Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 3.0.6A

March, 2007

Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 3.0.6A

Covers: SCMS SM 3.0.6A, SCMS SM 3.0.6, SCMS SM 3.0.5, SCMS SM 3.0.3, SCMS SM 3.0.1, SCMS SM 3.0.0

OL-8956-09

These release notes for the Cisco SCMS SM describe the enhancements provided in Cisco Release SCMS SM 3.0.6A. These release notes are updated as needed.

For a list of the caveats that apply to Cisco Service Manager (SCMS SM) 3.0.6A, see *Open Caveats* (on page 28).

CISCO SYSTEMS

Contents

Introduction

Cisco is proud to release version 3.0.6A of the Subscriber Manager software component.

SCMS SM 3.0.6A is a point release of the Subscriber Manager. 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 resolved issues of the SM 3.0.6A release. It 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 3.0.6A

Note SM 3.0.6A is released as build 34 of version 3.0.6.

Supported Operating Systems and Platforms

The following table details which operating systems and platforms are supported by the SM.

Component	Red-Hat ES\AS 3 On Intel architecture (32-bit)	Red-Hat ES\AS 4 On Intel architecture (32-bit)	Solaris 8 On SPARC architecture (64-bit)	Solaris 9 On SPARC architecture (64-bit)
SM VCS agents SCE-Sniffer RADIUS LEG SCE-Sniffer DHCP LEG RADIUS Listener LEG DHCP Lease Query LEG SM Java API SCE Subscriber API SOAP LEG	Supported	Supported	Supported	Supported
CNR LEG	Not Supported	Not Supported	Supported	Not Supported
SM C/C++ API	Supported	Not Supported	Supported	Not Supported
MPLS-VPN BGP LEG	Supported	Not Supported	Not Supported	Not Supported

Release Notes for Cisco Service Control Management Suite **Subscriber Manager (SCMS SM) 3.0.6A**

Resolved Issues

Subscribers cannot be Viewed or Modified by the SCA BB Console if Subscriber Name Case Sensitivity is turned off

- Cisco number: CSCsh36629

  Subscribers cannot be viewed or modified in the SCA BB Console when the *subscriber_id_case_sensitivity* parameter is set to **no** in the SM configuration file.

  This issue is fixed in the SM in release 3.0.6A.

Some SM API Methods have no Effect if Subscriber Name Case Sensitivity is turned off

- Cisco number: CSCsh43356

  When the *subscriber_id_case_sensitivity* parameter is set to **no** in the SM configuration file, the following SM API methods have no effect if the subscriber name parameter is not in lower case:

  - `removeCustomProperties`
  - `subscriberLoggedIn`
  - `removeSubsciber`
  - `logoutByName`
  - `logoutByNameFromDomain`
  - `getSubscriberNamesWithPrefix`
  - `getSubscriberNamesWithSuffix`

  When the *subscriber_id_case_sensitivity* is set to **no** in the SM configuration file, the following CLU commands have no effect if the subscriber name argument is not in lower case:

  - **p3subs --remove**
  - **p3subs --remove-mappings**

  This issue is fixed in the SM in release 3.0.6A.

PRPC Authentication does not work when there is NAT/Firewall between the SCA BB Console and the SM/SCE/CM

- Cisco number: CSCsh39763

  SCA BB Console authentication will fail when trying to connect to the SCE/SM/CM if there is a device located between the console and the SM/CM/SCE that changes their IP addresses; for example a NAT. The problem occurs when the PRPC security level on the SM/SCE/CM is configured to "semi" or "full".

  In addition, unauthenticated RPC sessions at the SM/CM/SCE are not closed.

  This issue is fixed in release 3.0.6A. The SM, SCE, CM, and the SCA BB Console must be upgraded to 3.0.6A to fix the problem.

RADIUS Listener—Login fails in certain circumstances

- Cisco number: CSCsh83365

  When using the RADIUS Listener LEG, RADIUS accounting events normally create a subscriber login to the SM. When the following conditions are met, the RADIUS accounting events are ignored and a login does not occur:

  - The RADIUS attribute for package assignment is 26: Vendor Specific Attributes (VSA).

  - The accounting packet contains the VSAs, but does not contain the VSA with the vendor-Id and sub-attribute that is needed for package assignment.

  This issue is fixed in the SM in release 3.0.6A.

Release SCMS SM 3.0.6

Supported Operating Systems and Platforms

The following table details which operating systems and platforms are supported by the SM.

Component	Red-Hat ES\AS 3 On Intel architecture (32-bit)	Red-Hat ES\AS 4 On Intel architecture (32-bit)	Solaris 8 On SPARC architecture (64-bit)	Solaris 9 On SPARC architecture (64-bit)
SM VCS agents SCE-Sniffer RADIUS LEG SCE-Sniffer DHCP LEG RADIUS Listener DHCP Lease Query LEG SM Java API SCE Subscriber API SOAP LEG	Supported	Supported	Supported	Supported
CNR LEG	Not Supported	Not Supported	Supported	Not Supported
SM C/C++ API	Supported	Not Supported	Supported	Not Supported
MPLS-VPN BGP LEG	Supported	Not Supported	Not Supported	Not Supported

Functional Enhancements

Removal of Inactive Subscribers

The Inactive Subscriber Removal feature facilitates the removal of subscribers who have been logged out of the SM and are not mapped to any network-Id for a configurable time period. Effective use of this mechanism can keep the size of the SM database relatively small and close to the number of active subscribers.

See the *Cisco SCMS Subscriber Manager User Guide* for further details.

Resolved Issues

The p3subsdb --remove-all-ip/vlan/mpls-vpn CLU fails

- Cisco number: CSCsh06728

  The **p3subsdb --remove-all** CLU fails for all mapping types. The following output is displayed:

  ```
  bash-3.00$ p3subsdb --remove-all-ip
  Error - Failed to remove the mappings
  removeAllMappings
  bash-3.00$ p3subsdb --remove-all-vlan
  Error - Failed to remove the mappings
  removeAllMappings
  bash-3.00$ p3subsdb --remove-all-mpls-vpn
  Error - Failed to remove the mappings
  removeAllMappings
  ```

  This issue is fixed in 3.0.6.

U.S. Daylight Saving Time Policy Changes

- Cisco number: CSCsh20239

  From March 2007, Daylight Saving Time (DST) in the U.S. will start three weeks earlier and end one week later. The start date will change from the first Sunday in April to the second Sunday in March. The end date will change from the last Sunday in October to the first Sunday in November.

  This has an impact on the aggregation time calculation in the Quota Manager, the displays of timestamps/lease-times, and timestamps in logs.

  This issue is fixed in the SM in release 3.0.6.

SCE Subscriber API is not Backward Compatible for Quota Management

- Cisco number: CSCsh22372

  The 3.0.5 release of the SCE Subscriber API cannot handle quota indications from SCEs with releases prior to 3.0.5.

  This issue is fixed in 3.0.6. The SCE Subscriber API can handle quota indications from previous releases of the SCE (3.0.0, 3.0.1, 3.0.3, 3.0.4, 3.0.5).

SCE Subscriber API Provides the Wrong Version Number

- Cisco number: CSCsg85375

    The SCE Subscriber API contains the `getAPIVersion()` method. This method returns the version number of the SCE Subscriber API. In version 3.0.5, it returns the string "SCE Subscriber API 3.0.3 build 30".

    This issue is fixed in 3.0.6.

Release SCMS SM 3.0.5

Supported Operating Systems and Platforms

The following table details which operating systems and platforms are supported by the SM.

Component	Red-Hat ES\AS 3 On Intel architecture (32-bit)	Red-Hat ES\AS 4 On Intel architecture (32-bit)	Solaris 8 On SPARC architecture (64-bit)	Solaris 9 On SPARC architecture (64-bit)
SM VCS agents SCE-Sniffer RADIUS LEG SCE-Sniffer DHCP LEG RADIUS Listener DHCP Lease Query LEG SM Java API SCE Subscriber API SOAP LEG	Supported	Supported	Supported	Supported
CNR LEG	Not Supported	Not Supported	Supported	Not Supported
SM C/C++ API	Supported	Not Supported	Supported	Not Supported
MPLS-VPN BGP LEG	Supported	Not Supported	Not Supported	Not Supported

Functional Enhancements

Quota Manager in the SM

Cisco provides a basic Quota Manager that enables you to control all of the subscribers' service buckets in real-time based on pre-configured quota rules. The Quota Manager resides in the SM process and controls subscriber quota via the SM. The Quota Manager capabilities complement the existing SCA BB internal quota management.

Quota allocation at the beginning of an aggregation period can be spread over time for different subscribers to avoid the buildup of traffic bursts.

See the *Cisco Quota Manager Solution Guide* for additional information.

PRPC Authentication in PRPC Protocol Level

The SCA BB console has been enhanced with the ability to authenticate the connection using the PRPC server on the SCE/SM/CM without the need for an external FTP server. It uses encrypted passwords to perform this operation.

The SM requires users and passwords to be added using the p3rpc CLU in order to be able to connect to the SCA-BB console.

The SCE uses the user-names and passwords based on the SCE AAA configuration.

See the *Cisco SCMS SM User Guide* for more information.

Note The SM and SCE subscriber API do not perform PRPC authentication when connecting to the SCEs; therefore, when using an SM or an SCE Subscriber API implementation, you cannot configure the security level in the SCE to be more than **semi**. I.e. configuring the security level in the SCE to **full** will cause the SCE to reject the SM connection.

Note The SM API and CNR LEG do not perform authentication when connecting to the SM; therefore, when using an SM API implementation or a CNR LEG, you cannot configure the security level in the SM to be more than **semi**. I.e. configuring the security level in the SM to **full** will cause the SM to reject SM API/CNR LEG connections.

RADIUS LEGs—Subscriber IP Extraction Enhancements

The RADIUS Listener and SCE-Sniffer RADIUS LEG are able to extract the subscriber IP address from a string or integer encoded RADIUS attribute, or if not configured, to extract the subscriber IP address from the Framed-Route or Framed-IP-Address attribute.

See the *Cisco SCMS SM RADIUS Listener Reference Guide* or the *Cisco SCMS SCE-Sniffer RADIUS LEG Reference Guide* for additional information.

SCE-Sniffer DHCP LEG—Supports CMTS IP-address for Package Association

The SCE-Sniffer DHCP LEG supports the ability to use the CMTS-IP (from the *giaddr* field of the DHCP packet header) for package association in addition with other DHCP options from the DHCP packets. This ability is not supported by the DHCP Lease Query LEG because this information cannot be sent using the DHCP Lease-Query protocol.

Subscriber-Id Case-Sensitivity Control

The user can configure whether the SM handles subscriber-Ids in a case-sensitive (default) manner or not. If the SM is case-insensitive, the service control solution views subscriber-Ids as being all lower-case.

Support for Subscriber IDs of up to 64 Characters

The supported subscriber-Id length was increased from 40 characters to 64 characters.

This feature can be used only with the SM 3.0.6 database structure; i.e., if you perform a clean install of 3.0.6, or if you perform the following procedure (requires SM downtime) on an upgraded SM:

To support Subscriber IDs of up to 64 characters:

Step 1 (Cluster setup) Stop the cluster using **hastop**.

Step 2 Export all of the subscriber data.

Step 3 Destroy the replicated (subscriber) database—In cluster setups, destroy the replicated database on both nodes.

Step 4 Load the SM to create the database tables

Step 5 (Cluster setup) Set the replication scheme using **p3db --set-rep-scheme**.

Step 6 (Cluster setup) Start the replication agent using **p3db --rep-start**.

Step 7 Import the subscriber data.

Step 8 (Cluster setup) Start up the cluster using **hastart**.

SOAP LEG

The SOAP LEG enables querying an external application server using SOAP and retrieving the subscriber data such as policy. Cisco provides a WSDL file that describes the interface used by the LEG to query the application server. This interface must be implemented on the server.

See the *Cisco SCMS SM SOAP LEG Reference Guide* for additional information.

Quota Indications are not Generated on the Standby SCE of a Cascade Pair

Starting from release 3.0.5, all quota indications are not generated on the standby SCE of a cascade pair. This eliminates the generation of network messages that have no impact on the subscriber quota. After failover, the new active machine will start to generate quota indications.

Resolved Issues

GUI Clients Require Login Authentication to SCE and SM with PRPC

- Cisco number: CSCpu10863

  GUI clients now require login authentication with PRPC when logging in to the SCE and the SM.

  This issue is fixed in 3.0.5. See *PRPC Authentication in PRPC Protocol Level* (on page 12).

SM-SCE Synchronization when Subscribers are in the SCE with no Mappings Causes Errors

- Cisco number: CSCsg32651

  The following error message appears in the SM server log file:

  ```
  com.pcube.management.framework.rpc.RpcErrorException: VLAN
  subscribers are not supported by the current tunneling mode
  ```

  This exception occurs when the SM synchronizes the SCE in pull mode while the SCE has subscribers that are not mapped to any IP/VLAN. This causes the SM to logout the subscriber from the SCE with the IP 0.0.0.0 and VLAN 0 which causes the error from the SCE.

  The SCE might have subscribers with no mappings if one of the following happens:

  1. The remove-all-mappings on timeout since SM disconnection feature is used.

  2. A subscriber was added to the SCE via CLI/import with no mapping.

  This issue is fixed in 3.0.5.

SCE API does not Connect to SCEs with an Underscore in their Name

- Cisco number: CSCsg45985

  The SCE API does not support underscores in the API name.

  The following error message appears when trying to create an instance of the SCE Subscriber API containing an underscore in the name:

  ```
  apiName parameter cannot have under-scores
  ```

  For example:

  PRPC_SCESubscriberApi api = new PRPC_SCESubscriberApi ("name_with_underscore",

  "1.1.1.1");

  This issue is fixed in 3.0.5.

Scripts added for bash and csh User Profiles

- Cisco number: CSCsg28893

  The SM installation/upgrade scripts do not add user profile scripts for bash and csh. The purpose of the user profile scripts is to allow using the SM CLU from every location under the ~pcube folder.

  This issue is fixed in 3.0.5.

Note The installation adds these scripts if such scripts do not exist on the machine during installation.

Slow Logon Rates to the SCE and Apply Failures

- Cisco number: CSCsf32818

  The management agent in the SCE runs a thread that is responsible for performing different operations if the SM/SCE subscriber API connections are down for more than a configurable timeout. The management agent fails to kill this thread at the end of its run; thus, when there is a high number of disconnections, a large number of threads are created and the free memory of the JVM is reduced to a point where the garbage collection takes a significant time and causes performance degradation.

  The problem symptoms are:

- Failure to apply application configuration

- Reduction in the rate of logon operations on the SM/SCE subscriber API. This can be verified by running the **netstat -a** command on the SM/SCE API machine. The TCP window for the SCE experiencing the described problem is decreased to 0 as shown in the following example:

```
Local Address Remote Address      Swind Send-Q Rwind Recv-Q State

...

sm01.58305    215.193.18.81.14374 40960 0 49664 0 ESTABLISHED

sm01.58305    215.193.18.82.14374     0 0 49664 0 ESTABLISHED
```

  This issue is fixed in 3.0.5.

Configuration Errors in Boot are not Visible

- Cisco number: CSCpu14108

  Configuration errors that occur during the SM boot are not displayed when running the **p3sm --sm-status** CLU.

  This issue is fixed in SM 3.0.5.

Release Notes for Cisco Service Control Management Suite **Subscriber Manager (SCMS SM) 3.0.6A**

> **Note** Configuration errors do not appear in the status message after running **p3sm --load-config** because they are displayed immediately after the load command.

SM Cluster Database Error during Upgrade Procedure from 3.0.0/1 to 3.0.3

- Cisco number: CSCse56761

  After the SM upgrade, the SM database is not initialized correctly. The following error appears after running p3sm --sm-status:

  ```
  [TimesTen][TimesTen 5.1.28 ODBC Driver][TimesTen]TT2211:
  Referenced column RD not found -- file "saCanon.c", lineno
  5284, procedure "sbPtTblScanOfColRef()"
  ```

  This issue is related to performing cluster installation upgrades from SM version 3.0.0 or 3.0.1 to SM version 3.0.3.

  This issue is fixed in the upgrade to 3.0.5.

The PRPC Server on the SCE is not Enabled by Default

- Cisco number: CSCse63556

  It is necessary to enable the PRPC server on the SCE by default.

  This issue is fixed in SM 3.0.5.

Every DHCP Sniffer and Lease Query LEGs Login adds Information to SM Userlog

- Cisco number: CSCse77234

  During default package assignment, the following message may appear in the userlog:

  ```
  2006-09-11 14:39:44 | INFO  | SM    | Assigned a default
  package to 000004650000 (package ID 100)
  ```

  ```
  logon_login_enable is set to false
  ```

  This issue is fixed in SM 3.0.5.

Incorrect Version Number for Folder Name of SM API

- Cisco number: CSCse44077

  When extracting the SM API distribution files (C or Java), a folder is created with the name of the release version and the build number. The values of the release version and build

number are wrong because they contain only two out of the three digits that identify the release version.

This issue is fixed in SM 3.0.5.

SM 2.5.1 Installation Fails on "groupadd pcube"

- Cisco number: CSCpu13950

The SM 2.5.1 installation fails on `groupadd pcube` because */usr/sbin* is not in the su PATH.

This issue is fixed in SM 3.0.5.

setReconnectTimeout Description not in Programmer Guide

- Cisco number: CSCse45294

The setReconnectTimeout method is not described in the *Cisco SCMS SM C/C++ API Programmer Guide*.

This issue is fixed in SM 3.0.5.

SM C/C++ API Deadlock During Connection Handshake

- Cisco number: CSCse79735

A deadlock can occur when the API client tries to connect to an SM that is responding very slowly. The deadlock is a recursive mutex lock.

This can occur either when the server side is heavily loaded and responding slowly to requests, or when the server side closes the connection when the client tries to reconnect.

This issue is fixed in SM 3.0.5.

Logins Fail with Sniffer LEGs with Domain Aliases after SM Restart

- Cisco number: CSCsf02532

This issue is relevant only to Sniffer LEG integration.

When the configuration includes domain aliases and the DHCP or RADIUS Sniffer LEG is in use, an SM restart may end with login failures.

After the restart, the configuration is loaded in a sequence that fails to load the configuration that includes the domain aliases.

This issue is fixed in SM 3.0.5.

SM-SCE Connection Remains Down after Changing Machine Time

- Cisco number: CSCsf99474

  After changing the time on the SM and then loading a configuration file with the SCEs configured, the SM-SCE connection which was down may stay down. Every new SM-SCE connection may also stay down.

  This issue is fixed in SM 3.0.5.

Performing Login with NULL Network-Id and isAdditive Flag set to False should Logout the Subscriber

- Cisco number: CSCse16642

  When invoking the `login` API method with the `network-Id` set to `NULL` and the `isAdditive` field set to `false`, the subscriber should be logged out from the SCE because it does not have any mappings. However, the subscriber remains in the SCE with no mappings, which is meaningless.

  This issue is fixed in SM 3.0.5.

SM-SCE Synchronization is Aborted when Clearing the DB

- Cisco number: CSCpu14132

  If you run **`p3subsdb --clear-all`** while the SM-SCE synchronization operation is being performed, the synchronization operation is aborted and the SM-SCE connection will remain not active. If you subsequently perform a manual synchronization, the synchronization appears to be successful, but it is not successful.

  This issue is fixed in SM 3.0.5.

Management Agent may not follow Time Zone Setting if Changed after Startup in SCE

- Cisco number: CSCpu09531

  If the time zone is modified as part of the startup configuration (at boot time), this may affect the agent. Also, if the user changes the time zone using the config command (via CLI), this may affect the management agent.

  This issue is fixed in SM 3.0.5.

PRPC Disconnects after Date and Time are Changed

- Cisco number: CSCse16642

  When the time is changed on the SCE, the PRPC server sometimes disconnects and reconnects.

  This issue is fixed in SM 3.0.5.

Release SCMS SM 3.0.3

Supported Operating Systems and Platforms

The following table details which operating systems and platforms are supported by the SM.

Component	Red-Hat ES\AS 3 On Intel architecture (32-bit)	Red-Hat ES\AS 4 On Intel architecture (32-bit)	Solaris 8 On SPARC architecture (64-bit)	Solaris 9 On SPARC architecture (64-bit)
SM VCS agents SCE-Sniffer RADIUS LEG SCE-Sniffer DHCP LEG RADIUS Listener DHCP Lease Query LEG SM Java API SCE Subscriber API	Supported	Supported	Supported	Supported
CNR LEG	Not Supported	Not Supported	Supported	Not Supported
SM C/C++ API MPLS-VPN BGP LEG	Supported	Not Supported	Supported	Not Supported

Resolved Issues

SM C API does not support Auto-Reconnect

- Cisco number: CSCsc09509

  Although the auto-reconnect feature is supported internally by the API, the functionality is not exposed to users.

  This issue is fixed in SM 3.0.3. setReconnectTimeout is now part of the C API and a new parameter has been added to C++ initialization function.

SM C API closes connection when it receives a message that is too large

- Cisco number: CSCsc09601

  The retrieval functions of the SM C API (blocking flavor) support a return value whose maximum size is 100 KB. If a return value that is larger than 100 KB is requested, the API connection is terminated abnormally.

  This issue is fixed in SM 3.0.3. If the size of the return value is greater than 100 KB, the message is discarded and an error code is returned to all threads to indicate that the message was too large.

Protocol Pack Upgrades can Remove Package Information and Anonymous Subscribers

- Cisco number: CSCsd56995

  Some protocol pack upgrades (with spqi) require a tear-down of the SLI file followed by a load of the new SLI file. This operation causes the removal of anonymous subscribers from the SCE, and the removal of policy information from dynamic subscribers.

  This issue is fixed in SM 3.0.3. The SM re-synchronizes to the SCE when an application is loaded, regardless of the introduction mode.

Database logs Accumulate and Cause a Reduction in Free Disk Space

- Cisco number: CSCsd93885

  Once a minute the SM performs a procedure called "check-pointing" on the database in order to backup the in-memory image of the database to the disk (*.dsX). This task performs additional maintenance jobs on the database. Between check-points, the database writes the transactions to the transaction logs (*.logX) in addition to the in-memory database.

  The database is able to recover from power failures by using the last database check-point file and the transaction logs. As part of the check-point operation, the database removes the logs whose transactions were written to the check-point file.

  In versions 3.0.0 and 3.0.1, a bug caused by incorrect timeout calculations for the next check-point operation time resulted in a value indicating a timeout length of infinity. This caused the thread handling the check-points to hang. This failure causes the transaction logs to accumulate fill up the system hard disk.

  This issue is fixed in SM 3.0.3. The timeout calculation has been altered.

SCE Subscriber API—getSubscribersBulkResponse does not supply null iterator

- Cisco number: CSCsb09327

  This method is used during pull synchronization process when using the SCE Subscriber API. The method sends all parties currently found in the SCE, in bulks, according to a configured

bulk size. To signal the end of iteration, this method should return null, but instead it returns the value 0x00FFFFFF.

This issue is fixed in SM 3.0.3. The client side portion of the API now correctly returns null when the iteration ends.

Veritas Cluster Server reports an error when trying to monitor the SM status

- Cisco number: CSCsc00725

In a cluster installation, the Veritas cluster daemon periodically monitors the SM status. To do the monitoring, the agent of the Veritas Cluster Server uses a PRPC connection to the SM. If no PRPC connection is available, it assumes the SM is not functioning and triggers a failover.

This issue is fixed in SM 3.0.3. The agent of the Veritas Cluster Server attempts to monitor the SM status up to five times with a one second sleep between retries before triggering a failover.

IllegalArgumentException when using NetworkAndSubscriberID_BULK constructor

- Cisco number: CSCsd22656

When using the SCE Subscriber API NetworkAndSubscriberID_BULK class constructor with the Network ID argument set to NULL, an IllegalArgumentException is raised when it should be allowed.

This issue is fixed in SM 3.0.3. The NetworkAndSubscriberID_BULK class constructor accepts a null for the Network ID argument when the subscriber ID argument is not set to null.

addBulkEntry method of QuotaOperation_BULK class allows NULL quotaOperation argument

- Cisco number: CSCsd22734

When calling the addBulkEntry method of the SCE Subscriber API QuotaOperation_BULK class, the quotaOperation argument should not be set to NULL and setting it to NULL should not be allowed.

This issue is fixed in SM 3.0.3. An IllegalArgumentException is thrown if the quotaOperation argument is null.

Slow Login Rate In Pull-Mode When the support_ip_ranges Parameter is Set

- Cisco number: CSCsc83413

In pull-mode when the support_ip_ranges configuration parameter is set to true (non-default value) the user might experience significant degradation in login operation performance.

This issue is fixed in SM 3.0.3. Using the support_ip_ranges configuration parameter causes a reduction of up to 20% in subscriber management operations.

SCE-Sniffer RADIUS/DHCP LEGs stop functioning after an SCE reload

- Cisco number: CSCse06469

After a reload of the SCE or an installation of a SCA-BB PQI file on the SCE, the SM configures the SCE with sniffer related parameters. In some cases this configuration fails, so the sniffer functionality of the SCE is not set.

This issue is fixed in SM 3.0.3.

RADIUS Listener—External Package Association Does Not Work

- Cisco number: CSCsc80511

The system fails to determine the subscriber package based on the relevant RADIUS attribute. This is due to the missing configuration parameter in the [Radius.Property.Package] section of the p3sm.cfg configuration file.

This issue is fixed in SM 3.0.3.

Release SCMS SM 3.0.1

Resolved Issues

SM Upgrade Causes Loss of Subscriber Data

- Cisco number: CSCsc96279

  When the SM was upgraded from an earlier SM version, the SM lost all of the subscriber data that existed in the database prior to the upgrade.

  During the upgrade process the subscriber data is restored to the new database, but on the first boot of SM3.0, the SM identified the database structure as being inconsistent with the SM3.0 database structure and performed a recovery process. The inconsistency was due to database structure changes made as part of 3.0.0 release. To overcome the database inconsistency, the SM re-created all of the database tables, which caused the loss of the whole dataset information.

  This issue is fixed in SM 3.0.1, and the missing table is created on upgrade.

RADIUS Listener—Cannot assign subscriber ID based on a VSA attribute

- Cisco number: CSCsd22965

  When subscriber ID association was configured based on a VSA attribute, the SM could not load this configuration, and gave the following error:

  Error value <VSA attribute> for property radius_attribute_type in section [Radius.Subscriber ID]. Optional values: [integer,integer]

  This issue is fixed in SM 3.0.1.

SCE RADIUS Sniffer Stopped Abnormally

- Cisco number: CSCsd27022

  After a few minutes of sniffing RADIUS traffic, the SCE-Sniffer RADIUS module stopped generating RADIUS RDRs, due to an internal error while extracting RADIUS attributes from the RADIUS traffic.

  This issue is fixed in version 3.0.1 (in the SCA BB package that is installed on the SCE platform).

Release SCMS SM 3.0.0

Resolved Issues

Subscriber Database CLU p3db Duplicate Operation

- Cisco number: CSCsb29048

  In the previous release documentation, the local and remote parameters for the duplicate operation were configured to the local and remote hostnames respectively. The assignments of the remote and local parameters should have been configured to the alias names of the replication NICs in 2.5.x release. In Release 3.0.0 the user is obligated to define replication aliases names SM_REP1 and SM_REP2. The duplicate operation was simplified to automatically use these aliases, so the user only needs to run the `p3db -duplicate` command with no additional parameters. The 3.0.0 release documentation reflects this change.

Anonymous Subscriber Group Export

- Cisco number: CSCsb29129

  In previous releases, deleting an anonymous subscriber group could have caused a following export operation to miss a few anonymous subscriber groups in the .csv file. This issue was fixed.

Synchronization of Subscribers from the SM to the SCE Device

- Cisco number: CSCsb35773

  In previous releases during high load, the SM might have failed to synchronize subscribers to the SCE device because of problems in the thread execution order. This was solved in release 3.0.0.

Subscriber Registration using the SM-API

- Cisco number: CSCsb60373

  It takes several seconds, even in a high availability installation, for the VCS to detect that a TimesTen process is down. During this period, subscriber registration using the SM-API successfully completes, with no errors being reported. The subscribers are never properly registered.

  In release 3.0.0, the SM returns an error to the user application via the SM-API.

Release Notes for Cisco Service Control Management Suite **Subscriber Manager (SCMS SM) 3.0.6A**

Checking the Hostname IP Mapping Before Operating the DHCP Lease Query LEG

- Cisco number: CSCsb63593

  When the DHCP Lease Query LEG sends lease query request messages to the DHCP server, it identifies itself with the IP address that is mapped to its hostname. If the IP address is the loopback IP (127.0.0.1), the DHCP is not able to send a reply message back to the DHCP Lease Query LEG.

  It is recommended to ensure that the hostname of the SM Linux/Solaris machine is not mapped to the loopback IP address before loading and operating the SM and the DHCP Lease Query LEG.

  In release 3.0.0, an error message was added to the user log if the hostname is set to *localhost* and the published IP address is 127.0.0.1 . The `client_ip_address` parameter was added to `leaseq.cfg`, to enable the user to configure the desirable IP address. The default value is the *localhost* supplied by the operating system.. .

An Error Occurred When Using the p3sm CLU Command

- Cisco number: CSCsb71730

  In previous releases, an error might occur when running the p3sm command and the SM could not open a new RPC connection. The error was caused by exceeding the maximum allowed connections. The p3sm CLU command was enhanced to display a clear error message when the maximum number of allowed RPC connections is reached.

RADIUS Installation Not Supported by the SM Cluster

- Cisco number: CSCsb79708

  In SM-cluster installations, the virtual IP (VIP) address of the SM-cluster is configured as the forwarding address in the RADIUS server. When the RADIUS accounting messages are sent to the virtual IP address of the cluster, the return message is sent using the actual SM IP address, which is configured as the *localhost* of the SM machine. This might cause the RADIUS server to drop the message because of a conflict between the requests destination IP and the response source IP.

  The following list provides options to resolve this issue:

  - In release 3.0.0—Configure the RADIUS server with the virtual IP address of the SM, and configure the RADIUS Listener LEG to bind to this IP address using the new RADIUS Listener LEG configuration parameter. The 3.0.0 release documentation contains a description of this parameter.

  - Configure the RADIUS server with both SM machines' management IP address as redundant destinations. Only the active SM replies to RADIUS messages.

C/C++ API Limited in Retrieving a Message More Than 8KB

- Cisco number: CSCsb93029

  The SM C/C++ API is limited in retrieving a message that is more than 8KB in size, which limits retrieving subscribers that have more than 375 IP addresses. The size of the retrieving message was increased to 100K in release 3.0.0.

Changing the SM Configuration for support_ip_ranges Does Not Clear the Original Tables

- Cisco number: CSCsc04848

  In previous releases, when the SM configuration parameter support_ip_ranges is `changed from no to yes`, the existing IP addresses are not deleted from the database, and are kept in a table that is not used in this mode. If an attempt to remove a subscriber is performed, the operation fails because of the existing IP address in the abandoned table and might leave the subscriber record without part of the information it had previously contained.

  A similar problem could occur when changing this parameter from **yes** to **no** as well.

  This issue was fixed in release 3.0.0 by deleting all of the mappings from the not used table. This means that changing the `support_ip_ranges` parameter back and forth will cause the removal of all IP mappings from the SM database.

RPC Connection in a Non-active SM Machine

- Cisco number: CSCsc49312

  In previous releases, the LEG applications PRPC connections could connect while the Subscriber Manager operational state is in *Initialization*. In release 3.0.0, the SM is started in a state where the LEG applications are not allowed to be connected until the SM operational state switches to *Active*.

VCS installation - TimesTen Daemon Resource Argument

- Cisco number: CSCsc49687

  In previous releases, an error might occur when configuring the Veritas Cluster Server Process-On-Only resource that monitors the TimesTen Daemon. The error message that appears on the VCS console is "TimesTenDaemon:monitor:process was not found, restarting it" . This occurs when there is a white space in the arguments attributes.

  For example:

```
path-name =
/home/pcube/lib/tt/TimesTen/pcubesm22/bin/timestend

arguments = -initfd 13 (with a space before)
```

To resolve this issue, ensure that the arguments attribute does not contain any spaces before the arguments.

In release 3.0.0, leading white-spaces are ignored by the Veritas Cluster Agent.

Open Caveats

SCE-Sniffer RADIUS LEG doesn't work because no RDRs are generated by the SCE application

- Cisco number: CSCse19753

  After installing a SCA BB PQI file on the SCE 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 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.

SCE cascade pair does not exchange all quota information

- Cisco number: CSCsf97557

  The SCE cascade pair exchange only a portion of the quota information, this causes the failover in the SCE cascade topology to be stateless with regard to quota.

  On SCE failover, all of the subscribers go into an immediate breach state, which is the same as the use-case for a first subscriber login. As a result of the subscribers being in a breach state, the external server must provide quota to all active subscribers immediately after the failover.

  The first quota notification after failover also contains an incorrect quota report which must be ignored. Ignoring the quota report means that there is quota leakage of the quota used since the last periodic update.

After an SCE failover there may be many breach notifications which can cause performance issues in the quota manager and the APIs.

Workaround:

- Ignore the value of the first quota notification from a new SCE regarding each subscriber.

- The Quota Manager must assume that the bucket values in the new SCE are incorrect; therefore, the Quota Manager must set the correct quota value via the API.

Obtaining Technical Assistance

Cisco provides Cisco.com 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 any time, 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 *http://www.cisco.com*.

Technical Assistance Center

The Cisco Technical Assistance Center (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 30), go to *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 http://www.cisco.com/tac/c*aseopen.

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 *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.

Release Notes for Cisco Service Control Management Suite **Subscriber Manager (SCMS SM) 3.0.6A**