato tra i controller.
- Traffico multicast non supportato.
- Per l'applicazione del controllo QoS è possibile utilizzare solo le applicazioni riconosciute con visibilità App.
- Collegamento dati non supportato per i campi NetFlow in AVC.
- Non è possibile mappare lo stesso profilo WLAN sia al profilo dei criteri non abilitato per AVC che al profilo dei criteri abilitato per AVC.
- Non è possibile utilizzare il profilo della policy con un meccanismo di commutazione diverso per la stessa WLAN per implementare AVC.
- AVC non è supportato sulla porta di gestione (Gig 0/0).
- La configurazione dei criteri QoS basati su NBAR è consentita solo su porte fisiche cablate. La configurazione dei criteri non è supportata sulle interfacce virtuali, ad esempio VLAN, canale della porta e altre interfacce logiche.
- Quando AVC è attivato, il profilo AVC supporta solo 23 regole, inclusa la regola DSCP predefinita. Se le regole sono superiori a 23, i criteri AVC non verranno trasferiti all'access point.

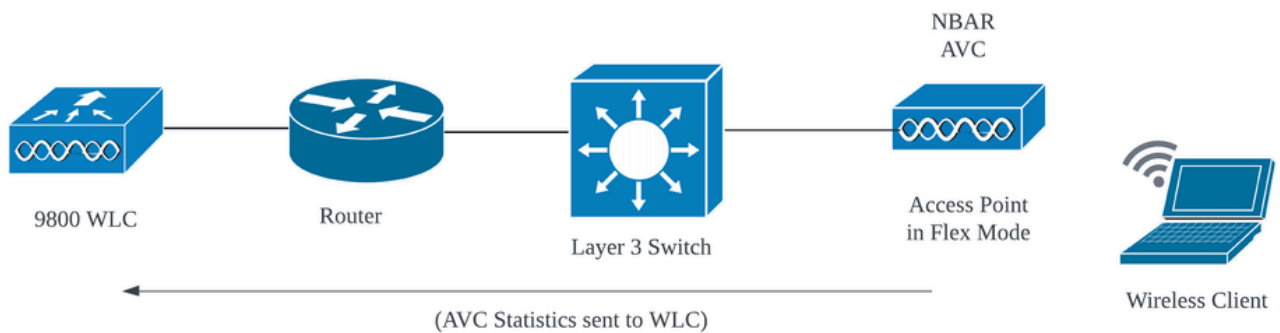
Topologia della rete

AP In Modalità Locale



AVC in modalità locale AP (switching centrale)

AP in modalità flex



AVC in modalità Flex AP

Configurazione di AVC su 9800 WLC

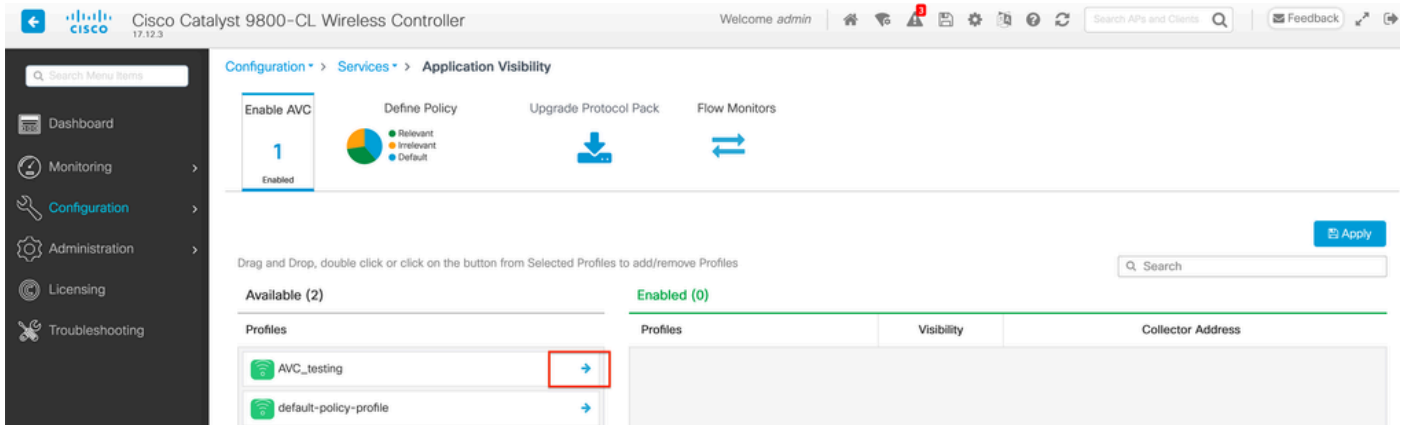
Durante la configurazione di AVC su 9800 WLC, è possibile utilizzarlo come NetFlow Collector o esportare i dati NetFlow in External NetFlow Collector.

Esportatore locale

Su un Cisco Catalyst 9800 Wireless LAN Controller (WLC), un agente di raccolta di NetFlow locale si riferisce alla funzionalità integrata nel WLC che consente di raccogliere e memorizzare localmente i dati NetFlow. Questa funzionalità consente al WLC di eseguire l'analisi dei dati NetFlow di base senza esportare i record di flusso in un agente di raccolta NetFlow esterno.

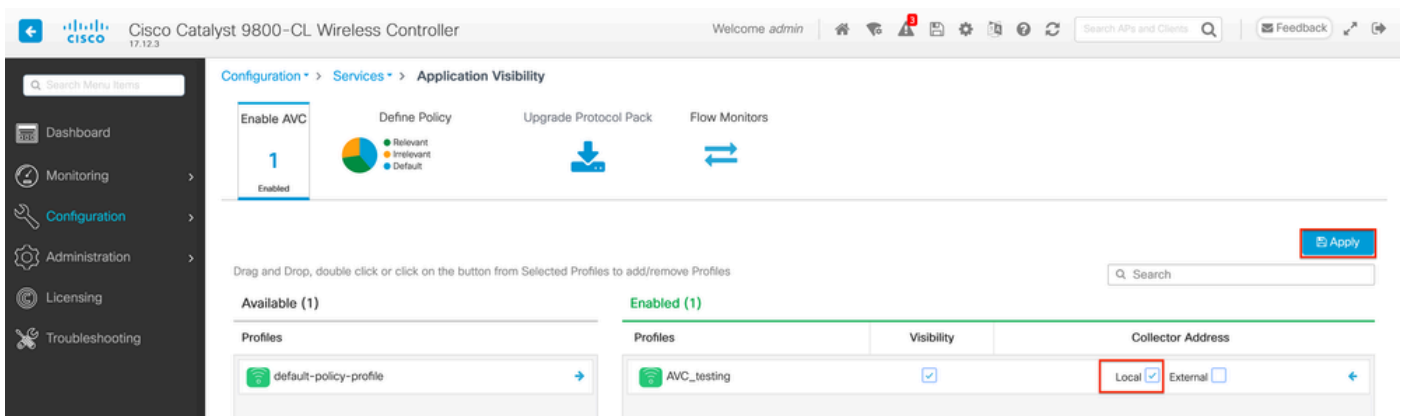
Tramite GUI

Passaggio 1: Per abilitare AVC su SSID specifico, passare a Configurazione > Servizi > Visibilità applicazione. Scegliere il profilo criteri specifico per il quale si desidera attivare AVC.



Abilitazione di AVC nel profilo dei criteri

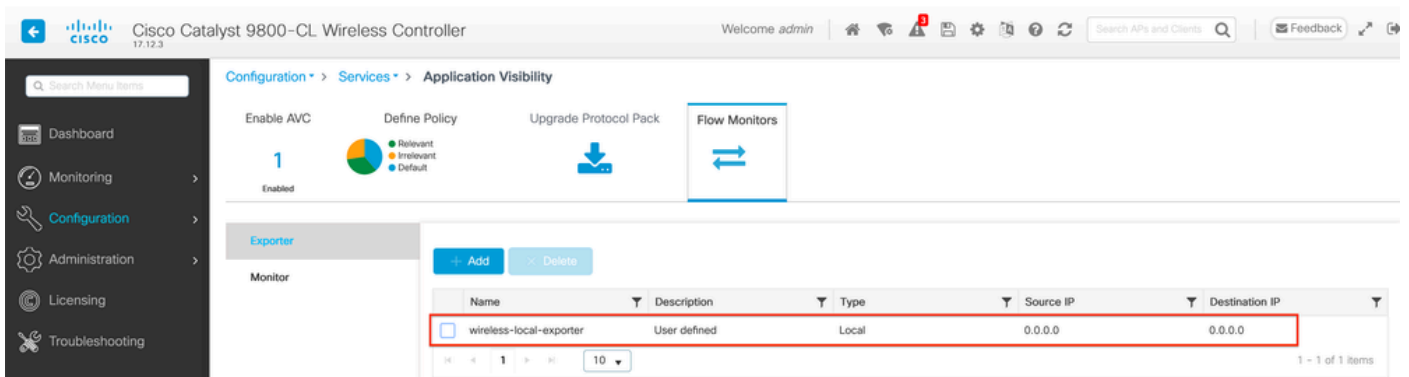
Passaggio 2: selezionare Local come Netflow Collector e fare clic su Apply.



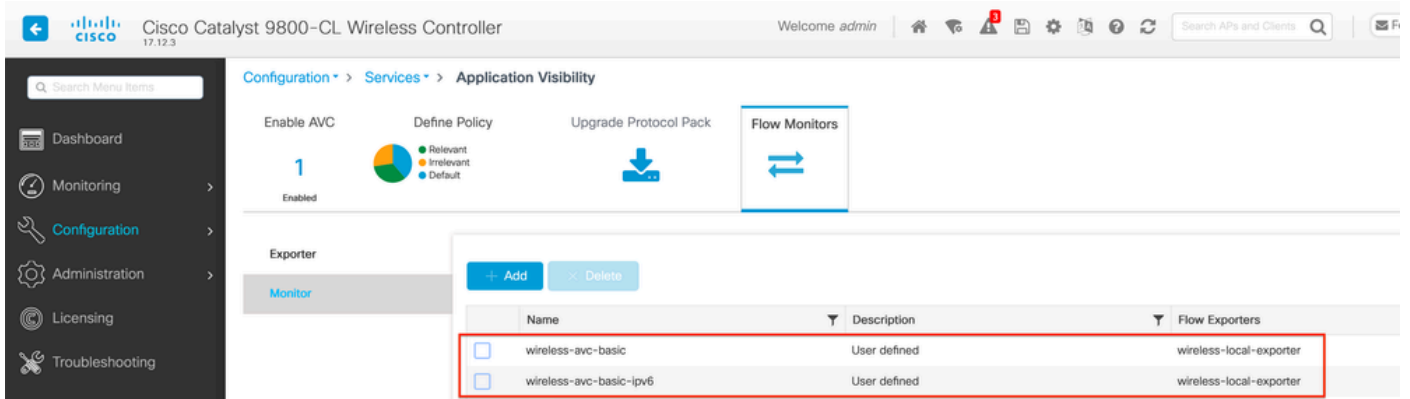
Selezione di Local NetFlow Collector

Una volta applicata la configurazione AVC, le impostazioni di NetFlow Exporter e NetFlow sono state configurate automaticamente in base alle preferenze specificate.

È possibile convalidare la stessa operazione selezionando Configurazione > Servizi > Visibilità applicazione > Monitor di flusso > Esportatore/monitor.

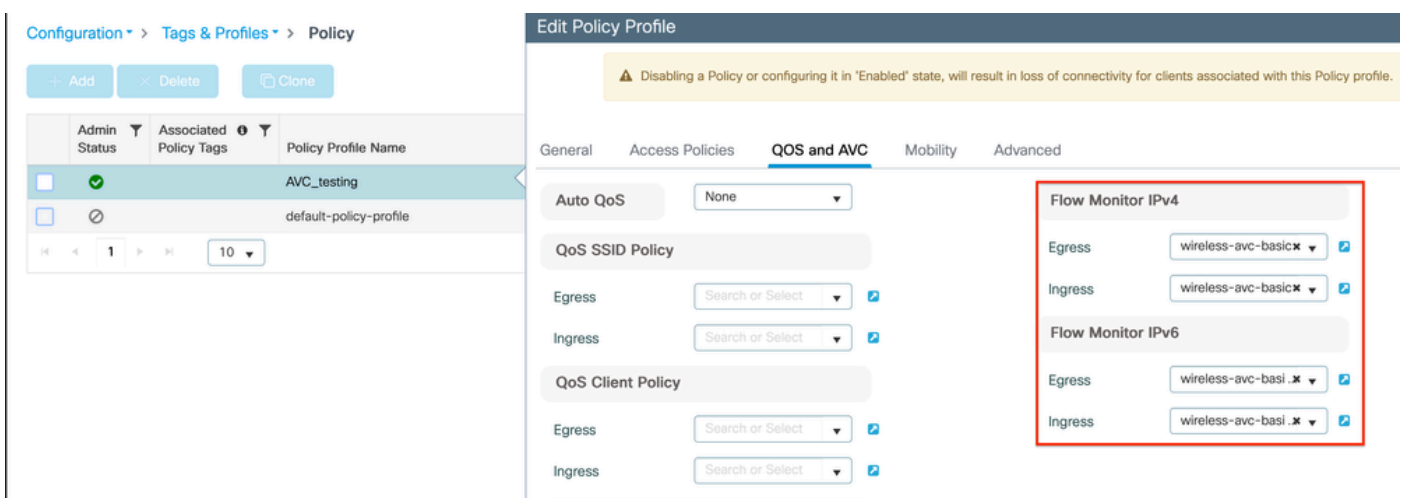


Configurazione Local Flow Collector su 9800 WLC



Configurazione del monitoraggio del flusso con l'agente di raccolta NetFlow locale

I monitor di flusso AVC IPv4 e IPv6 verranno associati automaticamente al profilo dei criteri. Selezionare Configurazione > Tag e profilo > Criterio. Fare clic su Policy Profile > AVC and QOS .



Configurazione Di Flow Monitor Nel Profilo Dei Criteri

Tramite CLI

Fase 1. Configurare 9800 WLC come Local Exporter.

```
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
```

Fase 2. Configurare IPv4 e IPv6 Network Flow Monitor per utilizzare Local(WLC) come Netflow Exporter.

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

Passaggio 3: mappare il monitoraggio del flusso IPv4 e IPv6 nel profilo dei criteri per il traffico in entrata e in uscita.

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

Disabling policy profile will result in associated AP/Client rejoin

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

External NetFlow Collector

Un agente di raccolta NetFlow esterno, quando utilizzato nel contesto di AVC (Application Visibility and Control) su un controller WLC (Cisco Catalyst 9800 Wireless LAN Controller), è un sistema o un servizio dedicato che riceve, aggrega e analizza i dati NetFlow esportati dal WLC. È possibile configurare solo l'agente di raccolta NetFlow esterno per monitorare la visibilità dell'applicazione oppure utilizzarlo insieme all'agente di raccolta locale.

Tramite GUI

Passaggio 1: Per abilitare AVC su SSID specifico, passare a Configurazione > Servizi > Visibilità applicazione. Scegliere il profilo criteri specifico per il quale si desidera attivare AVC. Selezionare Collector as External (Raccoglitore esterno) e configurare l'indirizzo IP di NetFlow Collector come Cisco Prime, SolarWind, StealthWatch, quindi fare clic su Apply (Applica).

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The navigation path is Configuration > Services > Application Visibility. The 'Enable AVC' toggle is set to 'Enabled'. Below this, there are four main sections: 'Define Policy' (with a pie chart showing Relevant, Irrelevant, and Default), 'Upgrade Protocol Pack' (with a download icon), and 'Flow Monitors' (with a double-headed arrow icon). The 'Flow Monitors' section contains a table with two columns: 'Available (1)' and 'Enabled (1)'. The 'Enabled (1)' table has three columns: 'Profiles', 'Visibility', and 'Collector Address'. The profile 'AVC_testing' is listed in the 'Enabled (1)' table with 'Visibility' checked and 'Collector Address' set to 'External' and '10.106.36.22'. An 'Apply' button is visible in the top right corner of the configuration area.

Configurazione AVC per External NetFlow Collector

Una volta applicata la configurazione AVC, le impostazioni di NetFlow Exporter e NetFlow sono state configurate automaticamente con l'indirizzo IP di NetFlow Collector come indirizzo di esportazione e l'indirizzo di esportazione come WLC 9800 con le impostazioni di timeout predefinite e la porta UDP 9995. È possibile convalidare la stessa operazione selezionando Configurazione > Servizi > Visibilità applicazione > Monitor di flusso > Esportatore/monitor.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The navigation path is Configuration > Services > Application Visibility. The 'Flow Monitors' section is highlighted. Below it, the 'Exporter' and 'Monitor' sections are visible. A table lists the configured flow monitors:

Name	Description	Type	Source IP	Destination IP
export_-1638039067	User defined	External	10.197.234.75	10.106.36.22

Configurazione di External NetFlow Collector su 9800 WLC

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The navigation path is Configuration > Services > Application Visibility. The 'Flow Monitors' section is highlighted. Below it, the 'Exporter' and 'Monitor' sections are visible. A table lists the configured flow monitors:

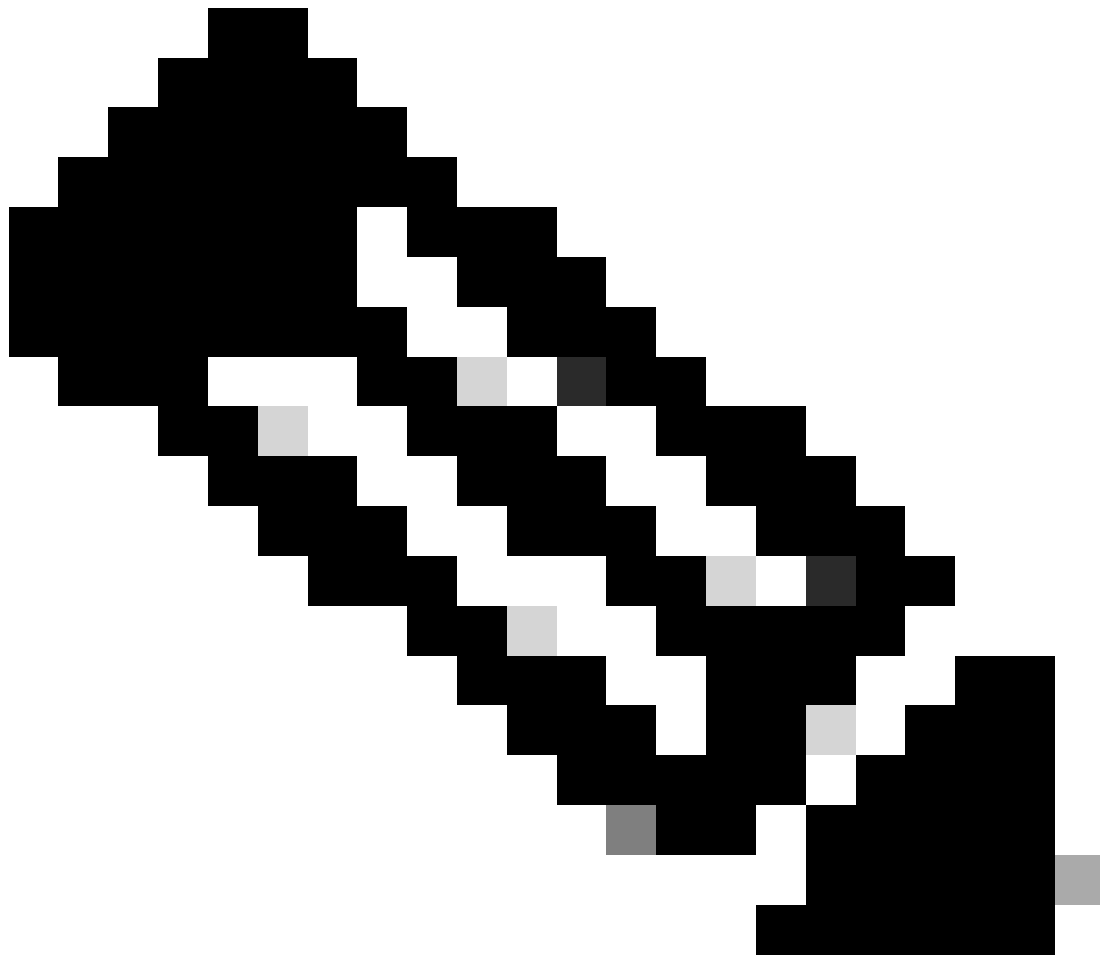
Name	Description	Flow Exporters
dwavc_-1638039067	User defined	export_-1638039067
dwavc_ipv6_-1638039067	User defined	export_-1638039067

Configurazione del monitoraggio del flusso con l'agente di raccolta NetFlow esterno

È possibile controllare la configurazione porta del monitoraggio NetFlow generato automaticamente passando a Configurazione > Servizi > NetFlow .

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The navigation path is Configuration > Services > NetFlow. A table lists the configured NetFlow templates:

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



Nota: se si configura AVC tramite GUI, NetFlow Exporter generato automaticamente verrà configurato per utilizzare la porta UDP 9995. Verificare di aver convalidato il numero di porta utilizzato dall'agente di raccolta NetFlow.

Ad esempio: se si utilizza Cisco Prime come NetFlow Collector, è essenziale impostare la porta di esportazione su 9991, poiché è la porta su cui Cisco Prime ascolta il traffico NetFlow. È possibile modificare manualmente la porta di esportazione nella configurazione NetFlow.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays the 'Configuration > Services > NetFlow' page. A table lists NetFlow templates:

Netflow Template	Interfaces/Profiles	Collector	Export Inte
<input checked="" type="checkbox"/> Wireless avc basic	Not Assigned	10.106.36.22	10.197.23...
<input type="checkbox"/> Wireless avc basic IPv6	Not Assigned	10.106.36.22	10.197.234
<input type="checkbox"/> Wireless avc basic	AVC_testing		10.197.234
<input type="checkbox"/> Wireless avc basic IPv6	AVC_testing		10.197.234

The 'Edit NetFlow' dialog is open, showing the following configuration:

- Netflow Template: Wireless avc basic
- Local Exporter:
- External Exporter:
- Collector Address*: 10.106.36.22
- Exporter Port*: 9991
- Available (1): Search
- Profiles: default-policy-profile
- Profiles: AVC_testing (Ingress: , Egress:)

A tooltip for the 'Exporter Port*' field states: 'Enter the port number on which your netflow collector configured above is listening.'

Tramite CLI

Passaggio 1: Configurare l'indirizzo IP di External NetFlow Collector con l'interfaccia di origine.

```
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
```

Fase 2. Configurare IPv4 e IPv6 Network Flow Monitor per utilizzare Local(WLC) come Netflow Exporter.

```
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
```

Passaggio 3: mappare il monitoraggio del flusso IPv4 e IPv6 nel profilo dei criteri per il traffico in entrata e in uscita.

```
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
```

Configurazione di AVC su 9800 WLC con Cisco Catalyst Center

Prima di procedere alla configurazione di AVC (Application Visibility and Control) su un Cisco Catalyst 9800 Wireless LAN Controller (WLC) con Cisco Catalyst Center, è importante verificare che la comunicazione di telemetria tra il WLC e il Cisco Catalyst Center sia stata stabilita correttamente. Verificare che il WLC sia presente in uno stato gestito all'interno dell'interfaccia del Cisco Catalyst Center e che il relativo stato di integrità sia in fase di aggiornamento attivo. Inoltre, per un monitoraggio efficace dello stato di salute, è importante assegnare correttamente sia il WLC che i punti di accesso (AP) ai rispettivi siti all'interno del Cisco Catalyst Center.

```
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

Verifica della connessione di telemetria su 9800 WLC

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 e AP in stato gestito

Network Devices

LATEST **67%** Healthy **TOTAL: 3**

No Devices



Router

No Devices



Core

No Devices



Distribution

No Devices



Access



40%

7:30p

7:30p

[View Network Health](#)

Stato di WLC e AP su Cisco Catalyst Center

Passaggio 1: configurare Cisco Catalyst Center come agente di raccolta dati NetFlow e abilitare la telemetria wireless nell'impostazione globale. Selezionare Design > Network Setting > Telemetry (Progettazione > Impostazioni di rete > Telemetria) e abilitare la configurazione desiderata, come mostrato.

Catalyst Center Design / Network Settings

Servers Device Credentials IP Address Pools Wireless **Telemetry** Security and Trust

Find Hierarchy Search Help

- Global
 - BGL TAC

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

Telemetria wireless e configurazione AVC

Passaggio 2: abilitare la telemetria delle applicazioni sul WLC 9800 desiderato per eseguire il push della configurazione AVC sul WLC 9800. Per eseguire questa operazione, selezionare Provisioning > Dispositivo di rete > Inventario. Scegliere il WLC 9800 su cui si desidera attivare la telemetria delle applicazioni, quindi selezionare Azione > Telemetria > Abilita telemetria delle applicazioni.

Catalyst Center Provision / Inventory

Global

All Routers Switches Wireless Controllers Access Points Sensors

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 ⓘ

Tags	Device Name	IP Address	Inventory	EoX Status	Manageability
<input checked="" type="checkbox"/>	9800WLC.cisco.com	10.105.193.156	Inventory >	Not Scanned	Managed
<input type="checkbox"/>	CW9164I-ROW1	10.105.193.152	Software Image >		
<input type="checkbox"/>	CW9164I-ROW2	10.105.60.35	Provision >		
<input type="checkbox"/>	SDA_WLC.cisco.com	10.106.38.185	Telemetry >		
			Device Replacement >		
			Compliance >		
			More >		

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Abilitazione della telemetria delle applicazioni su 9800 WLC

Passaggio 3: scegliere la modalità di distribuzione in base ai requisiti.

Locale: per abilitare AVC nel profilo criteri locale (switching centrale)

Flex/Fabric: per abilitare AVC in Flex Policy Profile (switching locale) o SSID basato su fabric.

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.

Selezione della modalità di distribuzione in Cisco Catalyst Center

Passaggio 4: viene avviata un'attività per attivare le impostazioni AVC e la configurazione corrispondente viene applicata al WLC 9800. È possibile visualizzare lo stato passando ad Attività > Registro di controllo.

Jul 18, 2024 09:22 PM [↻](#)

3:37p

8/1 9/1 10/1 11/1 12/1 1/1 2/1 3/1 4/1 5/1

[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]

Registri di controllo dopo l'abilitazione della telemetria su 9800 WLC

Cisco Catalyst Center distribuirà le configurazioni di Flow Exporter e Flow Monitor, incluse la porta specificata e altre impostazioni, e le attiverà all'interno del profilo di criteri modalità scelto, come mostrato di seguito:

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

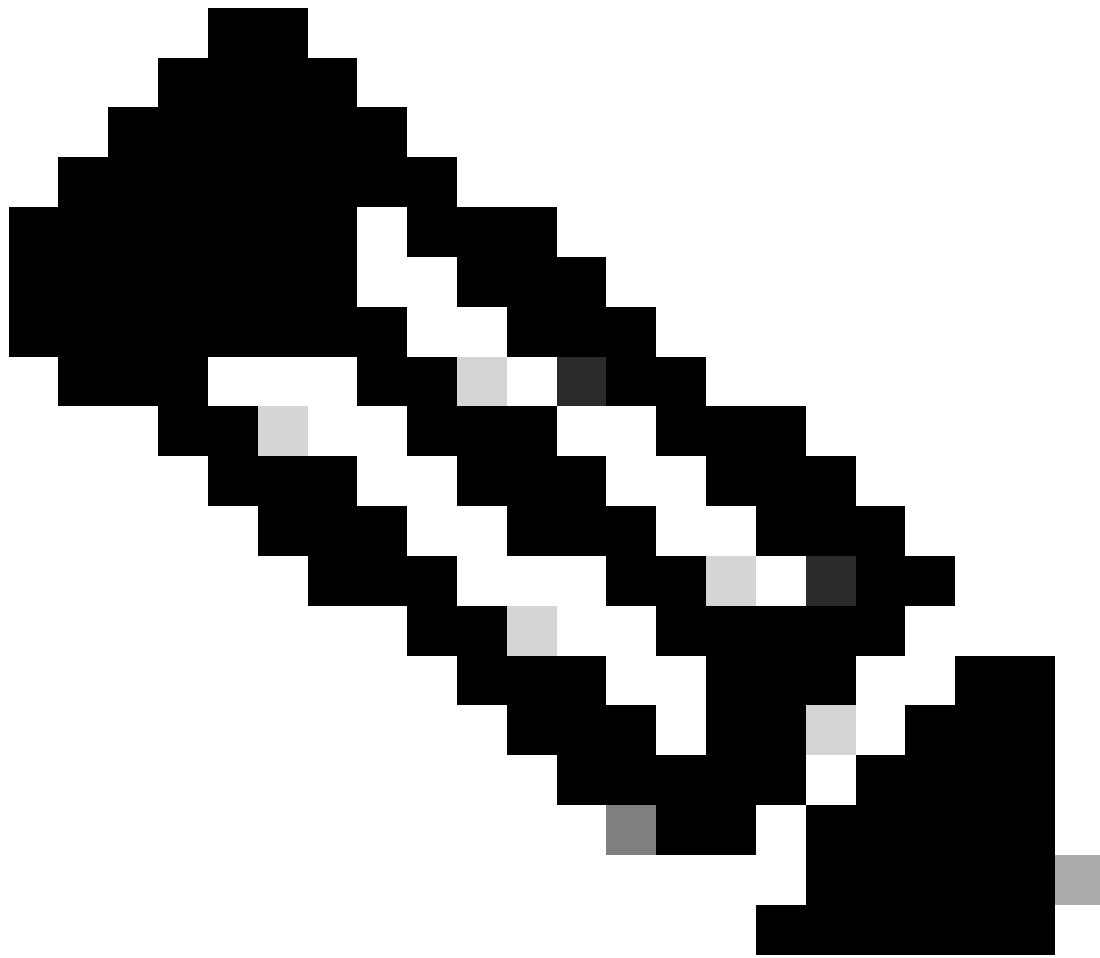
```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp 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
```

Verifica dell'AVC

Su 9800

Quando il WLC 9800 viene utilizzato come esportatore di flusso, è possibile osservare le seguenti statistiche AVC:

- Visibilità delle applicazioni per i client connessi tramite tutti gli SSID.
- Utilizzo di singole applicazioni per ogni client.
- Utilizzo specifico dell'applicazione su ogni SSID separatamente.



Nota: è possibile filtrare i dati in base alla direzione, sia per il traffico in entrata che per il traffico in uscita, nonché in base all'intervallo di tempo, con la possibilità di selezionare un intervallo fino a 48 ore.

Tramite GUI

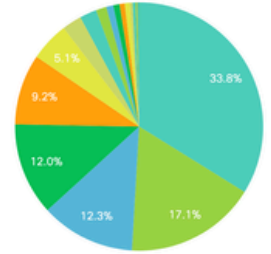
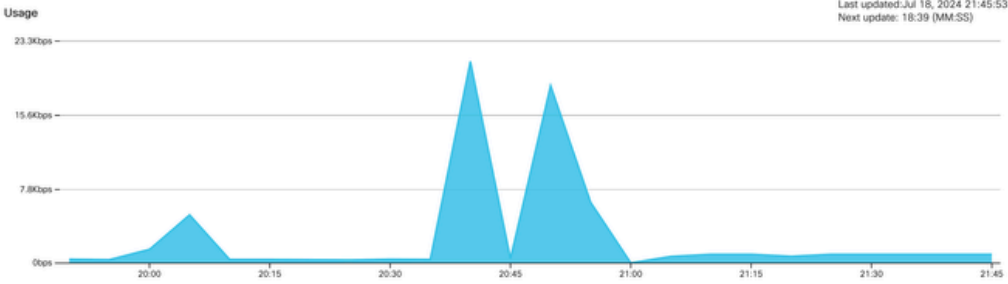
Passare a Monitoraggio > Servizi > Visibilità applicazione.

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

Visibilità delle applicazioni degli utenti connessi a AVC_testing SSID per il traffico in entrata e in uscita

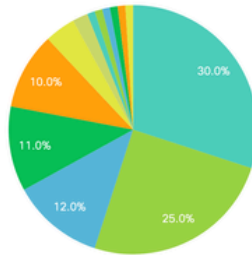
Per visualizzare le statistiche di visibilità dell'applicazione per ogni client, è possibile fare clic sulla scheda Client, scegliere un client specifico e quindi fare clic su Visualizza dettagli applicazione.

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)

Visibilità delle applicazioni per client specifici - 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

Visibilità delle applicazioni per client specifici - 2

Tramite CLI

Verifica stato AVC

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

AVC configuration complete: YES

Statistiche da NetFlow (cache FNF)

```
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

Verifica di AVC sulla CLI 9800

Per esaminare singolarmente il primo utilizzo dell'applicazione per ciascuna WLAN e i relativi client connessi:

```
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
```

Verificare il numero di pacchetti FNFv9 e lo stato di decodifica impostato su Control Plane (CP)

```
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

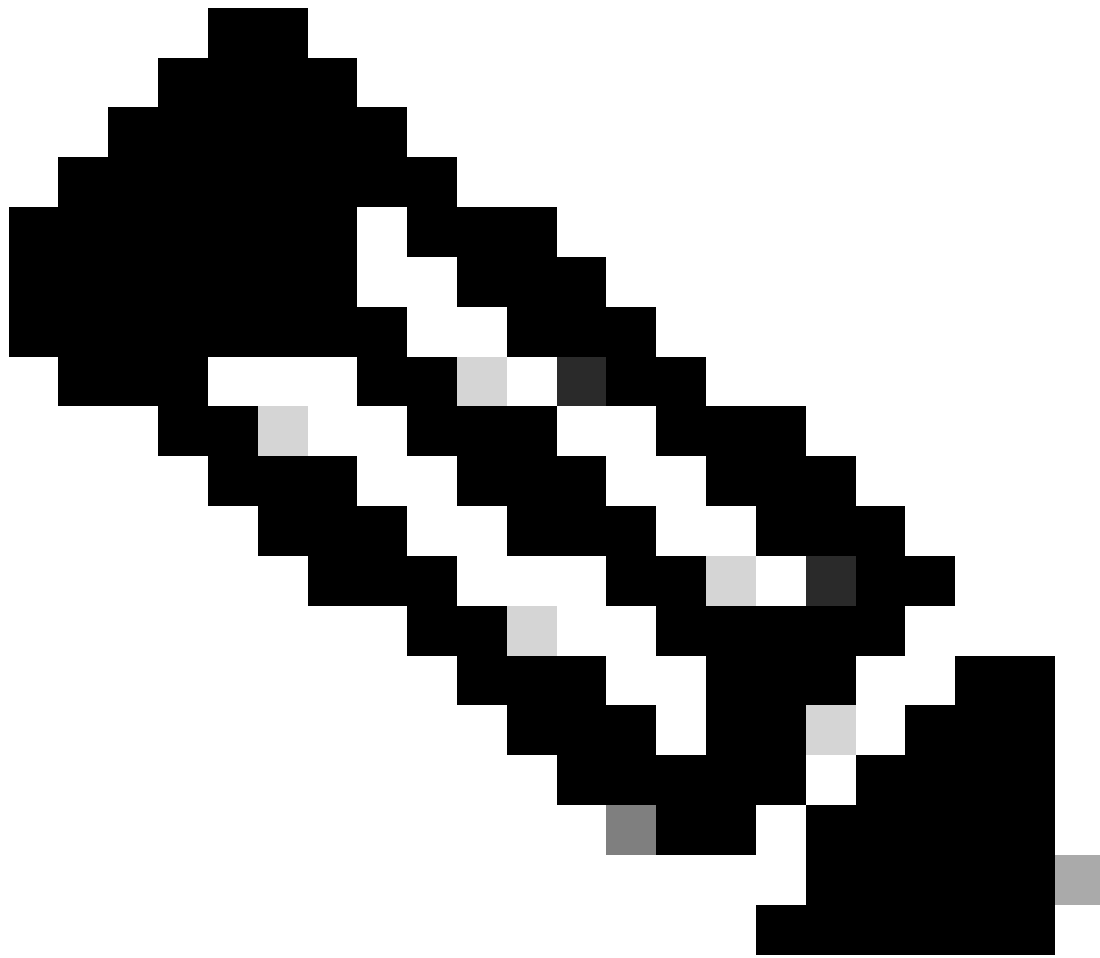
Record pacchetto FNFv9

È inoltre possibile controllare direttamente le statistiche di nbar.

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

Nelle modalità Fabric e Flex, è possibile ottenere lo stato NBAR da AP tramite:

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



Nota: in una configurazione con ancoraggio esterno, il WLC di ancoraggio funge da presenza di layer 3 per il client, mentre il WLC esterno funziona sul layer 2. Poiché l'AVC (Application Visibility and Control) funziona sul layer 3, i dati rilevanti sono osservabili solo sul WLC di ancoraggio.

Su DNAC

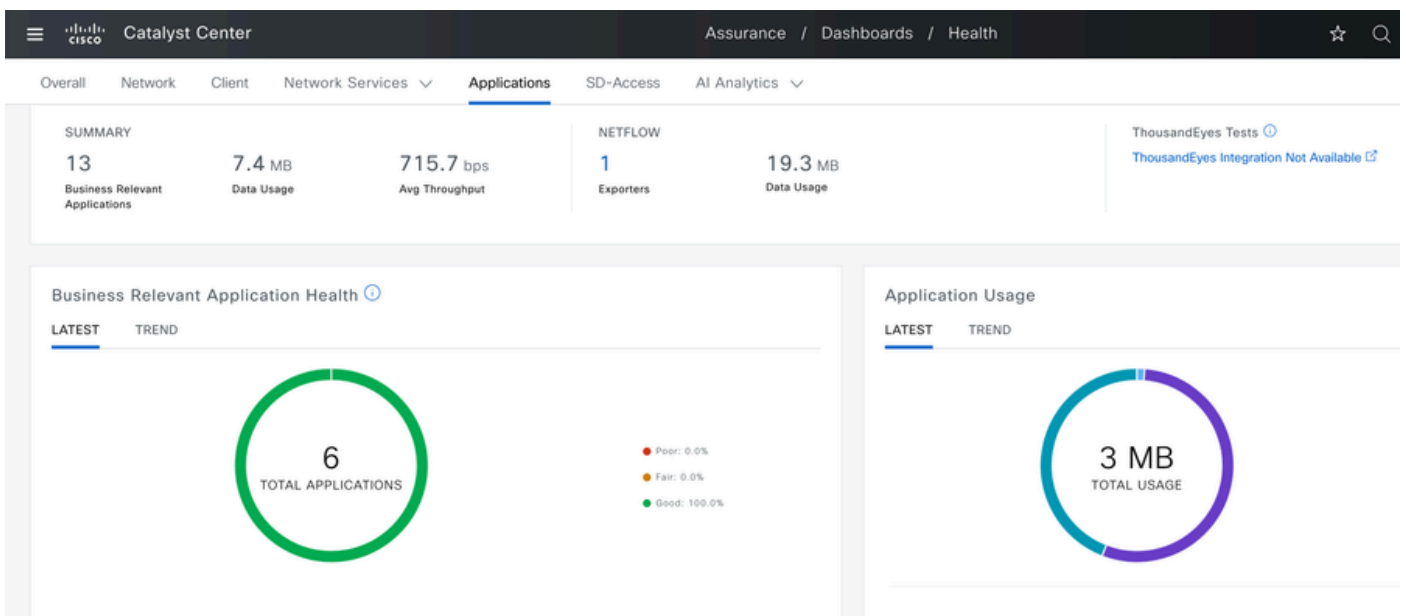
Dalla funzione di acquisizione dei pacchetti del 9800 WLC, è possibile verificare che i dati relativi alle applicazioni e al traffico di rete vengano inviati continuamente a Cisco Catalyst Center.

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]

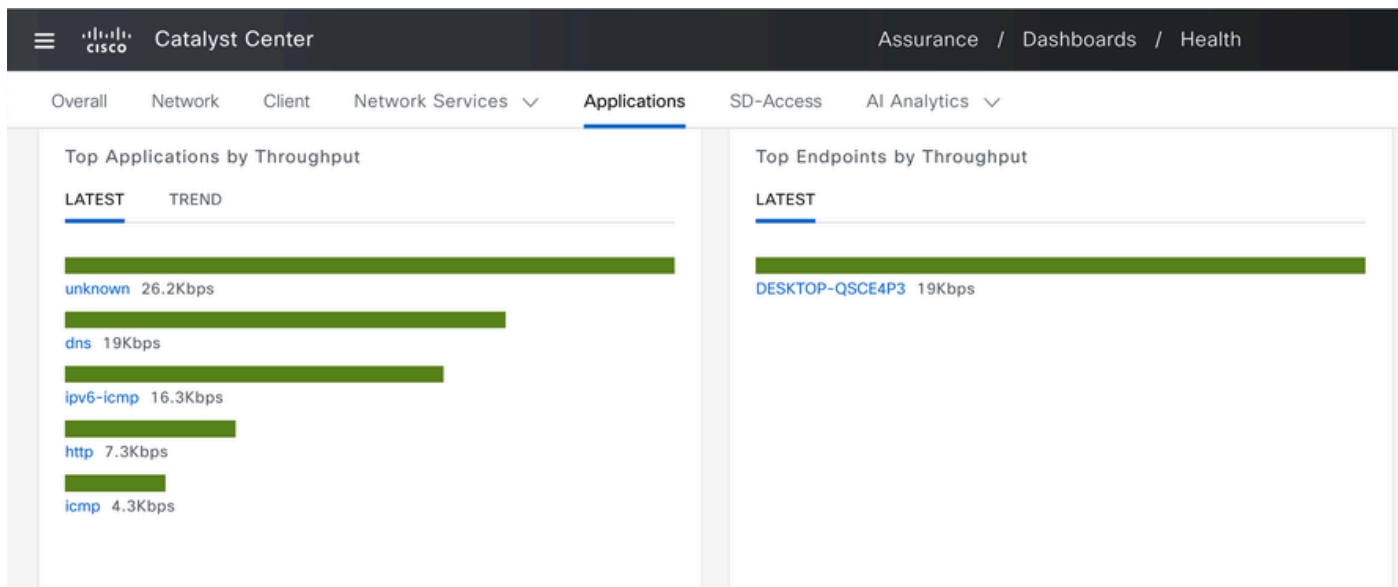
Packet Capture su 9800 WLC

Per visualizzare i dati dell'applicazione per i clienti connessi a un WLC specifico su Cisco Catalyst Center, selezionare Assurance > Dashboard > Health > Application.



Monitoraggio AVC su Cisco Catalyst Center

Possiamo tenere traccia delle applicazioni utilizzate più di frequente dai clienti e identificare i consumatori di dati più elevati, come illustrato in questa sezione.



Statistiche applicazione principale e utente larghezza di banda principale

È possibile impostare un filtro per un determinato SSID, che consente di monitorare il throughput complessivo e l'utilizzo delle applicazioni dei client associati a tale SSID.

Questa funzionalità consente di identificare le principali applicazioni e gli utenti che utilizzano la massima larghezza di banda all'interno della rete.

È inoltre possibile utilizzare la funzione Filtro temporale per esaminare i dati relativi ai periodi di tempo precedenti, offrendo informazioni cronologiche sull'utilizzo della rete.

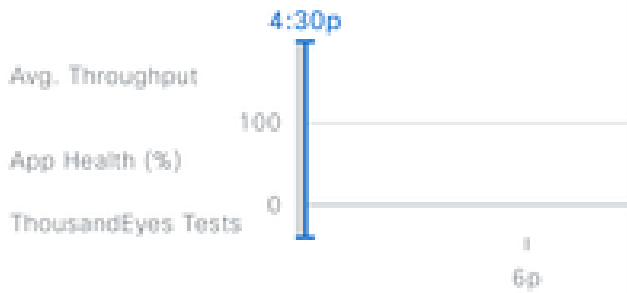
Global/BGL TAC/Shalini_AVC

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

Filtro temporale per visualizzare le statistiche AVC

By default, hourly data is show

SSID (1/14)

Clear Filter

Avg. Throughput

App Health (%)

ThousandEyes Tests

SSID: AVC_testing X

Cancel
Apply

Filtro SSID per visualizzare le statistiche AVC

In External NetFlow Collector

Esempio1: Cisco Prime as Netflow Collector

Quando si usa Cisco Prime come agente di raccolta Netflow, il WLC raccolto È possibile vedere 9800 WLC come origine dati che invia dati Netflow e il modello NetFlow verrà creato automaticamente in base ai dati inviati da 9800 WLC.

Dall'acquisizione dei pacchetti presa con 9800 WLC, possiamo verificare che stia inviando continuamente a Cisco Prime dati relativi alle applicazioni e al traffico di rete.

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]: 0009000120eb01e9669932b70000000400000400014f006c000000000000000000000000000000ff020000000000000000001
[Length: 128]

Acquisizione del pacchetto su 9800 WLC

Cisco Prime Infrastructure

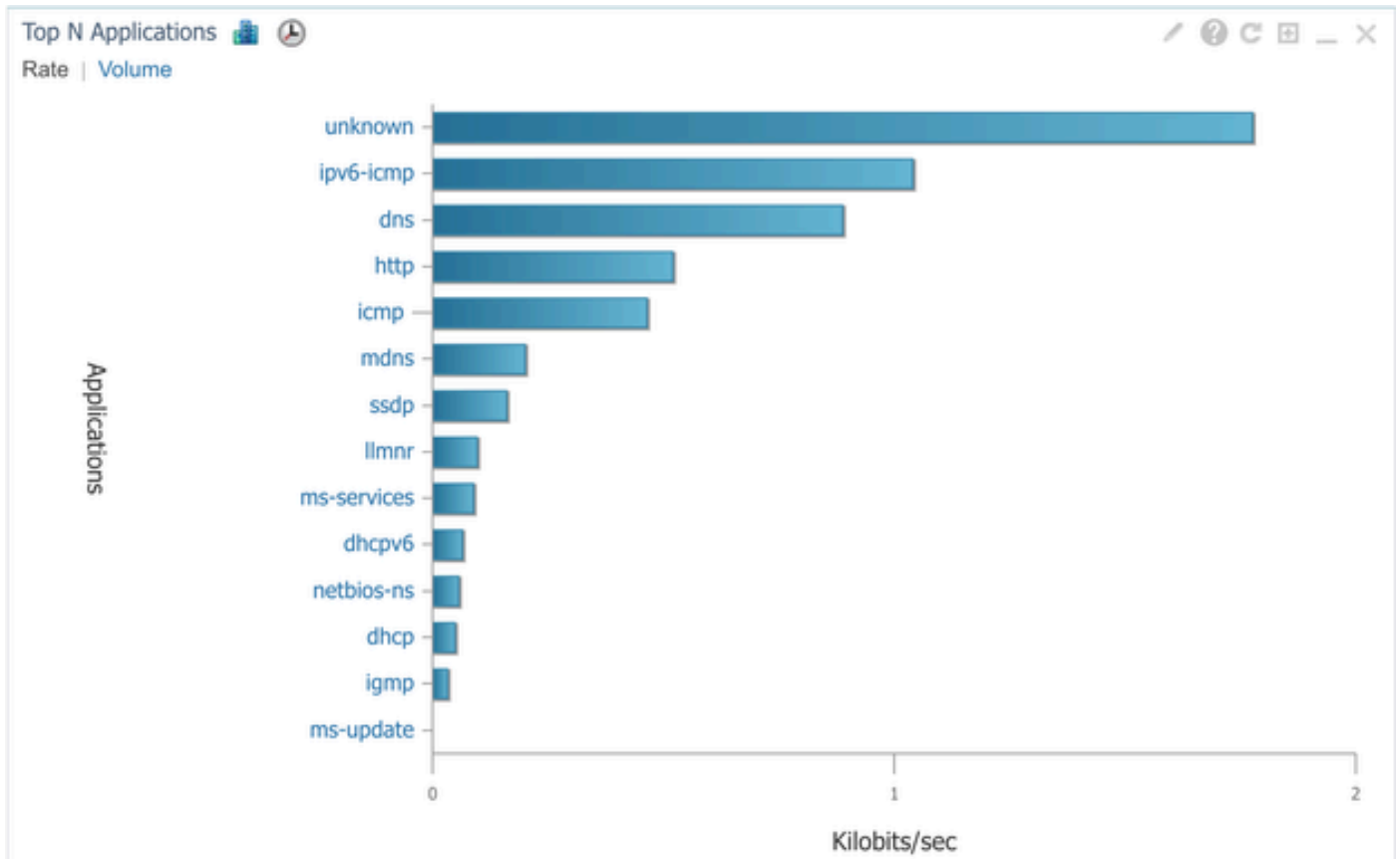
Services / Application Visibility & Control / Data Sources

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 Standa...

Cisco Prime Detection 9800 WLC come origine dati Netflow

È possibile impostare filtri basati su Applicazione, Servizi e persino su Client, utilizzando l'indirizzo IP per analisi di dati più mirate.

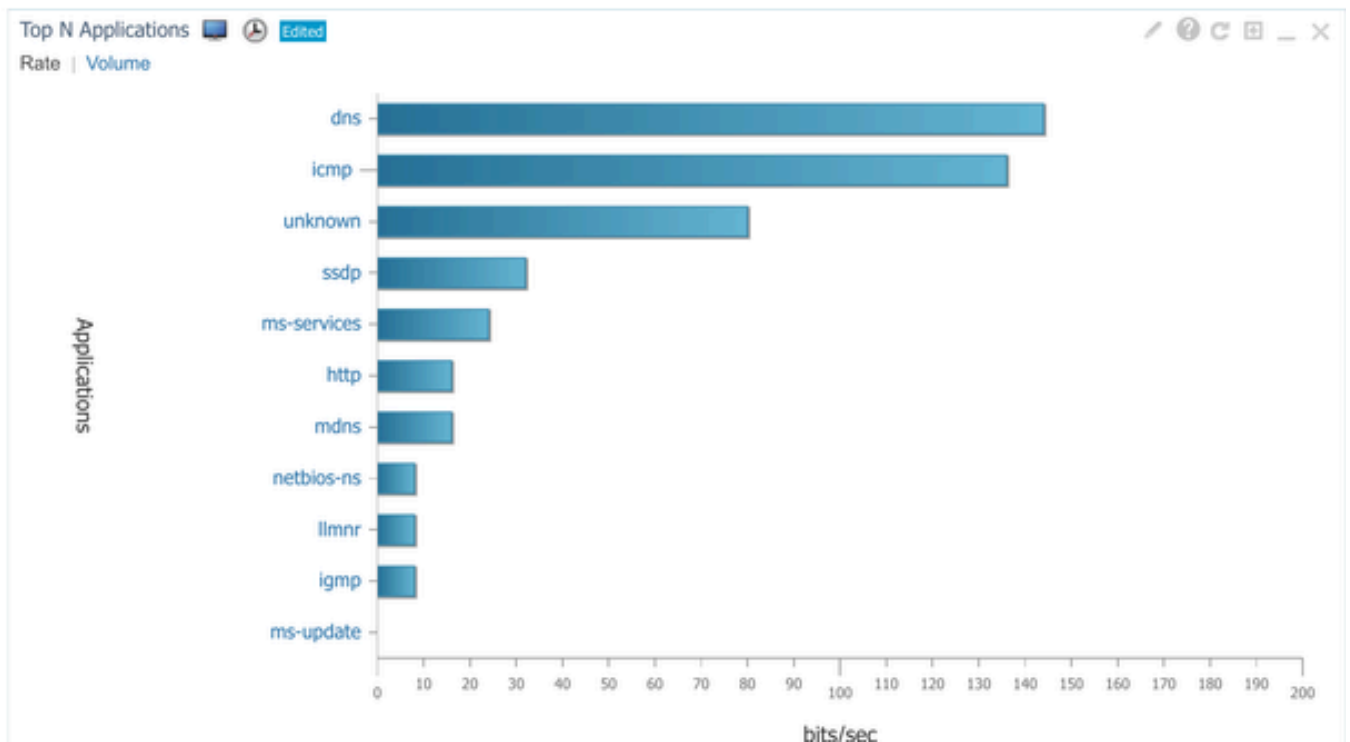


Visibilità delle applicazioni per tutti i client

Dashboard / Performance

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

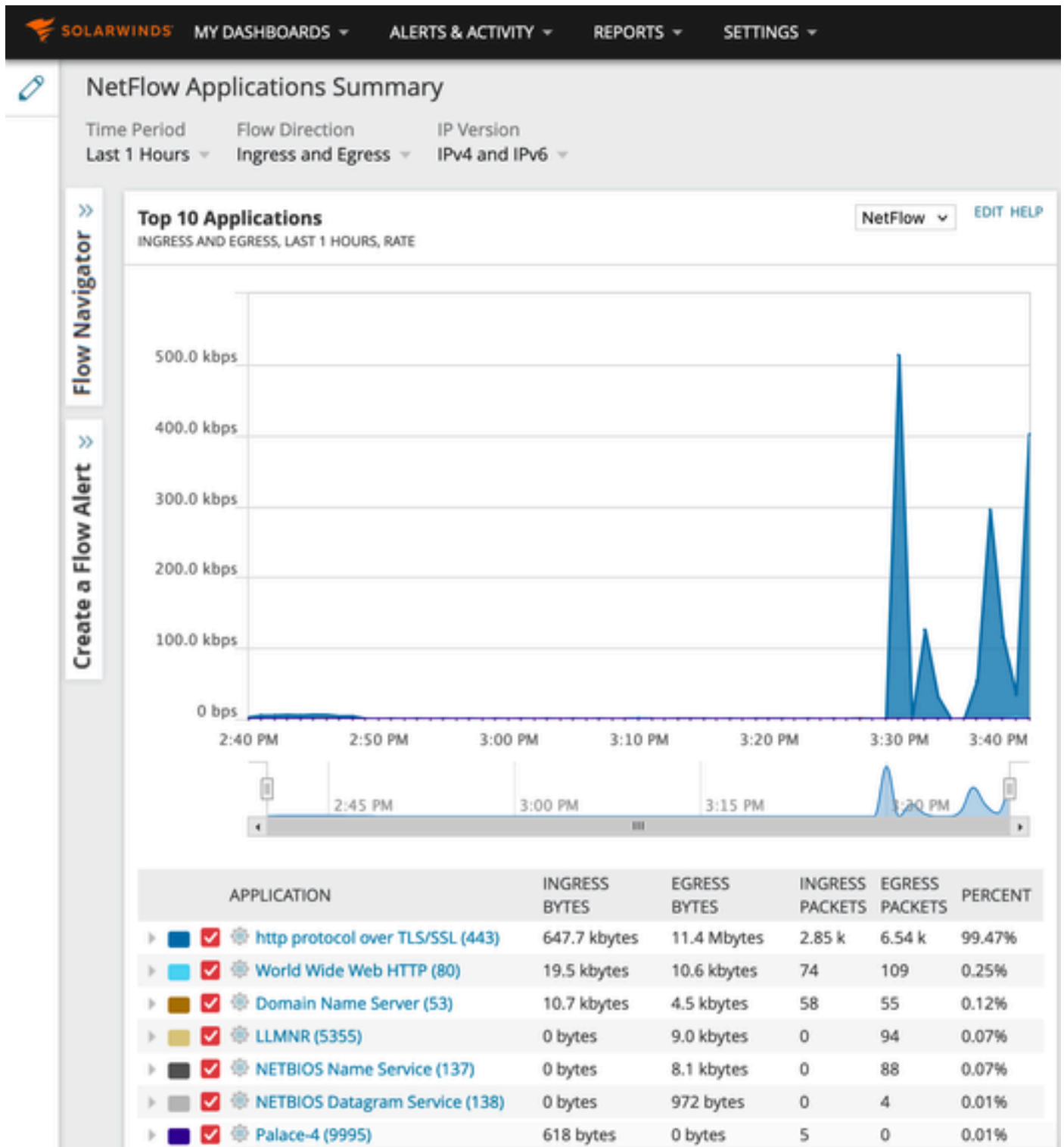
Filters *Client
 *Time Frame
 Application
 Network Aware



Applicazione di client specifici che utilizzano l'indirizzo IP

Esempio 2: agente di raccolta NetFlow di terze parti

In questo esempio, il collettore NetFlow di terze parti [SolarWinds] viene utilizzato per raccogliere le statistiche delle applicazioni. Il 9800 WLC impiega Flexible NetFlow (FNF) per trasmettere dati completi relativi alle applicazioni e al traffico di rete, che viene poi raccolto da SolarWinds.



Statistiche applicazione Netflow su SolarWind

Controllo del traffico

Il controllo del traffico si riferisce a una serie di funzionalità e meccanismi utilizzati per gestire e regolare il flusso del traffico di rete. Il monitoraggio del traffico o la limitazione della velocità sono meccanismi utilizzati nel controller wireless per controllare la quantità di traffico trasmesso dal client. Eseguire il monitoraggio della velocità dati per il traffico di rete e intervenire immediatamente quando viene superato un limite di velocità predefinito. Quando il traffico supera la velocità specificata, la limitazione della velocità può eliminare i pacchetti in eccesso o contrassegnarli modificandone i valori CoS (Class of Service) o DSCP (Differentiated Services Code Point). Per ottenere questo risultato, è possibile configurare QoS in 9800 WLC. Per una panoramica del funzionamento di questi componenti e della loro configurazione per ottenere risultati diversi, consultare il sito <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html>.

Risoluzione dei problemi

La risoluzione dei problemi di AVC implica l'identificazione e la risoluzione dei problemi che possono influire sulla capacità di AVC di identificare, classificare e gestire in modo accurato il traffico delle applicazioni sulla rete wireless. I problemi più comuni possono includere la classificazione del traffico, l'applicazione di policy o la creazione di report. Di seguito sono riportati alcuni passaggi e considerazioni per la risoluzione dei problemi di AVC su un Catalyst 9800 WLC:

- Verifica della configurazione AVC: verificare che AVC sia configurato correttamente sul WLC e associato ai profili e alle WLAN corretti.
- Quando si imposta AVC tramite la GUI, la porta 9995 viene assegnata automaticamente come predefinita. Tuttavia, se si utilizza un agente di raccolta esterno, verificare su quale porta è configurato per l'ascolto del traffico NetFlow. È fondamentale configurare accuratamente questo numero di porta in modo che corrisponda alle impostazioni del raccogliitore.
- Verificare il supporto del modello AP e della modalità di distribuzione.
- Fare riferimento alle limitazioni di 9800 WLC durante l'implementazione di AVC nella rete wireless.

Raccolta log

Log WLC

1. Abilitare l'opzione Timestamp per avere un riferimento temporale per tutti i comandi.

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

2. Per esaminare la configurazione

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

3. È possibile verificare lo stato avc e le statistiche netflow.

Controllare lo stato della configurazione AVC.

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

Controllare il numero di pacchetti FNFv9 e decodificare lo stato puntato al Control Plane (CP).

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

Controlla statistiche da NetFlow (cache FNF).

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

Selezionare Top n application usage per ogni wlan, dove n = <1-30> Immettere il numero di applicazioni.

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

Controllare l'utilizzo delle applicazioni per ogni client, dove n = <1-30> Immettere il numero di applicazioni.

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

Selezionare i primi n client connessi a una specifica WLAN usando l'applicazione specifica, dove n=<1-10> Immettere il numero di client.

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

Controllare le statistiche di nbar.

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

4. Impostare il livello di registrazione su debug/verbose.

```
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. Abilitare la traccia radioattiva (RA) per l'indirizzo MAC del client per convalidare gli stati AVC.

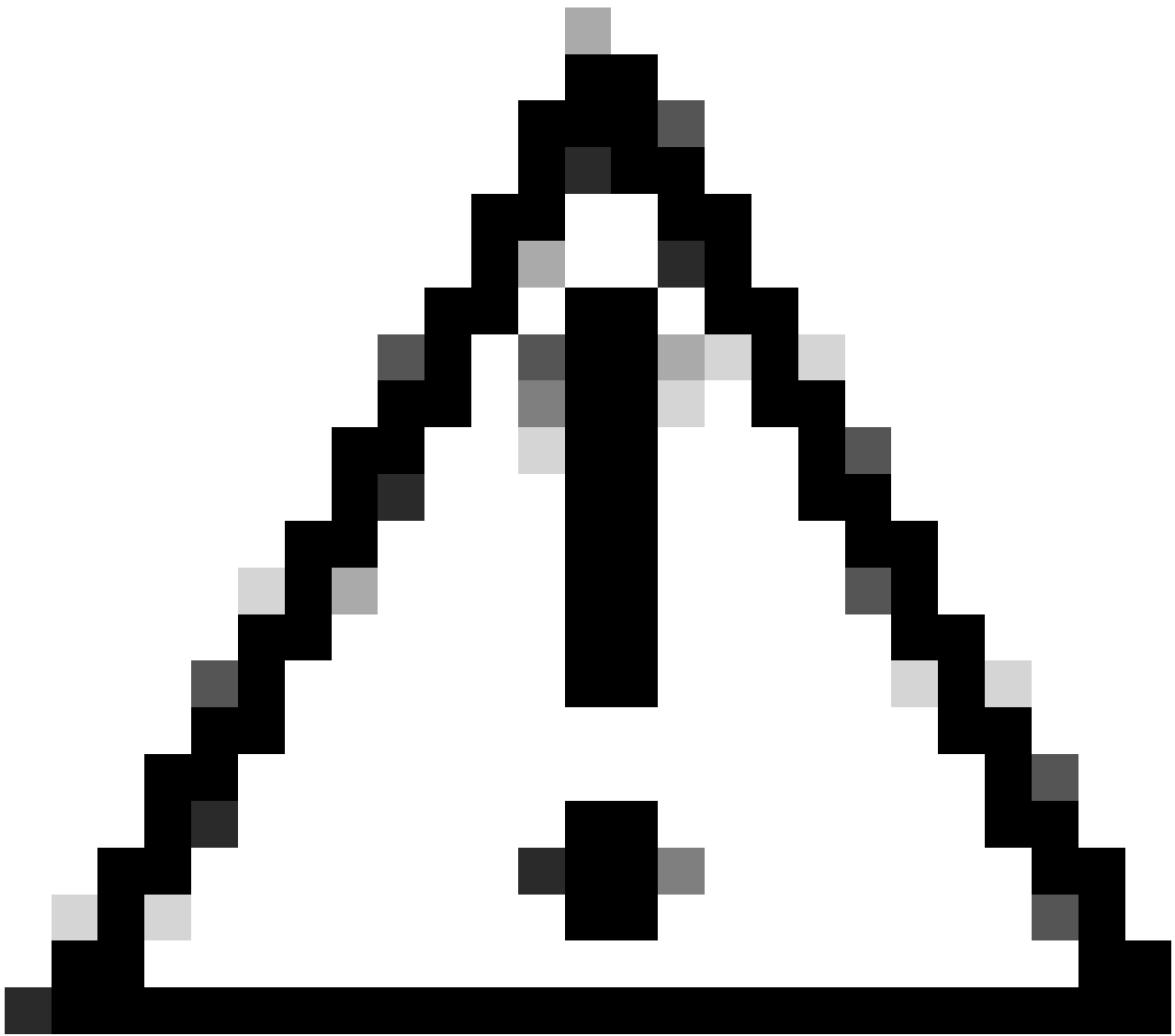
Tramite CLI

```
9800WLC#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
```

Attenzione: il debug condizionale abilita la registrazione a livello di debug che a sua volta aumenta il volume dei log generati. Se si lascia attiva questa opzione, si riduce il tempo di visualizzazione dei log. Si consiglia pertanto di disattivare sempre il debug al termine della sessione di risoluzione dei problemi.

```
# clear platform condition all  
# undebbug all
```

Tramite GUI

Passaggio 1. Passare a Risoluzione dei problemi > Traccia radioattiva.

Passaggio 2. Fare clic su Add (Aggiungi) e immettere l'indirizzo Mac del client per il quale si desidera risolvere il problema. È possibile aggiungere diversi indirizzi Mac da tracciare.

Passaggio 3. Quando si è pronti per avviare la traccia radioattiva, fare clic su Avvia. Una volta avviato, il log di debug viene scritto su disco in relazione a qualsiasi elaborazione del control plane

correlata agli indirizzi MAC tracciati.

Passaggio 4. Quando si riproduce il problema che si desidera risolvere, fare clic su Stop .

Passaggio 5. Per ogni indirizzo MAC sottoposto a debug, è possibile generare un file di log che fascicola tutti i log relativi a tale indirizzo facendo clic su Genera.

Passaggio 6. Scegliere il periodo di tempo che deve trascorrere prima che il file di registro fascicolato venga completato e fare clic su Applica al dispositivo.

Passaggio 7. È ora possibile scaricare il file facendo clic sull'icona accanto al nome del file. Questo file è presente nell'unità flash di avvio del controller e può anche essere copiato dalla CLI.

Di seguito è riportato un esempio di debug AVC nelle tracce RA

```
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. Acquisizioni incorporate filtrate in base all'indirizzo MAC del client in entrambe le direzioni, filtro MAC interno del client disponibile dopo la versione 17.1.

È particolarmente utile quando si utilizza un collettore esterno, in quanto aiuta a confermare se il WLC sta trasmettendo i dati NetFlow alla porta desiderata come previsto.

Tramite 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
```

Tramite GUI

Passaggio 1. Selezionare Risoluzione dei problemi > Acquisizione pacchetti > +Aggiungi .

Passaggio 2. Definire il nome dell'acquisizione del pacchetto. È consentito un massimo di 8 caratteri.

Passaggio 3. Definire gli eventuali filtri.

Passaggio 4. Selezionare la casella Monitora traffico di controllo se si desidera visualizzare il traffico puntato alla CPU del sistema e inserito nuovamente nel piano dati.

Passaggio 5. Definire le dimensioni del buffer. È consentito un massimo di 100 MB.

Passaggio 6. Definire il limite, in base alla durata, per un intervallo da 1 a 1000000 secondi, o in base al numero di pacchetti, per un intervallo da 1 a 100000 pacchetti, in base alle esigenze.

Passaggio 7. Scegliere l'interfaccia dall'elenco di interfacce nella colonna sinistra e selezionare la freccia per spostarla nella colonna destra.

Passaggio 8. Fare clic su Apply to Device (Applica al dispositivo).

Passaggio 9. Per avviare la cattura, selezionare Start.

Passaggio 10. È possibile lasciare in esecuzione l'acquisizione fino al limite definito. Per interrompere manualmente la cattura, selezionare Interrompi.

Passaggio 11. Una volta interrotto, il pulsante Esporta diventa disponibile e consente di scaricare il file di acquisizione (.pcap) sul desktop locale tramite il server HTTP o TFTP o il server FTP o il disco rigido o il flash del sistema locale.

Log AP

Modalità Fabric e Flex

1. mostrare al tecnico tutti i dettagli di configurazione e lo stato del client per l'access point.
2. mostra statistiche nbar avc statistiche nbar da AP
3. Debug AVC

```
AP#term mon
```

```
AP#debug capwap client avc <all/detail/error/event>
```

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

Informazioni correlate

[Guida alla configurazione di AVC](#)

[Limitazione della velocità su 9800 WLC](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).