Application Performance Monitoring

Feature History for Application Performance Monitoring

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Application Performance Monitoring

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	Application Performance Monitoring	This feature collects and exports assurance-related metrics (per application) of the flows forwarded through AP to the Cisco DNA Centre Assurance application.

Information About Application Performance Monitoring

Application Performance Monitoring feature collects and exports assurance-related metrics (per application) of the flows that are forwarded through specific interfaces of the access point to the Cisco Catalyst Center Assurance application. This feature supports two monitors—a general assurance monitor that computes quantitative metrics for TCP and UDP flows and qualitative metrics for TCP flows and a media monitor that computes qualitative and quantitative metrics for real-time protocol (RTP) flows. Voice applications such as Microsoft Teams and Session Initiation Protocol (SIP) use RTP monitors, while other applications use TCP and UDP monitor.

A flow monitor can be attached to:

- A interface that monitors all the flows from the attachment point.

- A wireless profile policy (the wireless profile policy that is associated with a WLAN or SSID) that monitors all the traffic passing through it.

Assurance performance monitoring is supported on the following platforms:

- Cisco Catalyst 9800 Series Controllers (9800-80, 9800-40, 9800-L, and 9800-CL)
- Cisco Catalyst 9100 Series APs (FlexConnect and fabric mode)
- Cisco Catalyst 9300 Series and 9400 Series switches (fabric mode)

Restrictions for Application Performance Monitoring

- Local flow exporter is not supported.
- The following commands are not supported:
  - **show avc wlan application top**
  - **show avc client top application**
- You cannot configure Application Performance Monitoring and Application Visibility and Control basic on a single policy profile. You can configure them only on two separate policy profiles.
- During CAPWAP restart, AP moves to standby mode, and the nitro engine is disabled. When CAPWAP is up and the nitro engine is enabled, an attempt is made to classify the flows. Since there is not enough information to classify the applications, they are marked as unknown. When the AP rejoins CAPWAP, client traffic gets marked or classified correctly.
- When a client roams while an application has an active-session, the specific session traffic is marked as unknown. The client has to start a new session to mark or classify the traffic correctly.

Workflow

Create a Flow Monitor

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor avc_assurance`	Creates a flow monitor.

	Command or Action	Purpose
Step 3	**description** *description* **Example:** `Device(config-flow-monitor)# description assurance monitor ID is 90`	Adds a description to the flow monitor.
Step 4	**record wireless avc** {**ipv4** | **ipv6**} **assurance** **Example:** `Device(config-flow-monitor)# record wireless avc ipv4 assurance`	Specifies the IPv4 assurance metrics for wireless.
Step 5	**exit** **Example:** `Device(config-flow-monitor)# exit`	Returns to global configuration mode.
Step 6	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor avc_assurance_rtp`	Creates a flow monitor.
Step 7	**description** *description* **Example:** `Device(config-flow-monitor)# description assurance-rtp monitor ID is 94`	Adds a description to the flow monitor.
Step 8	**record wireless avc** {**ipv4** | **ipv6**} **assurance-rtp** **Example:** `Device(config-flow-monitor)# record wireless avc ipv4 assurance-rtp`	Specifies the IPv4 assurance RTP metrics for wireless.
Step 9	**end** **Example:** `Device(config-flow-monitor)# end`	Returns to privileged EXEC mode.

Create a Wireless WLAN Profile Policy

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**wireless profile policy** *policy-name* **Example:** `Device(config)# wireless profile policy AVC_POL`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 4	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching.
Step 5	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance input`	Specifies the name of the IPv4 ingress flow monitor.
Step 6	**ipv4 flow monitor** *monitor-name* **input** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp input`	Specifies the name of the IPv4 ingress flow monitor.
Step 7	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance output`	Specifies the name of the IPv4 egress flow monitor.
Step 8	**ipv4 flow monitor** *monitor-name* **output** **Example:** `Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp output`	Specifies the name of the IPv4 egress flow monitor.
Step 9	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the policy profile.
Step 10	**end** **Example:** `Device(config-wireless-policy)# end`	Returns to privileged EXEC mode.

Create a Policy Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy mywlan_ssid`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-avc* **policy** *policy* **Example:** `Device(config-policy-tag)# wlan mywlan_ssid policy AVC_POL`	Attaches the policy tag to a WLAN.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Returns to privileged EXEC mode.

Attach the Policy Profile to an AP

Procedure

	Command or Action	Purpose
Step 1	**ap** *ap-ether-mac* **Example:** `Device(config)# ap 9412.1212.1201`	Enters AP configuration mode.
Step 2	**policy-tag** *policy-tag* **Example:** `Device(config-ap-tag)# policy-tag mywlan_ssid`	Specifies the policy tag that is to be attached to the AP.
Step 3	**end** **Example:** `Device(config-ap-tag)# end`	Returns to privileged EXEC mode.

Verify Application Performance Monitoring

Use the following commands to verify application performance monitoring configuration.

To check application performance monitoring statistics, use the following commands:

```
Device# show flow exporter statistics

Flow Exporter apm_exp:
  Packet send statistics (last cleared 4w1d ago):
    Successfully sent:         2082                  (216624 bytes)
!Packet sent count sent from controller to Cisco Cisco Catalyst Center
    Reason not given:          1099                  (114296 bytes)

  Client send statistics:
    Client: Flow Monitor avc
      Records added:           0
      Bytes added:             0


Device# show flow monitor assurance cache

Cache type:                                Normal (Platform cache)
  Cache size:                                200000
  Current entries:                                0
  High Watermark:                                 1
!Controller flow monitor cache statistics

  Flows added:                                    6
  Flows aged:                                     6
    - Active timeout      (    10 secs)           6
```

To check status of application performance monitoring, use the following command

```
Device# show avc status

VAP FNF-STATUS AVC-QOS-STATUS SD AVC-STATUS APM-STATUS
!APM-STATUS contains IPv4, IPv6 assurance and assurance-rtp monitors.

0   Disabled   Disabled       Enabled       IPV4,IPV4-RTP,IPV6,IPV6-RTP
1   Disabled   Disabled       Disabled      Disabled
2   Disabled   Disabled       Disabled      Disabled
3   Disabled   Disabled       Disabled      Disabled
4   Disabled   Disabled       Disabled      Disabled
5   Disabled   Disabled       Disabled      Disabled
6   Disabled   Disabled       Disabled      Disabled
7   Disabled   Disabled       Disabled      Disabled
8   Disabled   Disabled       Disabled      Disabled
9   Disabled   Disabled       Disabled      Disabled
10  Disabled   Disabled       Disabled      Disabled
11  Disabled   Disabled       Disabled      Disabled
12  Disabled   Disabled       Disabled      Disabled
13  Disabled   Disabled       Disabled      Disabled
14  Disabled   Disabled       Disabled      Disabled
15  Disabled   Disabled       Disabled      Disabled
```