# 了解Catalyst 9800无线局域网控制器上的AVC

# 目录

<u>简介</u>

<u>前提条件</u>

有关应用可视性与可控性(AVC)的信息

<u>AVC的工作原理</u>

<u>基于网络的应用程序识别 (NBAR)</u>

<u>启用策略配置文件上的NBAR协议</u> <u>升级9800 WLC上的NBAR</u>

<u>Netflow</u>

<u>灵活的Netflow</u>

<u>流监控器</u>

<u>支持AVC的接入点</u>

支持不同的9800部署模式

<u>在9800上实施AVC时的限制</u>

<u>网络拓扑</u>

<u>本地模式下的AP</u>

<u>处于flex模式下的AP</u>

<u>9800 WLC上的AVC配置</u>

<u>本地导出器</u>

<u>外部NetFlow收集器</u>

使用Cisco Catalyst Center在9800 WLC上配置AVC

<u>AVC验证</u>

<u>在9800上</u>

<u>在DNAC上</u>

<u>在外部NetFlow收集器上</u>

<u>示例1:Cisco Prime作为Netflow收集器</u>

<u>示例2:第三方NetFlow收集器</u>

<u>流量控制</u>

<u>故障排除</u>

<u>日志收集</u> WLC日志 <u>AP日志</u>

<u>相关信息</u>

# 简介

本文档介绍Cisco Catalyst 9800 WLC上的应用可视性与可控性(AVC),它可实现应用流量的精确管 理。

# 前提条件

Cisco 建议您了解以下主题:

- Cisco WLC 9800的基础知识。
- 本地和FlexConnect模式AP的基础知识。
- 接入点必须支持AVC。(不适用于本地模式AP)
- 要使AVC (QoS)的控制部分正常运行,必须配置带FNF的应用可视性功能。

# 有关应用可视性与可控性(AVC)的信息

应用可视性与可控性(AVC)是思科在无线和有线网络中用于深度包检测(DPI)技术的领先方法。通过 AVC,您可以执行实时分析并创建策略,从而有效地减少网络拥塞、最大限度地减少成本高昂的网 络链路使用,并避免不必要的基础设施升级。简而言之,AVC使用户能够通过基于网络的应用识别 (NBAR)实现全新级别的流量识别和整形。在9800 WLC上运行的NBAR软件包用于DPI,并且使用 Flexible NetFlow (FNF)报告结果。

除了可视性之外,AVC还能够优先处理、阻止或限制不同类型的流量。例如,管理员可以创建策略 来排定语音和视频应用的优先级,以确保服务质量(QoS)或限制在非关键应用在高峰工作时间可用 的带宽。它还可以与其他思科技术集成,例如用于基于身份的应用策略的思科身份服务引擎 (ISE),以及用于集中管理的Cisco Catalyst Center。

### AVC的工作原理

AVC利用FNF和NBAR2引擎等高级技术实现DPI。通过使用NBAR2引擎分析和识别流量,特定流量 会使用识别出的协议或应用进行标记。 控制器收集所有报告,并通过show命令、Web UI或其他 NetFlow导出消息将其呈现给外部NetFlow收集器(如Prime)。

建立应用可视性后,用户可以通过配置服务质量(QOS)创建具有客户端策略机制的控制规则。



基于网络的应用程序识别 (NBAR)

NBAR是集成在9800 WLC上的一种机制,用于执行DPI,以识别和分类网络上运行的各种应用。它可以识别和分类大量应用,包括加密和动态端口映射的应用,这些应用对于传统数据包检测技术通常是不可见的。



注意:要在Catalyst 9800 WLC上利用NBAR,必须正确启用和配置它,通常与特定AVC配置文件结 合使用,这些AVC配置文件定义根据流量分类采取的相应操作。

NBAR会持续定期更新,请务必保持WLC软件最新,以确保NBAR功能集保持最新且有效。

有关最新版本中支持的协议的完整列表,请访问<u>https://www.cisco.com/c/en/us/td/docs/ios-</u> <u>xml/ios/qos\_nbar/prot\_lib/config\_library/nbar-prot-pack-library.html</u>

启用策略配置文件上的NBAR协议

9800WLC#configure terminal 9800WLC(config)#wireless profile policy AVC\_testing 9800WLC(config-wireless-policy)#ip nbar protocol-discovery 9800WLC(config-wireless-policy)#end



注意:在执行此操作之前,需要禁用%策略配置文件。

9800WLC#show wireless profile policy detailed AVC\_testing | in NBAR NBAR Protocol Discovery : Enabled

升级9800 WLC上的NBAR

9800 WLC已拥有约1500个可识别应用。在新应用程序发布的情况下,将在需要从特定9800型号的

### 软件下载页面下载的最新NBAR中更新该应用程序的协议。

#### 通过GUI

### 导航到配置>服务>应用可视性。单击Upgrade Protocol Pack。

Cisco Cata	alyst 9800-CL V	Vireless Controller		Welcome admin	*	To A	<b>A</b> B
Q Search Menu Items	Configuration - >	Services -> Application Vi	sibility				
Deskheard	Enable AVC	Define Policy	Upgrade Protocol Pack	Flow Monitors			
Dashboard	2	Relevant     Irrelevant	<b>.</b>	⇒			
Monitoring >	Enabled	Default					
Configuration							

9800 WLC中的上传协议部分

# 单击Add,然后选择要下载的协议包并单击Upgrade。

Configuration - > Se	ervices - > Application	Visibility							
Enable AVC	Define Policy	Upgrade Protocol Pack	Flow Monitors						
2 Enabled	Relevant     Arrelevant     Arrelevant     Default	*	₹						
+ Add 🛛 🗙				Recognizable Ap	plications				
Protocol Pack		Add Protocol Pack			т	Protocol ID	Ŧ	Application ID	T
H 4 0 F	H 10 🔻					16777216		756	
		Source File Path*	E Select File			16777217		6	
			Dpp-adv-c			16777219		759	
						16777220		8	
		Destination	bootflash -	_		16777221		761	
			Free Space: 5772.00 MB	_		16777224		4	
						16777225		764	
		D Cancel		🕹 Upgrade		16777226		765	
						16777227		766	
				s < <b>1</b> 2	3 4	н. н	10 🔻	1 - 10 ol	

添加NBAR协议

升级完成后,您将看到添加了协议包。

Configuration • > \$	Services > Application	Visibility	
Enable AVC	Define Policy	Upgrade Protocol Pack	Flow Monitors
2	Relevant     Irrelevant     Default	*	₹
Enabled			
+ Add ×	Delete		
Protocol Pack	k		
bootflash:pp-a	adv-c9800-1712.1-49-70.0.0.p	ack	
H -	⊨ 10 👻	1 -	1 of 1 items

协议包验证

#### 通过CLI

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

To verify NBAR protocol pack version

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



注意:在NBAR协议包升级期间,不会出现服务中断。

### Netflow

NetFlow是用于收集IP流量信息和监控网络流量数据的网络协议。它主要用于网络流量分析和带宽 监控。 以下是NetFlow如何在Cisco Catalyst 9800系列控制器上工作的概述:

- 数据收集:9800 WLC收集有关流经它们的IP流量的数据。此数据包括源和目标IP地址、源和目标端口、使用的协议、服务类别以及流终止的原因等信息。
- 流记录:收集的数据被组织到流记录中。流被定义为共享一组常见属性(例如相同的源/目标 IP、源/目标端口和协议类型)的单向数据包序列。
- 导出数据:流记录会定期从支持NetFlow的设备导出到NetFlow收集器。收集器可以是本地 WLC或接收、存储和处理流数据的专用服务器或软件应用程序。
- 分析:您可以使用NetFlow收集器和分析工具来可视化流量模式、识别带宽、检测指示安全漏 洞的异常流量、优化网络性能和规划网络扩展。
- 特定于无线的信息:在无线控制器的环境中,NetFlow可以包含特定于无线网络的其他信息

,例如SSID、AP名称、客户端MAC地址以及与Wi-Fi流量相关的其他详细信息。

#### 灵活的Netflow

Flexible NetFlow (FNF)是传统NetFlow的高级版本,受Cisco Catalyst 9800系列无线局域网控制器 (WLC)支持。它为跟踪、监控和分析网络流量模式提供了更多自定义选项。Catalyst 9800 WLC上的 Flexible NetFlow的主要功能包括:

- 自定义:FNF允许用户定义要从网络流量收集哪些信息。这包括各种流量属性,如IP地址、端口号、时间戳、数据包和字节计数、应用类型等。
- 增强的可视性:通过利用FNF,管理员可以详细了解流经网络的流量类型,这对于容量规划、 基于使用情况的网络计费、网络分析以及安全监控至关重要。
- 协议独立性:FNF足够灵活,可支持IP以外的各种协议,因此可适应不同类型的网络环境。

在Catalyst 9800 WLC上,可以将FNF配置为将流记录导出到外部NetFlow收集器或分析应用。这些数据可用于故障排除、网络规划和安全分析。FNF配置包括定义流记录(要收集的内容)、流导出器(将数据发送到何处),以及将流监控器(将记录和导出器绑定)连接到适当的接口。



注意:FNF可以向外部第三方Netflow收集器(如Stealthwatch、Solarwinds等)发送17条不同的数 据记录(如RFC 3954中所定义),这些记录包括:应用标记、客户端Mac地址、AP Mac地址、 WlanMAC id、源IP、目标IP、源端口、目标端口、协议、流开始时间、流结束时间、方向、数据包 输出、字节计数、VLAN ID(本地模式)-管理/客户端和TOS - DSCP值

#### 流监控器

流监控器是与Flexible NetFlow (FNF)配合使用的组件,用于捕获和分析网络流量数据。在监控和了 解网络管理、安全和故障排除的流量模式方面,Cisco UCS Director发挥着重要作用。流监控器实 质上是FNF的一个应用实例,用于根据定义的标准收集和跟踪流数据。它与三个主要元素相关联:

- 流记录:定义流监控器必须从网络流量收集的数据。它指定包含在流数据中的密钥(如源和目标IP地址、端口、协议类型)和非密钥字段(如数据包和字节计数器、时间戳)。
- Flow Exporter:此关键字指定必须发送收集的流数据的目标。它包括NetFlow收集器的IP地址、传输协议(通常为UDP)以及收集器侦听的目标端口号等详细信息。
- 流监控器:流监控器本身将流记录和流导出器绑定在一起,并将它们应用于接口或WLAN以实际启动监控进程。它根据流记录中设置的标准和流导出器中的目标设置,确定必须如何收集和

导出流数据。

# 支持AVC的接入点

AVC仅在以下接入点上受支持:

- Cisco Catalyst 9100系列接入点
- Cisco Aironet 2800系列接入点
- Cisco Aironet 3800 系列接入器
- Cisco Aironet 4800 系列接入器

# 支持不同的9800部署模式

部署模式	9800 WLC	第1波接入点	第2波接入点	Wifi 6接入点
本地模式 (集中交换)	IPV4流量: 支持的AVC 支持FNF IPV6流量: 支持的AVC 支持FNF	在WLC级别处理	在WLC级别处理	在WLC级别处理
灵活模式 (集中交换)	IPV4流量: 支持的AVC 支持FNF IPV6流量: 支持的AVC 支持FNF	在WLC级别处理	在WLC级别处理	在WLC级别处理
灵活模式 (本地交换)	在AP级别处理	IPV4流量: 支持的AVC 支持FNF IPV6流量: 支持的AVC 不支持FNF	IPV4流量: 支持的AVC 支持FNF IPV6流量: 支持的AVC 支持FNF	IPV4流量: 支持的AVC 支持FNF IPV6流量: 支持的AVC 支持FNF
本地模式 (交换矩阵)	在AP级别处理	IPV4流量: 不支持AVC	IPV4流量: 支持的AVC	IPV4流量: 支持的AVC

	不支持FNF	支持FNF	支持FNF
	IPV6流量: 不支持AVC 不支持FNF	IPV6流量: 支持的AVC 支持FNF	IPV6流量: 支持的AVC 支持FNF

# 在9800上实施AVC时的限制

应用可视性与可控性(AVC)和Flexible NetFlow (FNF)是Cisco Catalyst 9800系列无线局域网控制器的强大功能,可增强网络可视性与可控性。但是,使用这些功能时需要记住一些限制和注意事项:

- 不支持跨控制器进行第2层漫游。
- 不支持组播流量。
- 只有通过应用可视性识别的应用才能用于应用QoS控制。
- AVC中的NetFlow字段不支持数据链路。
- 您不能将同一个WLAN配置文件同时映射到未启用AVC的策略配置文件和启用AVC的策略配置 文件。
- 您不能将具有不同交换机制的策略配置文件用于同一WLAN以实施AVC。
- 管理端口(Gig 0/0)不支持AVC。
- 只允许对有线物理端口进行基于NBAR的QoS策略配置。虚拟接口(例如VLAN、端口通道和 其他逻辑接口)不支持策略配置。
- 启用AVC时,AVC配置文件仅支持最多23条规则,包括默认DSCP规则。如果规则超过 23,则不会将AVC策略下推到AP。

# 网络拓扑

## 本地模式下的AP



本地模式AP下的AVC(集中交换)

## 处于flex模式下的AP



(AVC Statistics sent to WLC)

Flex模式AP中的AVC

# 9800 WLC上的AVC配置

在9800 WLC上配置AVC时,您可以将其用作NetFlow收集器,也可以将NefFlow数据导出到外部 NetFlow收集器。

### 本地导出器

在Cisco Catalyst 9800无线LAN控制器(WLC)上,本地NetFlow收集器是指WLC中允许其收集和本 地存储NetFlow数据的嵌入式功能。此功能使WLC能够执行基本的NetFlow数据分析,而无需将流记 录导出到外部NetFlow收集器。

通过GUI

第1步:要在特定SSID上启用AVC,请导航到配置>服务>应用可视性。 选择要为其激活AVC的特定 策略配置文件。

Cisco Cata	lyst 9800-CL Wireless Controller	Welcome admin	• 4 8 • 3 0	C Search APs and Clients Q Eeedback 2 (
Q. Search Menu Items	Configuration * > Services * > Application Visibility			
Dashboard	Enable AVC Define Policy Upgrade Protoco	DI Pack Flow Monitors		
Monitoring     Monitoring     Configuration	Enabled			
(O) Administration	Drag and Drop, double click or click on the button from Selected Profiles t	to add/remove Profiles		Q. Search
C Licensing	Available (2)	Enabled (0)		
X Troubleshooting	Profiles	Profiles	Visibility	Collector Address
	AVC_testing →			
	Gefault-policy-profile →			

在策略配置文件上启用AVC

第2步:选择本地作为Netflow收集器,然后点击应用。

Cisco Cisco	Catalyst 9800-CL Wireless Controller	Welcome admin 🛛 🐐 🕫 🦧 🖺 💠 🕯	C Search APs and Clients Q
Q. Search Menu Items	Configuration - > Services - > Application Visibility		
🚃 Dashboard	Enable AVC Define Policy Upgrade Protocol Pack	Flow Monitors	
Monitoring	1     Enabled	₽	
Configuration	>		
O Administration	> Drag and Drop, double click or click on the button from Selected Profiles to add/rem	iove Profiles	Q. Search
C Licensing	Available (1) Enable	ed (1)	
X Troubleshooting	Profiles Profile	s Visibility	Collector Address
	G default-policy-profile →	AVC_testing	Local 🗹 External 🗌 🗲

选择本地NetFlow收集器

### 请注意,应用AVC配置后,NetFlow导出器和NetFlow设置已根据指定的首选项自动配置。

您可以导航到Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor进 行验证。

Cisco Cata	lyst 9800-CL Wire	less Controller		Welcome admin	* *	A 🗅 🔅	000		Clients Q	Seedback x <sup>A</sup>
Q. Search Meriu Items	Configuration * > Se	rvices • > Application Vis	ibility							
Dashboard	Enable AVC	Define Policy Relevant	Upgrade Protocol Pack	Flow Monitors						
Monitoring >	1 Enabled	Irrelevant     Default	<b>.</b>	7						
Configuration	Exporter									
Administration	Monitor	+ Add	× Delete							
Licensing		Name wireless-l	Descr     Descr     User d	iption T	Type		Source II 0.0.0.0	2	Destination I	P <b>T</b>
X Troubleshooting		8 4 1	► H 10 ¥							1 - 1 of 1 items
9800 WLC上的本地	流量收集器配	,置								
9800 WLC上的本地	流量收集器配 talyst 9800-CL V	置 Vireless Controller		Welcom	e admin	* *	<b>2</b> B ¢	0 C		ents Q
9800 WLC上的本地 Cisco Cisco Ca Q. Search Mena Items	流量收集器配 talyst 9800-CL V Configuration * >	置 Vireless Controller Services - > Applicati	on Visibility	Welcom	e admin	<i>₫</i> ₩	e e 🕈	0 C		ents Q
9800 WLC上的本地 Cisco Cisco Ca Q. Search Menu Itams 园 Dashboard	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC	Wireless Controller Services > Applicati Define Policy Patement	on Visibility Upgrade Protocol I	Welcom Pack Flow Monito	e admin rs	* *	<b>2</b> B ¢	19 O S		ents Q
9800 WLC上的本地 Cisco Ca Cisco Ca Cisco Ca Ca Search Mona Items Dashboard Monitoring	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC 1 Enabled	ででは、 Wireless Controller Services・ > Applicati Define Policy ・ Peteuant ・ Defaut	on Visibility Upgrade Protocol I	Velcom Pack Flow Monito	e admin	* *	<b>e</b> n 🔅	19 O 2		ents Q
9800 WLC上的本地 < t <sup>th</sup> title Cisco Ca (2. Search Menu Items) 同 Dashboard ② Monitoring > ※ Configuration >	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC 1 Enabled	Image: Services ➤ Application Define Policy Image: Belevant → Relevant → Defunt	on Visibility Upgrade Protocol I	Velcom Pack Flow Monito	e admin rs	1 P 1	<b>2</b> • •	B 0 C		
9800 WLC上的本地 Cisco Ca Cisco Ca Cisco Ca Cisco Ca Configuration → Configuration → Administration →	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC 1 Enabled Exporter	Vireless Controller Services • > Applicati Define Policy • Relevant • Defaut	on Visibility Upgrade Protocol f	Velcom Pack Flow Monito	e admin rs	1 <b>7</b> 1	2 🗈 🌣	B 0 2		
9800 WLC上的本地 Cisco Cisco Ca Cisco Ca Casarch Manu Rama Dashboard Monitoring  Administration  Configuration	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC 1 Enabled Exporter Monitor	Image: Services * > Application          Services * > Application         Define Policy         ● Relevant         ● Default	on Visibility Upgrade Protocol I Line (Kalana) Mare	Welcom Pack Flow Monito	e admin rs	ation	A 🗈 🌣	0 0 C	Search APs and Cl	
9800 WLC上的本地 Cisco Ca Cisco Ca Configuration A Configuration A Cisco Ca Cisco Cisco Ca Cisco Cisco Cis	流量收集器配 talyst 9800-CL V Configuration * > Enable AVC 1 Enabled Exporter Monitor	Vireless Controller Services  Applicati Define Policy Biolevant Definet Policy Action Definet	on Visibility Upgrade Protocol I E Visitation Visitatio	Velcom Pack Flow Monito	rs T Descrip User de	종 🐨 🖌	£ D ¢	® @ ₽ T	Search APs and Cl	ents Q

使用本地NetFlow收集器的流量监控器配置

IPv4和IPv6 AVC流监控器将自动与策略配置文件关联。导航到配置>标签和配置文件>策略。单击 Policy Profile > AVC和QOS。

Configuration * > Tags & Profiles * > Policy	Edit Policy Profile
+ Add 🛛 × Delete	Disabiling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile
Admin T Associated O T Policy Profile Name	General Access Policies QOS and AVC Mobility Advanced
AVC_testing	Auto CoS
default-policy-profile	Auto Qos
∺ ≺ 1 ≻ ∺ 10 ▼	QoS SSID Policy Egress wireless-avc-basic * 🗸 💈
	Egress Search or Select 🕞 💈 Ingress wireless-avc-basic 🗙 🚽 💈
	Ingress Search or Select V P
	QoS Client Policy Egress wireless-avc-basi.x 🗸
	Egress Search or Select 🕞 💈 Ingress wireless-avc-basi.x 🗸 💈
	Ingress Search or Select -

策略配置文件中的流监控器配置

#### 通过CLI

#### 第1步:将9800 WLC配置为本地导出器。

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

#### 第2步:配置IPv4和IPv6网络流监控器以使用本地(WLC)作为Netflow导出器。

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

#### 第3步:在策略配置文件中映射入口和出口流量的IPv4和IPv6流监控器。

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

### 外部NetFlow收集器

外部NetFlow收集器在Cisco Catalyst 9800无线局域网控制器(WLC)上的应用可视性与可控性 (AVC)环境中使用时,是用于接收、聚合和分析从WLC导出的NetFlow数据的专用系统或服务。您 可以仅配置外部NeFlow收集器以监控应用可视性,也可以将其与本地收集器配合使用。

通过GUI

第1步:要在特定SSID上启用AVC,请导航到配置>服务>应用可视性。 选择要为其激活AVC的特定 策略配置文件。 选择Collector作为External,并配置NetFlow Collector的IP地址,如Cisco Prime、 SolarWind、StealthWatch,然后单击Apply。

e di	co C	isco Cata	alyst 9800-CL	Wireless Control	er		Welcome admin	* *	r 🔏 🖪	• 19	02		Q	S Feedback	x* @
Q Search	Mènu Items		Configuration -	> Services - > App	lication Visibility										
📻 Dashb	oard		Enable AVC	Define Polic	y Upg	rade Protoco	I Pack Flow Monitors								
🕜 Monito	oring		1 Enabled	Irrelevant     Default		<b>*</b>	<b>—</b>								
Real Config															Apply
ැලි Admin	istration		Drag and Drop	, double click or click on t	he button from Selec	cted Profiles to	o add/remove Profiles					Q. Search			(paper)
C Licens			Available (	1)			Enabled (1)								
💥 Troubl	eshooting		Profiles				Profiles		Visibility	'		Collector A	ddress		
			C default	-policy-profile		*	AVC_testing		2		Local 🗹 Ex	itemal 🗹	10.106.36.22		٠

外部NetFlow收集器的AVC配置

请注意,应用AVC配置后,NetFlow导出器和NetFlow设置已自动配置为将NetFlow收集器IP地址用 作导出器,将导出器地址配置为9800 WLC,默认超时设置和UDP端口9995。您可以导航到 Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor进行验证。

¢	cisco 17		W	elcome ad	dmin	<b>₩ %</b>	<b>&amp;</b> B	0 3	02			E Feedback					
Q	Search Menu Items		Configuration * >	Services -> Appl	cation Vis	ibility											
	Dashboard		Enable AVC	Define Polic	e e e e e e e e e e e e e e e e e e e	Upgrade Proto	col Pack	Flow M	lonitors								
000			1	Relevant     Irrelevant		+		-	<u>•</u>								
$\odot$	Monitoring	>	Enabled	• Defaut													
Ľ		,															
ഹ	Administration	,	Exporter	_	Add												
~~	Parimonution	ŕ	Monitor	_	- Add	× Delete											
C	Licensing				Name		₹ D	escription		T	Туре		Ŧ	Source IP	1	Destination IP	
×	Troubleshooting				export1	638039067	U	ser defined			External			10.197.234	.75	10.106.36.22	
0.0						· · · · · · · · · · · · · · · · · · ·											

9800 WLC上的外部NetFlow收集器配置

¢	cisco	Cisco C	atalyst 9800-CL	Wireles	roller			Welcome a	dmin 🖌 👫	6	4	\$ 0 G	Q		Q	
Q, Se	earch Menu It	ems	Configuration *	> Service	s•≻ A	pplicati	on Visibility									
🔜 Da	ashboard		Enable AVC		Define P	olicy	Upgrade Protocol	Pack	Flow Monitors							
<b>6</b> 4	lonitoring		1		<ul> <li>Relevant</li> <li>Irrelevant</li> <li>Default</li> </ul>	t A	<b>.</b>		₽							
	lonitoning		Enabled													
el c			Exporter													
ঠ্যি ন	dministratio					+ Ad	d X Delete									
© Lie	icensing		Monitor				Name		т	Description				Ţ	Flow Exporters	
X Tr	roubleshoo	ting					dwavc1638039067			User defined					export1638039067	1
~~							dwavc_ipv61638039067			User defined					export1638039067	

使用外部NetFlow收集器的流量监控器配置

# 导航到Configuration > Services > NetFlow,您可以检查自动生成的NetFlow监控器的端口配置。

Cisco Cata	alyst 9800-CL Wireless Co	ontroller	Welcome admin	* * * * *	Search APs and Clients	Q Feedback	
Q. Search Menu Items	Configuration * > Services *	NetFlow					
🚃 Dashboard	+ Add × Delete						
~	Netflow Template	Interfaces/Profiles	Y Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
( Monitoring >	Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
🖏 Configuration 🔹 🔸	Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



注意:如果通过GUI配置AVC,自动生成的NetFlow导出器将配置为使用UDP 9995端口。请确保验 证NetFlow收集器正在使用的端口号。

例如:如果您将Cisco Prime用作NetFlow收集器,则必须将导出器端口设置为9991,因为这是 Cisco Prime侦听NetFlow流量的端口。您可以在NetFlow配置中手动更改导出器端口。

Cisco Cata	lyst 9800-CL Wireless Controller	Welcome admin	****	Search APs and Clients Q	Feedback 🖌 🗭
Q. Search Menu Items	Configuration * > Services * > NetFlow	Edit Ne	etFlow		×
🚃 Dashboard	+ Add X Delete	Netflov	w Template	reless avc basic 🔻	
	Netflow Template T Interfaces/Profiles T Colle	actor Y Export Inte Local E	Exporter		
Monitoring >	Wireless avc basic Not Assigned 10.1	06.36.22 10.197.25 Extern	al Exporter		
Configuration >	Wireless avc basic IPv6 Not Assigned 10.1	06.36.22 10.197.234 Collect	tor Address*	.106.36.22	
	□ Wireless avc basic AVC_testing	10.197.234			
	Wireless avc basic IPv6 AVC_testing	10.197.234	ter Port*	Enter the port number on which	
C Licensing	H + 1 - H 10 -	Availa	able (1) Search Q	your netflow collector configured S€ above is listening.	
X Troubleshooting		Profile	\$	Profiles	Ingress Egress
		6	default-policy-profile	AVC_testing	V V *

在NetFlow配置中更改导出器端口号

#### 通过CLI

第1步:使用源接口配置外部NetFlow收集器的IP地址。

9800-Cl-VM#config t 9800-Cl-VM(config)#flow exporter External\_Exporter 9800-Cl-VM(config-flow-exporter)#destination 10.106.36.22 9800-Cl-VM(config-flow-exporter)#source \$Source\_Interface 9800-Cl-VM(config-flow-exporter)#transport udp \$Port\_Numbet 9800-Cl-VM(config-flow-exporter)#exit

第2步:配置IPv4和IPv6网络流监控器以使用本地(WLC)作为Netflow导出器。

9800-Cl-VM(config)#flow monitor wireless-avc-basic 9800-Cl-VM(config-flow-monitor)#exporter External\_Exporter 9800-Cl-VM(config-flow-monitor)#cache timeout active 60 9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 basic 9800-Cl-VM(config-flow-monitor)#exit

9800-Cl-VM(config)#flow monitor wireless avc ipv6 basic 9800-Cl-VM(config-flow-monitor)#exporter External\_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

第3步:在策略配置文件中映射入口和出口流量的IPv4和IPv6流监控器。

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

# 使用Cisco Catalyst Center在9800 WLC上配置AVC

在通过Cisco Catalyst Center在Cisco Catalyst 9800无线局域网控制器(WLC)上配置应用可视性与可 控性(AVC)之前,必须验证WLC和Cisco Catalyst Center之间的遥测通信是否已成功建立。确保 WLC在Cisco Catalyst Center接口内显示为受管状态,并且其运行状况正在主动更新。此外,为了 有效监控运行状态,必须将WLC和接入点(AP)正确分配到Cisco Catalyst Center中各自的站点。

9800WL Teleme	C#show telemetry etry connections	connection	all				
Index	Peer Address	F	Port	VRF	Source Address	State	State Description
170	10.78.8.84	2	25103	0	10.105.193.156	Active	Connection up

```
9800 WLC上的遥测连接验证
```



Cisco Catalyst Center上WLC和AP的运行状态

第1步:将Cisco Catalyst Center配置为NetFlow收集器并在全局设置中启用无线遥测。导航到设计 >网络设置>遥测,然后启用所需的配置(如图所示)。

≡ -listo	Catalyst Center				Design / Network Settings						
Servers	Device Credentials	IP Address Pools	Wireless	Telemetry	Security and Trust						
Q Find Hier	rarchy 🖓	Configure Syslog, assigned to a site	Traps and Ne or provisione	tFlow properties d.	for your devices. The system will deploy these settings when devices are						
V 🛛 Global		Catalyst Center is metrics gathered	your default s	SNMP collector. I ency with which t	t polls network devices to gather telemetry data. View details on the bev are collected.						
> 🎝 BGL	TAC	<ul> <li>Application</li> <li>Enable Netflow Ap by default upon no</li> </ul>	<ul> <li>Application Visibility</li> <li>Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR)</li> <li>by default upon network device site assignment <sup>①</sup></li> </ul>								
		Enable by def     Choose the destin     Use Catalyst     Use Cisco Tel	<ul> <li>Enable by default on supported wired access devices</li> <li>Choose the destination collector for Netflow records sent from network devices.</li> <li>Use Catalyst Center as the Netflow Collector</li> <li>Use Cisco Telemetry Broker (CTB) or UDP director</li> </ul>								
		<ul> <li>Wired Endp The primary funct network. Traffic re address). Other fe Access, and Assu</li> </ul>	boint Data ( ion of this fea acceived from e atures, such a rance, depend	Collection ture is to track th indpoints is used as IEEE 802.1X, v d on this identity	e presence, location, and movement of wired endpoints in the to extract and store their identity information (MAC address and IP veb authentication, Cisco Security Groups (formerly TrustSec), SD- information to operate properly.						
		Wired Endpoint Da	ata Collection	enables Device 1	fracking policies on devices assigned to the Access role in Inventory.						
		O Enable Cataly	st Center Wire	ed Endpoint Data	Collection At This Site						
		<ul> <li>Disable Cataly</li> </ul>	yst Center Wir	red Endpoint Dat	a Collection At This Site 🕖						
		<ul> <li>Wireless Control</li> <li>Enables Streaming</li> <li>access points and</li> </ul>	<ul> <li>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.</li> </ul>								
		Senable Wirele	ss Telemetry	]							

无线遥测和AVC配置

第2步:在所需的9800 WLC上启用应用遥测,以推送9800 WLC上的AVC配置。为此,请导航到调 配>网络设备>资产。 选择要在其上激活应用遥测的9800 WLC,然后导航到操作>遥测>启用应用遥 测。

≡ "lindu: Catalyst Center					Provision / Invent	ory			
<sup>⊘</sup> Global				All Routers	Switches Wireless C	Contro	Ilers Access Points Sensors		
DEVICE WORK ITEMS	Devic	Devices (5) Focus: Inventory V							
Unreachable	Q	Q Click here to apply basic or advanced filters or view recently applied filters							
Unassigned	1 Selec	ted Ta	g 🕀 Add Device 🥖 Edit Device	Delete Device	Actions A (i)				
Untagged		Tags	Device Name 🔺	IP Address	Inventory	>	EoX Status 🕕 Manageability 🕕		
Failed Provision					Software Image	>			
Non Compliant		0	9800WLC.cisco.com B	10.105.193.156	Provision	>	A Not Scanned 🛛 🔮 Managed		
Outdated Software Image	0	0	CW9164I-ROW1	10.105.193.152	Telemetry	>	Enable Application Telemetry		
No Golden Image	-	0		10.105.00.25	Device Replacement	>	Disable Application Telemetry		
Failed Image Prechecks		<u> </u>	GW91641-ROW2	10.105.60.35	Compliance	>	Unders Television Couloss		
Under Maintenance	< 🗆	0	SDA_WLC.cisco.com	10.106.38.185	More	>	update felemetry Settings		
<ul> <li>Security Advisories</li> </ul>									

在9800 WLC上启用应用遥测

### 本地:在本地策略配置文件(集中交换)中启用AVC

### Flex/Fabric:在灵活策略配置文件(本地交换)或基于交换矩阵的SSID中启用AVC。

Enable Application Telemetry								
You have chosen to enable Netflow with application telemetry on 1 wireless controllers. By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry. To override this default behavior, tag specific WLAN profile names with keyword * lan*. Once specific WLANs are tagged, only those WLANs will be monitored. For each wireless controller, select the AP modes where you would like to enable application telemetry. • For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.								
<ul> <li>For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).</li> <li>Leabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.</li> </ul>								
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.								
Cocal Flex/Fabric								
Include Guest SSIDs  Telemetry Source: NetFlow								
Note: Devices require Catalyst Center Advantage license for this feature to be enabled.								

Cisco Catalyst Center上的部署模式选择

### 第4步:它会启动一个任务来激活AVC设置,并且相应的配置将应用于9800 WLC。导航到活动>审 核日志可以查看状态。

Jul 18,	118, 2024 09:22 PM 🥰										
3:37p											
I					• • • • • • • • • • • • • • • • • • •	·····					
	8/1 9/1	10/1	11/1	12/1	1/1	2/1	3/1	4/1	5/1		
<b>∀</b> Filt	er										
Time	2	Description									
/ Toda	у										
	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 VIan1 transport udp 6007 export-protocol ipfix option vrf-table timeout 300 option ssid-table timeout 300 option application-table tim									
	Jul 18, 2024 20:36 PM (IST)	Request received to enable telemetry on device(s) : [10.105.193.156]									

在9800 WLC上启用遥测后审核日志

Cisco Catalyst Center将部署流导出器和流监控器配置,包括指定的端口和其他设置,并在选定的 模式策略配置文件中激活它们,如下所示: Configure Cisco Catalyst Center as Flow Exporter:

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

Configure 9800 WLC as Local Exporter

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

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

```
9800-Cl-VM(config)#flow monitor avc_ipv4_assurance
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
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)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 assurance
9800-C1-VM(config-flow-monitor)#exit
9800-Cl-VM(config)#flow monitor avc_ipv6_assurance
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
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)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv6 assurance
9800-C1-VM(config-flow-monitor)#exit
9800-Cl-VM(config)#flow monitor avc_ipv4_assurance_rtp
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-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-Cl-VM(config)#flow monitor avc_ipv6_assurance_rtp
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance-rtp
9800-Cl-VM(config-flow-monitor)#exit
```

Mapping the IPv4 and IPv6 Flow Minitor in Policy Profile 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 avc\_ipv4\_assurance input 9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc\_ipv4\_assurance output 9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc\_ipv4\_assurance\_rtp input 9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc\_ipv4\_assurance\_rtp input 9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc\_ipv4\_assurance\_rtp output 9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc\_ipv6\_assurance input 9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc\_ipv6\_assurance\_rtp output 9800-Cl-VM

9800-Cl-VM(config-wireless-policy)#exit

# AVC验证

### 在9800上

当9800 WLC用作流导出器时,可以观察到以下AVC统计信息:

·跨所有SSID连接的客户端的应用可视性。

·每个客户端的单个应用程序使用情况。

·每个SSID上的特定应用使用情况。



注意:您可以选择按方向过滤数据,包括传入(入口)和传出(出口)流量以及按时间间隔过滤数 据,可以选择最长48小时的时间范围。

通过GUI

导航到监控>服务>应用可视性。



连接到AVC\_testing SSID的用户对入口和出口流量的应用可视性

# 要查看每个客户端的应用可视性统计信息,可以单击"Clients"选项卡,选择特定的客户端,然后单击View Application Details。



特定客户端的应用可视性-1

Application Name	Y Avg Packet Size	▼ Packet Count	▼ Usage(%)	▼ Usage	▼ Sent	T Received	T
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	
limnr	81	159	1	12.6KB	6.9KB	5.7KB	
R ← 1 2 ► H 10 ¥						1 - 10	of 17 items

- Back to Client's

特定客户端的应用可视性-2

#### 通过CLI

验证AVC状态

9800WLC#show avc status wlan AVC\_testing WLAN profile name: AVC\_testing

-----

AVC configuration complete: YES

### 来自NetFlow的统计数据(FNF缓存)

9800WLC#show flow monitor \$Flow\_Monitor\_Name cache format table

9800WLC#show flo Cache type: Cache size: Current entrie High Watermark	ow monitor wirele es: <:	ss-avc-basic ca Norm 2000 1 1	iche format tabl al (Platform ca 00 02 02	e iche)				
Flows added: Flows aged:		1	02 0					
IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	FLOW DIRN	WIRELESS SSID	IP PROT	APP NAME	bytes long
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		prot icmp	148
10.105.193.59	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120

在9800 CLI上验证AVC

要单独检查每个WLAN及其连接的客户端的排名靠前的应用使用情况,请执行以下操作:

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

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

### 验证发送到控制平面(CP)的FNFv9数据包计数和解码状态

9800WLC#show platform software wlavc status decoder

9800WLC#show platform software wlavc status decoder AVC FNFv9 Decoder status:								
Pkt Count	Pkt Decoded	Pkt Errors	Data Records	Last decoded time	Last error time			
25703	25703	0	132480	07/20/2024 14:10:46	01/01/1970 05:30:00			

FNFv9数据包记录

您还可以直接检查nbar统计信息。

9800WLC#show ip nbar protocol-discovery

在Fabric和Flex模式下,您可以通过以下方式从AP获取NBAR统计信息:

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



注意:在外来锚点设置中,锚点WLC充当客户端的第3层在线状态,而外来WLC在第2层运行。由于 应用可视性与可控性(AVC)在第3层运行,因此只能在锚点WLC上查看相关数据。

在DNAC上

从9800 WLC捕获的数据包中,我们可以验证它是否持续向Cisco Catalyst Center发送有关应用和网络流量的数据。

ip.addr ==	10.78.8.84 and	udp.port == 6007	7					
No.	Time		Source	Destination	Protocol	Length	Info	
	72324 13.00	. 10. 303333	10.103.133.130	10.70.0.04	001	170	55140 - 0007	LCII-130
	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 13	32: 178 byte	s on wire (14	24 bits), 178 byt	es captured (1424 b	pits)			

> Ethernet II, Src:

> 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]: 000a00886698e17a00001fa700000100011800780a69c150080808080411003501242fd0daa7da00000002000000120d000309005c [Length: 136]

9800 WLC上的数据包捕获

### 要查看连接到Cisco Catalyst Center上特定WLC的客户端的应用数据,请导航到保证>控制面板>运 行状况>应用。

1	≡ "listli" Cataly	rst Center			Assurance / Dash	boards / Health	\$ Q
	Overall Network	Client Network	Services V Application	SD-Access	Al Analytics 🗸		
	SUMMARY 13 Business Relevant Applications	7.4 MB Data Usage	715.7 bps Avg Throughput	NETFLOW 1 Exporters	19.3 MB Data Usage		ThousandEyes Tests 🛈 ThousandEyes Integration Not Available 🗗
	Business Relev	ant Application Heal	th 🛈			Application Usage	
	6 TOTAL APPLICATIONS			<ul> <li>Pear:</li> <li>Fair:</li> <li>Geod:</li> </ul>	0.0% ).0% 100.0%	(	3 MB TOTAL USAGE

Cisco Catalyst Center上的AVC监控

### 我们可以跟踪客户最常使用的应用,并确定最高数据消费者,如此处所示。

≡ diulu Catalyst Center	Assurance / Dashboards / Health
Overall Network Client Network Services V Applications	s SD-Access Al Analytics V
Top Applications by Throughput LATEST TREND unknown 26.2Kbps dns 19Kbps ipv6-icmp 16.3Kbps http 7.3Kbps icmp 4.3Kbps	Top Endpoints by Throughput LATEST DESKTOP-QSCE4P3 19Kbps

排名靠前的应用和排名靠前的带宽用户统计信息

您可以为特定SSID设置过滤器,从而监控与该SSID关联的客户端的整体吞吐量和应用使用情况。

通过此功能,您可以确定网络中排名靠前的应用和消耗带宽最高的用户。

此外,您还可以使用时间过滤器功能检查此数据以前的时间段,提供有关网络使用情况的历史见解 。



Time Filter,用于显示AVC统计信息

o



## 在外部NetFlow收集器上

示例1: Cisco Prime作为Netflow收集器

当您使用Cisco Prime作为Netflow收集器收集时,您可以看到9800 WLC作为发送Netflow数据的数据源,并且NetFlow模板将根据由9800 WLC发送的数据自动创建。

从9800 WLC捕获的数据包中,我们可以验证它是否持续向Cisco Prime发送有关应用和网络流量的数据。

		٦	۲				×	C		٩		۲	2	•	₹			Œ	2	Q		• •	
in addr == 10 106 36 22 && udp port == 9991																							

in the	auur 10.100.	30.22 dd dup.port 3	1991			
No.		Time	Source	Destination	Protocol	Length Info
Г	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
	2206	30.E0.30 0E0040	10 105 100 155	10 106 26 22	UDD	270 E11E4 . 0001 Lon-220
-	07 170	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				

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

Ethernet II, Src:

> 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)

9800 WLC上的数据包捕获

₿	uluul cisco	Prime Infrastructure						O <sub>4</sub> + Applicatio	n Search		🐥 😣 62	roc	
٨	Assurance Memory States Assurance Memory States												
•	✓ Device Data Sources												
											Selected	10 / Total 1	
X Delete Enable Disable Quick Filter													
		Device Name	Data Source	▲ Type		Exporting Device		Last 5 min Flow Record Rate	Last Active Time				
		9800WLC.cisco.com	10.105.193.156	D NETFLOW	1	10.105.193.156	Ð	2	Friday, July 19 2024 at 0	4:50:1	18 AM India	Standa	

Cisco Prime Detecting 9800 WLC作为Netflow数据源

可以根据应用、服务,甚至按客户端设置过滤器,使用IP地址进行更有针对性的数据分析。



所有客户端的应用可视性

#### n Dashboard / Performance 🔺



#### 示例2:第三方NetFlow收集器

在本示例中,使用第三方NetFlow收集器[SolarWinds]来收集应用统计信息。9800 WLC采用Flexible NetFlow (FNF)传输有关应用和网络流量的综合数据,然后由SolarWinds收集。

¥	SOLARW	VINDS	MY DA	SHBOARD	S - ALER	TS & ACTIVIT	ΥΨ	REPORTS	→ SE	TTINGS	Ŧ		
0	Net	Flow A	\ppli	ications	Summar	у							
	Time Last	Time Period Flow Direction IP Version Last 1 Hours  V Ingress and Egress V IPv4 and IPv6 V											
	itor «	Top 10 INGRESS	AND EC	lications GRESS, LAST 1	HOURS, RATE						Ν	etFlow 🗸	EDIT HELP
	Flow Naviga	500.0	kbps										
	>>	400.0	kbps										
	v Alert	300.0	kbps										
	e a Flov	200.0	) kbps										
	Creat	100.0	) kbps										Ν
			0 bps										/
			2:4	0 PM	2:50 PM	3:00 8	PM	3:10 PM	4 3	3:20 PM	9	3:30 PM	3:40 PM
					2:45 PM		3:00 PM		3:15	PM		5:20 PM	
				τ.									
			A	PPLICATION	N		INGRES BYTES	is	EGRESS BYTES	GRESS INC YTES PAG		EGRESS PACKETS	PERCENT
		🕨 💼 🗹 🛞 http protocol over TLS/SSL (443)					647.7 k	bytes	11.4 Mbyt	Mbytes 2.85		6.54 k	99.47%
		) E 💼	₹ 🧐	World Wi	ide Web HTTP	(80)	19.5 kb	ytes	10.6 kbyte	es 7	4	109	0.25%
		) - E	2 4	Domain	Name Server (	53)	10.7 kb	ytes	4.5 kbytes	5 5	8	55	0.12%
		) ÷	⊻ <	ELLMNR (S	5355)		0 bytes		9.0 kbytes	s (	)	94	0.07%
		× 🔳	⊻ <	NETBIOS	Name Service	(137)	0 bytes		8.1 kbytes	s (	)	88	0.07%
		> 📖	⊻ <	NETBIOS	Datagram Ser	vice (138)	0 bytes		972 bytes	C	)	4	0.01%
		- F -	✓ 🤅	Palace-4	(9995)		618 by	tes	0 bytes	5	5	0	0.01%

Netflow在SolarWind上的应用统计

# 流量控制

流量控制是指用于管理和调节网络流量的一组功能和机制。流量管制或速率限制是无线控制器用于

控制从客户端传输的流量量的机制。监控网络流量的数据速率,并在超过预定义的速率限制时立即 采取行动。当流量超过指定速率时,速率限制会丢弃超额数据包或通过更改其Class of Service (CoS)或Differentiated Services Code Point (DSCP)值将其降级。这可以通过在9800 WLC中配置 QOS来实现,可以参阅<u>https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-</u> wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html,简要了解这些组件的工作 方式以及如何配置它们以实现不同的结果。

# 故障排除

对AVC问题进行故障排除涉及识别和解决可能影响AVC准确识别、分类和管理无线网络中的应用流 量的能力的问题。常见问题可能包括流量分类、策略实施或报告问题。以下是在Catalyst 9800 WLC上排除AVC故障时的一些步骤和注意事项:

- 验证AVC配置:确保AVC在WLC上正确配置并与正确的WLAN和配置文件关联。
- 当通过GUI设置AVC时,它将自动将端口9995分配为默认值。但是,如果您使用的是外部收集器,请验证将其配置为侦听NetFlow流量的端口。必须准确配置此端口号以匹配收集器的设置。
- 验证AP型号和部署模式支持。
- 在无线网络中实施AVC时,请参阅9800 WLC的限制。

#### 日志收集

#### WLC日志

1. 启用时间戳,使所有命令都有时间参考。

9800WLC#term exec prompt timestamp

#### 2. 查看配置

9800WLC#show tech-support wireless

3. 您可以检验avc状态和netflow统计信息。

#### 检查AVC配置状态。

9800WLC#show avc status wlan <wlan\_name>

#### 检查FNFv9数据包计数并解码被传送至控制平面(CP)的状态。

9800WLC#show platform software wlavc status decoder

检查来自NetFlow(FNF缓存)的统计信息。

9800WLC#show flow monitor <Flow\_Monitor\_Name>

检查每个wlan的前n个应用使用情况,其中n = <1-30>输入应用数量。

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

#### 检查每个客户端的前n个应用使用情况,其中n = <1-30>输入应用数量。

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

#### 检查使用特定应用连接到特定wlan的前n个客户端,其中n=<1-10>输入客户端数量。

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

#### 检查nbar统计信息。

9800WLC#show ip nbar protocol-discovery

#### 4. 将日志记录级别设置为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</pre>

!!Set logging level back to notice post troubleshooting
9800WLC#set platform software trace wireless all debug/verbose

### 5. 启用客户端MAC地址的放射性(RA)跟踪以验证AVC统计信息。 通过CLI

9800WLLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti 9800WLC#no debug wireless mac <Client\_MAC>

!!WLC generates a debug trace file with Client\_info, command to check for debug trace file generated. 9800WLC#dir bootflash: | i debug



注意:条件调试会启用调试级日志记录,从而增加生成的日志量。保持此运行状态可缩短查看日志 的时间间隔。因此,建议始终在故障排除会话结束时禁用调试。

# clear platform condition all
# undebug all

通过GUI

步骤1:导航到Troubleshooting(故障排除)> Radious Trace(放射性跟踪)。 第二步:单击Add并输入要排除故障的客户端Mac地址。您可以添加多个要跟踪的Mac地址。

第三步:准备好开始放射性示踪后,单击"开始"。启动后,调试日志记录会写入磁盘,记录与被跟 踪的MAC地址相关的任何控制平面处理。

第四步:重现要排除故障的问题时,单击Stop。

第五步:对于已调试的每个mac地址,可以通过单击Generate来生成一个日志文件,汇总与该 mac地址相关的所有日志。

第六步:选择希望经过整理的日志文件保留多长时间,然后单击Apply to Device。

步骤 7.现在,您可以通过点击文件名旁边的小图标下载文件。此文件存在于控制器的引导闪存驱动 器中,也可以通过CLI从机箱中复制出来。

下面简要介绍RA跟踪中的AVC调试

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

6. 按客户端MAC地址双向过滤的嵌入式捕获,客户端内部MAC过滤器在17.1之后可用。

在使用外部收集器时,它特别有用,因为它有助于确认WLC是否按照预期将NetFlow数据传输到目 标端口。

通过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 !! Inititiate different application traffic from user monitor capture MYCAP stop monitor capture MYCAP stop monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap

通过GUI 步骤1:导航到故障排除>数据包捕获> +Add。 第二步:定义数据包捕获的名称。最多允许8个字符。

第三步:定义过滤器(如果有)。

第四步:如果想要查看传送至系统CPU并注入数据平面的流量,请选中监控控制流量的复选框。

第五步:定义缓冲区大小。最多允许100 MB。

第六步:定义限制,可根据需要按持续时间或1至1000000秒的数据包数量来定义允许范围1至 100000的数据包。

步骤 7.从左侧列中的接口列表中选择接口,并选择箭头将其移动到右侧列。

步骤 8单击Apply to Device。

步骤 9要开始捕获,请选择Start。

步骤 10您可以让捕获运行到定义的限制。要手动停止捕获,请选择Stop。

步骤 11停止后,Export按钮变为可单击状态,其中包含用于通过HTTP或TFTP服务器、FTP服务器、本地系统硬盘或闪存将捕获文件(.pcap)下载到本地桌面的选项。

AP日志

在交换矩阵和灵活模式下

1. show tech显示所有AP配置详细信息和客户端统计信息。

2. 显示来自无线接入点的avc nbar统计信息nbar统计信息

#### 3. AVC调试

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

# 相关信息

<u>AVC配置指南</u>

<u>9800 WLC上的速率限制</u>

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。