Release Notes for Cisco Service Control Operating System, Release 5.1.0

First Published: February 18, 2015

Note This document supports the 5.1.0 release of the Cisco Service Control Operation System (Cisco SCOS).

The release notes for the Cisco SCOS describe the functional enhancements and fixes provided in the Cisco SCOS Release 5.1.x. These release notes are updated as needed.

For a list of the open caveats that are applicable to Cisco SCOS Release 5.1.0, see the “Open Caveats for SCE 10000 Platform in Cisco SCOS Release 5.1.0” section on page 5. The caveats are applicable only to the Cisco SCE 10000 and Cisco vSCE platforms.

Contents

- Introduction, page 2
- Limitations and Restrictions, page 2
- Cisco Service Control Operating System Release 5.1.0, page 3
Introduction

Cisco SCOS Release 5.1.0 for Cisco SCE platforms contains new features, as well as fixes for issues that were identified during internal testing and customer interaction.

This document outlines the functional enhancements and resolved issues delivered in Cisco SCOS Release 5.1.0. It assumes that the reader has substantial knowledge of the Cisco Service Control solution. For more information Cisco SCE products and features, see the Cisco SCE documentation.

To access the new Cisco Service Control online documentation site, do the following:
2. From the Products list, select Service Exchange > Cisco Service Control > Cisco Service Control Product.

Limitations and Restrictions

Port Scan on Cisco SCE

When you perform a port scan operation on the Cisco SCE platform management port, the platform may experience a reboot. This reboot occurs because of scheduling optimization for detecting failover conditions during periods of less than one second in a configuration involving two cascaded Cisco SCE platforms. We recommend the following:

- Use IP access lists to eliminate port scans that take place because of actual attacks.
- If the system administrator must perform a port scan operation as part of the security check, we recommend that you disable the Cisco SCE watchdog only for the period during which the port scan is performed.

To disable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset disabled
SCE(config)#> interface linecard 0
SCE(config-if)#> no watchdog
```

- To re-enable the Cisco SCE watchdog, use the following root-level CLI commands:

```
SCE#> configure
SCE(config)#> watchdog software-reset enabled
SCE(config)#> interface linecard 0
SCE(config-if)#> watchdog
```
Cisco Service Control Operating System Release 5.1.0

This section describes the compatibility information, new features, resolved issues, and open issues pertaining to Cisco SCOS Release 5.1.0:

- Compatibility Information, page 3
- New and Enhanced Features, page 3
- Resolved Caveats for SCE 10000 Platform in Cisco SCOS Release 5.1.0, page 4
- Open Caveats for SCE 10000 Platform in Cisco SCOS Release 5.1.0, page 5
- Resolved Caveats for SCE 8000 Platform in Cisco SCOS Release 5.1.0, page 7
- Open Caveats for SCE 8000 Platform in Cisco SCOS Release 5.1.0, page 7

Compatibility Information

For information about the Cisco SCE platforms that are compatible with Cisco SCOS Release 5.1.0, see the Cisco Service Control Application for Broadband Download Guide.

For SCOS 8000 Platform:
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Collection Manager Release 4.2.0,5.0.0,5.1.0.
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Subscriber Manager Release 4.2.0,5.0.0,5.1.0.

For SCOS 10000 Platform:
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Collection Manager Release 5.0.0,5.1.0.
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Subscriber Manager Release 5.0.0,5.1.0.

For SCOS vSCE Platform:
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Collection Manager Release 5.0.0,5.1.0.
- Cisco SCOS Release 5.1.0 is compatible only with Cisco Service Control Subscriber Manager Release 5.0.0,5.1.0.

New and Enhanced Features

This section describes the major Cisco SCE 8000, SCE 10000 platform-related new features and enhancements in Cisco SCOS Release 5.1.0:

- All 128 bits of native IPv6 address are used for hashing and subscriber identification for IANA subscribers.
- Residual drop packets can be added to the actual count of drop packets.
- Subscriber TPS support for 4K (2000/2000). TPS has been increased from 3000 to 4000.
- Maximum number of supported packages increased from 5000 to 10000 (SCE 10000 platform).
- Increased the maximum Telnet/SSH sessions from 5 to 20 sessions.
- IPv6 traffic wrapped in IPv4 L2TP should not treat these traffic as normal IPv6 traffic if L2TP skip is enabled.
- FC limit increased from 57 Mbps to 300 Mbps (SCE 10000 platform).
- Add-on packages.
Increased HTTP URL Flavors support to 2 million (SCE 10000 platform).
- DNS-Assisted classification.
- Flexible redirection.
- Bursty Convergence for GC(8000 platform).
- Increased PIR limit of PBWC/BWC to 1 Gbps (SCE 10000 platform).
- Redirection Rate-Limiting

Resolved Caveats for SCE 10000 Platform in Cisco SCOS Release 5.1.0

This section describes the resolved caveats pertaining to the Cisco SCE 10000 platform for Cisco SCOS Release 5.1.0:

CSCum70060
While pushing the DS-LITE traffic, the upstream and downstream volume for all the RDRs have mismatched values.

CSCum88134
When FD congestion occurs, the TX drop can be confirmed through Tx_Rg_Drop counter in the below CLI: debug slot 0 ppc 0 func RUC_HWCNTR_PrintPdFdStats.

CSCun85823
When IPv4 traffic is sent, high latency is produced and is increased when Cisco SCE box is loaded with 60G continuously.

CSCuo02242
When using BlackOps TCP protocol traffic, the number of handled packets count per flow is comparatively more in Cisco SCE 8000 device. In Cisco SCE 8000 device, the same protocol has handled 17 packets whereas the protocol handles 44 packets in Cisco SCE 10000 device.

CSCuo21416
In Block and Redirection of L2TP tunneling traffic, blocking occurs even when Tunnel Configuration - L2TP skip command is enabled and block and Redirection policy is mapped to subscriber of L2TP traffic. But, RST Packet from Network and Redirected Message Packet to Subscriber is not generated.

CSCuo54203
When dynamic lookup for flow filter is enabled, in debug slot 0 ppc 0 func CLI RUC_HWCNTR_PrintPdFdStats, the counter PD [pd index] Rx Byp increases due to the FD Congestion.

CSCuo72762
In certain cases, misclassification is observed for bundling traffic. In FD Bootlogs, you can observe the "readQ_AddStarTuple” failure messages.

CSCup02001
More RDR are sent than what is viewed in the Line attack Log. This error occurs only when detector is configured and traffic is of IPv6 type. The error does not happen consistently all time.

CSCup32156
Port Bandwidth is not shown properly in port bw cli. It is visible only at ingress rate which is greater than one Gbps.
CSCup34461
For VAS mirrored traffic, TOS marking does not happen even when both VAS Mirroring and TOS marking matches to the same type of traffic. This issue is applicable to Cisco SCE 10000.

CSCup34777
The data volume of usage for subscriber can be less for DS-Lite internal fragmented traffic, though the DS-Lite tunneling is configured and fragmented traffic especially for middle/last fragmented traffic.

CSCup34856
In general, VLAN tag is added for VAS mirrored packet. You cannot view the VLAN tagged packet in this case when the traffic is matched to Flow-Filter rule for Quick Forwarding.

CSCup41838
Specific TP's will get congestion and trigger FCID shortage issue. The traffic rate is higher at specific TP's or CPU utilization more on the specific TP's.

CSCup42275
Gy CCR-U timeouts counters increases when the package contains Gy quota profile with more than one bucket and Quota breach / Quota status is sent for more than one bucket at the same time in consecutive CCRs.

CSCup63068
When we select the CoS value in Cisco SCA BB and apply the policy, traffic is not mapping to appropriate Tx Queue selection. This symptom is observed when you create party and try to apply CoS value on that party.

CSCup69985
The number of open Gy sessions is less than the expected sessions when total quota RDRs for Gy generated per sec is 1700 (supported rate at this point is 1200).

CSCup76983
TP crash happens when SCE is stressed 40% more than FIF capacity and when aging is less than ten seconds, SCE box is not stable.

CSCup92285
Flow Filter counter mismatch in global attack UDP traffic.

CSCuq06739
If new installation of image is required, you need to change the grub configuration. This issue is applicable to Cisco SCE 10000.

CSCuq01457
In recovery state, management IP is not reachable. This issue is applicable to Cisco SCE 10000.

Open Caveats for SCE 10000 Platform in Cisco SCOS Release 5.1.0

This section describes the open caveats pertaining to the Cisco SCE 10000 platform for Cisco SCOS Release 5.1.0:

CSCur74618
SCE10K: More Deviation for Bursty Traffic in Link0.
**CSCur81832**
SCE10K: SW sustained flow open rate was not hitting 70k/TP.

**CSCus17201**
Packets are not received at port for 2-3 minutes with LFR under traffic.

**CSCus21681**
SBWC rate limit is not proper for increased flows in default GC.

**CSCus25905**
SCE10K: IPv6 - Latency increasing at last 2-links above 30 Gig.

**CSCus48485**
VAS Mirroring packets dropped when starting traffic at link2 or link3.

**CSCur69354**
SCE10K: Sometimes link is going down after multiple reload.

**Workaround**
Execute the below cli to recover the port.

```
SCE10000#>con
SCE10000(config)#>interface LineCard 0
SCE10000(config if)#>link mode all-links cutoff
```

Wait few seconds, then revert it back(cutoff to forwarding) with below cli

```
SCE10000#>con
SCE10000(config)#>interface LineCard 0
SCE10000(config if)#>link mode all-links forwarding
```

**CSCuj77097**
In IPv6 only mode, once traffic reaches 50Gbps, packets will be bypassed at FD level and there will be a service loss. In IPv6 only mode, congestion is observed at SP with 512 byte packet.

**Workaround**
There is no workaround, but system recovers once traffic rate is below 50Gbps.

**CSCuo11515**
The Flow Filter dynamic lookup is disabled by default and you cannot apply Flow Filter rule based on TCP flags and direction.

**Workaround**
Enable Flow Filter dynamic lookup, using the following debug command:

```
debug slot 0 ppc 0 func RUC_HWSRV_FF_Enable_Dynamic
```
Resolved Caveats for SCE 8000 Platform in Cisco SCOS Release 5.1.0

This section describes the resolved caveats pertaining to the Cisco SCE 10000 platform for Cisco SCOS Release 5.1.0:

CSCuq39691
The active-port can't be seen in the running-config and can't be saved.

CSCul49780
Cisco SCE may reboot due to kernel panic event.

CSCur05021
SCE evaluation for CVE-2014-6271 and CVE-2014-7169.

CSCtz74897
Total rate limit doesn't work for non default global controllers.

CSCuo86705
SCOS: Traffic not contained at GC level in 4.0.0p1.

CSCur50277
SCOS: AGC shows lower rate when traffic above 6.4Gig.

CSCus31933
After SM restart, active subs get additional 128 mapping for IAPD.

Open Caveats for SCE 8000 Platform in Cisco SCOS Release 5.1.0

This section describes the open caveats pertaining to the Cisco SCE 10000 platform for Cisco SCOS Release 5.1.0:

CSCus27279
December 2014 - NTPd.org Vulnerabilities.

CSCtj50046
"on failure cutoff“ command does not work.

CSCtk67558
Delayed notification of first QuotaStatus RDR.

CSCtu12409
IPv6 byte count is displayed in DP L2TP control packets.

CSCty13726
Problem in handling non-first fragments in l2tp skip mode in cascade set.

CSCub93514
3.7.5-p1: diameter Gy interface enabled upon reload.
CSCuh57649
PUR IP_Type_TAS count is incorrect when Subscriber has IPv6 & DSLiteflow.

CSCur56349
SCE/CM: Incorrect value reported for the field TOTAL_ACTIVE_SUBSCRIBERS.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation at:

Subscribe to What’s New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.