

# Comprendre AVC sur le contrôleur LAN sans fil Catalyst 9800

## Table des matières

---

[Introduction](#)

[Prérequis](#)

[Informations sur la visibilité et le contrôle des applications \(AVC\)](#)

[Fonctionnement d'AVC](#)

[Network-Based Application Recognition \(NBAR\)](#)

[Activer le protocole NBAR sur le profil de stratégie](#)

[Mise à niveau de NBAR sur WLC 9800](#)

[NetFlow](#)

[Flexible Netflow](#)

[Moniteur de flux](#)

[Points d'accès pris en charge AVC](#)

[Prise en charge de différents modes de déploiement du 9800](#)

[Restrictions lors de la mise en oeuvre de AVC sur le 9800](#)

[Topologie du réseau](#)

[AP en mode local](#)

[Point d'accès en mode flexible](#)

[Configuration de l'AVC sur le WLC 9800](#)

[Exportateur local](#)

[Collecteur NetFlow externe](#)

[Configuration d'AVC sur le WLC 9800 à l'aide de Cisco Catalyst Center](#)

[Vérification de l'AVC](#)

[Sur le 9800](#)

[Sur DNAC](#)

[Sur le collecteur NetFlow externe](#)

[Exemple 1 : Cisco Prime en tant que collecteur Netflow](#)

[Exemple 2 : collecteur NetFlow tiers](#)

[Contrôle Du Trafic](#)

[Dépannage](#)

[Collecte des journaux](#)

[Journaux WLC](#)

[Journaux AP](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit la visibilité et le contrôle des applications (AVC) sur un WLC Cisco Catalyst 9800 qui permet une gestion précise du trafic des applications.

## Prérequis

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du contrôleur Cisco WLC 9800.
- Connaissance de base du point d'accès local et du mode de connexion flexible.
- Les points d'accès doivent être compatibles AVC. (Non applicable avec le point d'accès en mode local)
- Pour que la partie contrôle de l'AVC (QoS) fonctionne, la fonctionnalité de visibilité des applications avec FNF doit être configurée.

## Informations sur la visibilité et le contrôle des applications (AVC)

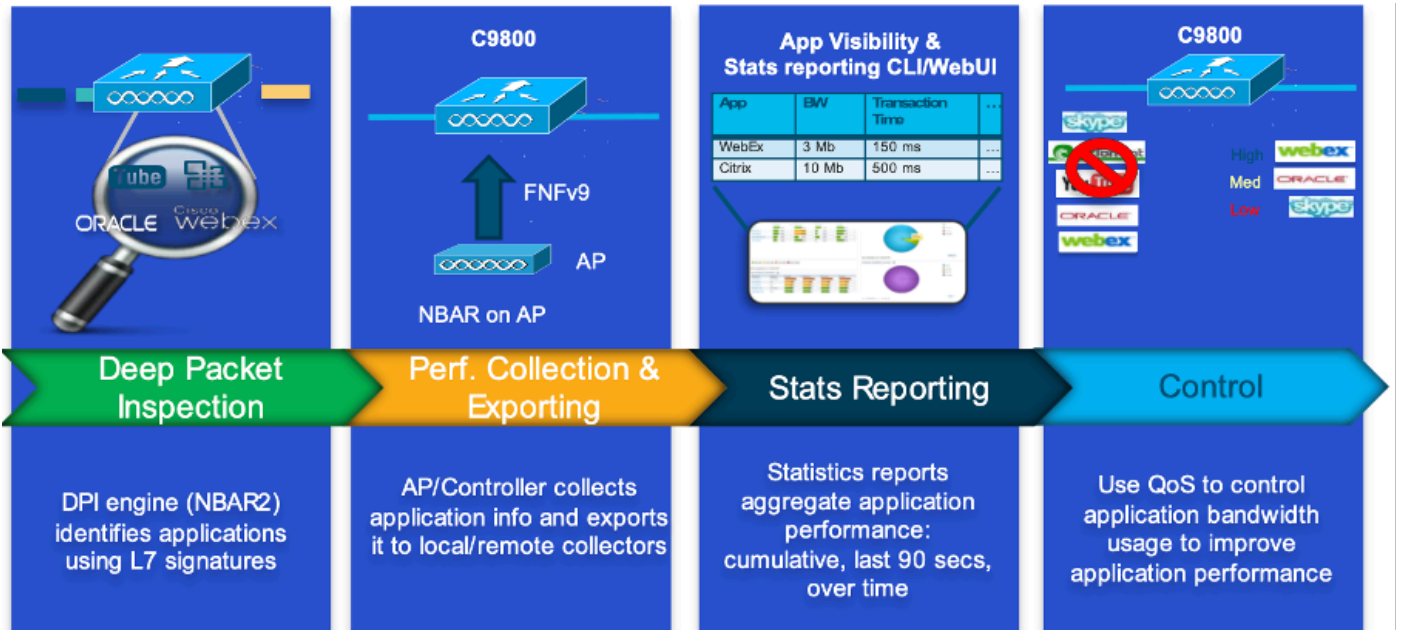
AVC (Application Visibility and Control) est l'approche de pointe de Cisco en matière de technologie d'inspection approfondie des paquets (DPI) sur les réseaux filaires et sans fil. Avec AVC, vous pouvez effectuer une analyse en temps réel et créer des politiques pour réduire efficacement la congestion du réseau, réduire l'utilisation coûteuse des liaisons réseau et éviter les mises à niveau d'infrastructure inutiles. En bref, AVC permet aux utilisateurs d'atteindre un tout nouveau niveau de reconnaissance et de formatage du trafic grâce à la reconnaissance d'applications réseau (NBAR). Les packages NBAR exécutés sur le WLC 9800 sont utilisés pour DPI et les résultats sont signalés à l'aide de Flexible NetFlow (FNF).

En plus de la visibilité, AVC offre la possibilité de hiérarchiser, de bloquer ou de réguler différents types de trafic. Par exemple, les administrateurs peuvent créer des politiques qui donnent la priorité aux applications vocales et vidéo afin de garantir la qualité de service (QoS) ou de limiter la bande passante disponible pour les applications non essentielles pendant les heures de pointe. Il peut également être intégré à d'autres technologies Cisco, telles que Cisco Identity Services Engine (ISE) pour les politiques d'applications basées sur l'identité et Cisco Catalyst Center pour la gestion centralisée.

### Fonctionnement d'AVC

AVC utilise des technologies avancées telles que le moteur FNF et NBAR2 pour la résolution en PPP. En analysant et en identifiant les flux de trafic à l'aide du moteur NBAR2, des flux spécifiques sont marqués avec le protocole ou l'application reconnu. Le contrôleur collecte tous les rapports et les présente via les commandes show, l'interface utilisateur Web ou des messages d'exportation NetFlow supplémentaires aux collecteurs NetFlow externes tels que Prime.

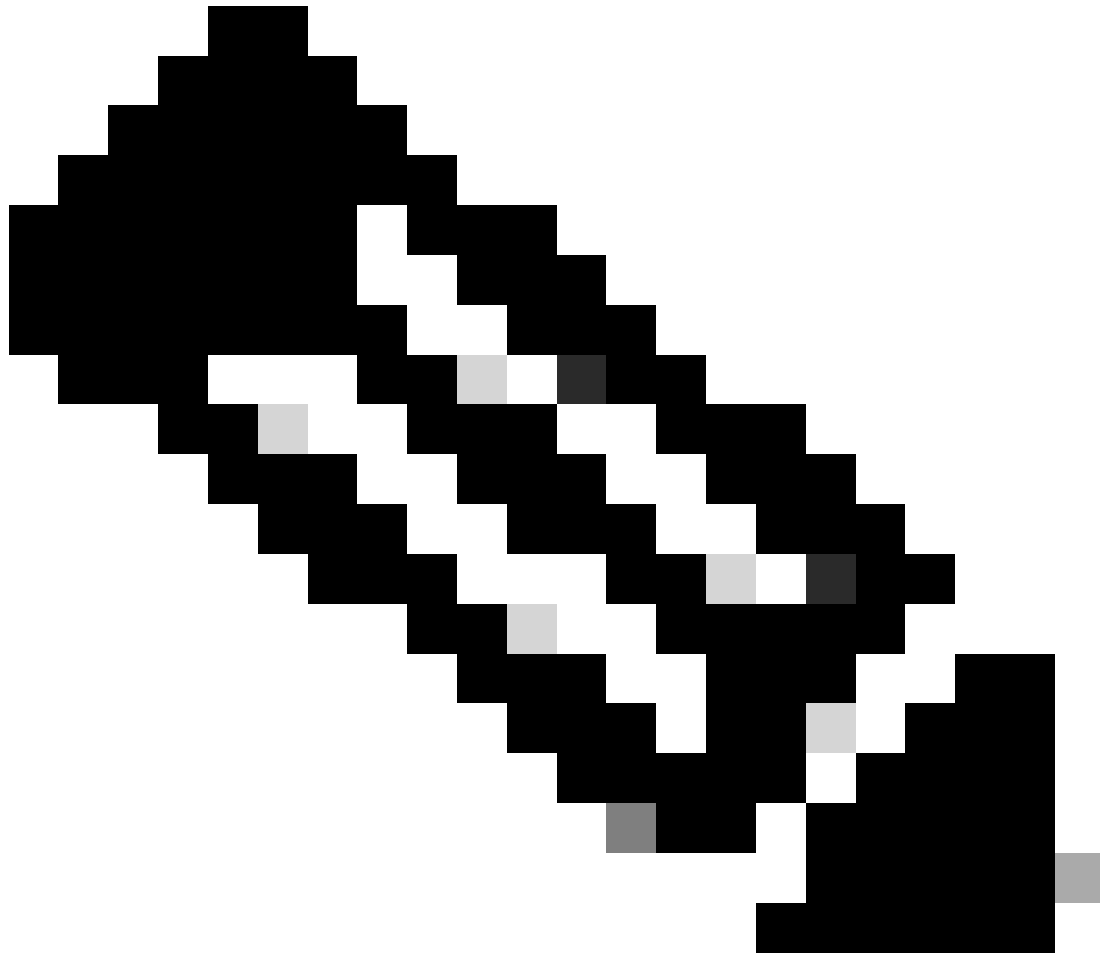
Une fois la visibilité des applications établie, les utilisateurs peuvent créer des règles de contrôle avec des mécanismes de réglementation pour les clients en configurant la qualité de service (QoS).



mécanisme de travail de l'AVC

## Network-Based Application Recognition (NBAR)

Le NBAR est un mécanisme intégré au WLC 9800, qui est utilisé pour effectuer l'analyse par défaut (DPI) afin d'identifier et de classer une grande variété d'applications exécutées sur un réseau. Il peut reconnaître et classer un grand nombre d'applications, y compris les applications cryptées et mappées de manière dynamique sur les ports, qui sont souvent invisibles pour les technologies traditionnelles d'inspection des paquets.



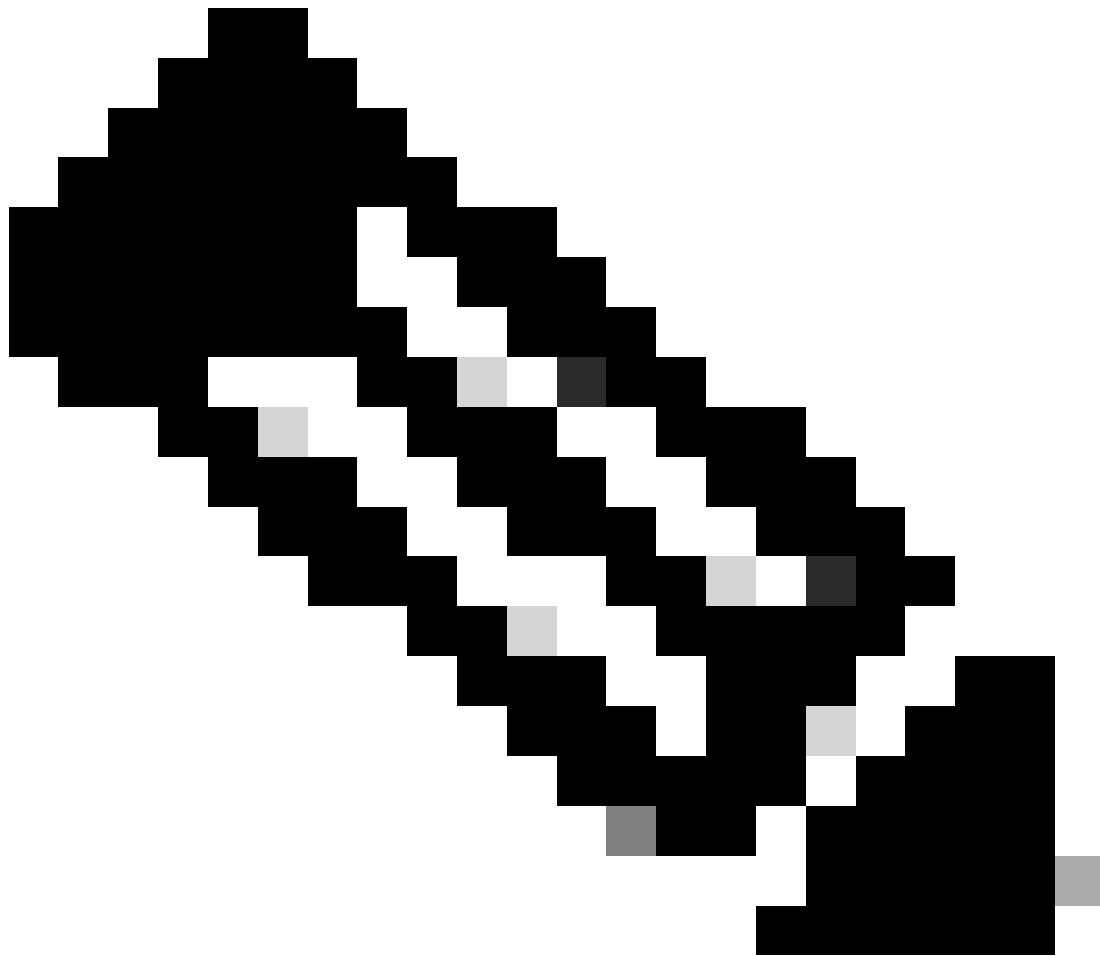
Remarque : pour tirer parti de NBAR sur le WLC Catalyst 9800, il est nécessaire de l'activer et de le configurer correctement, souvent en conjonction avec des profils AVC spécifiques qui définissent les actions appropriées à entreprendre en fonction de la classification du trafic.

NBAR continue d'être mis à jour périodiquement, et il est important de maintenir le logiciel WLC à jour pour s'assurer que l'ensemble de fonctionnalités NBAR reste à jour et efficace.

Une liste complète des protocoles pris en charge dans les dernières versions est disponible à l'adresse [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)

Activer le protocole NBAR sur le profil de stratégie

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



Remarque : le profil de stratégie % doit être désactivé avant d'effectuer cette opération.

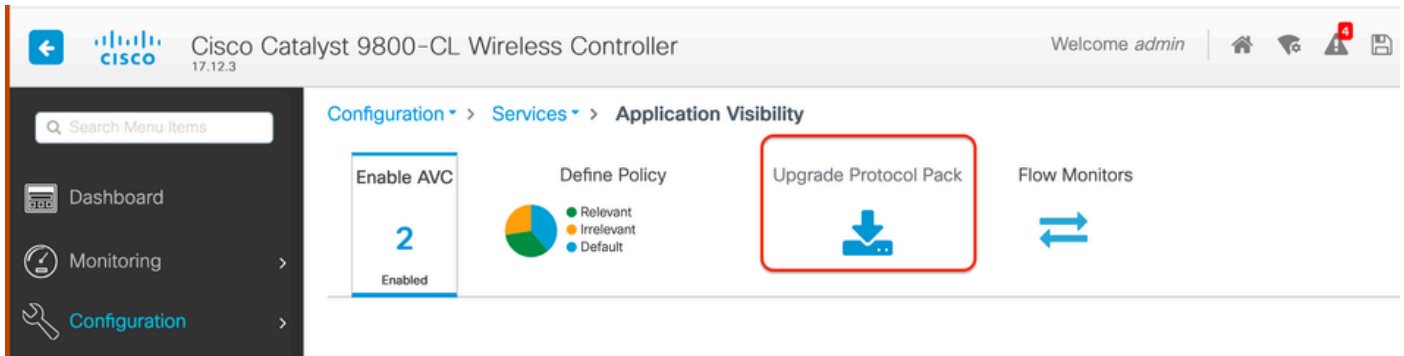
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR  
NBAR Protocol Discovery : Enabled
```

Mise à niveau de NBAR sur WLC 9800

Le WLC 9800 a déjà environ 1500 applications reconnaissables. Dans le cas où une nouvelle application est publiée, le protocole correspondant sera mis à jour dans le dernier NBAR, qui devra être téléchargé depuis la page de téléchargement de logiciels pour le modèle 9800 spécifique.

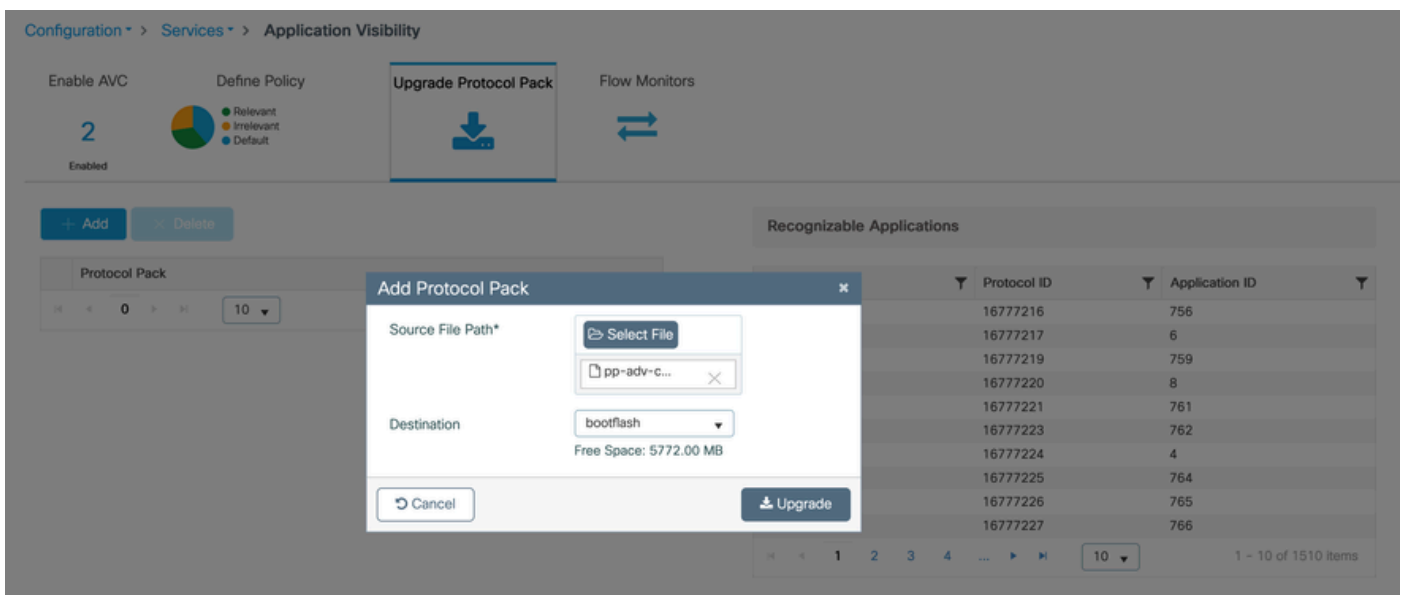
Via GUI

Accédez à Configuration > Services > Application Visibility. Cliquez sur Upgrade Protocol Pack .



Section Upload Protocol dans le WLC 9800

Cliquez sur Add, puis choisissez le pack de protocoles à télécharger et cliquez sur Upgrade .



Ajout du protocole NBAR

Une fois la mise à niveau terminée, le pack de protocoles est ajouté.

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

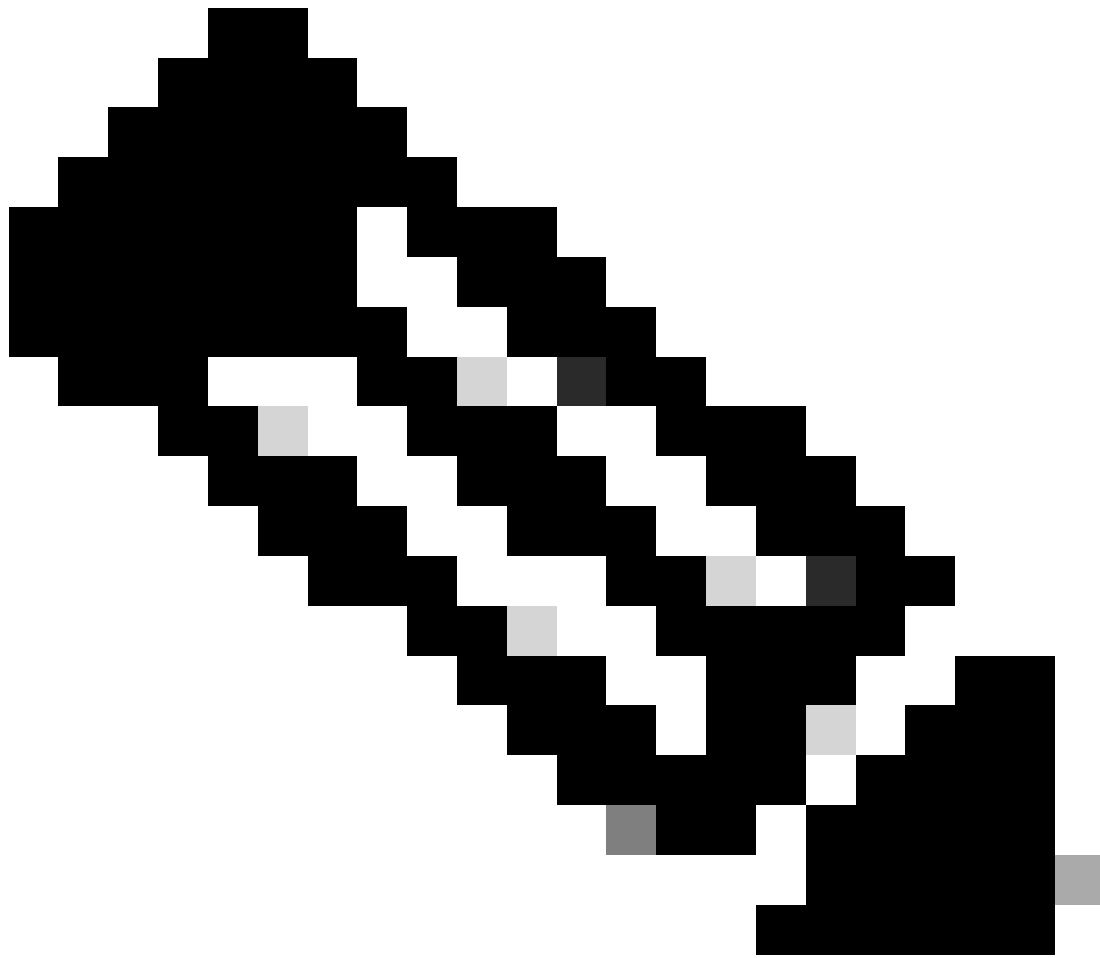
Vérification du pack de protocoles

### Via 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
```



Remarque : aucune interruption de service ne se produira pendant la mise à niveau du pack de protocoles NBAR.

## NetFlow

NetFlow est un protocole réseau utilisé pour collecter des informations sur le trafic IP et surveiller les données de flux réseau. Il est principalement utilisé pour l'analyse du trafic réseau et la surveillance de la bande passante. Voici une présentation du fonctionnement de NetFlow sur les contrôleurs de la gamme Cisco Catalyst 9800 :

- Collecte de données : le WLC 9800 collecte des données sur le trafic IP qui les traverse. Ces données comprennent des informations telles que les adresses IP source et de destination, les ports source et de destination, les protocoles utilisés, la classe de service et la cause de la terminaison du flux.
- Enregistrements de flux : les données collectées sont organisées en enregistrements de flux. Un flux est défini comme une séquence unidirectionnelle de paquets partageant un



ensemble d'attributs communs, tels que la même adresse IP source/destination, les mêmes ports source/destination et le même type de protocole.

- Exportation des données : les enregistrements de flux sont régulièrement exportés du périphérique NetFlow vers un collecteur NetFlow. Le collecteur peut être un WLC local ou un serveur dédié ou une application logicielle qui reçoit, stocke et traite les données de flux.
- Analyse : vous pouvez utiliser les collecteurs NetFlow et les outils d'analyse pour visualiser les modèles de trafic, identifier la bande passante, détecter les flux de trafic inhabituels indiquant des failles de sécurité, optimiser les performances du réseau et planifier l'extension du réseau.
- Informations spécifiques au réseau sans fil : dans le contexte des contrôleurs sans fil, NetFlow peut inclure des informations supplémentaires spécifiques au réseau sans fil, telles que le SSID, les noms des points d'accès, les adresses MAC des clients et d'autres détails relatifs au trafic Wi-Fi.

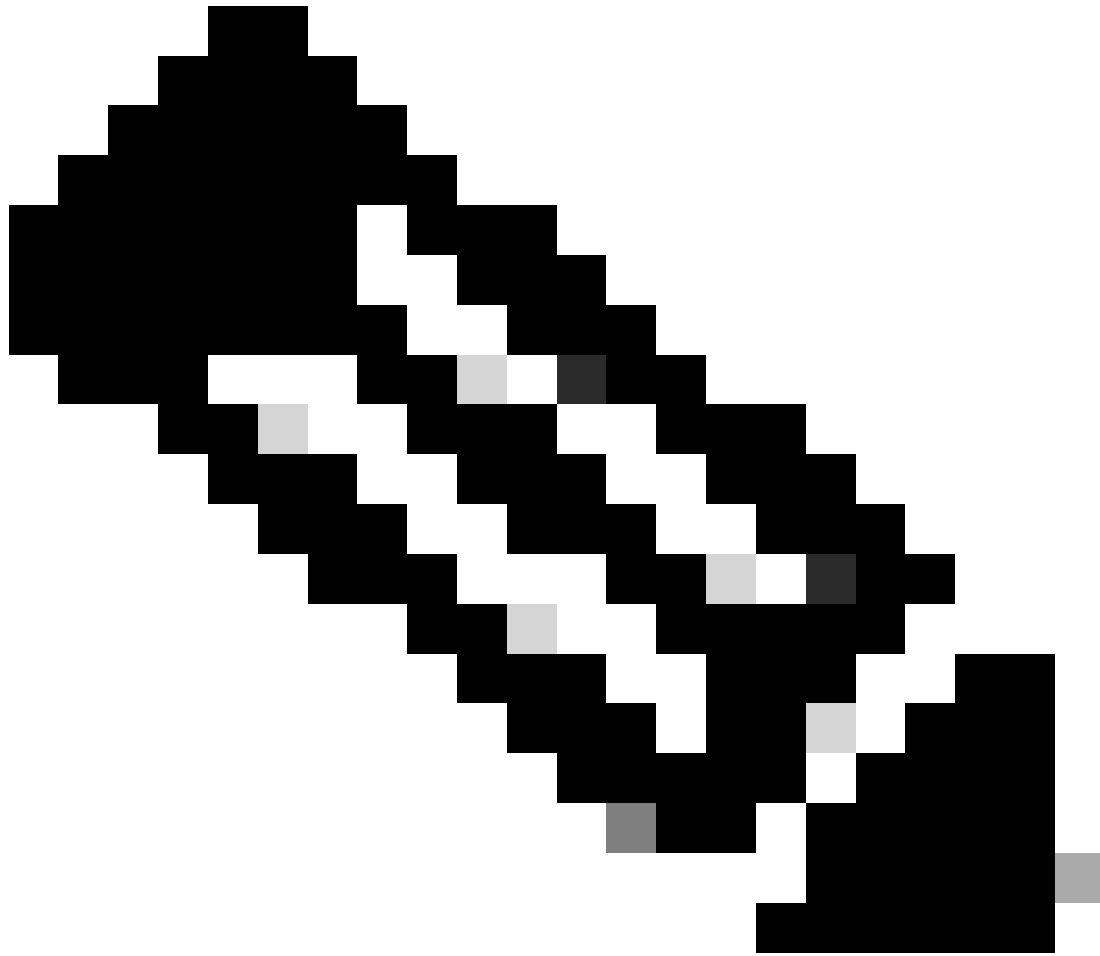
## Flexible Netflow

Flexible NetFlow (FNF) est une version avancée de NetFlow traditionnel, prise en charge par les contrôleurs LAN sans fil (WLC) de la gamme Cisco Catalyst 9800. Il offre davantage d'options de personnalisation pour le suivi, la surveillance et l'analyse des modèles de trafic réseau.

Fonctionnalités clés de Flexible NetFlow sur le WLC Catalyst 9800 :

- Personnalisation : FNF permet aux utilisateurs de définir les informations qu'ils souhaitent collecter sur le trafic réseau. Cela inclut un large éventail d'attributs de trafic tels que les adresses IP, les numéros de port, les horodatages, le nombre de paquets et d'octets, les types d'applications, etc.
- Visibilité améliorée : en exploitant FNF, les administrateurs bénéficient d'une visibilité détaillée sur les types de trafic circulant sur le réseau, ce qui est essentiel pour la planification des capacités, la facturation basée sur l'utilisation, l'analyse du réseau et la surveillance de la sécurité.
- Indépendance de protocole : FNF est suffisamment flexible pour prendre en charge divers protocoles au-delà du protocole IP, ce qui le rend adaptable à différents types d'environnements réseau.

Sur le WLC Catalyst 9800, FNF peut être configuré pour exporter des enregistrements de flux vers un collecteur ou une application d'analyse NetFlow externe. Ces données peuvent ensuite être utilisées pour le dépannage, la planification du réseau et l'analyse de la sécurité. La configuration FNF implique la définition d'un enregistrement de flux (ce qu'il faut collecter), d'un exportateur de flux (où envoyer les données) et la connexion du moniteur de flux (qui lie l'enregistrement et l'exportateur) aux interfaces appropriées.



Remarque : FNF peut envoyer 17 enregistrements de données différents (tels que définis dans la RFC 3954) au collecteur Netflow externe tiers, tel que Stealthwatch, Solarwinds et d'autres qui sont : Application Tag, Client Mac Address, AP Mac address, WlanID, Source IP, Destination IP, Source Port, Destination Port, Protocol, Flow Start Time, Flow End Time, Direction, Packet out, Byte count, VLAN ID (mode local) - Mgmt/Client et TOS - DSCP Value

## Moniteur de flux

Un moniteur de flux est un composant utilisé conjointement avec Flexible NetFlow (FNF) pour capturer et analyser les données de trafic réseau. Il joue un rôle crucial dans la surveillance et la compréhension des modèles de trafic pour la gestion du réseau, la sécurité et le dépannage. Le moniteur de flux est essentiellement une instance appliquée de FNF qui collecte et suit les données de flux en fonction de critères définis. Il est associé à trois éléments principaux :

- Flow Record : définit les données que le moniteur de flux doit collecter à partir du trafic réseau. Elle spécifie les clés (telles que les adresses IP source et de destination, les ports, les types de protocoles) et les champs non-clés (tels que les compteurs de paquets et

d'octets, les horodatages) qui seront inclus dans les données de flux.

- Flow Exporter : indique la destination où les données de flux collectées doivent être envoyées. Il inclut des détails tels que l'adresse IP du collecteur NetFlow, le protocole de transport (généralement UDP) et le numéro du port de destination où le collecteur écoute.
- Moniteur de flux : le moniteur de flux lui-même relie l'enregistrement de flux et l'exportateur de flux et les applique à une interface ou à un WLAN pour démarrer réellement le processus de surveillance. Il détermine comment les données de flux doivent être collectées et exportées en fonction des critères définis dans l'enregistrement de flux et de la destination définie dans l'exportateur de flux.

## Points d'accès pris en charge AVC

AVC est pris en charge uniquement sur ces points d'accès :

- Points d'accès Cisco Catalyst 9100
- Point d'accès Cisco Aironet 2800
- points d'accès Cisco Aironet, série 3800
- Points d'accès Cisco Aironet, série 4800

## Prise en charge de différents modes de déploiement du 9800

Mode de déploiement	9800 WLC	Point d'accès Vague 1	Point d'accès Wave 2	Point d'accès Wi-Fi 6
Mode local (Commutation centrale)	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF pris en charge	Traitement au niveau du WLC	Traitement au niveau du WLC	Traitement au niveau du WLC
Mode flexible (Commutation centrale)	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 :	Traitement au niveau du WLC	Traitement au niveau du WLC	Traitement au niveau du WLC

	Prise en charge AVC FNF pris en charge			
Mode flexible (Commutation locale)	Traitement au niveau AP	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF non pris en charge	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF pris en charge	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF pris en charge
Mode local (Fabric)	Traitement au niveau AP	Trafic IPV4 : AVC non pris en charge FNF non pris en charge  Trafic IPV6 : AVC non pris en charge FNF non pris en charge	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF pris en charge	Trafic IPV4 : Prise en charge AVC FNF pris en charge  Trafic IPV6 : Prise en charge AVC FNF pris en charge

## Restrictions lors de la mise en oeuvre de AVC sur le 9800

Les fonctionnalités AVC (Application Visibility and Control) et FNF (Flexible NetFlow) sont des fonctionnalités puissantes des contrôleurs LAN sans fil Cisco Catalyst 9800 qui améliorent la visibilité et le contrôle du réseau. Cependant, il convient de garder à l'esprit certaines limitations et considérations lors de l'utilisation de ces fonctionnalités :

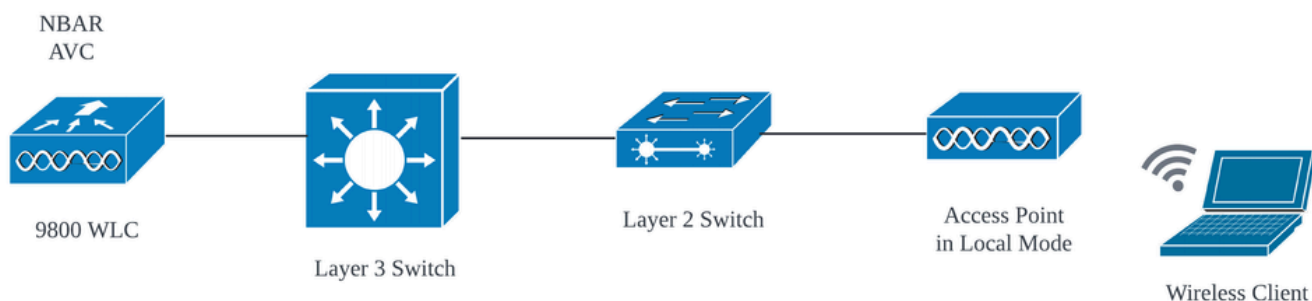
- L'itinérance de couche 2 n'est pas prise en charge sur les contrôleurs.
- Le trafic multidiffusion n'est pas pris en charge.
- Seules les applications reconnues avec la visibilité sur les applications peuvent être utilisées pour l'application du contrôle QoS.
- La liaison de données n'est pas prise en charge pour les champs NetFlow dans AVC.
- Vous ne pouvez pas mapper le même profil WLAN à la fois au profil de stratégie AVC non activé et au profil de stratégie AVC activé.
- Vous ne pouvez pas utiliser le profil de stratégie avec un mécanisme de commutation

différent sur le même WLAN pour implémenter AVC.

- AVC n'est pas pris en charge sur le port de gestion (Gig 0/0).
- La configuration de la stratégie QoS basée sur NBAR est autorisée uniquement sur les ports physiques câblés. La configuration de la stratégie n'est pas prise en charge sur les interfaces virtuelles, par exemple, VLAN, port channel et autres interfaces logiques.
- Lorsque AVC est activé, le profil AVC prend en charge jusqu'à 23 règles, ce qui inclut la règle DSCP par défaut. La politique AVC ne sera pas poussée vers le bas vers l'AP, si les règles sont plus de 23.

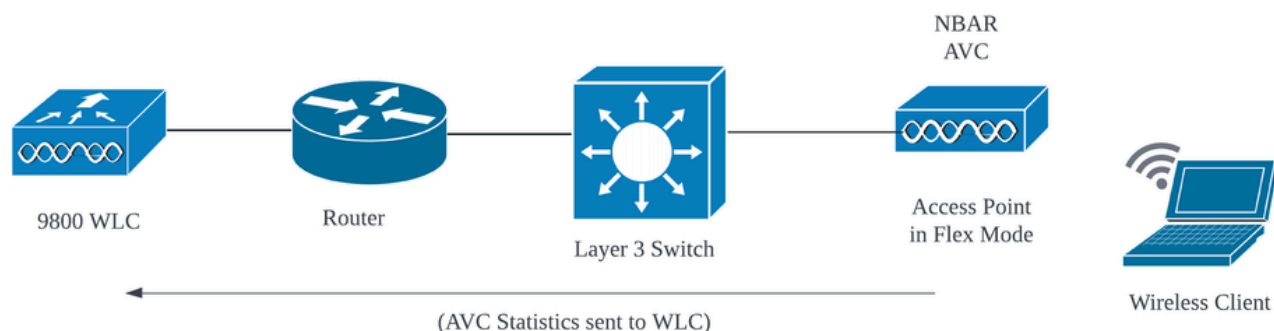
## Topologie du réseau

### AP en mode local



AVC en mode local AP (Commutation centrale)

### Point d'accès en mode flexible



AVC en mode flexible AP

## Configuration de l'AVC sur le WLC 9800

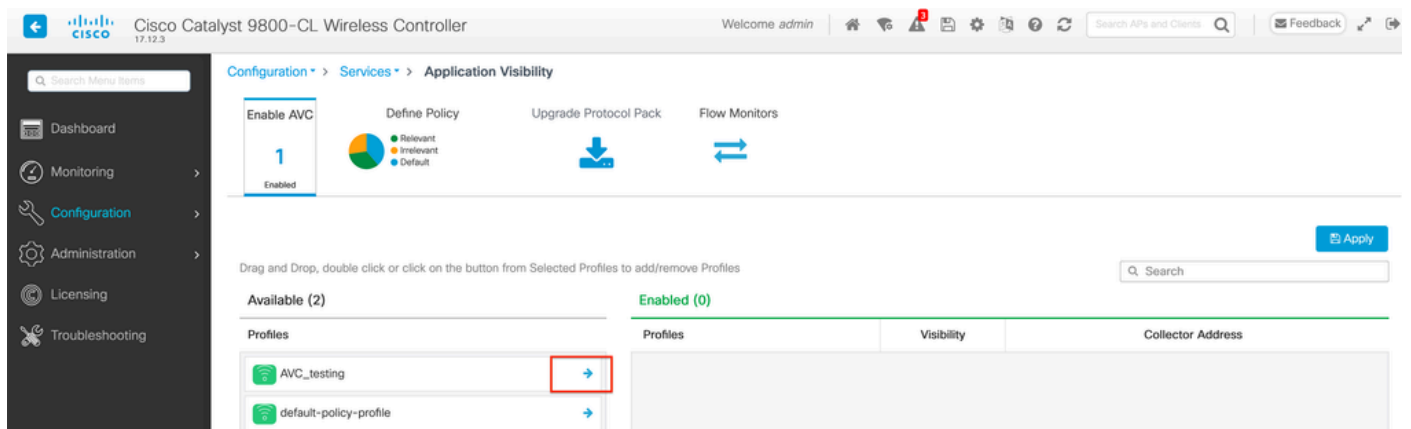
Lors de la configuration d'AVC sur le WLC 9800, vous pouvez l'utiliser comme collecteur NetFlow ou exporter les données NetFlow vers le collecteur NetFlow externe.

## Exportateur local

Sur un contrôleur LAN sans fil (WLC) Cisco Catalyst 9800, un collecteur NetFlow local fait référence à la fonctionnalité intégrée au WLC qui lui permet de collecter et de stocker localement des données NetFlow. Cette fonctionnalité permet au WLC d'effectuer une analyse de base des données NetFlow sans devoir exporter les enregistrements de flux vers un collecteur NetFlow externe.

Via GUI

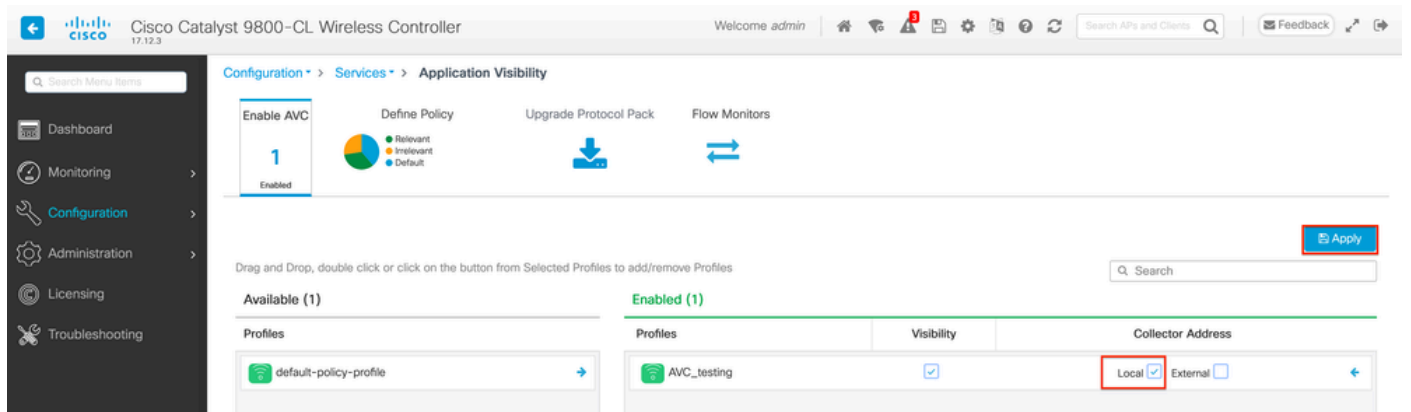
Étape 1 : Pour activer AVC sur un SSID spécifique, accédez à Configuration > Services > Application Visibility. Sélectionnez le profil de stratégie particulier pour lequel vous souhaitez activer AVC.



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 four tabs: 'Enable AVC', 'Define Policy', 'Upgrade Protocol Pack', and 'Flow Monitors'. The main area contains a table with two columns: 'Available (2)' and 'Enabled (0)'. The 'Available' column lists two profiles: 'AVC\_testing' and 'default-policy-profile'. A red box highlights the right-pointing arrow next to the 'AVC\_testing' profile. The 'Enabled' column is currently empty.

Activation d'AVC sur le profil de stratégie

Étape 2 : Sélectionnez Local comme collecteur Netflow et cliquez sur Apply.

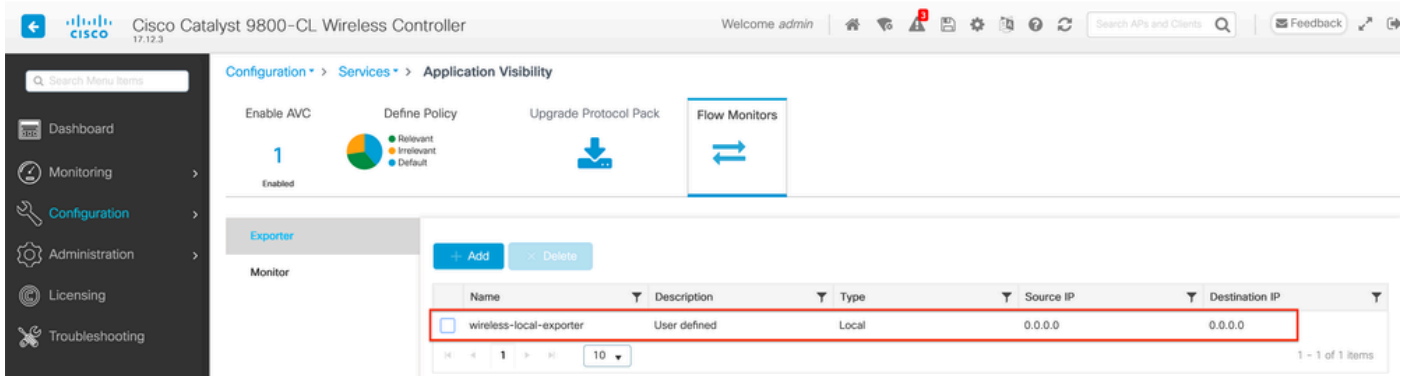


The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Services > Application Visibility. The 'Enable AVC' toggle is set to 'Enabled'. Below this, there are four tabs: 'Enable AVC', 'Define Policy', 'Upgrade Protocol Pack', and 'Flow Monitors'. The main area contains a table with two columns: 'Available (1)' and 'Enabled (1)'. The 'Available' column lists one profile: 'default-policy-profile'. The 'Enabled' column lists one profile: 'AVC\_testing'. The 'Collector Address' column for 'AVC\_testing' has 'Local' selected with a checked checkbox, and 'External' is unselected. A red box highlights the 'Local' checkbox.

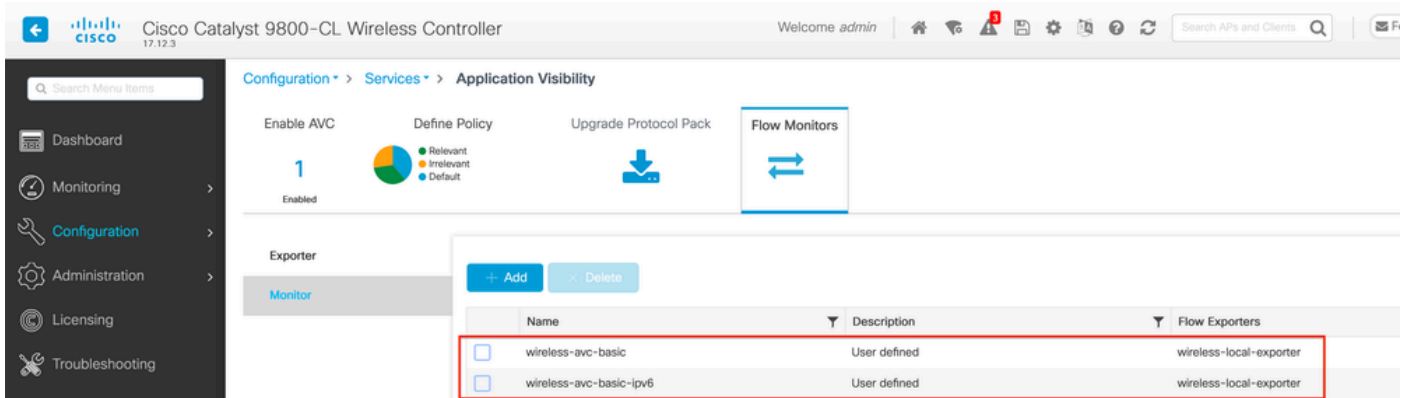
Sélection du collecteur NetFlow local

Notez que les paramètres NetFlow Exporter et NetFlow ont été automatiquement configurés en fonction des préférences spécifiées une fois que vous avez appliqué la configuration AVC.

Vous pouvez valider la même chose en naviguant vers Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor .

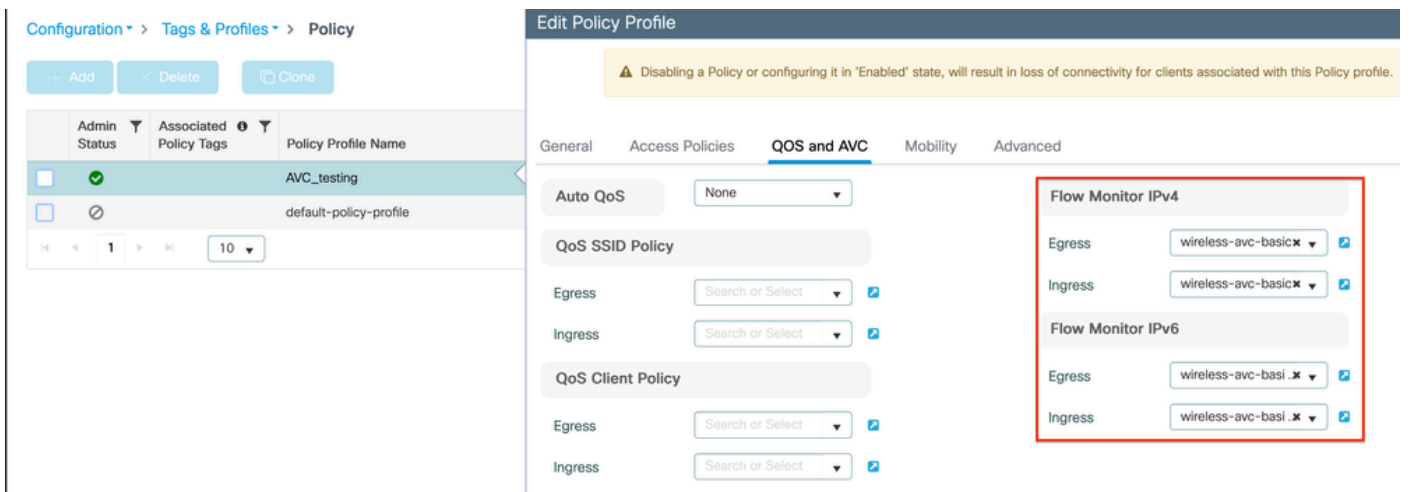


Configuration du collecteur de flux local sur le WLC 9800



Configuration de Flow Monitor avec le collecteur NetFlow local

Les moniteurs de flux AVC IPv4 et IPv6 sont automatiquement associés au profil de stratégie. Accédez à Configuration > Tags & Profile > Policy. Cliquez sur Policy Profile > AVC and QOS .



Configuration Du Moniteur De Flux Dans Le Profil De Stratégie

Via CLI

Étape 1 : Configurez le WLC 9800 en tant qu'exportateur local.

```
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
```

Étape 2 : Configurez le Moniteur de flux réseau IPv4 et IPv6 pour utiliser Local(WLC) en tant qu'exportateur Netflow.

```
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
```

Étape 3 : Mappez le Moniteur de flux IPv4 et IPv6 dans le profil de stratégie pour le trafic entrant et sortant.

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

## Collecteur NetFlow externe

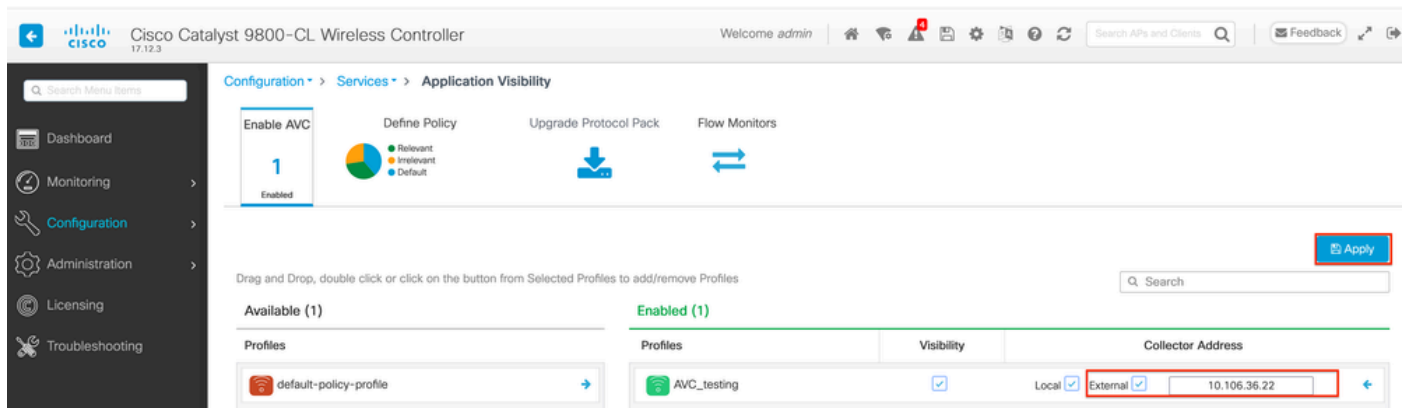
Un collecteur NetFlow externe, lorsqu'il est utilisé dans le contexte de la visibilité et du contrôle des applications (AVC) sur un contrôleur LAN sans fil (WLC) Cisco Catalyst 9800, est un système ou un service dédié qui reçoit, agrège et analyse les données NetFlow exportées depuis le WLC. Vous pouvez soit configurer uniquement le collecteur NetFlow externe pour surveiller la visibilité de l'application, soit l'utiliser avec le collecteur local.

Via GUI

Étape 1 : Pour activer AVC sur un SSID spécifique, accédez à Configuration > Services > Application Visibility. Sélectionnez le profil de stratégie particulier pour lequel vous souhaitez

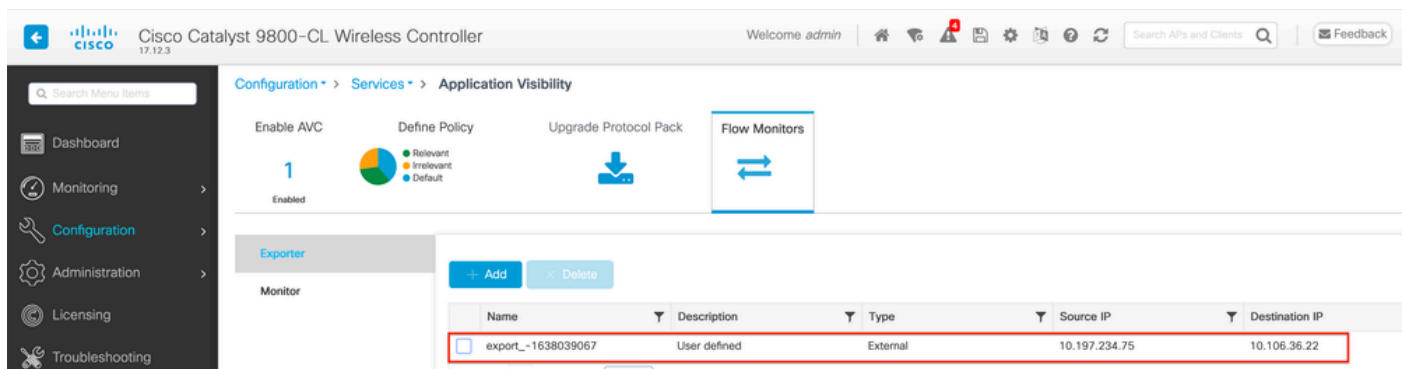


activer AVC. Sélectionnez Collector comme External et configurez l'adresse IP de NetFlow Collector comme Cisco Prime, SolarWind, StealthWatch et cliquez sur Apply.

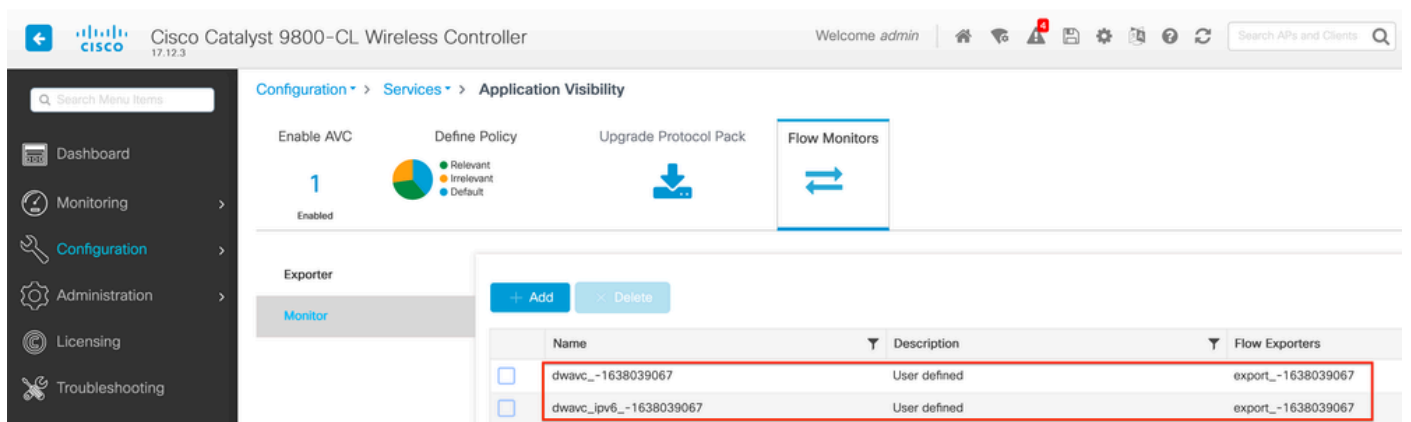


Configuration AVC pour collecteur NetFlow externe

Notez qu'une fois la configuration AVC appliquée, les paramètres NetFlow Exporter et NetFlow ont été automatiquement configurés avec l'adresse IP du collecteur NetFlow comme adresse d'exportateur et l'adresse d'exportateur comme WLC 9800 avec les paramètres de délai d'attente par défaut et le port UDP 9995. Vous pouvez valider la même chose en naviguant vers Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor .



Configuration du collecteur NetFlow externe sur le WLC 9800



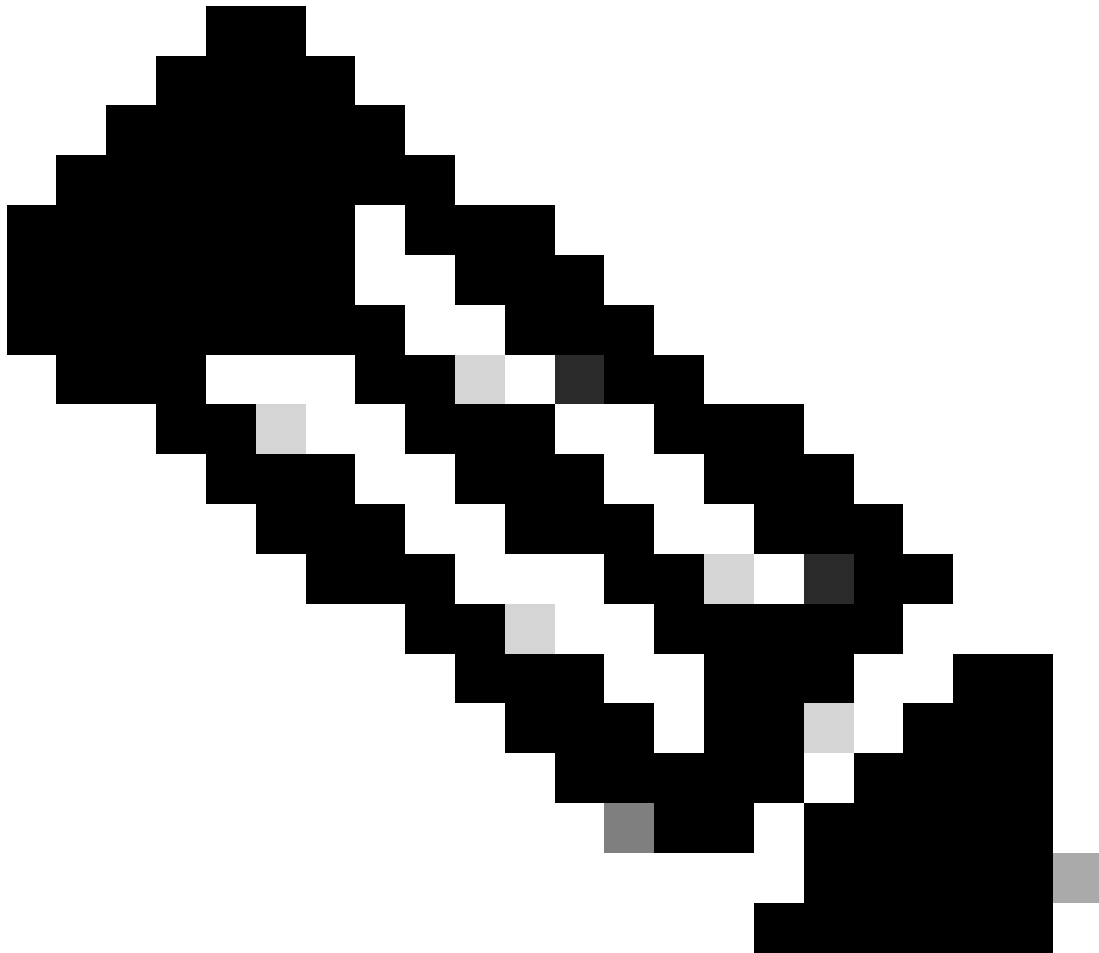
Configuration du Moniteur de flux avec le collecteur NetFlow externe

Vous pouvez vérifier la configuration des ports du Moniteur NetFlow généré automatiquement en naviguant vers Configuration > Services > NetFlow .

Cisco Catalyst 9800-CL Wireless Controller  
Welcome admin

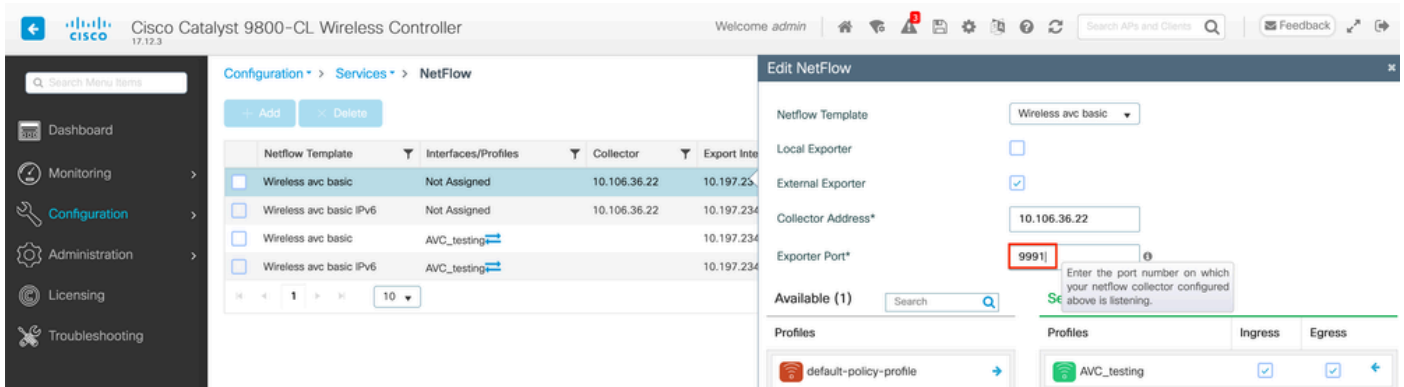
Configuration > Services > NetFlow

Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
<input checked="" type="checkbox"/> Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
<input type="checkbox"/> Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



Remarque : si vous configurez AVC via l'interface utilisateur graphique, l'exportateur NetFlow généré automatiquement sera configuré pour utiliser le port UDP 9995. Assurez-vous de valider le numéro de port utilisé par votre collecteur NetFlow.

Par exemple : si vous utilisez Cisco Prime comme collecteur NetFlow, il est essentiel de définir le port Exporter sur 9991, car il s'agit du port sur lequel Cisco Prime écoute le trafic NetFlow. Vous pouvez modifier manuellement le port d'exportateur dans la configuration NetFlow.



Modification du numéro de port de l'exportateur dans la configuration NetFlow

## Via CLI

Étape 1 : configurez l'adresse IP du collecteur NetFlow externe avec l'interface source.

```
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
```

Étape 2 : Configurez le Moniteur de flux réseau IPv4 et IPv6 pour utiliser Local(WLC) en tant qu'exportateur Netflow.

```
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
```

Étape 3 : Mappez le Moniteur de flux IPv4 et IPv6 dans le profil de stratégie pour le trafic entrant et sortant.

```
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

```

## Configuration d'AVC sur le WLC 9800 à l'aide de Cisco Catalyst Center

Avant de procéder à la configuration de la visibilité et du contrôle des applications (AVC) sur un contrôleur LAN sans fil (WLC) Cisco Catalyst 9800 via Cisco Catalyst Center, il est important de vérifier que la communication télémétrique entre le WLC et Cisco Catalyst Center a été établie avec succès. Assurez-vous que le WLC apparaît dans un état géré dans l'interface de Cisco Catalyst Center et que son état est mis à jour activement. En outre, pour une surveillance efficace de l'état de santé, il est important d'attribuer correctement le WLC et les points d'accès (AP) à leurs sites respectifs au sein de 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

Vérification de connexion de télémétrie sur WLC 9800

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 et AP sont à l'état Géré

### Network Devices

LATEST **67%** Healthy TOTAL: 3

No Devices



Router

No Devices



Core

No Devices



Distribution

No Devices



Access



1/1



Wireless Controller

1/2



Access Point

40%

7:30p

7:30p

[View Network Health](#)

État de santé du WLC et du point d'accès sur Cisco Catalyst Center

Étape 1 : Configurez Cisco Catalyst Center en tant que collecteur NetFlow et activez la télémétrie sans fil dans le paramètre Global. Accédez à Design > Network Setting > Telemetry et activez la configuration souhaitée comme indiqué.

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

Télémetrie sans fil et configuration AVC

Étape 2 : Activez la télémétrie d'application sur le WLC 9800 souhaité pour pousser la configuration AVC sur le WLC 9800. Pour cela, accédez à Provisionner > Périphérique réseau > Inventaire. Choisissez le WLC 9800 sur lequel vous souhaitez activer la télémétrie d'application, puis accédez à Action > Telemetry > Enable Application Telemetry .

Catalyst Center Provision / Inventory

Global

All Routers Switches Wireless Controllers Access Points Sensors

DEVICE WORK ITEMS

- Unreachable
- Unassigned
- Untagged
- Failed Provision
- Non Compliant
- Outdated Software Image
- No Golden Image
- Failed Image Prechecks
- Under Maintenance
- Security Advisories

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

Activation de la télémétrie d'application sur le WLC 9800

Étape 3 : choisissez le mode de déploiement selon les besoins.

Local : pour activer AVC dans le profil de stratégie local (Commutation centrale)

Flex/Fabric : pour activer AVC dans le profil Flex Policy (commutation locale) ou le SSID basé sur le 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.

Sélection du mode de déploiement sur Cisco Catalyst Center

Étape 4 : Il lance une tâche pour activer les paramètres AVC, et la configuration correspondante sera appliquée au WLC 9800. Vous pouvez afficher l'état en accédant à Activités > Journal d'audit

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]

Journaux d'audit après activation de la télémétrie sur le WLC 9800

Cisco Catalyst Center déploiera les configurations Flow Exporter et Flow Monitor, y compris le port spécifié et d'autres paramètres, et les activera dans le profil de stratégie de mode choisi, comme indiqué ci-dessous :

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

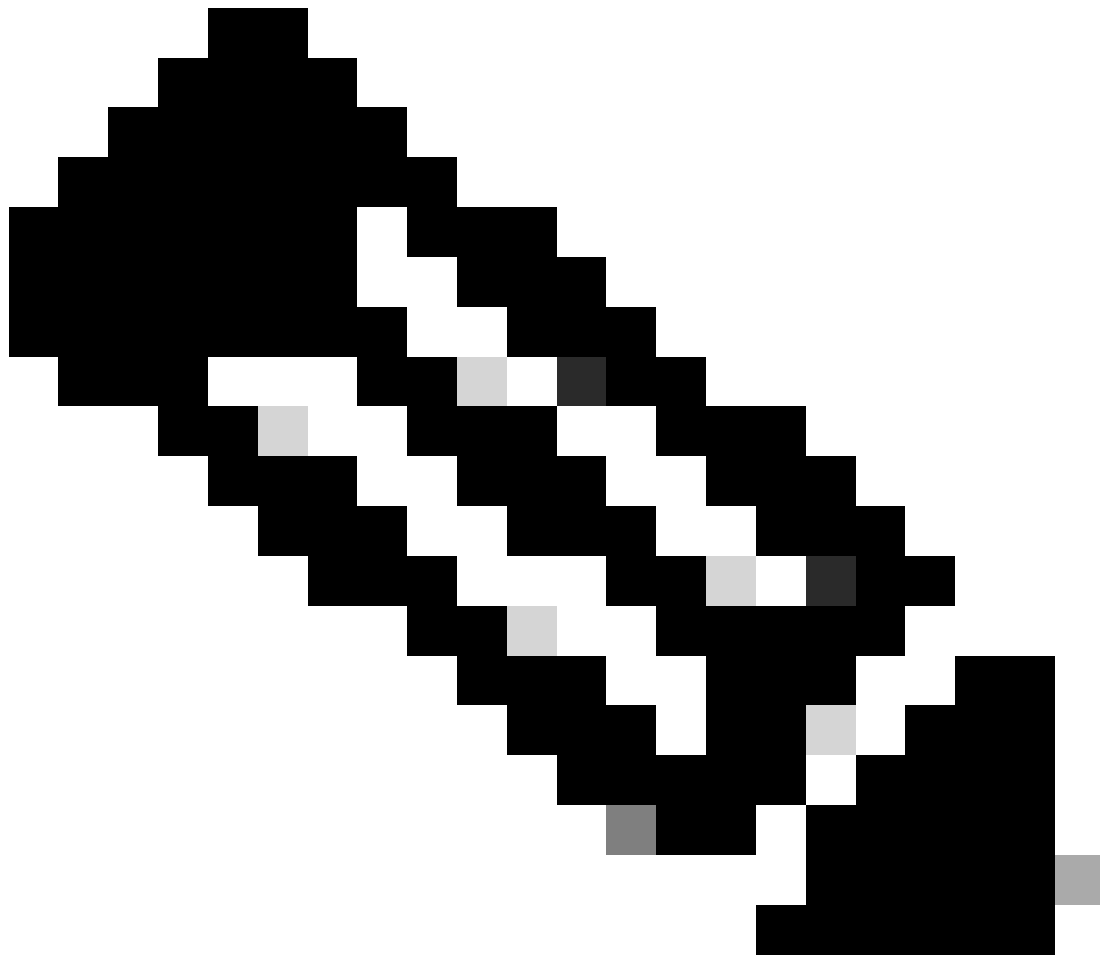
```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp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

## Vérification de l'AVC

### Sur le 9800

Lorsque le WLC 9800 est utilisé comme exportateur de flux, les statistiques AVC suivantes peuvent être observées :

- Visibilité des applications pour les clients connectés sur tous les SSID.
- Utilisation d'applications individuelles pour chaque client.
- Utilisation spécifique des applications sur chaque SSID séparément.



Remarque : vous avez la possibilité de filtrer les données par direction, couvrant à la fois le trafic entrant (entrant) et sortant (sortant), ainsi que par intervalle de temps, avec la possibilité de sélectionner une plage allant jusqu'à 48 heures.

Via GUI

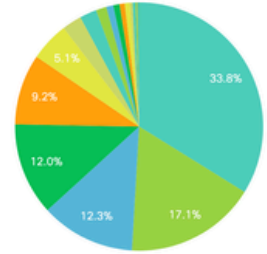
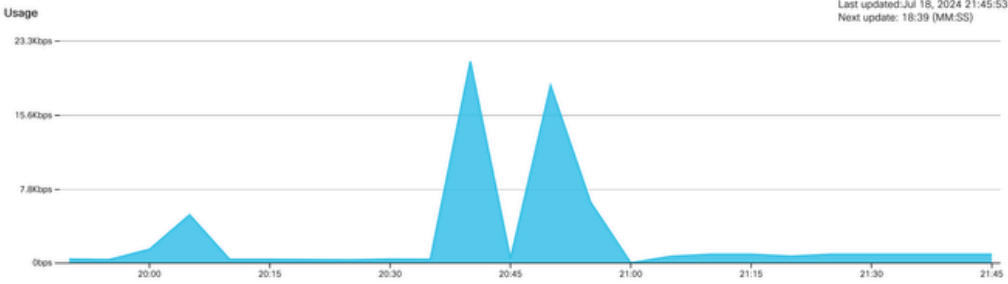
Accédez à Surveillance > Services > Application Visibility .

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

Visibilité des applications des utilisateurs connectés au SSID AVC\_testing pour le trafic entrant et sortant

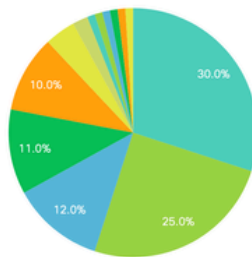
Pour afficher les statistiques de visibilité sur les applications pour chaque client, vous pouvez cliquer sur l'onglet Clients, choisir un client spécifique, puis cliquer sur Afficher les détails de l'application.

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)

Visibilité des applications pour un client spécifique - 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

Visibilité des applications pour un client spécifique - 2

Via CLI

Vérifier l'état AVC

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

-----

AVC configuration complete: YES

Statistiques de 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

Vérification de l'AVC sur la CLI 9800

Pour examiner individuellement l'utilisation des principales applications pour chaque WLAN et ses clients connectés :

```
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
```

Vérifier le nombre de paquets FNFv9 et le statut de décodage transmis au plan de contrôle (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

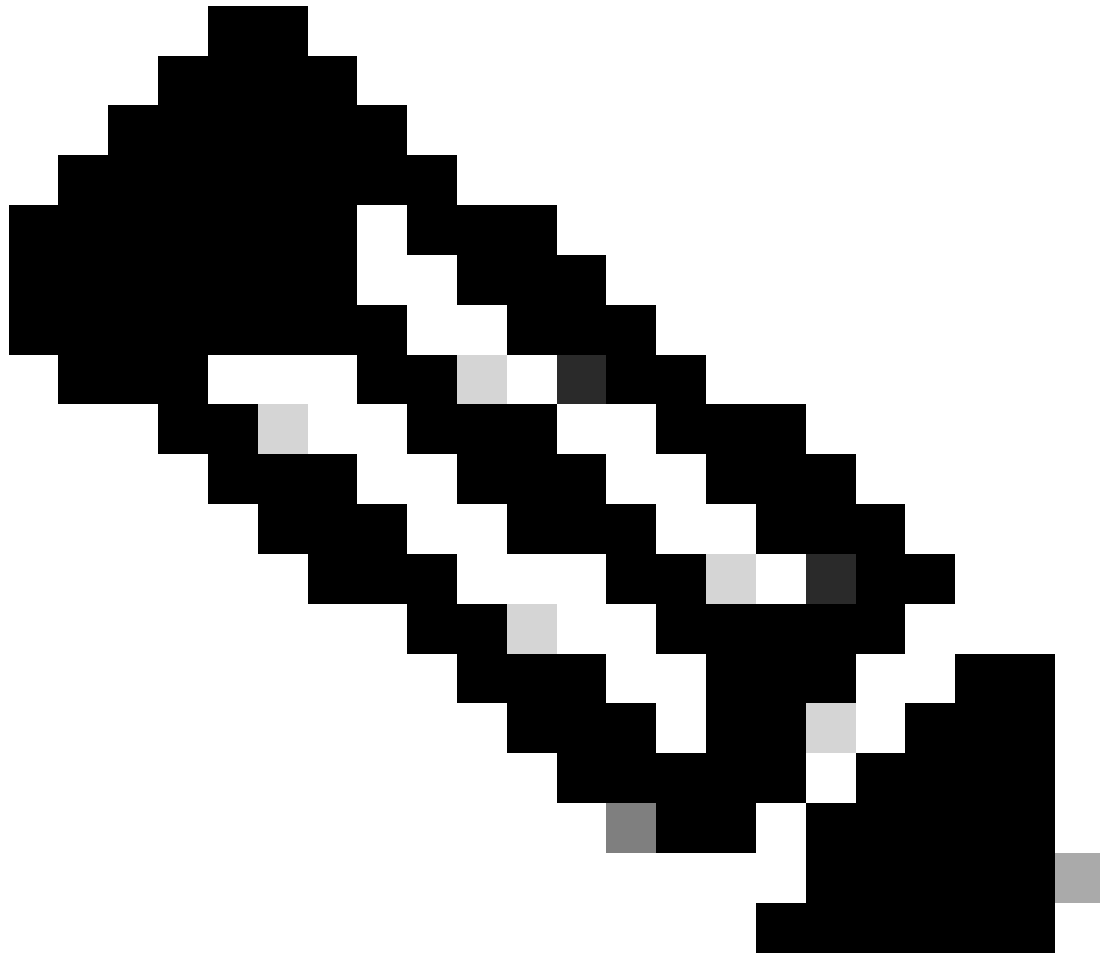
Enregistrement de paquet FNFv9

Vous pouvez également consulter directement les statistiques nbar.

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

En modes Fabric et Flex, vous pouvez obtenir les statistiques NBAR du point d'accès via :

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



Remarque : dans une configuration d'ancrage étranger, le WLC d'ancrage sert de présence de couche 3 pour le client, tandis que le WLC étranger fonctionne au niveau de la couche 2. Comme la visibilité et le contrôle des applications (AVC) fonctionnent au niveau de la couche 3, les données pertinentes ne sont observables que sur le WLC d'ancrage.

## Sur DNAC

À partir de la capture de paquets effectuée sur le WLC 9800, nous pouvons confirmer qu'il envoie continuellement des données concernant les applications et le trafic réseau à Cisco Catalyst Center.

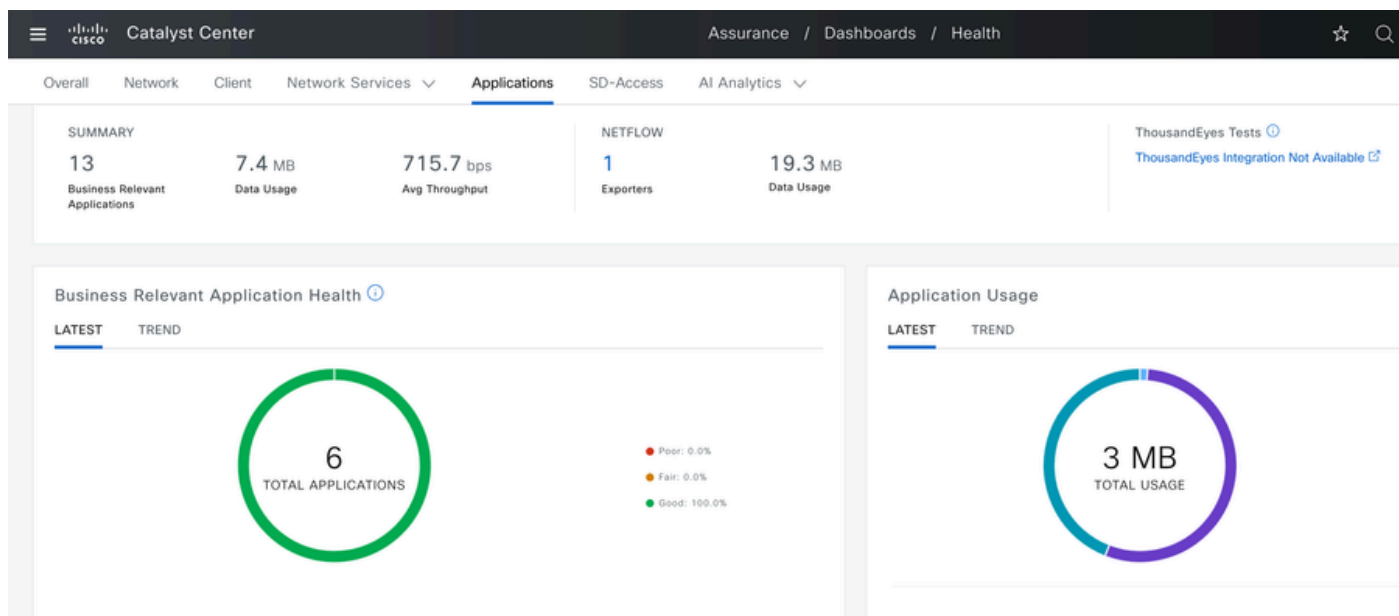
ip.addr == 10.78.8.84 and udp.port == 6007

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]

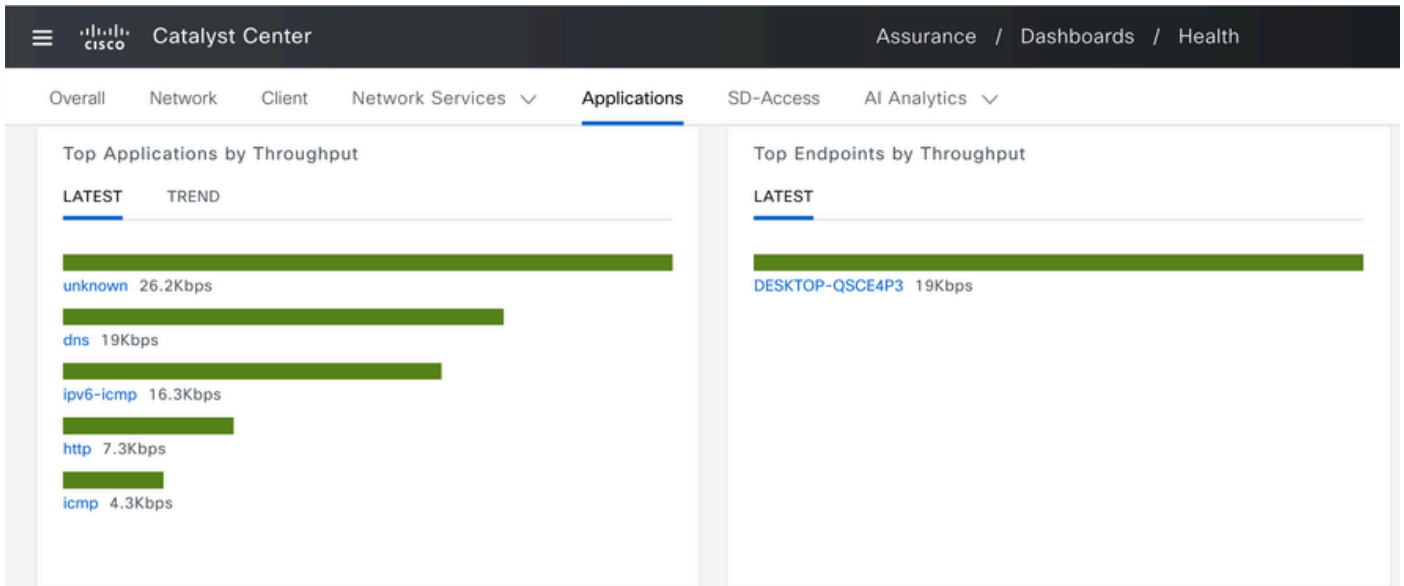
Capture de paquets sur WLC 9800

Pour afficher les données d'application pour les clients connectés à un WLC spécifique sur Cisco Catalyst Center, accédez à Assurance > Dashboards > Health > Application .



Surveillance AVC sur Cisco Catalyst Center

Nous pouvons suivre les applications les plus fréquemment utilisées par les clients et identifier les consommateurs de données les plus importants, comme illustré ici.



Principales statistiques utilisateur d'applications et de bande passante

Vous avez la possibilité de définir un filtre pour un SSID particulier, ce qui vous permet de surveiller le débit global et l'utilisation des applications des clients associés à ce SSID.

Cette fonctionnalité vous permet d'identifier les principales applications et les utilisateurs les plus gourmands en bande passante sur votre réseau.

En outre, vous pouvez utiliser la fonction de filtre temporel pour examiner ces données pour des périodes précédentes, offrant des aperçus historiques de l'utilisation du réseau.



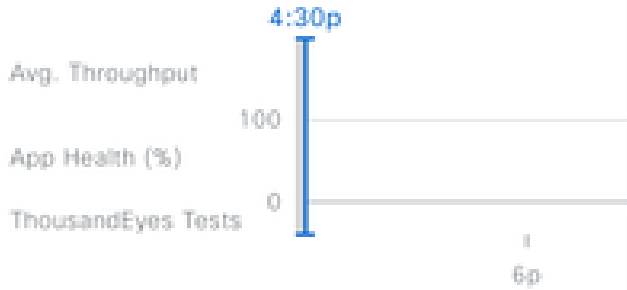
Global/BGL TAC/Shalini\_AVC

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

Time Filter pour afficher les statistiques AVC

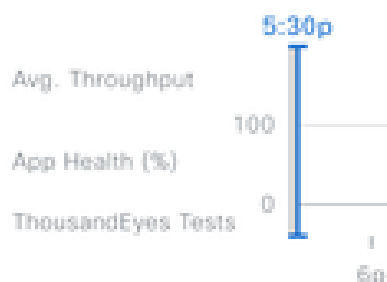


By default, hourly data is show

SSID (1/14)

Clear Filter

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



SSID: AVC\_testing

Cancel

Apply

Filtre SSID pour afficher les statistiques AVC

## Sur le collecteur NetFlow externe

Exemple 1 : Cisco Prime en tant que collecteur Netflow

Lorsque vous utilisez Cisco Prime comme collecteur Netflow, le WLC 9800 collecté s'affiche comme source de données envoyant les données Netflow et le modèle NetFlow est créé automatiquement en fonction des données envoyées par le WLC 9800.

À partir de la capture de paquets effectuée sur le WLC 9800, nous pouvons confirmer qu'il envoie des données concernant les applications et le trafic réseau à Cisco Prime en continu.

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

> 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]: 0009000120eb01e9669932b70000000400000400014f006c000000000000000000000000000000ff020000000000000000000011  
 [Length: 128]

Capture de paquets effectuée sur le WLC 9800

Prime Infrastructure

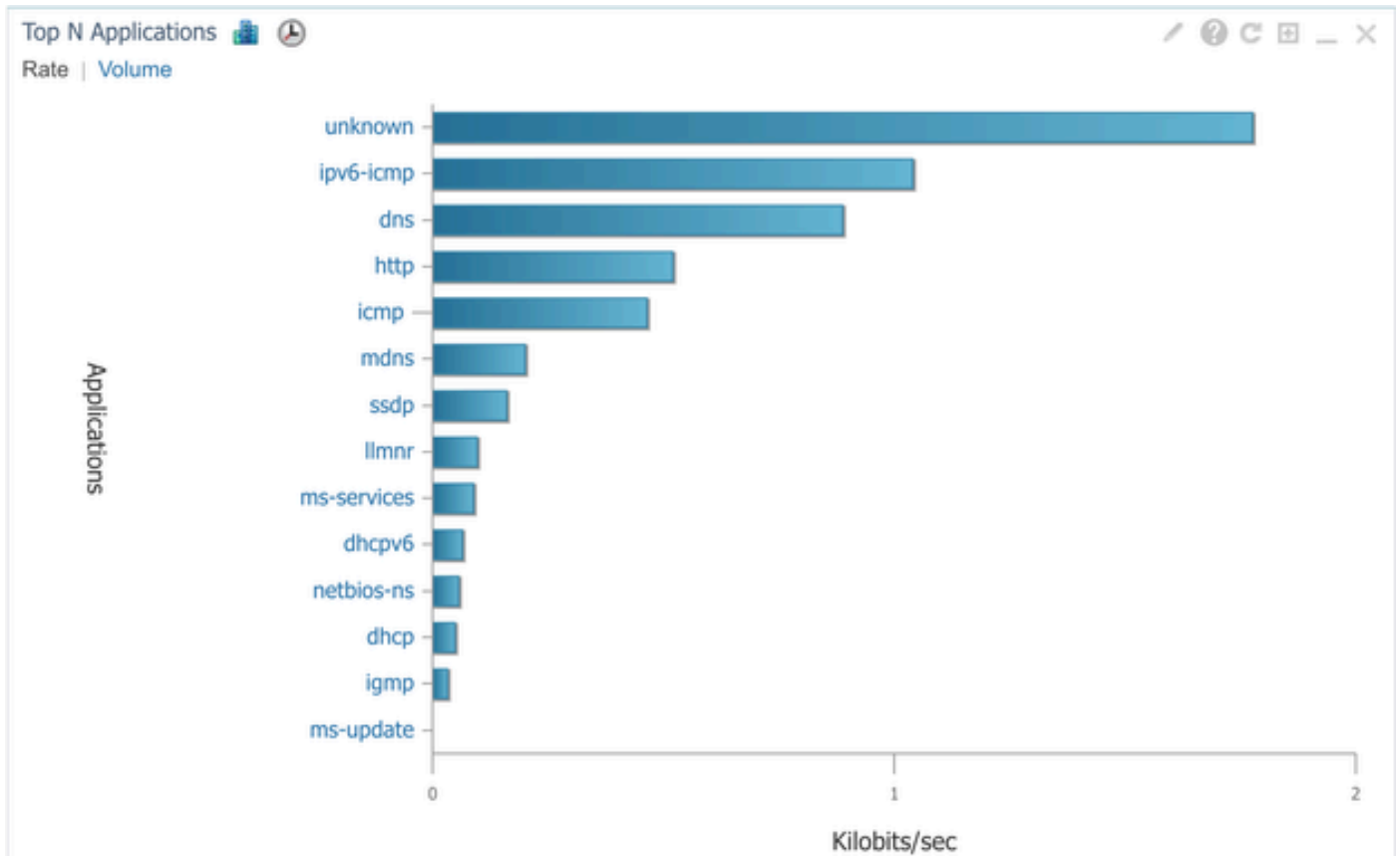
Services / Application Visibility & Control / Data Sources

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...

WLC de détection Cisco Prime 9800 comme source de données Netflow

Vous pouvez définir des filtres basés sur l'application, les services et même par client, en utilisant l'adresse IP pour une analyse de données plus ciblée.

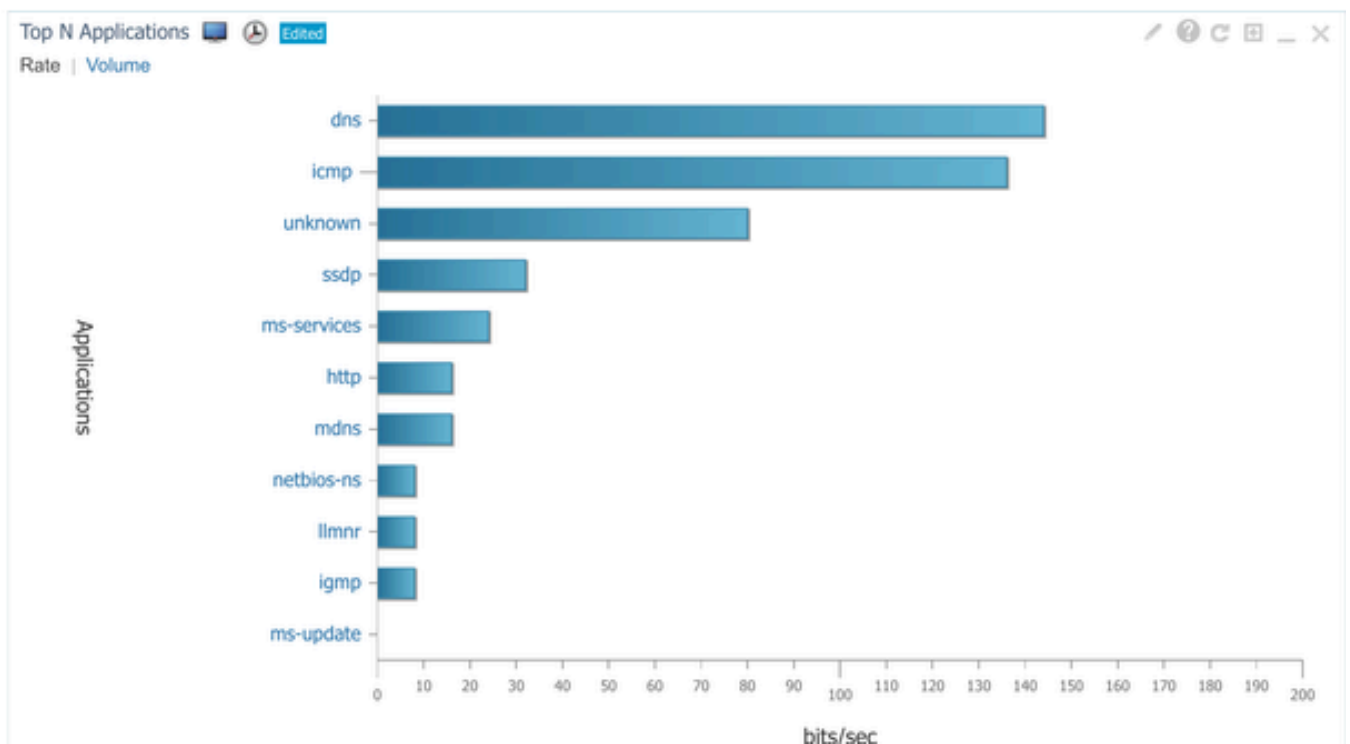


Visibilité des applications pour tous les clients

## Dashboard / Performance

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

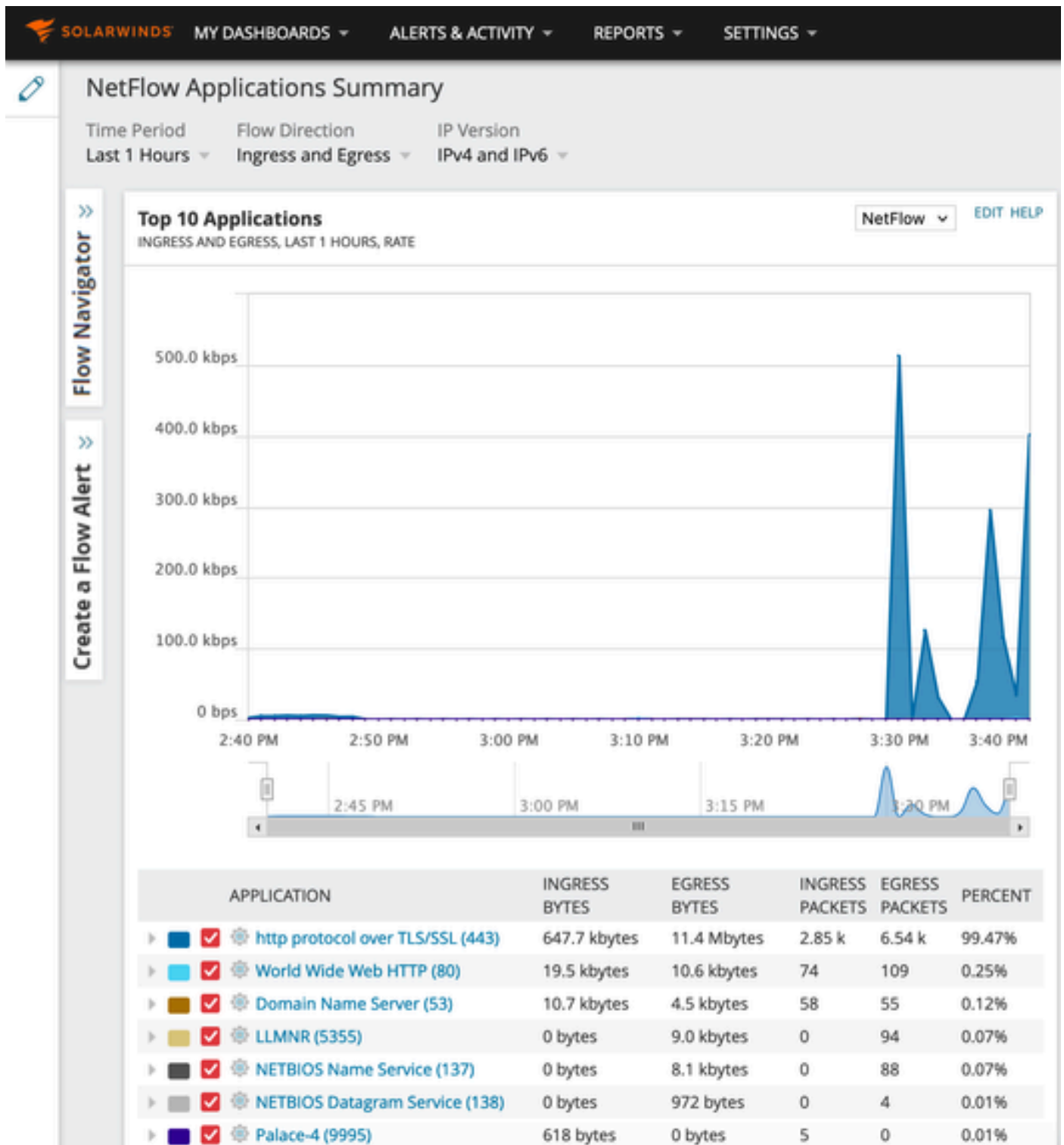
Filters  \*Client  
 \*Time Frame  
 Application  
 Network Aware



Application d'un client spécifique utilisant une adresse IP

## Exemple 2 : collecteur NetFlow tiers

Dans cet exemple, le collecteur NetFlow tiers [SolarWinds] est utilisé pour collecter les statistiques d'application. Le WLC 9800 utilise Flexible NetFlow (FNF) pour transmettre des données complètes concernant les applications et le trafic réseau, qui sont ensuite collectées par SolarWinds.



Statistiques d'application Netflow sur SolarWind

## Contrôle Du Trafic

Le contrôle du trafic fait référence à un ensemble de fonctionnalités et de mécanismes utilisés pour gérer et réguler le flux du trafic réseau. La réglementation du trafic ou la limitation du débit sont des mécanismes utilisés dans un contrôleur sans fil pour contrôler la quantité de trafic transmise à partir du client. Il surveille le débit de données pour le trafic réseau et prend des mesures immédiates lorsqu'une limite de débit prédéfinie est dépassée. Lorsque le trafic dépasse le débit spécifié, la limitation du débit peut supprimer les paquets excédentaires ou les marquer en changeant leurs valeurs de classe de service (CoS) ou de point de code de services différenciés (DSCP). Cela peut être réalisé en configurant QOS dans 9800 WLC, Vous pouvez vous référer à <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html> pour obtenir la vue d'ensemble de la façon dont ces composants fonctionnent et comment ils peuvent être configurés pour obtenir différents résultats.

## Dépannage

Le dépannage des problèmes AVC implique l'identification et la résolution des problèmes susceptibles d'affecter la capacité de l'AVC à identifier, classer et gérer avec précision le trafic des applications sur votre réseau sans fil. Les problèmes courants peuvent inclure la classification du trafic, l'application des politiques ou la création de rapports. Voici quelques étapes et considérations pour le dépannage des problèmes AVC sur un WLC Catalyst 9800 :

- Vérification de la configuration AVC : assurez-vous qu'AVC est correctement configuré sur le WLC et associé aux WLAN et profils corrects.
- Lors de la configuration d'AVC via l'interface graphique utilisateur, le port 9995 est automatiquement affecté comme port par défaut. Cependant, si vous utilisez un collecteur externe, vérifiez sur quel port il est configuré pour écouter le trafic NetFlow. Il est essentiel de configurer précisément ce numéro de port pour qu'il corresponde aux paramètres de votre collecteur.
- Vérifiez la prise en charge du modèle AP et du mode de déploiement.
- Reportez-vous aux limitations du WLC 9800 lors de la mise en oeuvre de l'AVC dans votre réseau sans fil.

## Collecte des journaux

### Journaux WLC

1. Activez l'horodatage pour avoir une référence temporelle pour toutes les commandes.

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

2. Pour vérifier la configuration

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

3. Vous pouvez vérifier le statut de l'AVC et les statistiques de netflow.

Vérifiez l'état de la configuration AVC.

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

Vérifiez le nombre de paquets FNFv9 et décodez l'état transmis au plan de contrôle (CP).

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

Vérifiez les statistiques de NetFlow (cache FNF).

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

Cochez la case Top n application usage for each wlan, où n = <1-30> Saisissez le nombre d'applications.

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

Vérifiez l'utilisation des n premières applications pour chaque client, où n = <1-30> Saisissez le nombre d'applications.

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

Cochez les n premiers clients connectés à un réseau local sans fil spécifique à l'aide de l'application spécifique, où n=<1-10> Saisissez le nombre de clients.

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

Vérifiez les statistiques nbar.

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

4. Définissez le niveau de journalisation sur 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. Activez le suivi radioactif (RA) pour l'adresse MAC du client afin de valider les statistiques AVC.

Via CLI

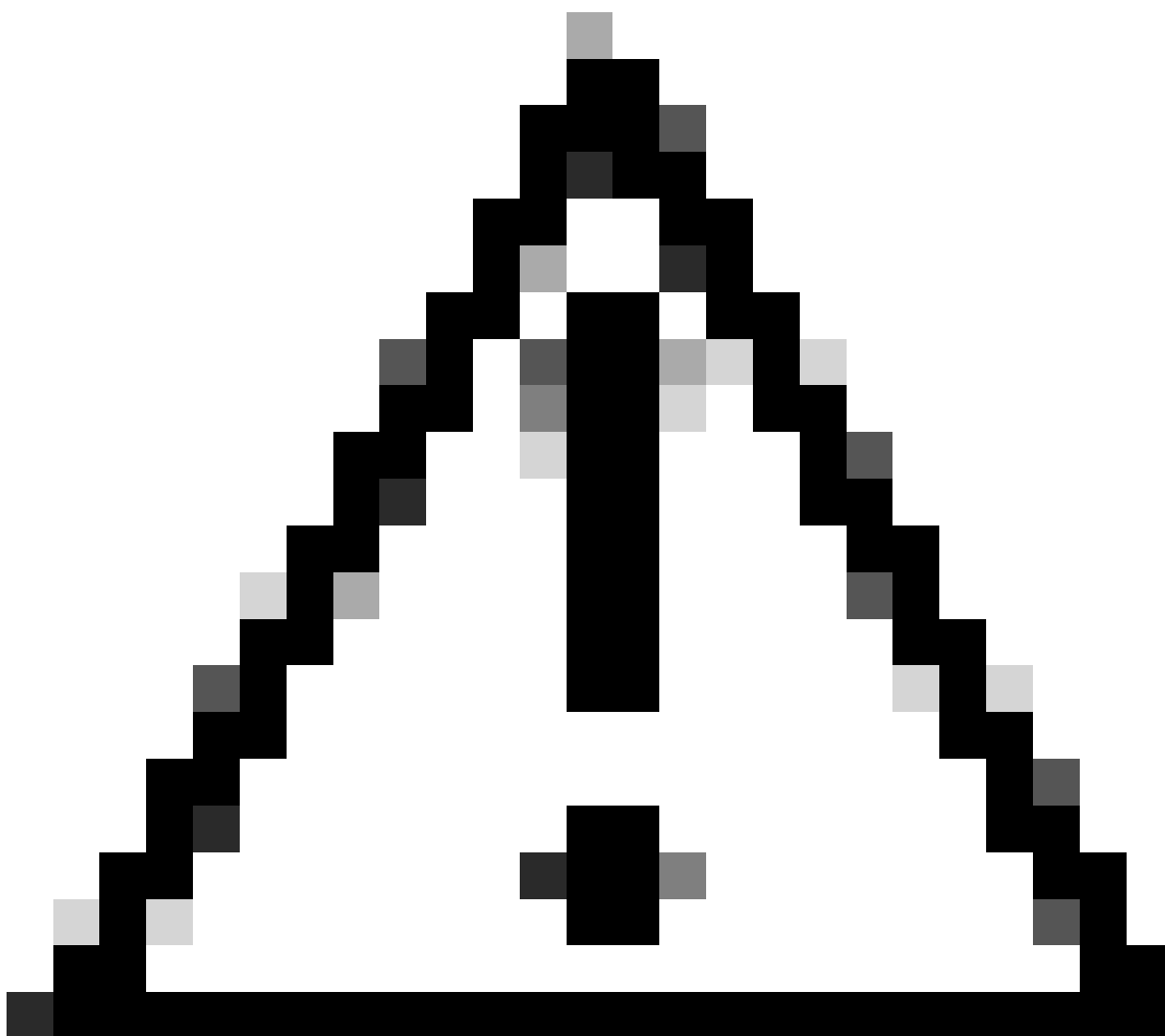
```
9800WLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti
```

```
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
```





Attention : le débogage conditionnel active la journalisation au niveau du débogage qui à son tour augmente le volume des journaux générés. Laisser cette opération en cours réduit le retard dans le temps à partir duquel vous pouvez afficher les journaux. Il est donc recommandé de toujours désactiver le débogage à la fin de la session de dépannage.

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

Via GUI

Étape 1. Accédez à Troubleshooting > Radioactive Trace .

Étape 2. Cliquez sur Add et entrez l'adresse Mac du client que vous souhaitez dépanner. Vous pouvez ajouter plusieurs adresses Mac à suivre.

Étape 3. Lorsque vous êtes prêt à démarrer le suivi radioactif, cliquez sur Démarrer. Une fois démarré, la journalisation de débogage est écrite sur le disque à propos de tout traitement du plan

de contrôle lié aux adresses MAC suivies.

Étape 4. Lorsque vous reproduisez le problème que vous souhaitez dépanner, cliquez sur Stop .

Étape 5. Pour chaque adresse mac déboguée, vous pouvez générer un fichier journal rassemblant tous les journaux appartenant à cette adresse mac en cliquant sur Générer .

Étape 6. Choisissez le délai d'attente avant la création du fichier journal et cliquez sur Apply to Device (Appliquer au périphérique).

Étape 7. Vous pouvez maintenant télécharger le fichier en cliquant sur la petite icône située à côté du nom du fichier. Ce fichier est présent dans le lecteur flash d'amorçage du contrôleur et peut également être copié à partir de la boîte via CLI.

Voici un aperçu des débogages AVC dans les traces 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. Captures intégrées filtrées par adresse MAC client dans les deux directions, filtre MAC interne client disponible après 17.1.

Il est particulièrement utile lors de l'utilisation d'un collecteur externe, car il aide à confirmer si le WLC transmet les données NetFlow au port prévu comme prévu.

Via 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
```

Via GUI

Étape 1. Accédez à Troubleshooting > Packet Capture > +Add .

Étape 2. Définissez le nom de la capture de paquets. Un maximum de 8 caractères est autorisé.

Étape 3. Définissez les filtres, le cas échéant.

Étape 4. Cochez cette case pour surveiller le trafic de contrôle si vous voulez voir le trafic envoyé au processeur du système et réinjecté dans le plan de données.

Étape 5. Définissez la taille du tampon. Un maximum de 100 Mo est autorisé.

Étape 6. Définissez la limite, soit par la durée qui permet une plage de 1 à 1000000 secondes, soit par le nombre de paquets qui permet une plage de 1 à 100000 paquets, selon vos besoins.

Étape 7. Choisissez l'interface dans la liste des interfaces de la colonne de gauche et sélectionnez la flèche pour la déplacer vers la colonne de droite.

Étape 8. Cliquez sur Apply to Device.

Étape 9. Pour démarrer la capture, sélectionnez Start .

Étape 10. Vous pouvez laisser la capture s'exécuter jusqu'à la limite définie. Pour arrêter manuellement la capture, sélectionnez Arrêter.

Étape 11. Une fois arrêté, un bouton Export devient disponible pour cliquer avec l'option pour télécharger le fichier de capture (.pcap) sur le bureau local via HTTP ou serveur TFTP ou serveur FTP ou disque dur du système local ou flash.

Journaux AP

Modes Fabric et Flex

1. show tech pour avoir tous les détails de configuration et les statistiques du client pour le point d'accès.

2. show avc nbar statistics nbar stats from AP

3. Débogages AVC

```
AP#term mon
```

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

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

## Informations connexes

[Guide de configuration AVC](#)

[Limitation du débit sur le WLC 9800](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.