AVC Notes, Limitations, and Caveats

Revised: November 21, 2013, OL-30581-01

This section includes the following topics:

Notes

Hidden Fields

Two hidden fields (first/last timestamp) are implicitly added to each record, even when these fields are not explicitly configured. When the fields are not explicitly configured, the fields are not exported and are not displayed using **show** commands. Because of these two hidden fields, the effective maximum number of supported fields is the upper limit defined for the release, minus two.

Cache Size Recommendation

The cache size to configure is determined by the traffic profile. The cache should be large enough to store all traffic records, but not excessively large. A warning message may appear if the configured cache exceeds 25% of DRAM. For troubleshooting information, see Memory/Cache Warning, page 5-3.

Limitations

ISSU Limitations

Cisco In-Service Software Upgrade (ISSU) provides transparent router software upgrade or downgrade. ISSU enables bug fixes, deployment of new features, and even complete upgrade of the Cisco IOS software image. For more information, see:
http://www.cisco.com/en/US/products/ps7149/products_ios_protocol_group_home.html

This section describes ISSU limitations for AVC.

Removing Aliases before Downgrading from Cisco IOS 15.4(1)T / Cisco IOS XE 3.10 or Later

Cisco IOS Platforms	Cisco IOS XE Platforms
Applicable to release 15.4(1)T and later	Applicable to release 3.10S and later

In Cisco IOS XE release 3.10S and Cisco IOS release 15.4(1)T, aliases were introduced to the AVC monitor configuration syntax. Using the **all** alias simplifies configuration statements and optimizes performance. (See CLI Field Aliases, page 4-31.)

Before downgrading from one of these releases, or a later release, to a version that does not support aliases, remove the aliases and manually expand the statements to specify each of the required fields explicitly. Failure to remove aliases before downgrading will result in undesired behavior, including possible system crash.

Downgrading to an IOS XE Version that Does Not Support More than 32 Fields

Cisco IOS Platforms	Cisco IOS XE Platforms
Not applicable	Applicable to release 3.10S and later

AVC for Cisco IOS XE 3.10 introduced support for configuring records containing 40 fields. If a record configuration includes more than 32 fields, downgrading to an IOS XE version that does not support more than 32 fields is not supported.

Before downgrading from Cisco IOS XE 3.10 or later, to a version, such as IOS XE 3.9, that does not support more than 32 fields, remove any record configuration of more than 32 fields.

Note Some record configurations include hidden fields. Hidden fields count toward the total supported number of fields. See Hidden Fields, page 6-1.

Note Upgrading from a version that does not support more than 32 fields to a version that does support more than 32 fields is supported.

Error Caused By Using a Performance Monitor With Default Cache Size

Cisco IOS Platforms	Cisco IOS XE Platforms
Not applicable	Applicable to release 3.11S and later

Symptom

Using a performance monitor when the cache size is set to its default value may cause an error during the Cisco In-Service Software Upgrade (ISSU) process. An error in the console log will indicate a failure to update the monitor cache size.

Conditions

1. Applicable to all Cisco IOS XE platforms.
2. Occurs when running ISSU, which provides transparent router software upgrade or downgrade.
3. May occur when doing either one of the following:
   - Upgrading from Cisco IOS XE 3.10 or earlier to IOS XE 3.11 or later version
   - Downgrading from IOS XE 3.11 (or later) to a version earlier than 3.11

Workaround

A preventive workaround and typical use case is to configure the cache size manually rather than using the default.

If using the default cache size, use the following workaround to avoid the error:

1. Remove the service policy.
2. Run the system upgrade or downgrade.
3. Re-attach the service policy.

Performance Monitor Limitations

Cisco IOS Platforms	Cisco IOS XE Platforms
Applicable	This limitation is not applicable.

Performance monitors operate in different modes, depending on the metrics that they are configured to collect. For maximum performance, any of the following metrics may be used. Including other metrics may impact performance.

- Match Fields
  - match application name [account-on-resolution]
  - match connection client ipv4 (or ipv6) address
  - match connection server ipv4 (or ipv6) address
  - match connection client transport port
  - match connection server transport port
  - match ipv4 protocol

  - match policy qos index
  - match routing vrf input
- Collect Fields
  - collect application http host
  - collect application http uri statistics
  - collect connection all
  - collect datalink mac source address
  - collect interface [input/output]
  - collect ip dscp
  - collect ipv4 ttl (or ipv6 hop-limit)
  - collect policy qos classification hierarchy
  - collect policy qos queue [drops/index]
  - collect timestamp sys-uptime first
  - collect timestamp sys-uptime last

Example of Record Including Metrics That Do Not Reduce Performance

```
flow record type performance-monitor Conversation-Traffic-Stats-IPv4(6)
    match ipv4 protocol
    match application name account-on-resolution
    match connection client ipv4 (or ipv6) address
    match connection server ipv4 (or ipv6) address
    match connection server transport port
    match routing vrf input
    collect interface input
    collect interface output
    collect ipv4 dscp
    collect connection client counter packets long
    collect connection server counter packets long
    collect connection client counter bytes long
    collect connection server counter bytes long
    collect connection new-connections
    collect connection sum-duration
    collect ipv4 ttl   (or ipv6 hop-limit)
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

flow record type performance-monitor Application-Response-Time-IPv4(6)
    match ipv4 protocol
    match application name account-on-resolution
    match connection client ipv4 (or ipv6) address
    match connection server ipv4 (or ipv6) address
    match connection server transport port
    match routing vrf input
    collect interface input
    collect interface output
    collect ipv4 dscp
    collect connection client counter packets long
    collect connection server counter packets long
    collect connection client counter bytes long
    collect connection server counter bytes long
    collect connection new-connections
    collect connection sum-duration
    collect ipv4 ttl   (or ipv6 hop-limit)
    collect connection delay application sum
```

```
    collect connection delay application max
    collect connection delay response to-server sum
    collect connection delay response client-to-server sum
    collect connection delay network client-to-server sum
    collect connection delay network to-client sum
    collect connection delay network to-server sum
    collect connection transaction duration sum
    collect connection transaction counter complete
    collect connection client counter packets retransmitted
    collect connection server counter responses
    collect connection delay response to-server histogram late
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

flow record type performance-monitor URL-IPv4(6)
    match ipv4 protocol
    match application name account-on-resolution
    match connection client ipv4 (or ipv6) address
    match connection server ipv4 (or ipv6) address
    match connection server transport port
    match routing vrf input
    collect interface input
    collect interface output
    collect ipv4 dscp
    collect connection client counter packets long
    collect connection server counter packets long
    collect connection client counter bytes long
    collect connection server counter bytes long
    collect connection new-connections
    collect connection sum-duration
    collect ipv4 ttl   (or ipv6 hop-limit)
    collect connection delay application sum
    collect connection delay application max
    collect connection delay response to-server sum
    collect connection delay response client-to-server sum
    collect connection delay network client-to-server sum
    collect connection delay network to-client sum
    collect connection delay network to-server sum
    collect connection transaction duration sum
    collect connection transaction counter complete
    collect connection client counter packets retransmitted
    collect connection server counter responses
    collect connection delay response to-server histogram late
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
    collect application http uri statistics
    collect application http host
```

Caveats

Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

To view caveats related to the use of AVC, see the release notes for your platform.

If you have an account on Cisco.com, you can also use the Bug Search tool to find select caveats of any severity. See:
https://tools.cisco.com/bugsearch/search

(If the defect that you have requested is not displayed, it may be that the defect number does not exist, the defect does not have a customer-visible description, or the defect is for internal Cisco use.)

Derived Fields Caveat

Cisco IOS Platforms	Cisco IOS XE Platforms
Not applicable	Releases prior to 3.10S

Caveat **CSCue53207**, described in the *Cisco ASR 1000 Series Aggregation Services Routers Release Notes*, describes a bug in some earlier releases, in which a record that contains certain derived fields (listed below) may be punted incorrectly to the route processor (RP) and lost. When using any of the **connection delay** fields listed in the Workaround description below, downgrading to a release that contains this bug is not recommended.

The following is a description of the bug:

Symptom

A record that contains certain derived fields (listed below) may be punted incorrectly to the route processor (RP) and lost.

Conditions

Records can collect "derived" fields; calculating derived fields is dependent on the values of other fields. The fields listed below are incorrectly defined as derived and dependent on other fields. When a record contains one of these fields and does not include its dependent fields, the record is punted to the route processor (RP) to complete the record processing. Punting these records might lead to record loss.

Workaround

When configuring a monitor to collect one of the fields listed below, collect each of the dependent fields also. The list indicates the dependencies:

1. “connection delay application sum” is dependent on:
   - connection delay response to-server sum
   - connection delay network to-server sum
   - connection server response sum
2. “connection delay application min” is dependent on:
   - connection delay response to-server min
   - connection delay network to-server sum
3. “connection delay application max” is dependent on:
   - connection delay response to-server max
   - connection delay network to-server sum
4. “connection delay response client-to-server sum” is dependent on:
   - connection delay response to-server sum
   - connection delay network to-server sum
   - connection server response sum

5. “connection delay response client-to-server min” is dependent on:

   connection delay response to-server min

   connection delay network to-server sum

   connection server response sum

   connection delay response to-server sum

   connection delay network to-server min

6. “connection delay response client-to-server max” is dependent on:

   connection delay response to-server max

   connection delay network to-server sum

   connection server response sum

   connection delay response to-server sum

   connection delay network to-server max

Oversubscribed FNF Monitor Caveat

Cisco IOS Platforms	Cisco IOS XE Platforms
Not applicable	Releases prior to 3.10S

Caveat **CSCud15949**, described in the *Cisco ASR 1000 Series Aggregation Services Routers Release Notes*, describes a bug affecting releases prior to IOS XE 3.10S. For these releases, you can attach up to two policies per interface and direction. The total number of monitors included in the two policies should not exceed 10. In calculating the total number of monitors:

- Each policy is considered to include at least five monitors, even if fewer than five monitors are configured for the policy.
- An FNF static monitor is counted as 1 monitor.

The bug may occur (on the affected releases) if these limits are exceeded on any interface, either for ingress or egress traffic on the interface. This condition is called “oversubscribed.”

When a system is oversubscribed, downgrading to a release that contains this bug is not recommended. For oversubscribed systems, Cisco In-Service Software Upgrade (ISSU) does not enable downgrading to a release prior to 3.10S.

The following is a description of the bug:

Symptom

The CPP traceback notifying monitor cannot be reserved.

Conditions

The issue was seen when the MMA policy, mediatrace policy, and one FNF monitor were attached to an interface.

Workaround

Ensure that the total number of monitors does not exceed the limits outlined above, in the description of this bug.

Use Synchronized Cache for Optimized Monitors

Cisco IOS Platforms	Cisco IOS XE Platforms
Release 15.4(1)T	Not applicable

Caveat **CSCuh87789** describes a limitation affecting routers running Cisco IOS 15.4(1)T. On affected releases, use "synchronized cache" when configuring optimized monitors. Do not use, for example, the "normal cache" option. Synchronized cache is the default cache mode for the router.

Using a cache option other than synchronized may result in failure to export certain metrics, resulting in incomplete records.

Network Time Mismatch Between IOS and QFP Causing Dropped Records

Cisco IOS Platforms	Cisco IOS XE Platforms
Release 15.4(1)T	Not applicable

Caveat **CSCul27478** describes a problem that may occur when there is a clock mismatch between Cisco IOS and the router's QuantumFlow Processor (QFP). When this occurs, records punted from the QFP to IOS may be identified as late records, and incorrectly dropped instead of being exported.

The workaround for this issue is to configure an NTP server that allows the IOS clock to be synchronized with network time.