Release Notes for Cisco Service Control Operating System (SCOS) 3.1.0

June, 2007

Release Notes for Cisco Service Control Operating System (SCOS) 3.1.0.

Supports: SCOS 3.1.0.

OL-8955-12

These release notes for the Cisco Service Control Operating System describe the new features and fixes provided in Cisco Release SCOS 3.1.0.

For further information regarding features added and issues resolved in the 3.0.x train, please refer to Release Notes for Cisco Service Control Operating System (SCOS) 3.0.6.

For a list of the caveats that apply to Cisco Release SCOS 3.1.0 see *Open Caveats*, page 11.

Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Introduction

Cisco is proud to release version 3.1.0 of the SCOS (Service Control Operating System) for its SCE platform.

SCOS 3.1.0 is a time-based release. It includes new features, as well as fixes of issues that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the new features and fixes delivered in the SCOS 3.1.0 release. It assumes the reader already has a good working knowledge of the Cisco Service Control solution. For additional information, please refer to the Cisco Service Control Engine documentation.

RELEASE SCOS 3.1.0

New Features

Uni-directional classification for support of asymmetric routing

In a situation in which the routing scheme directs the two directions of a flow to follow different routes, each direction flows through a different SCE platform. The effect of different routing is that each SCE platform can classify only one direction of the flow. The 'asymmetric routing' mode enables the SCE platform to handle such traffic, allowing SCA BB to classify traffic based on a single direction and to apply basic reporting and global control features to uni-directional traffic.

See "Asymmetric Routing Topology" in the chapter "Configuring the Connection" in the *Cisco Service Control Engine Software Configuration Guide*, and the relevant topics in the *Cisco Service Control Application for Broadband User Guide.*

NetFlow V9

Starting from Release 3.1.0 of SCOS for Cisco Service Control, the product can deliver gathered reporting data over the NetFlow V9 export protocol. This protocol is an industry standard for delivering gathered reporting data for external application for collecting, aggregation, storage, and processing. The NetFlow export protocol enables the Service Control solution to integrate with a wide range of existing data collectors and reporters.

See the chapter "Raw Data Formatting: The RDR Formatter and NetFlow Exporting" in the *Cisco Service Control Engine Software Configuration Guide*.

Subscriber synchronization in cascade setups

SCOS 3.1.0 enhances support of failover in cascade topologies by adding a synchronization process between the active and the standby SCE platforms. This process keeps the standby SCE platform constantly updated with the latest subscriber-related information (login, logout, and quota updates), in order to minimize information loss in the event of fail-over.

See the section "*Synchronizing Subscriber Information in a Cascade System*" in Chapter 9 "Managing Subscribers" in the *Cisco Service Control Engine Software Configuration Guide*.

Compatibility Information

SCOS 3.1.0 may be installed on the following Service Control Engine platforms:

- SCE 2020 4xGBE
- SCE 2020 4/8xFE
- SCE 1010 2xGBE (2-U only)

SCOS 3.1.0 is not compatible with the following Service Control Engine platform:

- SCE 1010 2xGBE (1.5U)

Resolved Issues

The following issues were resolved in this release.

SSH activity sometimes ended in an unstable state

- Cisco Number CSCsh49563

  During SSH activity, which usually includes session logout and login operations, the system sometimes ended in an unstable state due to file system violation.

  This issue is fixed in SCOS 3.1.0.

Redirect packet was sometimes transmitted on wrong link

- Cisco Number CSCsh74592

  When a flow using different links for upstream and downstream was redirected, the redirect packet to the subscriber was transmitted on the downstream link, but included the source MAC address from the GET packet seen on the upstream link as destination MAC address. This MAC address was sometimes unknown to the device receiving it.

  This issue is fixed in SCOS 3.1.0.

Dynamic Signature (DSS) caused a reboot after dozens of consecutive Apply operations

- Cisco Number CSCsi40164

  Applying a policy using DSS sometimes caused an infinite loop, resulting in a reboot of the SCE platform.

  This issue is fixed in SCOS 3.1.0.

Reload of the SCE due to an expiry of an internal watchdog mechanism

- Cisco Number CSCsi53483

  Under the following conditions, the SCE platform sometimes reloaded due to an expiry of an internal watchdog mechanism:

  - SCE platform working past its capacity envelope

  AND

  - The rate of the warning messages that BW controllers cannot be allocated is very high

  This issue is fixed in SCOS 3.1.0.

The saving process of application configuration was not resilient to reload

- Cisco Number CSCsi44806

  Running configuration of the application was not saved in cases of sudden reboots. In such cases, the SCE platform came up with no application configuration.

  This issue is fixed in SCOS 3.1.0.

Failure to retrieve support file using FTP

- Cisco number: CSCse63425

  An error occurred when attempting to retrieve a support file using FTP.

  The failure to retrieve the support file was caused by a timeout on the FTP server. When the SCE produces the support file (in zip format), it first produces the contents locally and then adds the contents to the zip file. When the support file is created over an FTP connection, there are long periods of no data transfer during the creation of the zip internal data. These long periods of no data transfer can trigger a connection timeout on the FTP server.

  This issue is fixed in SCOS 3.1.0.

PRPC authentication security level was set to default after RPC adapter restart

- Cisco number: CSCsh71764

  The PRPC connection to the SCE failed after restarting the PRPC server.

  This occurred when the security level was changed to something other than the default (semi) and the PRPC server was restarted. After the restart, the security level reverts back to the default value.

  This issue is fixed in SCOS 3.1.0.

Part of the quota information was not exchanged between two cascaded SCE platforms

- Cisco Number CSCsf97557

  Part of the quota information was not exchanged between two cascaded SCE platforms. This caused the failover in SCE cascade topology to be stateless with regard to quota.

  This issue is fixed in SCOS 3.1.0 (see *Subscriber synchronization in cascade setups* on page 5.)

Subscriber with many mappings did not send all lease time expiration notifications

- Cisco Number CSCsg02338

  A subscriber with many mappings did not send lease time expiration notification on some mappings.

  This issue is fixed in SCOS 3.1.0.

Link reflection failed to operate after long uptime

- Cisco Number CSCsh73979

  Link failure reflection sometimes failed to operate on a system with uptime of more than 24 days.

  This issue is fixed in SCOS 3.1.0.

Attack-detector port-list showed random numbers in running-config

- Cisco Number CSCsi11990

  When a port list was configured for an attack-detector, the specified ports were not saved correctly to the running-config. A list of random numbers was saved.

  This issue is fixed in SCOS 3.1.0.

Potential discard of packet under extreme network conditions

- Cisco Number CSCsi24848

  Under certain conditions, the Flow Filter rule used for congestion handling took effect a few mSec too late, allowing some packets to be discarded.

  This issue is fixed in SCOS 3.1.0.

Access violation when configuring anonymous groups

- Cisco Number CSCsg37325

  The following two scenarios sometimes caused an access violation:

  - Configure: **`subscriber anonymous-group name sub1 IP-range 0.0.0.0/32`** and transmit traffic. Then remove this group and wait for the flow to end.

    Then configure: **`subscriber anonymous-group name sub1 IP-range 0.0.0.0/0`** and transmit traffic.

  - Configure **`anonymous-group name sub1 IP-range 0.0.0.0/32`** and **`anonymous-group name sub2 IP-range 0.0.0.0/0`**

    Then remove sub1.

  This issue is fixed in SCOS 3.1.0.

destConnectionStatus of the rdr-formatter group was missing in 'show snmp MIB pcube-SE-MIB rdr-formatter' command

- Cisco Number CSCsf29452

  The MIB object *`destConnectionStatus`* of the rdr-formatter group was missing in CLI '**`show snmp MIB pcube-SE-MIB rdr-formatter`**' command.

  This issue is fixed in SCOS 3.1.0.

rdrActiveConnectionTrap was not sent after reload of the SCE platform

- Cisco Number CSCsg83522

  The proprietary trap '*rdrActiveConnectionTrap*', which should be sent after completing a successful establishment of a connection with the RDR collector, was not sent upon system initialization.

  This issue is fixed in SCOS 3.1.0.

Link up/down traps were not sent on all ports

- Cisco Number CSCsh31706

  The SNMP traps 'link up'/'link down', which should be sent for each port upon system initialization, were sent only on the first four ports of the SCE platform.

  This issue is fixed in SCOS 3.1.0.

MIB object 'pmoduleType' returned wrong value in cascade setups

- Cisco Number CSCsh34432

  The MIB object *pmoduleType* of PcubeSeMib returned the wrong value in cascade setups, indicating that there were only two GBE ports in the SCE platform.

  This issue is fixed in SCOS 3.1.0.

MIB variable ifMtu returned wrong value for traffic ports

- Cisco Number CSCsh99422

  The MIB-II variable *ifMtu* returned an incorrect value for the maximum packet size of the SCE platform traffic ports.

  This issue is fixed in SCOS 3.1.0.

Some rdr-formatter MIB objects returned information only for category 1

- Cisco Number CSCsi01850

  Global MIB objects in the *RdrFormatterGrp* in the PcubeSeMib should indicate total values for all categories of the RDR formatter. Previously these objects contained only the values for Category 1.

  This issue is fixed in SCOS 3.1.0.

Limitations and Restrictions

The upgrade to the SCOS 31.0 release may result in re-initialization of the SCE 1010 or SCE 2020 hardware Bypass module. This re-initialization process may cause a failure of the GBE link where the system stalls for a period of less than 1 sec.

The table below states the various cases when this re-initialization may occur (marked as "Yes").

To From	2.5.0	2.5.1	2.5.2	2.5.5	2.5.6	2.5.7	2.5.8	2.5.9	3.0.0	3.0.1	3.0.3	3.04	3.0.5	3.0.6	3.1.0
2.5.0	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.1	-	-	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.2	-	-	-	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.5	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.6	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.7	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.8	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2.5.9	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes
3.0.0	-	-	-	-	-	-	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
3.0.1	-	-	-	-	-	-	-	-	-	-	No	No	No	No	No
3.0.3	-	-	-	-	-	-	-	-	-	-	-	No	No	No	No
3.0.4	-	-	-	-	-	-	-	-	-	-	-	-	No	No	No
3.0.5	-	-	-	-	-	-	-	-	-	-	-	-	-	No	No
3.0.6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	No

Open Caveats

SCE-Sniffer RADIUS LEG might not work after PQI installation

- Cisco number: CSCse19753

  After installing a SCA BB PQI file on the SCE platform and before applying a service configuration for the first time, the SCE application ignores all open flows. When a service configuration is applied for the first time, the SCE application starts processing new flows. However, older flows that were opened earlier are not processed, and no RDRs are generated for them. RADIUS sniffing is susceptible to this limitation because it is likely that the relevant RADIUS flow would be open before the first time a service configuration is applied.

  Workaround:

  The flow should be re-opened by restarting the SCE line-card after the service configuration is applied for the first time.

  To restart the line-card through the Network Navigator GUI:

  1. Select the relevant SCE platform from the Network Navigator device tree.
  2. Stop the SCE line-card: from the Network menu, select Stop Traffic Processing.
  3. Start the line-card: from the Network menu, select Start Traffic Processing.

  After the line-card is restarted, the RADIUS flow is treated by the SCE application as a new flow, and is processed and reported.

Radius/DHCP sniffing might be permanently interrupted

- Cisco Number CSCsi82268

  In cases of errors, such as memory shortage or expiration of internal protection mechanisms, the SCE platform Radius sniffer may stop working. The errors cause the system to bypass Radius flows and stop generating RDRs until reboot or aging of the flows, which ever comes first.

Long SSH session cleanup time may result in temporary unavailability

- Cisco Number CSCsi68582

  Frequent SSH logouts and logins with less than a minute between a logout operation and login operation, along with other management operations, may result in system memory shortage and reload of the SCE platform.

  Workaround: Wait at least one minute after logging out from an SSH session before logging in again.

Upgrading the SM causes SCE failover in cascade topology

- Cisco Number CSCsi70273

  SCE platform performs failover procedure between active and standby SCE platforms in a cascaded pair when the connection to the SM goes down, even if no failover behavior is configured for this situation.

Problems may be encountered in downgrading from Release 3.1.0 (or higher) to a previous release

- Cisco Number CSCsi30584

  When downgrading from SCOS 3.1.0 to previous release, a jvm exception is thrown. The SCE platform fails to downgrade and reboots continuously.

  Workaround:

- If the SCE platform has not rebooted, do the following

  Uninstall the pqi before downgrading using the following commands:

```
SCE2000#>configure

SCE2000(config)#>in li 0

SCE2000(config if)#>pqi uninstall file <file-name>
```

Note The already installed pqi file is required in order to perform this operation. If the installation has been performed using the SCA BB console, the file will not be available on the SCE platform disk and it will first have to be uploaded via ftp using the following CLI command:

```
copy ftp://username:password@host-ip-address/full path
/tffs0/app/install-pqi-name.pqi
```

- If the SCE platform has already rebooted or the previous workaround cannot be applied, do the following:

  1. Reload the system in recover mode.
  2. Connect via telnet.
  3. Delete the following file: *tffs0/system/p3hidden/um/mbeancfg/engage.txt.*
  4. Reload the system again.

     3.0.x can now be installed correctly.

Problems may be encountered in downgrading from Release 3.0.5 (or higher) to a previous release

- Cisco Number CSCse74400

  Downgrading from a system running SCOS 3.0.5 (or higher) to a previous SCOS release may be unsuccessful until a second reload is performed. This is due to subscriber database incompatibility between 3.0.5 and previous versions resulting from the increase in the subscriber name size.

  Workaround: Clear the subscriber database after package installation of the downgraded version and prior to the reload by deleting all files under the directory */tffs0/system/p3hidden/partydb/.*

RDRV1 destination startup configuration will fail in downgrading from Release 3.1.0 to a previous release

- Cisco Number CSCsi96575

  When configuring RDR formatter RdrV1 destinations (even when using the old, backward-compatible command syntax), the running-config and hence the startup-config are updated with the new (as of 3.1.0) format of the command, which implicitly states the protocol and transport type.

  Due to this behavior, in a downgrade scenario, the startup configuration will fail to configure the RDR formatter destination, since protocol and transport type are not supported. This may result in loosing reports.

  Workaround: Configure the RDR formatter again using the old syntax. The details can be derived from *the config.txt* file under */tffs0/system*

Link failure may be reflected to all ports if a port is flickering due to a HW problem

- Cisco Number CSCsg46885

  When link reflection on all ports with linecard aware is configured, the link failure may be reflected to all ports (rather than only to the relevant link) if one of the ports that is connected to the failed linecard is flickering due to a hardware problem.

Subscribers data synchronization is slower when static subscribers are configured

- Cisco Number CSCsi82338

  After the cascade links are up, the active box synchronizes the subscriber database to the standby box at a rate of ~1000 updates/sec. However the standby box can support this login rate only for dynamic subscribers. If there are static subscribers configured, it can take up to an hour to synchronize the subscriber database after the cascade links are up. However, once the standby box is synchronized, new subscribers are replicated to the standby box normally (at a maximal delay of 2 minutes).

CLI command ‘IP address’ should indicate to the user that a reload of the SCE is required

- Cisco Number CSCsi56724

  After a change is made to the management IP/subnet, the SCE platform CLI should output a message notifying the customer that a reload is required for the changes to take effect.

'no service telnetd' command does not block the Telnet port

- Cisco Number CSCsh21957

  Disabling the Telnet server of the SCE (using the CLI command **`'no service telnetd'`**) disables any new Telnet connection to the SCE platform, but does not block the Telnet port.

  Workaround: There is no workaround that will enable blocking this specific service at a lower level.

  Use the ‘**`ip access-class`**’ command to restrict access to the SCE platform at the IP level. Configuring the SCE platform to deny a certain IP address would prevent communication with that address using any IP-based protocol, including Telnet, FTP, ICMP and SNMP. The basic IP interface is low-level, blocking the IP packets before they reach the higher level services.

TCP Learning doesn't close flows that start with SYN-ACK

- Cisco Number CSCsg85546

  In MPLS/VPN auto-learn mode, upstream SYN-ACK packets of unlearned labels reach the software even though they should not.

  This is relevant mainly when using anonymous subscribers with a range that contains addresses that appear in one of the VPNs. In this case, anonymous subscribers may be incorrectly spawned for addresses inside VPNs. Such subscribers see very little, if any traffic.

Errors on invalid management agent notification during SCE reload

- Cisco Number CSCse37172

  The following error may appear in the boot log file after an upgrade of the SCE platform from a release prior to 3.0.5 to release 3.0.5 and up:

  “`Error - Notification <number> does not exist.`“

  This occurs because some notification IDs are not valid since release 3.0.5. The fact that this command does not succeed does not cause any harm.

  Workaround: Run the CLI command ‘**`copy running-config startup-config`**’. This removes the old notification IDs from the configuration file.

BWC controller gives less bandwidth than configured

- Cisco Number CSCsg32201

  When BWC has many short UDP flows associated with it, such as eMule flows with very few packets each, the bandwidth given to all flows is lower than configured.

  Workaround: Configure Global Controllers to control the bandwidth

  There is no workaround when working with Service Bandwidth Controllers.

Potential memory overrun in cascaded environment with a high number of subscribers

- Cisco Number CSCsc96282

  Under rare conditions, the standby SCE platform of a cascaded pair crashes and restarts. This may happen in a scenario involving a heavy load of anonymous subscribers in cascade topology.

  In such a case, only the standby box is affected, and therefore:

  - overall service is not compromised
  - fault tolerance is compromised only for the time it takes the standby box to restart.

The configured attack threshold is set for each PPC separately

- Cisco Number CSCsd48922

  For certain types of attacks, an attack is detected by the SCOS attack-filter module only if it is three times stronger (as measured by flow rate per second) than the configured value.

  This happens when the IP address common to all the flows of the attack is on the network side of the SCE platform, so all attacks of type 'single-side-network' have this problem.

When the VAS Health Check initializes, the CLI command ‘show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>’ shows the server being UP even if it is actually Down

- Cisco Number CSCse05325

  The operative state of a VAS server while the Health Check is in Init state is considered to be Up as shown in the CLI command "show interface linecard 0 VAS-traffic-forwarding VAS server-id <id>". In addition, during this time, the SCE platform may forward VAS traffic to this server.

Flow ‘opened from VAS’ is misrouted if there is a FF rule to bypass

- Cisco Number CSCsc49573

  When VAS mode is enabled, the system generally assumes that traffic with a VLAN tag is VAS traffic coming from the VAS servers, and therefore forwards it to the non-VAS link. However, under the following conditions, a flow will be forwarded by the SCE platform on the same link on which it was received and with no VLAN tag:

  - VAS mode is enabled
  - The FIF packet has a VLAN tag
  - There is a traffic rule to bypass the flow *or* the SCE platform is in congestion

  In some topologies this behavior may cause VAS traffic to be incorrectly routed back to the VAS link.

Packet Loss during Application Installation or Upgrade

- Cisco Number CSCpu11798

  When a PQI application file is installed or upgraded on the SCE, the SCE may lose a few packets for a few seconds. The overall percentage of this phenomenon is very low.

  Workaround: It is advised to perform the upgrade in non peak time.

rdrActiveConnectionTrap is not sent upon re-establishment of connection when forwarding mode is multicast

- Cisco Number CSCsg90919

  In an environment with several RDR formatter categories and different destinations configured for multicast forwarding, if the connection is lost between one of the destinations and the RDR formatter, when the connection is re-established, the *rdrActiveConnectionTrap* is not sent

‘show snmp MIB pcube-SE-MIB port’ returns wrong number of ports

- Cisco Number CSCsg45606

  The CLI command ‘**`show snmp MIB pcube-SE-MIB port’`** returns the wrong number of ports, because Mng port 2 is treated as traffic port instead of 2nd management port.

  Workaround: Use SNMP browser rather than CLI command.

Obtaining Technical Assistance

Cisco provides *Cisco.com* (on page 17) as a starting point for all technical assistance. Customers and partners can obtain documentation., troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page 17), go to the following website:

http://tools.cisco.com/RPF/register/register.do

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.