Application Performance Monitoring

APM

Application performance monitoring features are assurance solutions that

- collect and export assurance-related metrics for each application when flows are sent through specific AP interfaces
- aggregate these metrics using Cisco Catalyst 9800 Series controllers, and
- export the aggregated data to Cisco Catalyst Center for analysis.

Supported platforms

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

Note FNFv9 flows transit through the C9800 controller before being sent to Cisco Catalyst Center.

Supported monitors

- A general assurance monitor collects quantitative metrics for TCP and UDP flows, and qualitative metrics for TCP flows.
- A media monitor computes both qualitative and quantitative metrics for real-time protocol (RTP) flows.

Voice applications, such as Microsoft Teams and SIP, use RTP monitors. Other applications use TCP and UDP monitors.

A flow monitor can be attached to

- an 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.

Restrictions

- Local flow exporter is not supported.
- These 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 each feature on separate policy profiles.
- During Control and Provisioning of Wireless Access Points (CAPWAP) restart, the 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.

Configure APM

Create a flow monitor

Configure flow monitors to collect wireless AVC assurance metrics.

Use these steps to set up flow monitors on a Cisco device for wireless assurance monitoring.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a flow monitor.

Example:

```
Device(config)# flow monitor avc_assurance
```

Step 3 Add a description to the flow monitor using the **description***description* command.

Example:

```
Device(config-flow-monitor)# description assurance monitor ID is 90
```

Step 4 Specify the IPv4 assurance metrics for wireless.

Example:

```
Device(config-flow-monitor)# record wireless avc ipv4 assurance
```

Step 5 Return to global configuration mode.

Example:

```
Device(config-flow-monitor)# exit
```

Step 6 Create a flow monitor.

Example:

```
Device(config)# flow monitor avc_assurance_rtp
```

Step 7 Add a description to the flow monitor using the **description***description* command.

Example:

```
Device(config-flow-monitor)# description assurance-rtp monitor ID is 94
```

Step 8 Specify the IPv4 assurance RTP metrics for wireless.

Example:

```
Device(config-flow-monitor)# record wireless avc ipv4 assurance-rtp
```

Step 9 Return to privileged EXEC mode.

Example:

```
Device(config-flow-monitor)# end
```

The flow monitors for wireless AVC assurance and assurance RTP metrics are successfully created on the device.

Create a wireless WLAN profile policy

Define and configure a WLAN policy profile using CLI commands for wireless network management.

Create a WLAN policy profile when you need to control traffic handling, enable advanced monitoring, or specify flow monitors for your wireless network on Cisco devices.

- Ingress flow monitors track incoming (received) traffic and help pinpoint what enters your wireless network.
- Egress flow monitors monitor outgoing (sent) traffic. This allows you to know what leaves your network.
- Multiple monitors (such as `avc_assurance` and `avc_assurance_rtp`) can be assigned to analyze different kinds of traffic or applications (for example, general application traffic and real-time media).

Before you begin

Know the profile name and flow monitor names you plan to use.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy policy-name
```

Step 3 Disable the policy profile.

Example:

```
Device(config-wireless-policy)# shutdown
```

Step 4 Disable central switching.

Example:

```
Device(config-wireless-policy)# no central switching
```

Step 5 Specify the name of the IPv4 ingress flow monitor for general application traffic using the **ipv4 flow monitor** *monitor-name***input** command.

Example:

```
Device(config-wireless-policy)# ipv4 flow monitor avc_assurance input
```

Step 6 Specify the name of the IPv4 ingress flow monitor for real-time media traffic (RTP).

Example:

```
Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp input
```

Step 7 Specify the name of the IPv4 egress flow monitor for general application traffic.

Example:

```
Device(config-wireless-policy)# ipv4 flow monitor avc_assurance output
```

Step 8 Specify the name of the IPv4 egress flow monitor for real-time media traffic (RTP).

Example:

```
Device(config-wireless-policy)# ipv4 flow monitor avc_assurance_rtp output
```

Step 9 Enable the policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 10 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The WLAN policy profile is created and configured with the specified settings. Traffic monitoring and switching behavior are now defined by the profile.

Create a policy tag

Define and attach a policy tag to a WLAN using the CLI.

Policy tags associate WLANs with specific policies on a Cisco wireless controller. When you create a policy tag and link it to a WLAN, you can apply policy profiles.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a policy tag and enter policy tag configuration mode.

Example:

```
Device(config-policy-tag)# wireless tag policy policy-tag-name
```

Step 3 Attach the policy tag to a WLAN.

Example:

```
Device(config-policy-tag)# wlan wlan-avc  policy policy
```

Step 4 Return to privileged EXEC mode.

Example:

```
Device(config-policy-tag)# end
```

The policy tag is created and associated with the specified WLAN and policy.

Attach the policy profile to an AP

Assign a policy profile to a specific AP to enforce wireless network policies.

Use this procedure when you need to apply or change the policy profile for an AP in your wireless network using CLI commands.

Procedure

Step 1 Enter AP configuration mode.

Example:

```
Device(config)# ap ap-ether-mac
```

Example:

```
Device(config)# ap 9412.1212.1201
```

Step 2 Specify the policy tag that is to be attached to the AP.

Example:

```
Device(config-ap-tag)# policy-tag policy-tag
```

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config-ap-tag)# end
```

The AP is now configured with the specified policy profile.

Verify APM

Use the following commands to verify application performance monitoring configuration.

To check application performance monitoring statistics, use these 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 these 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
```