Configuring Sup-region TCAM Monitoring

This chapter contains the following sections:

- Information About Sup-region TCAM Monitoring, on page 1
- Licensing Requirements for Sup-region TCAM Monitoring, on page 2
- Guidelines and Limitations for Sup-region TCAM Monitoring, on page 2
- Default Setting for Sup-region TCAM Monitoring, on page 2
- Configuring Sup-region TCAM Monitoring, on page 3
- Verifying Sup-region TCAM Monitoring, on page 6
- Configuration Examples for Sup-region TCAM Monitoring, on page 6
- Additional References for Sup-region TCAM Monitoring, on page 6
- Feature History for Sup-region TCAM Monitoring, on page 7

Information About Sup-region TCAM Monitoring

The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting and correction of sup-region TCAM entry corruption. This monitoring mechanism provides the following functionalities:

- Detection—Checks for corruptions in any sup-region TCAM entry and reports it.
- Correction—Provides corrective mechanism to rewrite the corrupted sup-region TCAM entry.

On-demand Detection of Corrupted Sup-region TCAM Entries

Use the **hardware sup-tcam monitoring trigger-detection** command to verify if any sup-region TCAM entry is corrupted. This command triggers a verification iteration that involves reading each sup-region TCAM entry and comparing this TCAM entry data with the stored content.

Periodic Detection of Corrupted Sup-region TCAM Entries

By default, the periodic sup-region TCAM entry corruption detection mechanism is disabled. Use the **hardware sup-tcam monitoring enable** command to enable periodic sup-region TCAM entry corruption detection. By default, the periodic corruption detection mechanism is set to run once every 1440 minutes or 1 day.

A syslog is generated if any sup-region TCAM entry is found to be corrupt. This syslog entry has details about the TCAM entry index, ASIC and slot number.

In-Service Software Upgrades and In-Service Software Downgrades

The sup-region TCAM entry monitoring mechanism tracks the content of the programmed TCAM entry by storing the TCAM entry content in the Persistent Storage Service (PSS). After a non-disruptive In-Service Software Upgrade (ISSU), this content is restored for verification. Before an ISSU is done, all configurations will be stored in the PSS. Statistics are not stored in the PSS.

You cannot restore a sup-region TCAM entry after a non-disruptive ISSU from a Cisco NX-OS version on which sup-region TCAM monitoring is not supported to a Cisco NX-OS version on which sup-region TCAM monitoring is supported. During such a scenario, syslogs are not generated for any corrupted sup-region TCAM entries and all commands related to sup-region TCAM monitoring will be disabled. You have to then reload the switch to trigger sup-region TCAM monitoring.

The Sup-region TCAM Monitoring feature does not support In-Service Software Downgrade (ISSD). Disable the Sup-region TCAM Monitoring feature before performing an ISSD.

Licensing Requirements for Sup-region TCAM Monitoring

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	Sup-region TCAM Monitoring requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the License and Copyright Information for Cisco NX-OS Software.

Guidelines and Limitations for Sup-region TCAM Monitoring

- The sup-region TCAM entry at 3844 is not verified during detection of corrupted sup-region TCAM entries.
- Reload the switch to trigger sup-region TCAM monitoring after a non-disruptive ISSU from a Cisco NX-OS version on which sup-region TCAM Monitoring is not supported to a Cisco NX-OS version on which sup-region TCAM Monitoring is supported.
- ISSD is not supported.

Default Setting for Sup-region TCAM Monitoring

Parameter	Default
Sup-region TCAM Monitoring	Disabled

Configuring Sup-region TCAM Monitoring

Configuring On-Demand Detection of Corrupted Sup-region TCAM Entries

Procedure

Step 1 Trigger a verification iteration that involves reading each sup-region TCAM entry and comparing this TCAM entry data with the stored content:

switch# **hardware sup-tcam monitoring trigger-detection**

Note A syslog is generated if there is a mismatch.

Step 2 (Optional) Display details about sup-region TCAM monitoring:

switch# **show platform afm info sup-tcam monitoring info**

Running Configuration

This example shows how to enable on-demand detection of corrupted sup-region TCAM entries, followed by a verification command that displays the sup-region TCAM monitoring details.

```
hardware sup-tcam monitoring trigger-detection
.
.
.
switch# show platform afm info sup-tcam monitoring info
SUP TCAM Monitoring Info
========================
Periodic Monitoring Status      : Disabled
Timer expiry                    : 0 minutes
Number of iterations run        : 0
Last iteration run at           : --
SUP TCAM corruption detected    : NO
Feasibility                     : Feasible
DB Restore status               : Restored
```

Configuring Periodic Detection of Corrupted Sup-region TCAM Entries

Procedure

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Required: Enable a continuous periodic detection of corrupted sup-region TCAM entries:

switch(config)# **[no] hardware sup-tcam monitoring enable**

Note By default, the periodic corruption detection mechanism is set to run once every 1440 minutes or 1 day.

Step 3 (Optional) Change the periodic corruption detection mechanism timer value:

switch(config)# **hardware sup-tcam monitoring timer-expiry** *timeout-in-minutes*

Note The range for the timer is from 5 to 2880 minutes (2 days).

Step 4 (Optional) Display details about sup-region TCAM monitoring:

switch# **show platform afm info sup-tcam monitoring info**

Running Configuration

This example shows how to configure periodic detection of corrupted sup-region TCAM entries, followed by a verification command that displays the sup-region TCAM monitoring details. Replace the placeholder with relevant values for your setup.

```
configure terminal

  hardware sup-tcam monitoring enable

  hardware sup-tcam monitoring timer-expiry <1500>
.
.
.
switch# show platform afm info sup-tcam monitoring info
SUP TCAM Monitoring Info
========================
Periodic Monitoring Status         : Enabled
Timer expiry                       : 1500 minutes
Number of iterations run           : 1
Last iteration run at              : Mon Aug 22 15:23:28 2016

SUP TCAM corruption detected       : NO
Feasibility                        : Feasible
DB Restore status                  : Not restored
```

Correcting the Corrupted Sup-region TCAM Entries

Procedure

Step 1 Rewrite a corrupted sup-region TCAM entry content with the stored content:

switch# **hardware sup-tcam correction asic** {*ASIC-ID* | **all**} **entry** {*TCAM-INDEX* | **all**}

Step 2 (Optional) Display write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload:

switch# **show platform afm info tcam access stats** [*ASIC-ID*]

Running Configuration

This example shows how to correct a corrupted sup-region TCAM entry, followed by verification commands that display the write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload. Replace the placeholders with relevant values for your setup.

```
hardware sup-tcam correction asic <2> entry <5>
.
.
.
switch# show platform afm info tcam access stats <2>
*NA - Not Available
Slot/Asic       ASIC ID TCAM Index      Writes  Clears  Corrupt Last Operation  Timestamp
=============================================================================================
0/2             2       4               1       2       NA      Clear   Tue Aug 16 06:43:12
 2016
0/2             2       5               1       2       NA      Clear   Tue Aug 16 06:43:12
 2016
0/2             2       122             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       123             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       124             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       125             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       126             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       127             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       128             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       129             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       130             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       131             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       132             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       133             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       134             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       135             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       136             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       137             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       138             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
0/2             2       139             1       1       NA      Write   Tue Aug 16 07:10:33
 2016
```

Verifying Sup-region TCAM Monitoring

To display sup-region TCAM monitoring information, perform one of the following tasks:

Command	Purpose
show platform afm info sup-tcam monitoring info	Display details about sup-region TCAM monitoring.
show platform afm info tcam access stats [*ASIC-ID*]	Display write access statistics per TCAM entry per ASIC per slot, along with the number of writes, clears and timestamps of the writes and clears since the previous switch reload.

Configuration Examples for Sup-region TCAM Monitoring

This section provides configuration examples for sup-region TCAM Monitoring.

Configuring On-Demand Detection of Corrupted Sup-region TCAM Entries

This example shows how to perform an on-demand detection of corrupted sup-region TCAM entries:

```
hardware sup-tcam monitoring trigger-detection
```

Configuring Periodic Detection of Corrupted Sup-region TCAM Entries

This example shows how to configure periodic detection of corrupted sup-region TCAM entries:

```
configure terminal
  hardware sup-tcam monitoring enable
  hardware sup-tcam monitoring timer-expiry 1500
```

Correcting the Corrupted Sup-region TCAM Entries

This example shows how to correct the corrupted sup-region TCAM entries:

```
hardware sup-tcam correction asic 2 entry 2172
```

Additional References for Sup-region TCAM Monitoring

This section describes additional information related to implementing Sup-region TCAM Monitoring.

Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	

Feature History for Sup-region TCAM Monitoring

This table lists the release history for this feature.

Table 1: Feature History for Sup-region TCAM Monitoring

Feature Name	Release	Feature Information
Sup-region TCAM Monitoring	Cisco NX-OS Release 7.1(4)N1(1)	The Sup-region Ternary Content-Addressable Memory (TCAM) Monitoring feature is a monitoring mechanism that enables detection, reporting and correction of sup- region TCAM entry corruption.