Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 2.5.8

December 30, 2005

Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 2.5.8

Supports: SCMS SM 2.5.8, 2.5.7, 2.5.6, 2.5.5, 2.5.2, 2.5.1, SCMS SM 2.5

OL-7083-06

The release notes for the Cisco SCMS SM describe the enhancements provided in Cisco Release SCMS SM 2.5.8.

Corporate Headquarters:

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

Contents

Introduction

Cisco is proud to release version 2.5.8 of the Subscriber Manager infrastructure.

SCMS SM 2.5.8 is a point release of SM 2.5. It includes various fixes of bugs that were identified as part of Cisco's on-going internal testing and during our interaction with our customers.

This document outlines the enhancements of the SM 2.5 releases, and assumes the reader already has a good working knowledge of the Cisco solution. For additional information, please refer to the Cisco Service Control Engine documentation.

Release SCMS SM 2.5.8

Functional Enhancements

Package Association Based on RADIUS Attribute Prefix\Suffix

In Release 2.5.8, the RADIUS listener can be configured to strip a RADIUS attribute based on a selected character. This provides a convenient method for obtaining the package ID by associating it with the domain name.

For example, the package ID can be obtained from the USERNAME attribute value of *subscriber@domain-name* by stripping the characters before the "at" sign (@) to produce the *domain-name*. Note that the user must define a conversion table for converting the domain-name to a valid package-Id value (number).

The following are the relevant sections of the *p3sm.cfg* configuration file:

```
# The following section defines the RADIUS attribute on which
# subscriber ID association is based. Default association is
# based on the 'user name' attribute. Uncomment this section if
# you want to base subscriber ID association on a different
# attribute.

# [Radius.Subscriber ID]

# Radius protocol attribute number.
# Use number 26 in case of Vendor Specific Attributes (VSA).
# radius_attribute=-1

# the type of the attribute (type "integer" or "string")
# radius_attribute_type = string
#
# Use following parameters only if association is based on
# vendor specific attribute (VSA) -

# radius_attribute_vendor_id=-1
# radius_sub_attribute=-1

# the following parameters define ways to manipulate the RADIUS
# attribute value. There are three options to define the
# strip_type’parameter:
# 1. remove_suffix – strip off the suffix of the attribute
#    beginning from a certain character (defined by the
#    ‘strip_character’ parameter)
# 2. remove_prefix - remove the prefix of the attribute ending
#    at a certain character (defined by the ‘strip_character’
#    parameter)
# 3. dont_strip - leave the attribute value as is (default)
#
#
# strip_character=@
# strip_type= dont_strip

# The following section defines RADIUS attribute from which
# subscriber package is retrieved.
# Uncomment this section if you want to retrieve subscriber
# package from a different attribute.

# [Radius.Property.Package]

# Radius protocol attribute number.
# Use number 26 in case of Vendor Specific Attributes (VSA).
# radius_attribute = <insert the attribute number here>

# the type of the attribute (type "integer" or "string")
# radius_attribute_type = integer

# Radius protocol packet types to look for the attribute
# Optional values: "access-request", "access-accept",
# "accounting-request", "accounting-response" , "all" or "none"
# separated with ',')
# packet_types = access-accept , accounting-request

# Use following parameters only if association is based on
# vendor specific attribute (VSA)

# radius_sub_attribute = <insert the attribute number here>
# radius_attribute_vendor_id = <insert the vendor identifier
# number here>

# Following parameters defines whether to use default value and
# what value to use if the attribute was not found (when not
# mandatory)
# use_default = true
# default = 0

# the following parameters define ways to manipulate the RADIUS
# attribute value. There are three options to define the
# strip_type’parameter:
# 1. remove_suffix – strip off the suffix of the attribute
#    beginning from a certain character (defined by the
#    ‘strip_character’ parameter)
# 2. remove_prefix - remove the prefix of the attribute ending
#    at a certain character (defined by the ‘strip_character’
#    parameter)
# 3. dont_strip - leave the attribute value as is (default)
#
#
# strip_character=@
# strip_type= dont_strip

# the following parameter define a conversion table between the
# result of the attribute value manipulation and the property
# value. To define this conversion use the following format:
# mapping_table.<attribute-value>=<property-value>
# for example:
# mapping_table.gold=1
# mapping_table.silver=2
#
# mapping_table.<attribute-value>=<property-value>
```

Expanded RDR DHCP LEG subscriber-ID Options

In order to support subscriber management integration in non-cable DHCP environments, the RDR DHCP LEG (DHCP Sniffer) now supports using other DHCP options in addition to option 82 (sub-option 2 – remote-Id) as subscriber-Id with a fallback to a subscriber-Id which uses the IP address in the format IP_a.b.c.d.

The chain of decisions regarding the subscriber-Id is as follows:

Step 1. Use the configured DHCP option as subscriber-Id if it exists.

Step 2. Otherwise, if the fallback to IP is enabled, use the IP address.

Step 3. Otherwise attempt to extend the lease based solely on the IP address (will work only if the IP address is in the DB).

The following are the relevant sections of the *p3rdr_dhcp.cfg* configuration file:

```
# the following section defines the functionality of the LEG in
# regads to subscriber ID handling. the subscriber ID can be
# taken fron a DHCP option with the ability to fallback to using
# the allocated IP as subscriber ID.
[Subscriber ID]

# the following parameter defines what DHCP option to use as the
# subscriber ID.
# the format of this parameter is the option number itself or
# for DHCP options which have sub-options the format is the DHCP
# option and sub-option type separated by a colon. for example:
# 43:123 or 61
# (default Relay-Agent-Information using the Remote-Id
# information i.e. 82:2)
#dhcp_option=82:2

# The following parameter defines the format type of the DHCP
# option defined by the 'dhcp_option' parameter. optional values
# are 'binary' (binary string which is converted to an ascii
# hexadecimal string) or 'string' (ascii string).
# (default: bianry)
#dhcp_option_type=binary

# the following parameter defines whether in cases where the
# 'dhcp_option' is not found in the DHCP packet and if the IP
# address which the DHCP message relates to is not already in
# the SM database to fallback to a different way to define the
# subscriber ID.
# the supported fallbacks are:
# ip - use the allocated IP to create a subscriber Id in the
# format of: IP_aaa.bbb.ccc.ddd
# not setting this parameter - no fallback. will fail the login.
# (default not set)
#default_id=
```

Resolved Issues

Subscriber Locked When Working with App Lock and SM GUI

- Cisco Number CSCsb66184

When the parameter *application_subscriber_lock* is set to true in the p3sm.cfg file, the action of adding a new subscribers from the Subscriber Manager GUI causes the SM to lock this subscriber infinitely. No other operation on this subscriber record can be performed after the lock occurs.

The displayed error message in the GUI is: *unlock of a non-locked object <subscriber name>*

This bug was fixed in SM 2.5.8

Radius Installation Not Supported in Cluster Mode

- Cisco Number CSCsb79708

When the accounting messages are sent to the RADIUS Listener using the virtual IP of the SM-cluster, the return message is sent using the localhost IP address of the SM machine as the source IP. The RADIUS device that sent the message throws such packets, because the source IP is not a known IP address and is not associated with this accounting message flow.

In release 2.5.8 the user can configure the IP address to be used by the RADIUS Listener using the *ip* parameter in the *Radius Listener* section.

This bug was fixed in SM 2.5.8

Veritas Cluster Server 4.0 Support without Workaround

- Cisco Number CSCsb29633

Veritas Cluster Server 4.0 introduced a ProcessOnOnly bundled agent that caused a clash of agent names with the Cisco ProcessOnOnly custom cluster agent.

This issue is fixed in Release 2.5.8. The SM ProcessOnOnly agent name is changed to OnOnlyProcess with no functional change.

Release SCMS SM 2.5.7

SM Cluster Failover Issues

When two SM servers operate in cluster mode and the standby SM gets activated after a failure of the active SM, the standby SM loads from the database part of the subscriber information. This operation includes a timeout of 20 seconds. When SM manages a significant number of subscribers (half a million or more), the operation may last more than 20 seconds, so this timeout may expire.

When this happens, a fatal error is issued and the cluster fail-over does not go into action. In addition, this timeout is not configurable in SM 2.5.6. When the failure takes place, it also triggers a series of events that might cause the SCE platform to malfunction.

The following two fixes were implemented in SM 2.5.7:

- The timeout was changed to 40 seconds and was changed to be configurable (but still hidden – ask Cisco TAC for support if needed).
- A fix was implemented in the SCE platform, causing it to switch to the connection with the new active SM regardless of the current connection state.

Canceling the pcubeSync File and Mechanism

The SM uses a system file (pcubeReg, stored in the root directory), to store the PRPC port to which the SM listens. The CLU process reads this file and opens a PRPC connection accordingly. In SM 2.5.6, another system file (pcubeSync), is used for synchronizing the access to the pcubeReg file.

In SM 2.5.7, the usage of the pcubeSync file and mechanism was cancelled, since it caused various issues. The SM now operates correctly without it.

Standby SM Performs Active Operations on the SM database

In SM 2.5.6, in cases where a non-default domain is used, the Standby SM performs operations on the SM database which caused loss of information on the Active SM.

This issue was fixed in the SM 2.5.7 and now the Standby SM only performs active operations on the SM database when it becomes the Active SM.

Support for the Multi-GBE SCP Solution

SM 2.5.7 supports the solution where a Cisco 7600/6500 is used for load-balancing among several SCE platforms. When one SCE platform fails, subscriber traffic is redistributed to a different SCE platform. The SM must remove these subscribers from the failed SCE platform and send the relevant subscriber information to the new SCE platform. To support this functionality, the *`force-subscriber-on-one-sce`* configuration parameter is set in the p3sm.cfg configuration file.

Release SCMS SM 2.5.6

The following issues were identified and fixed:

Dynamic package ID assignment

The dynamic package-ID assignment functionality did not operate correctly as part of the DHCP lease query configuration.

This occurred when using the DHCP lease query LEG or when using the RDR DHCP LEG.

The problem was that these two LEG SW components did not support null-terminated strings for package-ID assignment.

Backward compatibility

When the SM is running SM 2.5.X with SCOS 2.0.X and operating in Pull mode, it replies to pull requests from the SCE platforms, but does not maintain the subscriber-ID to SCE mapping. As a result, the SM does not propagate updates on logout of subscribers and on package-ID changes to the relevant SCE.

Lease-query User Log messages

Wrong User Log messages are produced on some occasions after a DHCP server response to a lease-query request coming from the DHCP lease-query LEG. The problem that was identified is that log messages of the Lease-Query LEG contain corrupted IP address for the relay-agent and for the subscriber.

This issue occurs in the 2.5.1 to 2.5.5 SM releases, and was fixed in SM 2.5.6.

Configuration of subscriber-Id option in Lease-query

When the SM operates in DHCP environments, the MAC address of the cable modem is normally used as the subscriber ID. The MAC address of the cable modem is extracted from option 82 (Remote Id sub-option of the DHCP Relay Agent Information Option). Therefore, the DHCP server is required to support and store option 82 for each CPE. This default can now be overwritten by configuration. Furthermore, a LEG can assign the subscriber IP address as a fallback subscriber-Id (using an IP_a.b.c.d format) if the option does not exist in the server response. This fallback is disabled by default.

Release SCMS SM 2.5.5

The following issues were identified and fixed:

Sending VLAN mapping to the SCE

When the SM and SCE loose connection and then the connection is restored, the SM and SCE perform resynchronization of the subscriber-related information.

During this resynchronization phase, subscriber-related information of subscribers that were identified through VLAN tags was not sent correctly to the SCE.

This issue is now fixed and the information is now sent correctly to the SCE.

Supporting domain=Null at some of the API functions

Some functions in the SM API can now be used in parallel both by a LEG component and by a provisioning system. In order to allow parallel use, the ability to call the login functions with a value of Domain=null was added.

When the login function is called with Domain=null and the subscriber is already mapped to a domain, the mapping will not be affected. If, on the other hand, the subscriber still does not exist in the database, a subscriber will be created without a specific domain.

When the getSubscriberNameByMapping method is called with Domain=Null the subscriber name will be retrieved regardless of the subscriber's mapping to a domain.

Propagation of package ID updates to the SCE

In a few rare cases, the SM was not aware of the fact that a subscriber was managed by an SCE, and did not propagate package ID updates to the relevant SCE.

This issue was fixed.

SM-LEG failure handling

When the SM-LEG Handling feature is enabled (clear_all_mappings configuration parameter is set to true) and the LEG is associated to a domain (LEG-Domains Association section), the SM will start the "clear-all-mappings" timer on valid disconnections of the LEG. A "valid disconnection" is for example a situation where a LEG is restarted. In this case, if the LEG does not reconnect within the timeout, the SM clears all of the mapping in the domain.

In previous releases, in case of other types of failures, such as when the machine on which the LEG was running crashed, or in case of a networking disconnection between the LEG and the SM, the failure was ignored.

This issue was fixed.

Release SCMS SM 2.5.2

The following issues were identified and fixed:

SM Synchronization after SCE Reboot

A problem was found in the SM sync mechanism that is activated after an SCE unexpectedly reboots.

This issue was fixed in SM 2.5.2.

Replying to Pull Requests

In SM 2.5, when the SM receives a Pull request from the SCE (request of subscriber information issued by the SCE when new subscriber IP address was identified in the traffic), it responds with the details of the subscriber that is mapped to the IP address in the Pull request, without checking whether the lease period of the IP address was expired (this is relevant only for Cable or Satellite deployments, where IP addressees are allocated with a lease period)

In SM 2.5.2, when the SM receives a Pull request, it performs the relevant checks, and in case the IP address's lease period expired, the SM does not reply to the Pull request. The SCE then applies a default policy to this IP address.

Non-UNIX Veritas Configuration File

The configuration file of the ProcessOnOnly Veritas cluster agent was not in the correct UNIX format. This causes the Veritas cluster server to fail during startup.
This issue was fixed in SM 2.5.2

Support Lease Renewals in the CNR LEG without Requiring Option 82

When the CNR LEG operates in “CM as Subscriber” mode, it used to require the existence of option 82 in the DHCP renewal transaction. This was required for being able to associate the IP address whose lease is being extended with a specific Cable Modem MAC address. In SM 2.5.2 this is no longer required, as extending the lease is solely based on the IP address. Option 82 is still required for the first login of the subscriber.

Release SCMS SM 2.5.1

Two new LEG components were added to the SM infrastructure.

New LEG Component: DHCP Lease Query LEG & DHCP Forwarder

The DHCP Lease Query LEG is an extension to the SM software and runs as part of the SM.

The DHCP Lease Query LEG handles pull-requests from the SCE platforms that the SCMS SM was unable to handle. The LEG queries the DHCP server using a DHCP Lease-Query transaction.

The following figure shows a sequence diagram representing the operation of the DHCP Lease Query LEG & DHCP Forwarder LEG:

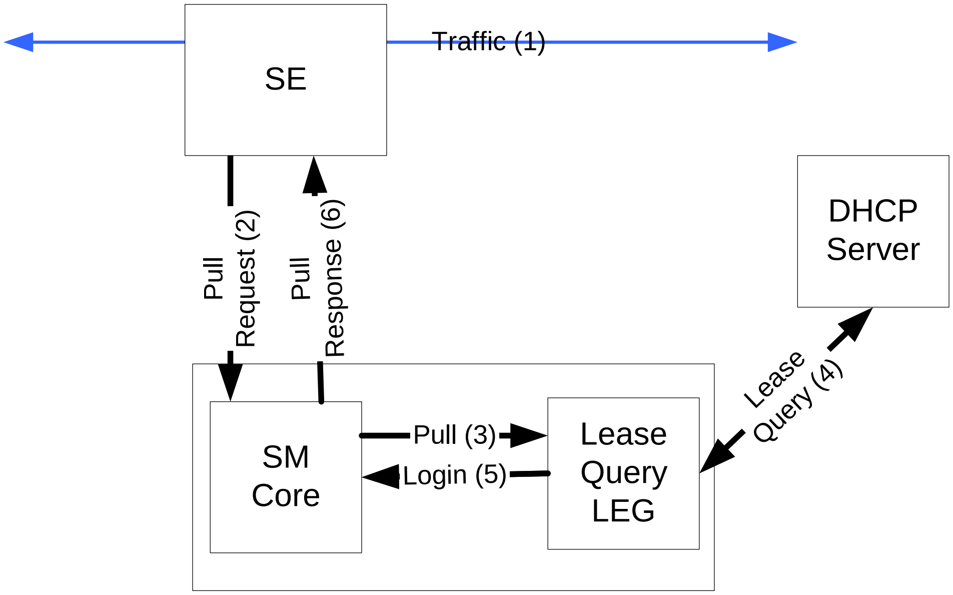

Figure 1: DHCP Lease Query LEG & DHCP Forwarder LEG

The subscriber traffic (1) triggers a pull-request from the SCE and (2) the SCMS SM receives the request for processing. If the SCMS SM does not find a subscriber with a matching IP address in the subscriber database it passes the pull request to the DHCP Lease Query LEG (3). The LEG queries the DHCP server. If the server finds a match for the IP in its database, the server replies with the subscriber information (4). The LEG performs a login operation. (5) Based on the received information, this operation updates the subscriber database and logs the subscriber into the SCE (6) which triggered the pull request.

The DHCP Lease-Query LEG includes a component called the DHCP forwarder, which acts as a bridge between the DHCP Lease-Query LEG and the DHCP servers.

The DHCP Lease-Query transaction is defined as an IETF draft. The LEG supports version 7 of the draft. For more information see http://www.ietf.org/internet-drafts/draft-ietf-dhc-leasequery-07.txt.

New LEG Component: RDR DHCP LEG

The new DR DHCP LEG software module receives RDR (Raw Data Report) messages containing DHCP information from SCE devices configured with a DHCP sniffer service.

The SCE device analyzes DHCP traffic, and reports the DCHP transactions to the SCMS SM device using the RDR protocol. The DHCP transactions that are relevant for the operation of the LEG are `initial login`, `lease extension`, and `release`.

The SCMS SM extracts the modem MAC address, the CPE IP address, and optionally the subscriber package information from the RDR, and triggers a logon or logout operation to the SCMS SM.

The following figure shows a sequence diagram representing the operation of the RDR DHCP LEG:

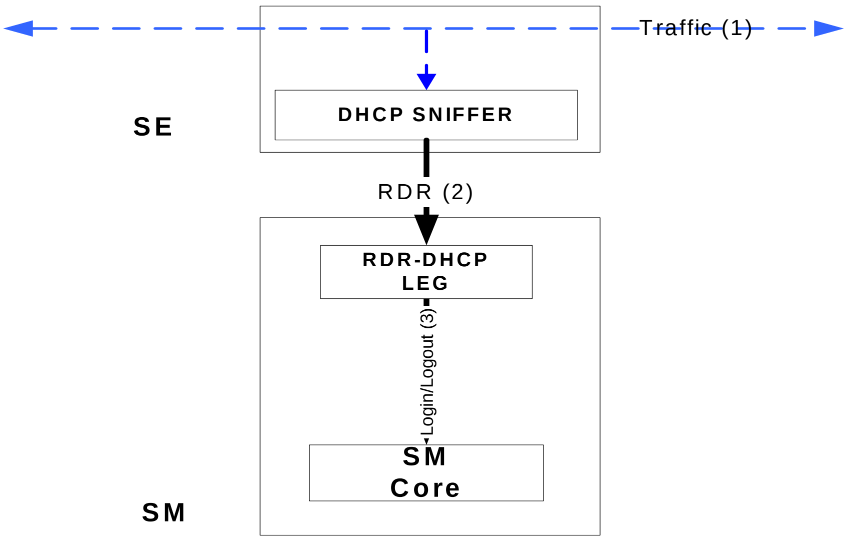

Figure 2: RDR DHCP LEG Sequence Operation

Release SCMS SM 2.5

Porting the SCMS SM to Linux

Previous versions of the SCMS SM ran only on Solaris 8. Version 2.5 offers the option of running the SCMS SM software on Red Hat Linux AS 3.0 and ES 3.0 (and up).

The following components of the SCMS SM SW package were ported to Linux:

- SCMS SM SW and the Command Line Utilities (CLU)
- SCMS SM Java and C / C++ APIs
- RADIUS Listener LEG
- Upgrade and installation procedures and Veritas agents
- 3rd party SW packages, such as the TimesTen In-Memory database and the Veritas Cluster Server

The CNR LEG was NOT ported and it continues to run on Solaris and Windows only.

SCMS SM Capacity Increase

Cisco is currently involved in very large deployments were the SCMS SM is required to support more than 1 million active subscribers in a single SCMS SM machine.

SCMS SM 2.5 supports deployments of up to 3 million subscribers on a single SCMS SM machine. This number of subscribers requires a strong machine with more than 2Gbyte of RAM.

This capability of increased number of subscribers requires a 64-bit machine for the SCMS SM. The increased capacity is supported on Solaris\Sparc machines, while Linux\X86 is normally used with 32-bit machines.

Reliable SCMS SM Java API

In SCMS SM 2.5 the Java SCMS SM API was updated to support a reliable connection. That is, if the connection fails, the logon operations are stored in a buffer and re-sent when the connection is re-established. Furthermore, the Java SCMS SM API now includes a feature of automatic re-connect to the SCMS SM with no intervention needed by the API user.

Issues to Note in Version SCMS SM 2.5

Backward Compatibility with SCOS

SCMS SM 2.5 can operate with SCE platforms that run SCOS versions 2.0.6 and up . This was implemented for cases were the service provider wants to deploy SCMS SM 2.5 (for Linux support for example), but continue to operate SCE platforms with SCOS 2.0.6 and up.

Installing SCMS SM 2.5

In SM 2.5, the installation script checks which operating system it runs on, and installs the relevant components accordingly.

The following parameters are available for the installation:

Usage: **`install-sm.sh [-h] [[-d INSTALLDIR] | -o] [-v VARDIR] [-n] [-m] [-j]`**

Options (switches):

`-d INSTALLDIR`

Select install directory for ~pcube the default is <*`default_installdir`*>. The directory must not exist prior to installation.

`-o`

Use an existing home of user pcube. The flags **`-d`** and **`-o`** cannot be used together

`-v VARDIR`

Indicate a directory for data storage. The default is *`INSTALLDIR/var`*. The directory should not exist prior to installation, and must be on a partition with at least 1GB of free space.

`-n`

Do not install TimesTen.

`-m`

Do not install SM DSN for TimesTen.

`-j`

Do not install JRE (Java Runtime).

`-32`

Install 32bit version.

`-h`

Print this help and exit.

Note The 64-bit TimesTen/JRE versions will be installed unless '-32' option was used

Note `-j` and `-32` are new installation options

Note When installing SM 2.5, a JRE package is installed under the `pcube h`ome directory.

Upgrading to a New Software Release

SM 2.5 includes upgrade procedures from SM 1.5, 2.0 and 2.2 to the SM 2.5 version. Please refer to the SM 2.5 User Guide for a detailed description of these procedures.

The following table summarizes upgrade support from different versions to various distributions of SM 2.5:

Table 1 Upgrade Support Table

To: From:	Solaris 32bit 2.5	Solaris 64 bit 2.5	Linux 32 bit 2.5
Solaris 32bit 1.5	×	✓	×
Solaris 32bit 2.0	×	✓	×
Solaris 32bit 2.2	✓	✓	×
Solaris 32bit 2.5	✓	✓	×
Solaris 64bit 2.5	×	✓	×
Linux 32bit 2.5	×	×	✓

Note SM 2.5 supports upgrade to a newer version of TimesTen 32bit version for customers with existing 32bit deployments and no need for a subscriber database larger than 2GB RAM.

Note When upgrading to ANY distribution of Solaris, a 64bit JRE 64bit package is installed.

Note To upgrade from 32bit to 64bit TimesTen database, a 64bit version installation is required. Therefore, the subscribers are exported and imported again after the 64bit version is installed.

Note Default upgrade option: 32bit for 32 bit versions, and 64bit for 64bit versions. The exception is upgrade from SM 2.0 (32bit) when the TimesTen version needs upgrade from 4.5 to 5.0. In this case, the 64bit version is installed by default.

Note It is not possible to downgrade from the 64bit version to the 32bit version.

Upgrade Options

Syntax:

```
./upgrade-sm.sh [-d] [-p] [-64] [-h]
```

Options (switches):

`-d`	destroy database during upgrade
`-p`	pause the upgrade for PQI installation
`-64`	upgrade to 64bit version
`-h`	show this message

Changes in the CLU

p3net

- The *domain* option was removed
- A new **`–detail`** option was added. This option is used with **`–show-all`** option order to display detailed info about all SCE platforms in table format

p3sm

- The **`--show-logging`** option was removed. The information it presented is now presented under **`p3sm –show CLU`**.
- A **`--remote=IP[:port]`** option was added. It is used with the **`--load-config`** option for loading the local configuration file to the local and remote SMs.
- A **`--detail`** option was added. It is used with the **`–sm-status`** option to display a detailed view of the status of the SCMS SM.
- A **`--wait`** option was added. It is used with **`--start`** or **`--restart`** for signaling to the CLU that it should return only when the SCMS SM is up.

p3db

- A **`--keep-in-mem`** SECS option was added. This option sets a timeout for saving the database in the shared-memory from the time the last connection to the DB is down. This improves the SCMS SM restart time.
- A **`--duplicate --local=<LOCAL_MACHINE> --remote=<REMOTE_MACHINE>`** option was added. This option copies the data-store from the "remote" machine to the "local" machine

Open Caveats

Upgrade of SCMS SM Fails due to Shell Message on su

- Cisco number CSCsb38557

When the upgrade-*sm.sh script* is run, it checks the existing SM version by running an SM CLU. This CLU is run under the user *pcube* privilege using the *su* command. In some shells, a message is displayed before the operation result, which confuses the script.

Workaround: When running the "*su – pcube …*" command, make sure the shell used for the user *pcube* does not display the OS version.

Restart of SCMS SM Sun Machine Required after Time Change

- Cisco number 7426

  After changing the time on the machine running the SCMS SM, the operator must manually restart the SCMS SM. If the machine is not restarted, it may not be possible to log into the SCMS SM from any of Cisco's Management clients.

Deleted Subscribers Manually Configured

- Cisco Number 9134

  If an SCE platform is part of an SCMS SM domain, and it is also configured directly with subscriber through CLI, the SCMS SM will perform synchronization of the SCE platform subscriber database and will erase the subscribers that were manually configured.

  Workaround: Be aware of this caveat when designing and configuring the system.

Clearing the Subscriber Information in the SCMS SM

- Cisco Number 9570

  When the *`SM-LEG Failure Handling`* parameter in the SCMS SM configuration file is configured to *`Clear_ all_ mappings= true`*, the subscriber information that was manually entered using CLU commands is also erased.

  Workaround: Be aware of this caveat when designing and configuring the system.

Solaris Time Zone and Locale Prerequisites

- Cisco Number: n/a

  Setting the time zone and locale should be done through editing the /etc/TIMEZONE configuration file.

  Note that changes in this file require a reboot to take effect.

Time zone

- Cisco Number: n/a

  Setting the OS time zone as offset from GMT in POSIX format is not supported and may lead to corrupted log files.

  It is best to set the time zone by country name, for example:

TZ=Israel

Note If GMT offset must be used, use the "zoneinfo" format by attaching a **`:Etc/`**' prefix, for example **`TZ=:Etc/GMT+5`**

Locale

- Cisco Number: n/a

  For correct SCMS SM operation, English locale must be used. The easiest way to set it is by adding the line

  ```
  LANG=en_US
  ```

  To the **`/etc/TIMEZONE`** configuration file

Standby SCMS SM Failure Status

- Cisco Number 12383

  When the standby SCMS SM fails, the Veritas agent notes the user on that through a “monitor time-out” status notification.

SM-LEG Failure Handling is Not Operational in SM 2.5.1 & 2.5.2.

- Cisco Number 13682

  When SM-LEG Handling feature is enabled (*`clear_all_mappings`* is set to true) and the LEG is associated to a domain (LEG-Domains Association section), the SM will start the “clear-all-mappings” timer on valid disconnections of the LEG.. A “valid disconnection” is, for example, when a LEG is restarted. In this case, if the LEG does not reconnect within the timeout, the SM clears all of the mapping in the domain.

  For other types of failures, for example, a crash of the machine running the LEG, or a network disconnect between the LEG and the SM, the failure is ignored!

  Based on this caveat, it is recommended not to use this functionality. Note that this functionality is disabled by default.

Obtaining Technical Assistance

Cisco provides Cisco.com (on page 22) 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 22), 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.