



SRC-PE Software

SRC XML API Configuration Reference

Release 3.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

This product includes the following software: Fontconfig, X FreeType library, X Render extension headers, and X Render extension library, copyright © 2001, 2003 Keith Packard.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Keith Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Keith Packard makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

KEITH PACKARD DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL KEITH PACKARD BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

SRC-PE Software SRC XML API Configuration Reference
Release 3.0.x
Copyright © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Linda Creed, Justine Kangas, Betty Lew
Editing: Fran Mues
Cover Design: Edmonds Design

Revision History
15 August 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.

- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License

("GPL") or the GNU Library General Public License ("LGPL")). Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

About This Guide

- SRC Guides and Release Notes on page v
- Audience on page v
- Documentation Conventions on page v
- Related Juniper Networks Documentation on page vii
- Obtaining Documentation on page ix
- Documentation Feedback on page ix
- Requesting Technical Support on page ix

SRC Guides and Release Notes

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with JUNOS routers and JUNOS routing platforms in an Internet access environment. We assume that readers know how to use the routing platforms, directories, and RADIUS servers that they will deploy in their SRC networks.

If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

Table 1 on page xviii defines the notice icons used in this guide. Table 2 on page xviii defines text conventions used throughout this documentation.

Table 1: Notice Icons





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2: Text Conventions

Convention	Description	Examples
Bold text like this	<ul style="list-style-type: none"> ■ Represents keywords, scripts, and tools in text. ■ Represents a GUI element that the user selects, clicks, checks, or clears. 	<ul style="list-style-type: none"> ■ Specify the keyword exp-msg. ■ Run the install.sh script. ■ Use the pkgadd tool. ■ To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must type.	<code>user@host# set cache-entry-age cache-entry-age</code>
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre>nic-locators { login { resolution { resolver-name /realms/ login/A1; key-type LoginName; value-type SaeId; } } }</pre>
Regular sans serif typeface	<ul style="list-style-type: none"> ■ Represents configuration statements. ■ Indicates SRC CLI commands and options in text. ■ Represents examples in procedures. ■ Represents URLs. 	<ul style="list-style-type: none"> ■ <code>system ldap server{ stand-alone;</code> ■ Use the <code>request sae modify device failover</code> command with the <code>force</code> option ■ <code>user@host# . . .</code> ■ <code>http://www.juniper.net/techpubs/software/management/src/api-index.html</code>
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<code>user@host# set local-address local-address</code>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <code>< gfwif ></code> .
Key name	Indicates the name of a key on the keyboard.	Press Enter.

Table 2: Text Conventions (*continued*)

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> ■ Emphasizes words. ■ Identifies book names. ■ Identifies distinguished names. ■ Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> ■ There are two levels of access: <i>user</i> and <i>privileged</i>. ■ <i>SRC-PE Getting Started Guide</i> ■ <i>o = Users, o = UMC</i> ■ The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \net.juniper.srmt.sae.plugin\RADIUSTrackingPluginEvent
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic line

Related Juniper Networks Documentation

With each SRC software release, we provide the *SRC Documentation CD*, which contains the documentation described in Table 3 on page xix.

A complete list of abbreviations used in this document set, along with their spelled-out terms, is provided in the *SRC —PE Getting Started Guide*.

Table 3: Juniper Networks C-series and SRC Technical Publications

Document	Description
Core Documentation Set	
<i>C2000 and C4000 Hardware Guide</i>	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
<i>C2000 and C4000 Quick Start Guide</i>	Describes how to get the C-series Controller up and running quickly. Intended for experienced installers who want to expedite the installation process.
<i>SRC-PE Getting Started Guide</i>	Describes the SRC software, how to set up an initial software configuration, how to integrate RADIUS servers, and how to upgrade the SRC software. It also explains how to manage a C-series Controller. The guide describes how to set up and start the SRC CLI and the C-Web interface, as well as other SRC configuration tools. It includes reference material for the SRC documentation.
<i>SRC-PE CLI User Guide</i>	Describes how to use the SRC CLI, configure and monitor the platform with the CLI, and control the CLI environment. The guide also describes how to manage SRC components with the CLI.

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
<i>SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP</i>	Describes how to use and configure the SAE, the NIC, and the SRC-ACP (Admission Control Plug-In) application. This guide also provides detailed information about using JUNOS routers, JUNOS routing platforms, and other network devices in the SRC network.
<i>SRC-PE Services and Policies Guide</i>	Describes how to work with services and policies. The guide provides an overview, configuration procedures, and management information. The guide also provides information about the SRC tools for configuring policies.
<i>SRC-PE Subscribers and Subscriptions Guide</i>	Describes how to work with residential and enterprise subscribers and subscriptions. The guide provides an overview, configuration procedures, and management information. This guide also provides information about the enterprise service portals, including the Enterprise Manager Portal.
<i>SRC-PE Monitoring and Troubleshooting Guide</i>	Describes how to use logging, the SNMP agent, the SRC CLI, and the C-Web interface to monitor and troubleshoot SRC components. This guide also describes the SNMP traps.
<i>SRC-PE Solutions Guide</i>	Provides high-level instructions for SRC implementations. The guide documents the following scenarios: managing QoS services on JUNOS routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); and mirroring subscriber traffic on JUNOS routers.
<i>SRC-PE CLI Command Reference, Volume 1</i> <i>SRC-PE CLI Command Reference, Volume 2</i>	Together constitute information about command and statement syntax; descriptions of commands, configuration statements, and options; editing level of statement options; and a history of when a command was added to the documentation.
<i>SRC-PE NETCONF API Guide</i>	Describes how to use the NETCONF application programming interface (API) to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software.
<i>SRC-PE XML API Configuration Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to configuration statements in the SRC command-line interface (SRC CLI).
<i>SRC-PE XML API Operational Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to operational commands in the SRC command-line interface (SRC CLI).
Application Library	
<i>SRC Application Library Guide</i>	Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, an application to provide threat mitigation, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, and an application to control volume usage .
Release Notes	

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
<i>SRC-PE Release Notes</i>	In the <i>Release Notes</i> , you will find the latest information about features, changes, known problems, resolved problems, supported platforms and network devices (such as Juniper Networks routers and CMTS devices), and third-party software. If the information in the <i>Release Notes</i> differs from the information found in the documentation set, follow the <i>Release Notes</i> .
<i>SRC Application Library Release Notes</i>	
Release notes are available on the Web.	

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To order a documentation CD, which contains this guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation CDs and at <http://www.juniper.net/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs]*)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf>.

- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at <https://tools.juniper.net/SerialNumberEntitlementSearch/>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Manager tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

Summary of SRC XML API Configuration Tag Elements

This document lists the configuration tag elements for the SRC XML API that are equivalent to configuration statements in the SRC command-line interface (SRC CLI). For information about the notation used in this document, see Table 2 on page vi. For information about the tag elements that client applications use to request, change, and commit configuration information, see the *SRC-PE NETCONF API Guide*.

Tag elements are listed in alphabetical order for the following components:

- CLI and System
- Juniper Networks Database
- SAE
- Network Information Collector (NIC)
- SNMP Agent
- Juniper Policy Server (JPS)
- Service API
- Policy API
- Subscriber API
- Redirect Server
- SRC Admission Control Plug-In (SRC-ACP)
- External Subscriber Monitor
- Dynamic Service Activator
- DIAMETER Application

CLI and System Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for controlling and using the SRC CLI environment and for managing the C-series Controller. The table lists the SRC CLI configuration commands and statements that have corresponding SRC XML tag elements, and maps each command or statement to its tag element. CLI configuration commands and statements are listed in alphabetical order.

CLI Configuration Command/Statement	Configuration Tag Element
commit	<u>< commit-configuration ></u>
copy	<u>< copy ></u>
delete	<u>< delete ></u>
insert	<u>< insert ></u>
interfaces	<u>< interface ></u>
interfaces name group	<u>< group ></u>
interfaces name group arp-monitoring	<u>< arp-monitoring ></u>
interfaces name tunnel	<u>< tunnel ></u>
interfaces name unit	<u>< unit ></u>
interfaces name unit unit-number family inet	<u>< inet ></u>
interfaces name unit unit-number family inet6 address	<u>< address ></u>
rename	<u>< rename ></u>
rollback	<u>< rollback-configuration ></u>
routing-options static route	<u>< route ></u>
set	<u>< set ></u>
show	<u>< get ></u>
slot	<u>< slot ></u>
system	<u>< system ></u>
system ipmi	<u>< ipmi ></u>
system ipmi user	<u>< user ></u>

system ldap client	<u>< client ></u>
system login	<u>< login ></u>
system login class	<u>< class ></u>
system login user	<u>< user ></u>
system login user user-name authentication	<u>< authentication ></u>
system ntp	<u>< ntp ></u>
system ntp authentication-key	<u>< authentication-key ></u>
system ntp broadcast	<u>< broadcast ></u>
system ntp multicast-client	<u>< multicast-client ></u>
system ntp peer	<u>< peer ></u>
system ntp server	<u>< server ></u>
system radius-server	<u>< radius-server ></u>
system services	<u>< services ></u>
system services editor	<u>< editor ></u>
system services editor policy-editor	<u>< policy-editor ></u>
system services netconf	<u>< netconf ></u>
system services ssh	<u>< ssh ></u>
system services web-management http	<u>< http ></u>
system services web-management https	<u>< https ></u>
system services web-management logger	<u>< logger ></u>
system services web-management logger name file	<u>< file ></u>
system services web-management logger name syslog	<u>< syslog ></u>
system static-host-mapping	<u>< static-host-mapping ></u>
system syslog file	<u>< file ></u>
system syslog file file-name	<u>< contents ></u>
system syslog host	<u>< host ></u>

system syslog host log-host-name	< contents >
system syslog user	< user >
system syslog user user-name	< contents >
system tacplus-server	< tacplus-server >

<commit-configuration>

Usage

```
<rpc>  
  <commit-configuration>  
    <check/>  
    <and-quit/>  
  </commit-configuration>  
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Commit the set of changes and cause the changes to take operational effect.

Contents

<check>— (Optional) Verify whether the syntax is correct, but do not apply changes.

<and-quit>— (Optional) Exit from configuration mode if the commit operation is successful.

Required Privilege Level

config-control

<copy>

Usage

```

<rpc>
  <copy>
    <parent1> parent1 </parent1>
    <identifier1> identifier1 </identifier1>
    <position> position-choice </position>
    <parent2> parent2 </parent2>
    <identifier2> identifier2 </identifier2>
  </copy>
</rpc>

```

Release Information

Command introduced in SRC Release 3.0.0

Description

Copy an existing configuration statement or identifier.

Contents

<parent1>— Path to an existing configuration statement or identifier.

Value—Path of a collection object

<identifier1>— Existing identifier or statement.

Value— Identifier or statement

<position>— Configuration path.

Value

- to— Transition.

<parent2>— Path to a new configuration statement or identifier.

Value—Path of a collection object

<identifier2>— New identifier or statement.

Value— Identifier or statement

Required Privilege Level

config-control

<delete>

Usage

```
<rpc>
  <delete>
    <force/>
    <object> object </object>
    <value> value </value>
  </delete>
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete a configuration statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.

Contents

<force>— Flag indicating that no confirmation is requested before the software clears the configuration.

Default—false

<object>— Name of the statement or identifier to delete.

Value—Path of a configuration object

<value>— Value of the statement to delete.

Value—Valid value for selected object

Required Privilege Level

config-control

<insert>

Usage

```
<rpc>
  <insert>
    <parent> parent </parent>
    <identifier1> identifier1 </identifier1>
    <position> position-choice </position>
    <identifier2> identifier2 </identifier2>
  </insert>
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Insert an identifier into an existing configuration hierarchy. You must configure the identifiers before you reorder them. The **insert** command does not create new identifiers.

Contents

<parent>— Path in the configuration hierarchy to an existing configuration statement.

Value— Hierarchy path

<identifier1>— Existing identifier.

Value— Name of existing identifier

<position>— Ordering of identifiers.

Value

- *after*— Place *identifier1* after *identifier2*.
- *before*— Place *identifier1* before *identifier2*.

<identifier2>— New identifier to insert.

Value—Valid value for selected object

Required Privilege Level

config-control

<interface> (configuration/interfaces)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <name>name</name> <!-- identifier -->
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure interfaces on the C-series platform.

Contents

<name>— Name of interface

Value— Interface name

Required Privilege Level

interface

<group> (configuration/interfaces/interface)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <group>
        <mode>mode-choice</mode>
        <downdelay>downdelay</downdelay>
        <updelay>updelay</updelay>
        <lacp-rate>lacp-rate-choice</lacp-rate>
        <mii-monitoring-interval>mii-monitoring-interval</mii-monitoring-
interval>
        <interfaces>interfaces</interfaces>
        <primary>primary</primary>
        <transmit-hash-policy>transmit-hash-policy-choice</transmit-hash-
policy>
      </group>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Ethernet interface group

Contents

<mode>—Grouping mode

Value

- `balance-rr`—Round-robin policy: Transmit packets in sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.
- `active-backup`—Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. When a failover occurs in active-backup mode, bonding will issue one or more gratuitous ARPs on the newly active slave.

One gratuitous ARP is issued for the bonding master interface and each VLAN interfaces configured above it, provided that the interface has at least one IP address configured. Gratuitous ARPs issued for VLAN interfaces are tagged with the appropriate VLAN id.

This mode provides fault tolerance. The primary option, documented below, affects the behavior of this mode.

- `balance-xor`— XOR policy: Transmit based on the selected transmit hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count]. Alternate transmit policies may be selected via the `xmit_hash_policy` option, described below. This mode provides load balancing and fault tolerance.
- `broadcast`— Broadcast policy: transmits everything on all slave interfaces. This mode provides fault tolerance.
- `802.3ad`— IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.

Slave selection for outgoing traffic is done according to the transmit hash policy, which may be changed from the default simple XOR policy via the `xmit_hash_policy` option, documented below. Note that not all transmit policies may be 802.3ad compliant, particularly in regards to the packet mis-ordering requirements of section 43.2.4 of the 802.3ad standard. Differing peer implementations will have varying tolerances for noncompliance.

- `balance-tlb`— Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
- `balance-alb`— Adaptive load balancing: includes `balance-tlb` plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server. Receive traffic from connections created by the server is also balanced. When the local system sends an ARP Request the bonding driver copies and saves the peer's IP information from the ARP packet. When the ARP Reply arrives from the peer, its hardware address is retrieved and the bonding driver initiates an ARP reply to this peer assigning it to one of the slaves in the bond. A problematic outcome of using ARP negotiation for balancing is that each time that an ARP request is broadcast it uses the hardware address of the bond. Hence, peers learn the hardware address of the bond and the balancing of receive traffic collapses to the current slave. This is handled by sending updates (ARP Replies) to all the peers with their individually

assigned hardware address such that the traffic is redistributed. Receive traffic is also redistributed when a new slave is added to the bond and when an inactive slave is re-activated. The receive load is distributed sequentially (round robin) among the group of highest speed slaves in the bond. When a link is reconnected or a new slave joins the bond the receive traffic is redistributed among all active slaves in the bond by initiating ARP Replies with the selected mac address to each of the clients. The updelay parameter (detailed below) must be set to a value equal or greater than the switch's forwarding delay so that the ARP Replies sent to the peers will not be blocked by the switch.

`<downdelay>`—(Optional) Specifies the time, in milliseconds, to wait before disabling a slave after a link failure has been detected. This option is only valid for the miimon link monitor. The downdelay value should be a multiple of the miimon value; if not, it will be rounded down to the nearest multiple.

Value—Integer in the range 0–2147483647 ms

`<updelay>`—(Optional) Specifies the time, in milliseconds, to wait before enabling a slave after a link recovery has been detected. This option is only valid for the miimon link monitor. The updelay value should be a multiple of the miimon value; if not, it will be rounded down to the nearest multiple.

Value—Integer in the range 0–2147483647 ms

`<lacp-rate>`—(Optional) Specify the rate in which we'll ask our link partner to transmit LACPDU packets in 802.3ad mode.

Value

- `slow`— Request partner to transmit LACPDUs every 30 seconds.
- `fast`— Request partner to transmit LACPDUs every 1 second.

`<mii-monitoring-interval>`—(Optional) Specifies the MII link monitoring frequency in milliseconds. This determines how often the link state of each slave is inspected for link failures. A value of zero disables MII link monitoring. A value of 100 is a good starting point. The `use_carrier` option, below, affects how the link state is determined.

Value—Integer in the range -2147483648–2147483647 ms

`<interfaces>`—(Multivalue) Ethernet interfaces in this group

Value—Text

`<primary>`—(Optional) The specified device will always be the active slave while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one slave is preferred over another, e.g., when one slave has higher throughput than another.

Value—Text

`<transmit-hash-policy>`—(Optional) Selects the transmit hash policy to use for slave selection in balance-xor and 802.3ad modes.

Value

- `layer2`— Uses XOR of hardware MAC addresses to generate the hash. The formula is (source MAC XOR destination MAC) modulo slave count. This algorithm will place all traffic to a particular network peer on the same slave. This algorithm is 802.3ad compliant.
- `layer34`— This policy uses upper layer protocol information, when available, to generate the hash. This allows for traffic to a particular network peer to span multiple slaves, although a single connection will not span multiple slaves. The formula for unfragmented TCP and UDP packets is ((source port XOR dest port) XOR ((source IP XOR dest IP) AND 0xffff) modulo slave count. For fragmented TCP or UDP packets and all other IP protocol traffic, the source and destination port information is omitted. For non-IP traffic, the formula is the same as for the layer2 transmit hash policy. This policy is intended to mimic the behavior of certain switches, notably Cisco switches with PFC2 as well as some Foundry and IBM products. This algorithm is not fully 802.3ad compliant. A single TCP or UDP conversation containing both fragmented and unfragmented packets will see packets striped across two interfaces. This may result in out of order delivery. Most traffic types will not meet this criteria, as TCP rarely fragments traffic, and most UDP traffic is not involved in extended conversations. Other implementations of 802.3ad may or may not tolerate this noncompliance.

Required Privilege Level

interface

<arp-monitoring> (configuration/interfaces/interface/group)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <group>
        <arp-monitoring>
          <interval>interval</interval>
          <ip-target>ip-target</ip-target>
        </arp-monitoring>
      </group>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

ARP link monitoring

Contents

<interval>— Specifies the ARP link monitoring frequency in milliseconds. If ARP monitoring is used in an etherchannel compatible mode (modes 0 and 2), the switch should be configured in a mode that evenly distributes packets across all links. If the switch is configured to distribute the packets in an XOR fashion, all replies from the ARP targets will be received on the same link which could cause the other team members to fail. ARP monitoring should not be used in conjunction with miimon.

Value—Integer in the range 1–2147483647 ms

<ip-target>—(Multivalue) Specifies the IP addresses to use as ARP monitoring peers when arp_interval is > 0. These are the targets of the ARP request sent to determine the health of the link to the targets. Specify these values in ddd.ddd.ddd.ddd format. At least one IP address must be given for ARP monitoring to function. The maximum number of targets that can be specified is 16.

Value—IP address

Required Privilege Level

interface

< tunnel > (configuration/interfaces/interface)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <tunnel>
        <mode>mode-choice</mode>
        <destination>destination</destination>
        <source>source</source>
        <key>key</key>
        <interface>interface</interface>
        <ttl>ttl</ttl>
      </tunnel>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a tunnel interface. A tunnel allows direct connection between a remote location and an application running on the C-series platform; a tunnel lets you use the redirect server in deployments where the JUNOS router does not have a direct connection to the C-series platform.

Contents

<mode>— Type of tunnel interface.

Value

- `ipip`— IP-over-IP. Encapsulates IP packets within IP packets.
- `gre`— GRE. Encapsulates traffic that uses various routing protocols within IP.
- `sit`— IPv6 in IPv4 tunnel

Default— No value

<destination>— IP address of the remote end of the tunnel.

Value—IP address
Default— No value

<source>—(Optional) Local IP address, that will not change, to receive tunneled packets.
 If you specify a source address, also specify a local interface.

Value—IP address
Default— No value

<key>—(Optional) For a GRE tunnel, a GRE key.

Value—Integer in the range -2147483648–2147483647
Default— No value

<interface>—(Optional) Existing physical interface. If you configured a source address, specify an interface.

Value— Name of interface.

Example: eth0

Default— No value

<ttl>—(Optional) Lifetime of tunneled packets.

Value—Integer in the range 1–255

Required Privilege Level

interface

<unit> (configuration/interfaces/interface)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <unit>
        <unit-number>unit-number</unit-number> <!-- identifier -->
      </unit>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logical interfaces on a physical Ethernet interface on the C-series platform. You can create different units to configure numerous IP addresses on an interface.

Contents

<unit-number>— Number of the unit (logical interface).

Value—Integer in the range 0–16385

Required Privilege Level

interface

<inet> (configuration/interfaces/interface/unit/family)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <unit>
        <family>
          <inet>
            <address>address</address>
            <broadcast>broadcast</broadcast>
          </inet>
        </family>
      </unit>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for IPv4.

Contents

<address>—(Optional) IP address with destination prefix for interface.

Value— IP address/destination prefix

Default— No value

<broadcast>—(Optional) Broadcast address.

Value—IP address

Default— No value

Required Privilege Level

interface

<address> (configuration/interfaces/interface/unit/family/inet6)

Usage

```
<configuration>
  <interfaces>
    <interface>
      <unit>
        <family>
          <inet6>
            <address>
              <address>address</address> <!-- identifier -->
            </address>
          </inet6>
        </family>
      </unit>
    </interface>
  </interfaces>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<address>—Interface address/destination prefix

Value— IP address/destination prefix

Required Privilege Level

interface

<rename>

Usage

```
<rpc>
  <rename>
    <parent> parent </parent>
    <identifier1> identifier1 </identifier1>
    <position> position-choice </position>
    <identifier2> identifier2 </identifier2>
  </rename>
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Rename an existing configuration statement or identifier.

Contents

<parent>— Path to an existing configuration statement or identifier.

Value—Path of a collection object

<identifier1>— Existing identifier or statement.

Value— Identifier or statement

<position>— Configuration path.

Value

- to— Transition.

<identifier2>— New identifier or statement.

Value—Valid value for selected object

Required Privilege Level

config-control

<rollback-configuration>

Usage

```
<rpc>  
  <rollback-configuration>  
  </rollback-configuration>  
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Return to a previously committed configuration.

Note: You can enter the **rollback** command only at the top level of the configuration hierarchy.

Required Privilege Level

config-control

<route> (configuration/routing-options/static)

Usage

```
<configuration>
  <routing-options>
    <static>
      <route>
        <destination>destination</destination> <!-- identifier -->
        <next-hop>next-hop</next-hop>
        <reject/>
      </route>
    </static>
  </routing-options>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure static routes to point to routers that connect to other networks to allow connectivity to devices on other networks.

Contents

<destination>— Destination network and mask. To configure the default route use destination 0.0.0.0/0

Value—Text

<next-hop>—(Optional) Address of next hop from the C-series platform to the destination.

Value—IP address

Default— No value

<reject>—(Optional) Drop packets to the specified destination, and send an ICMP unreachable message.

Required Privilege Level

routing

<set>

Usage

```
<rpc>
  <set>
    <object> object </object>
    <value> value </value>
  </set>
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Create a statement hierarchy and set identifier values. When you enter a **set** command, the current level in the hierarchy does not change.

Contents

<object>— Configuration statement or identifier

Value—Path of a configuration object

<value>— Value configured for a configuration statement.

Value—Valid value for selected object

Required Privilege Level

config-control

<get>

Usage

```
<rpc>  
  <get>  
    <object> object </object>  
  </get>  
</rpc>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about a configuration object.

Contents

<object>— (Optional) Configuration object for which to display information. The object can be a configuration statement or an identifier for a statement.

Value—Path of a configuration object

Required Privilege Level

config-view

<slot> (configuration)

Usage

```
<configuration>
  <slot>
    <number>number</number> <!-- identifier -->
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure slot number for component.

Contents

<number>— Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

Required Privilege Level

system

<system> (configuration)

Usage

```
<configuration>
  <system>
    <host-name>host-name</host-name>
    <domain-name>domain-name</domain-name>
    <domain-search>domain-search</domain-search>
    <name-server>name-server</name-server>
    <authentication-order>authentication-order-choice</authentication-order>
    <time-zone>time-zone</time-zone>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system properties.

Contents

<host-name>—Hostname for the C-series platform.

Value— hostname

Default— No value

<domain-name>—(Optional) Name of the domain in which the C-series platform is located. This is the default domain name that is appended to hostnames that are not fully qualified.

Value— domain name

Default— No value

<domain-search>—(Optional) (Multivalue) List of domains to search.

Value— domain name

Default— No value

<name-server>—(Optional) (Multivalue) Domain name server(s).

Value— name server

Default— No value

<authentication-order>—(Optional) (Multivalue) Order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order configured, until the password matches.

Value

- radius— RADIUS authentication
- tacplus—TACACS+ authentication services
- password—Traditional password authentication

<time-zone>—(Optional) Name of the local time zone.

Value— time-zone

Default—UTC

Required Privilege Level

system

<ipmi> (configuration/system)

Usage

```
<configuration>
  <system>
    <ipmi>
      <address>address</address>
      <gateway>gateway</gateway>
    </ipmi>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the IPMI interface.

Contents

<address>—(Optional) IP address/destination prefix of IPMI interface. You must enter a value for the C2000 Controller. For the C4000 Controller, the address is automatically set to the IP address of the eth0 unit 0 interface.

Value—Text

<gateway>— IP address of the gateway.

Value—IP address

Required Privilege Level

system

<user> (configuration/system/ipmi)

Usage

```
<configuration>
  <system>
    <ipmi>
      <user>
        <name>name</name> <!-- identifier -->
        <encrypted-password>encrypted-password</encrypted-password>
      </user>
    </ipmi>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<name>— Username that is used to login to the IPMI interface of a C-series platform

Value— username

<encrypted-password>— Password in encrypted format.

Value— Encrypted-password

Required Privilege Level

system

<client> (configuration/system/ldap)

Usage

```
<configuration>
  <system>
    <ldap>
      <client>
        <base-dn>base-dn</base-dn>
        <url>url</url>
        <backup-urls>backup-urls</backup-urls>
        <principal>principal</principal>
        <credentials>credentials</credentials>
        <timeout>timeout</timeout>
        <time-limit>time-limit</time-limit>
        <eventing/>
        <polling-interval>polling-interval</polling-interval>
        <connection-manager-id>connection-manager-id</connection-manager-id>
        <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        <event-base-dn>event-base-dn</event-base-dn>
        <signature-dn>signature-dn</signature-dn>
        <blacklist/>
      </client>
    </ldap>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure directory properties used by the CLI to connect to the directory that contains SRC data.

On a C-series platform, you use the Juniper Networks database and typically use the default configuration for the directory connection. You can add backup directories and change the password to the directory.

Contents

<base-dn>—(Optional) DN of the root directory for SRC components and applications.

Value— DN

Default—o = UMC

`<url>`—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—`ldap://127.0.0.1:389`

`<backup-urls>`—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— URL

Default— No value

`<principal>`—(Optional) DN that defines the username with which an SRC component accesses the directory.

Value— DN

Default—`cn = conf,o = Operators, < base >`

`<credentials>`—(Optional) Password used for authentication with the directory server.

Value—Secret text

Default—`conf`

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 0–600 s

Default— No value

`<time-limit>`—(Optional) The number of milliseconds to wait for directory results before returning. If set to 0, wait indefinitely.

Value—Integer in the range 0–2147483647 ms

Default— 5000

`<eventing>`—(Optional) Enable an SRC component to poll the directory for changes.

Default—TRUE

`<polling-interval>`—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–86400 s

Default— No value

`<connection-manager-id>`—(Optional) CLI identifier of the connection manager for the directory eventing system (within the JNDI framework).

Value— Identifier for connection manager

Example—DIRAGENT_POOL_VR

`<dispatcher-pool-size>`—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

`<event-base-dn>`—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default— o = umc, < base >

`<signature-dn>`—(Optional) DN of the directory entry that specifies the `usedDirectory` attribute for the SRC CLI. The `usedDirectory` attribute identifies the vendor of the directory server.

Value— DN

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Required Privilege Level

system

<login> (configuration/system)

Usage

```
<configuration>  
  <system>  
    <login>  
      <announcement>announcement</announcement>  
    </login>  
  </system>  
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system announcement to be displayed at user login.

Contents

<announcement>—(Optional) Announcement displayed to every user after login.

Value— Announcement text

Default— No value

Required Privilege Level

system admin

<class> (configuration/system/login)

Usage

```
<configuration>
  <system>
    <login>
      <class>
        <name>name</name> <!-- identifier -->
        <allow-commands>allow-commands</allow-commands>
        <allow-configuration>allow-configuration</allow-configuration>
        <deny-commands>deny-commands</deny-commands>
        <deny-configuration>deny-configuration</deny-configuration>
        <idle-timeout>idle-timeout</idle-timeout>
        <permissions>permissions-choice</permissions>
      </class>
    </login>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define login classes. You can define any number of login classes.

Contents

<name>— Name that you choose for a login class.

Value— Name

<allow-commands>—(Optional) Operational mode commands that members of a login class can use.

If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Operational-mode commands to allow

Default— No value

`<allow-configuration>`—(Optional) Configuration mode commands that members of a login class can use.

If you omit this statement and the `deny-configuration` statement, users can issue only those commands for which they have access privileges through the permissions statement

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Configuration-mode commands to allow

Default— No value

`<deny-commands>`—(Optional) Operational mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

If you omit this statement and the `allow-commands` statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any wildcard characters, enclose it in quotation marks.

Value— Operational mode commands to deny

Default— No value

`<deny-configuration>`—(Optional) Configuration mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

If you omit this statement and the `allow-configuration` statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Configuration mode commands to deny

Default— No value

`<idle-timeout>`—(Optional) Maximum amount of time that a session can be idle before

the user is logged off the C-series platform. The session times out after remaining at the CLI operational mode prompt for the specified time.

If you omit this statement, a user is never forced off the system after extended idle times.

Value— Number of minutes

Default— No value

<permissions>—(Optional) (Multivalue) Access privileges for each login class.

Value

- **admin**— Can view user account information in configuration mode and with the `show configuration` command.
- **admin-control**— Can view user accounts and configure them (at the [edit system login] hierarchy level).
- **all**— Has all permissions.
- **clear**— Can clear (delete) information learned from the network that is stored in various network databases (by using the `clear` commands).
- **configure**— Can enter configuration mode (by using the `configure` command).
- **control**— Can modify any configuration values.
- **field**— Reserved for field (debugging) support.
- **firewall**— Can view the firewall filter configuration in configuration mode.
- **firewall-control**— Can view and configure firewall filter information.
- **interface**— Can view the interface configuration in configuration mode and with the `show configuration operational mode` command.
- **interface-control**— Can modify interface configuration.
- **maintenance**— Can perform system maintenance, including starting a local shell on a C-series platform, and can halt and reboot a C-series platform (by using the `request system` commands).
- **network**— Can access the network by entering commands such as SSH or Telnet.
- **reset**— Can restart software processes by using the `restart` command and can configure whether software processes are enabled or disabled.
- **routing**— Can view routing information in configuration and operational modes.
- **routing-control**— Can view general routing information and modify routing configuration.
- **secret**— Can view passwords and other authentication keys in the configuration.
- **secret-control**— Can view passwords and other

- authentication keys in the configuration and can modify them in configuration mode.
- `security`— Can view security configuration in configuration mode and with the `show configuration operational mode` command.
 - `security-control`— Can view security configuration in configuration mode and with the `show configuration operational mode` command.
 - `shell`— Can start a local shell on the router by entering the `start shell` command.
 - `snmp`— Can view SNMP configuration information in configuration and operational modes.
 - `snmp-control`— Can view SNMP configuration information and configure SNMP (at the `[edit snmp]` hierarchy level).
 - `system`— Can view system-level information in configuration and operational modes.
 - `system-control`— Can view and configure system-level configuration information.
 - `view`— Can use various commands to display current system-wide values and statistics.
 - `view-configuration`— Can view all system configuration, excluding any secret configurations.
 - `service`— Can view service and policy definitions.
 - `service-control`— Can view and configure service definitions and policy definitions.
 - `subscriber`— Can view information about subscriber definitions.
 - `subscriber-control`— Can view and configure information about subscriber definitions.

Required Privilege Level

system admin

<user> (configuration/system/login)

Usage

```
<configuration>
  <system>
    <login>
      <user>
        <user-name>user-name</user-name> <!-- identifier -->
        <class>class</class>
        <full-name>full-name</full-name>
        <uid>uid</uid>
        <gid>gid</gid>
        <prompt>prompt</prompt>
        <level>level-choice</level>
        <complete-on-space>complete-on-space-choice</complete-on-space>
      </user>
    </login>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access permissions for individual users.

Contents

<user-name>— Username that is used to log in to a C-series platform.

Value— Username

<class>— User's login class. Configure one class for each user. The class referenced must already be configured.

Value— Class-name

<full-name>— Full name of the user. If the name contains spaces, enclose it in quotation marks.

Value— Name

`<uid>`— User identifier for the login account.

Value—Integer in the range 0–64000

`<gid>`— Group identifier for the login account.

Value—Integer in the range 0–64000

`<prompt>`—(Optional) Default prompt that this user sees at the SRC CLI.

Value— Prompt-text

`<level>`—(Optional) Editing level available to the user. The setting for the editing level determines which configuration commands are visible to the user.

Value

- `basic`— Minimal set of configuration statements and commands— only the statements that must be configured are visible.
- `normal`— Normal set of configuration statements and commands— the common and basic statements are visible.
- `advanced`— All configuration statements and commands, including the common and basic ones, are visible.
- `expert`— All configuration statements, including common, basic, and internal statements and commands used for debugging, are visible.

Default— Normal

`<complete-on-space>`—(Optional) Set the CLI to complete a partial command entry when you type a space. This statement enables command completion for all user sessions for this user.

To enable command completion for an active user session, use the `set cli complete-on-space` operational mode command.

Value

- `on`— Turn on command completion—allow either a space or a tab to be used for command completion.
- `off`— Turn off command completion—a space or a tab after a partial command name does not complete the command.

Default— On

Required Privilege Level

system admin

<authentication> (configuration/system/login/user)

Usage

```
<configuration>
  <system>
    <login>
      <user>
        <authentication>
          <plain-text-password-value>plain-text-password-value</plain-text-
password-value>
          <encrypted-password>encrypted-password</encrypted-password>
          <ssh-authorized-keys>ssh-authorized-keys</ssh-authorized-keys>
        </authentication>
      </user>
    </login>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Authentication methods that a user can use to log in to a C-series platform. You can assign multiple authentication methods to a single user.

Contents

<plain-text-password-value>—(Optional) Plain-text password that is autoencrypted.

Value— Password characters

<encrypted-password>—(Optional) Password in encrypted format.

Value— Encrypted-password

<ssh-authorized-keys>—(Optional) (Multivalue) Public key for SSH.

Value— Public-key

Required Privilege Level

system admin

<ntp> (configuration/system)

Usage

```
<configuration>
  <system>
    <ntp>
      <boot-server>boot-server</boot-server>
      <broadcast-client/>
      <trusted-key>trusted-key</trusted-key>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NTP.

We strongly recommend that you configure NTP on every server used for an SRC deployment. The system may not recognize subscriber sessions if the clocks are not synchronized.

Contents

<boot-server>—(Optional) Server that NTP queries when at boot time to determine the local date and time.

When you boot the system on which the SRC software runs, the system issues an `ntpdate` request, which polls a network server to determine the local date and time. You can configure a server that the system uses to determine the time at startup. If no boot server is configured, NTP uses one of the configured servers to set the initial time.

Value— IP address of an NTP server

Default— No value

<broadcast-client>—(Optional) Listen for NTP broadcast messages on the local network to discover other servers on the same subnet.

<trusted-key>—(Optional) (Multivalue) List of keys you are allowed to use when you configure the local system to synchronize its time with other systems on the network.

Value— Positive signed 32-bit integer (1–2147483647)
Default— No value

Required Privilege Level

system

<authentication-key> (configuration/system/ntp)

Usage

```
<configuration>
  <system>
    <ntp>
      <authentication-key>
        <key-number>key-number</key-number> <!-- identifier -->
        <value>value</value>
      </authentication-key>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NTP authentication keys so that the C-series platform can send authenticated packets. If you configure the C-series platform to operate in authenticated mode, you must configure a key.

NTP authentication uses the MD5 encryption algorithm.

Contents

<key-number>— Positive integer that identifies the NTP authentication key.

Value—Integer in the range 1–2147483647

<value>— The value of the NTP authentication, which can contain 1–8 ASCII characters.

Value—Secret text

Default— No value

Required Privilege Level

system

<broadcast> (configuration/system/ntp)

Usage

```
<configuration>
  <system>
    <ntp>
      <broadcast>
        <address>address</address> <!-- identifier -->
        <key>key</key>
        <t1>t1</t1>
        <version>version</version>
      </broadcast>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series platform to operate in broadcast mode with the remote system at the specified address. In this mode, the local system sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Typically, you include this statement only when the local system is operating as a transmitter.

Contents

<address>— IP address to receive broadcast or multicast periodic broadcast messages.

Value— IP address

<key>—(Optional) Value of the authentication key used to encrypt authentication fields in all packets sent to the broadcast or multicast address.

Value— Positive signed 32-bit integer (1–2147483647)

Default— No value

<t1>—(Optional) TTL value to transmit.

Value—Integer in the range 1–255

Default— No value

`<version>`—(Optional) Version number of NTP to use in outgoing NTP packets.

Value—Integer in the range 1–4

Default— No value

Required Privilege Level

system

<multicast-client> (configuration/system/ntp)

Usage

```
<configuration>
  <system>
    <ntp>
      <multicast-client>
        <address>address</address>
      </multicast-client>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Listen for NTP multicast messages on the local network to discover other servers on the same subnet.

Contents

<address>—(Optional) IP address(s). If you specify more than one address, the system joins those multicast groups.

Value—IP address

Default— No value

Required Privilege Level

system

<peer> (configuration/system/ntp)

Usage

```
<configuration>
  <system>
    <ntp>
      <peer>
        <address>address</address> <!-- identifier -->
        <key>key</key>
        <version>version</version>
        <prefer/>
      </peer>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series platform to operate in symmetric active mode with the remote system at the specified address. In this mode, the C-series platform and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or the remote system might be a better source of time.

Contents

<address>— IP address of an NTP peer. Do not specify a hostname.

Value—IP address

<key>—(Optional) Key number used to encrypt all authentication fields in packets sent to the specified address.

Value— Positive signed 32-bit integer (1-2147483647)

Default— No value

<version>—(Optional) Version number of NTP to be used in outgoing packets.

Value—Integer in the range 1-4

Default— No value

`<prefer>`—(Optional) Remote system is the preferred host. This remote system is then selected for synchronization among a set of systems that are operating correctly.

Required Privilege Level

system

<server> (configuration/system/ntp)

Usage

```
<configuration>
  <system>
    <ntp>
      <server>
        <address>address</address> <!-- identifier -->
        <key>key</key>
        <version>version</version>
        <prefer/>
      </server>
    </ntp>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series platform to operate in client mode with the remote system at the specified address. In this mode, the C-series platform can be synchronized with the remote system, but the remote system can never be synchronized with the C-series platform.

Contents

<address>— IP address of an NTP server. Do not specify a hostname.

Value—IP address

<key>—(Optional) Key number used to encrypt all authentication fields in packets sent to the specified address.

Value— Positive signed 32-bit integer (1-2147483647)

Default— No value

<version>—(Optional) Version number of NTP to be used in outgoing packets.

Value—Integer in the range 1-4

Default— No value

<prefer>—(Optional) Remote system is the preferred host. This remote system is then selected for synchronization among a set of systems that are operating correctly.

Required Privilege Level

system

<radius-server> (configuration/system)

Usage

```
<configuration>
  <system>
    <radius-server>
      <address>address</address> <!-- identifier -->
      <port>port</port>
      <secret>secret</secret>
      <timeout>timeout</timeout>
      <retry>retry</retry>
    </radius-server>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure RADIUS authentication. To use more than one RADIUS server, include a `radius-server` statement for each server. The software contacts the servers in order in a round-robin fashion until it receives a valid response from one of the servers or until the retry limit is reached for all servers.

To configure RADIUS for authentication, also include `radius` in the `authentication-order` option for the `system` statement.

For a user authenticated through RADIUS to be able to log in to the C-series platform, you must create either a local profile or a remote profile to define common access privileges for all users authenticated through RADIUS or TACACS+. For information about creating user profiles, see the `system login user` statement.

Contents

`<address>`— IP address of RADIUS server.

Value— IP address

`<port>`—(Optional) Port number on which to connect to a RADIUS server.

Value—Integer in the range 0–65535

Default— 1812

`<secret>`— Password to use with the RADIUS server. This secret password is used by the C-series platform and must match the password on the RADIUS server.

Value— password

`<timeout>`—(Optional) Amount of time that the C-series platform waits to receive a response from the RADIUS server.

Value—Integer in the range 1–90 s

Default—3

`<retry>`—(Optional) Number of times the C-series platform tries to contact a RADIUS server.

Value—Integer in the range 1–10

Default—3

Required Privilege Level

system

<services> (configuration/system)

Usage

```
<configuration>
  <system>
    <services>
      <telnet/>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system services.

Contents

<telnet>—(Optional) Allow Telnet connections from remote systems to the C-series platform.

Note: Telnet connections do not allow access through `root`.

Required Privilege Level

system

<editor> (configuration/system/services)

Usage

```
<configuration>
  <system>
    <services>
      <editor>
        <password-encryption>password-encryption-choice</password-encryption>
      </editor>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access properties for external access to the Policies, Services, and Subscribers Editor.

Contents

<password-encryption>—(Optional) Encrypt the passwords of users who remotely access the Policies, Services, and Subscribers Editor using the specified encryption algorithm.

Value

- `crypt`— UNIX crypt, a one-way encryption.
- `md5`— Message Digest 5 (MD5), a 128-bit message digest.
- `sha`— SHA message digest, a 160-bit message digest.
- `plain`— No encryption.

Required Privilege Level

system

<policy-editor> (configuration/system/services/editor)

Usage

```
<configuration>
  <system>
    <services>
      <editor>
        <policy-editor>
          <directory-eventing/>
        </policy-editor>
      </editor>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

`<directory-eventing>`—(Optional) Enable policy editor to poll the directory for changes.

Default—true

Required Privilege Level

system

<netconf> (configuration/system/services)

Usage

```
<configuration>
  <system>
    <services>
      <netconf>
        <ssh/>
      </netconf>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Allow connections through NETCONF to the C-series platform.

Contents

<ssh>—(Optional) Use SSH for NETCONF connections.

Required Privilege Level

system

<ssh> (configuration/system/services)

Usage

```
<configuration>
  <system>
    <services>
      <ssh>
        <root-login>root-login-choice</root-login>
        <protocol-version>protocol-version-choice</protocol-version>
      </ssh>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Allow SSH requests from remote systems to the C-series platform.

Contents

<root-login>—(Optional) Control user access through SSH.

Value

- allow— Allow users to login in to the C-series platform as root through SSH.(Default)
- deny— Disable users from logging in to the C-series platform as root through SSH.
- deny-password— Allow users to log in to the C-series platform as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

<protocol-version>—(Optional) SSH protocol versions accepted.

Value

- v1—SSH version 1

- v2—SSH version 2 (Default)

Required Privilege Level

system

<http> (configuration/system/services/web-management)

Usage

```
<configuration>
  <system>
    <services>
      <web-management>
        <http>
          <port>port</port>
          <interface>interface</interface>
        </http>
      </web-management>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Use HTTP without encryption.

Contents

<port>—(Optional) TCP port to be used for incoming connections to the C-Web interface.

Value—Integer in the range 1–65535

Default—80

<interface>—(Optional) (Multivalue) List of network interfaces to accept incoming connections. If you do not specify any interfaces, the software accepts connections from all interfaces.

Value— Name of external interface, such as eth0.

Required Privilege Level

system system

<https> (configuration/system/services/web-management)

Usage

```
<configuration>
  <system>
    <services>
      <web-management>
        <https>
          <port>port</port>
          <interface>interface</interface>
          <local-certificate>local-certificate</local-certificate>
        </https>
      </web-management>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Use secure HTTP with encryption.

Contents

<port>—(Optional) TCP port to be used for incoming connections to the C-Web interface.

Value—Integer in the range 1–65535

Default—443

<interface>—(Optional) (Multivalue) List of network interfaces to accept incoming connections. If you do not specify any interfaces, the software accepts connections from all interfaces.

Value— Name of external interface, such as eth0.

<local-certificate>—(Optional) Name of the security certificate (in X.509 format) on the local system. This certificate is used to secure connections from external Web browsers to the C-Web interface.

Value— Name of digital security certificate.

Required Privilege Level

system system

<logger> (configuration/system/services/web-management)

Usage

```
<configuration>
  <system>
    <services>
      <web-management>
        <logger>
          <name>name</name> <!-- identifier -->
        </logger>
      </web-management>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a logging component for the C-Web interface. Logging can be to a file or to the system logging utility.

Contents

<name>— Name of a logging component.

Value—Text

Required Privilege Level

system system

<file> (configuration/system/services/web-management/logger/logger)

Usage

```
<configuration>
  <system>
    <services>
      <web-management>
        <logger>
          <logger>
            <file>
              <filter>filter</filter>
              <filename>filename</filename>
              <rollover-filename>rollover-filename</rollover-filename>
              <maximum-file-size>maximum-file-size</maximum-file-size>
            </file>
          </logger>
        </logger>
      </web-management>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application

server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value— Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system system

<syslog> (configuration/system/services/web-management/logger/logger)

Usage

```
<configuration>
  <system>
    <services>
      <web-management>
        <logger>
          <logger>
            <syslog>
              <filter>filter</filter>
              <host>host</host>
              <facility>facility</facility>
              <format>format</format>
            </syslog>
          </logger>
        </logger>
      </web-management>
    </services>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

<facility>—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

<format>—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Required Privilege Level

system system

<static-host-mapping> (configuration/system)

Usage

```
<configuration>
  <system>
    <static-host-mapping>
      <host-name>host-name</host-name> <!-- identifier -->
      <inet>inet</inet>
      <alias>alias</alias>
    </static-host-mapping>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure static mapping to resolve hostnames.

Contents

<host-name>— Fully-qualified name of the system.

Value—Text

<inet>—(Optional) (Multivalue) IP addresses to which you want to map the hostname.

Value—IP address

<alias>—(Optional) (Multivalue) Aliases for the hostname.

Value—Text

Required Privilege Level

system system

<file> (configuration/system/syslog)

Usage

```
<configuration>
  <system>
    <syslog>
      <file>
        <name>name</name> <!-- identifier -->
      </file>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a file to store information that has been collected.

Contents

<name>— Name of the file in which to log system messages.

Value— filename

Required Privilege Level

system

<contents> (configuration/system/syslog/file)

Usage

```
<configuration>
  <system>
    <syslog>
      <file>
        <contents>
          <name>name-choice</name> <!-- identifier -->
          <any/>
          <emergency/>
          <alert/>
          <critical/>
          <error/>
          <warning/>
          <notice/>
          <info/>
          <none/>
        </contents>
      </file>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Contents

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- any— Messages from all facilities.
- authorization— Authentication and authorization attempts.
- daemon— Actions performed or errors encountered by various system processes.
- ftp— Actions performed or errors encountered by an FTP process.

- `kernel`— Actions performed or errors encountered by the kernel.
- `user`— Actions performed or errors encountered by various user processes.
- `local7`— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- `any`— Messages for all severity levels.
- `emergency`— System panic or other condition that causes the system to stop functioning.
- `alert`— Conditions that require immediate correction.
- `critical`— Critical conditions, such as hard drive errors.
- `error`— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- `warning`— Conditions that warrant monitoring.
- `notice`— Conditions that are not errors but might warrant special handling.
- `info`— Events or nonerror conditions of interest.
- `none`— Messages are not generated for any condition.

Required Privilege Level

`system`

<host> (configuration/system/syslog)

Usage

```
<configuration>
  <system>
    <syslog>
      <host>
        <name>name</name> <!-- identifier -->
      </host>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the IP address or hostname of the remote host to receive system log messages. The remote machine must be running a standard syslogd utility.

Contents

<name>— IP address or hostname of a remote system to receive system log messages. The remote machine must be running a standard syslogd utility.

Value— IP address or hostame

Required Privilege Level

system

<contents> (configuration/system/syslog/host)

Usage

```
<configuration>
  <system>
    <syslog>
      <host>
        <contents>
          <name>name-choice</name> <!-- identifier -->
          <any/>
          <emergency/>
          <alert/>
          <critical/>
          <error/>
          <warning/>
          <notice/>
          <info/>
          <none/>
        </contents>
      </host>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Contents

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- any— Messages from all facilities.
- authorization— Authentication and authorization attempts.
- daemon— Actions performed or errors encountered by various system processes.
- ftp— Actions performed or errors encountered by an FTP process.

- `kernel`— Actions performed or errors encountered by the kernel.
- `user`— Actions performed or errors encountered by various user processes.
- `local7`— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- `any`— Messages for all severity levels.
- `emergency`— System panic or other condition that causes the system to stop functioning.
- `alert`— Conditions that require immediate correction.
- `critical`— Critical conditions, such as hard drive errors.
- `error`— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- `warning`— Conditions that warrant monitoring.
- `notice`— Conditions that are not errors but might warrant special handling.
- `info`— Events or nonerror conditions of interest.
- `none`— Messages are not generated for any condition.

Required Privilege Level

`system`

<user> (configuration/system/syslog)

Usage

```
<configuration>
  <system>
    <syslog>
      <user>
        <name>name</name> <!-- identifier -->
      </user>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Notify a specified user by means of a terminal session.

Contents

<name>— Name of user to receive messages.

Value— Username

Required Privilege Level

system

<contents> (configuration/system/syslog/user)

Usage

```
<configuration>
  <system>
    <syslog>
      <user>
        <contents>
          <name>name-choice</name> <!-- identifier -->
          <any/>
          <emergency/>
          <alert/>
          <critical/>
          <error/>
          <warning/>
          <notice/>
          <info/>
          <none/>
        </contents>
      </user>
    </syslog>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Contents

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- any— Messages from all facilities.
- authorization— Authentication and authorization attempts.
- daemon— Actions performed or errors encountered by various system processes.
- ftp— Actions performed or errors encountered by an FTP process.

- `kernel`— Actions performed or errors encountered by the kernel.
- `user`— Actions performed or errors encountered by various user processes.
- `local7`— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- `any`— Messages for all severity levels.
- `emergency`— System panic or other condition that causes the system to stop functioning.
- `alert`— Conditions that require immediate correction.
- `critical`— Critical conditions, such as hard drive errors.
- `error`— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- `warning`— Conditions that warrant monitoring.
- `notice`— Conditions that are not errors but might warrant special handling.
- `info`— Events or nonerror conditions of interest.
- `none`— Messages are not generated for any condition.

Required Privilege Level

system

<tacplus-server> (configuration/system)

Usage

```
<configuration>
  <system>
    <tacplus-server>
      <address>address</address>
      <secret>secret</secret>
    </tacplus-server>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure TACACS + authentication.

To configure TACACS + for authentication, also include `tacplus` in the `authentication-order` option for the `system` statement.

For a user authenticated through TACACS + to be able to log into the C-series platform, you must create either a local profile or a remote profile to define common access privileges for all users authenticated via RADIUS or TACACS +. For information about creating user profiles, see the `system login user` statement.

Contents

<address>—(Multivalue) Address of TACACS + authentication server.

Value— IP address

Default— No value

<secret>— Password to use with the RADIUS or TACACS + server. The secret password used by the C-series platform must match that used by the server.

Value—Secret text

Default— No value

Required Privilege Level

system

Juniper Networks Database Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the Juniper Networks Database. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
system ldap server	<u>< server ></u>
system ldap server community	<u>< community ></u>
system ldap server security	<u>< security ></u>

<server> (configuration/system/ldap)

Usage

```
<configuration>
  <system>
    <ldap>
      <server>
        <stand-alone/>
      </server>
    </ldap>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the Juniper Networks database to run in standalone mode. This database contains the SRC configuration information.

Typically, you run the database in standalone mode only in testing environments. If you want to run the Juniper Networks database in a community (or group) of databases, use the `system ldap server community` statement.

Enable the Juniper Networks database in either standalone or community mode; a Juniper Networks database can run either standalone or in a community, but not both. If you do not enable the database, it will not run.

Contents

Value

- `stand-alone`— Standalone mode for the Juniper Networks database.

Required Privilege Level

system

<community> (configuration/system/ldap/server)

Usage

```
<configuration>
  <system>
    <ldap>
      <server>
        <community>
          <role>role-choice</role>
          <primary-neighbors>primary-neighbors</primary-neighbors>
          <secondary-neighbors>secondary-neighbors</secondary-neighbors>
        </community>
      </server>
    </ldap>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the Juniper Networks database to operate as part of a community (group) of other Juniper Networks databases. The Juniper Networks database contains the SRC configuration information.

If you want to run the Juniper Networks database standalone, use the `stand-alone` option at the `system ldap server` hierarchy level.

Enable the Juniper Networks database in either standalone or community mode; a Juniper Networks database can run either standalone or in a community, but not both. If you do not enable the database, it will not run.

Contents

`<role>`— Role of the database. The role determines the read and write access to the database.

Value

- `primary`— A database that provides read and write access to client applications. It replicates its data and distributes changes to any Juniper Networks databases configured as neighbors.
- `secondary`— A database that provides read access to client applications. If client applications try to write data to this database, the database refers the client to a primary database.

Default— No value

`<primary-neighbors>`—(Optional) (Multivalue) A database that propagates changes that it receives to other Juniper Networks databases configured as neighbors. A primary neighbor must be assigned a primary role.

Value— Primary neighbor identified by one of the following:

- IP address; for example, 192.2.4.0
- Hostname that the C-series Controller can resolve through the domain name system; for example, myhostname1
- Fully qualified hostname; for example, myhostname1.mycompany.com

Default— No value

`<secondary-neighbors>`—(Optional) (Multivalue) A database that only receives database changes. A secondary neighbor must be assigned a secondary role.

Value— Secondary neighbor identified by one of the following:

- IP address; for example, 192.2.4.0
- Hostname that the C-series Controller can resolve through the domain name system; for example, myhostname1
- Fully qualified hostname; for example, myhostname1.mycompany.com

Default— No value

Required Privilege Level

system

<security> (configuration/system/ldap/server)

Usage

```
<configuration>
  <system>
    <ldap>
      <server>
        <security>
          <enable/>
          <strict/>
        </security>
      </server>
    </ldap>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

You can secure connections to a Juniper Networks database by:

- Allowing only Secure Lightweight Directory Access Protocol (LDAPS) connections from remote systems. In this case, both database replication and remote SRC components connect through LDAPS. Restricting all remote connections through LDAPS is supported only on C-Series Controllers.
- Allowing only LDAPS connections for database replication, but LDAP or LDAPS connections for other applications. In this case, remote SRC components can connect through LDAP or LDAPS.

To allow access to the Juniper Networks database only through LDAP, use the `delete security` command at the `system ldap server` hierarchy level.

Contents

Secure connections to the Juniper Networks database.

Value

- `enable`— Use LDAPS to secure connections to other Juniper Networks databases for data replication.
- `strict`— Use LDAPS to secure remote connections to the Juniper Networks database. Local SRC components have LDAP access the database.

Required Privilege Level

system

SAE Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the SAE. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
shared auth-cache cached-dhcp-profile	<u>< cached-dhcp-profile ></u>
shared network application-manager-group	<u>< application-manager-group ></u>
shared network device	<u>< device ></u>
shared network device name interface-classifier rule	<u>< rule ></u>
shared network device name interface-classifier rule name condition	<u>< condition ></u>
shared network device name virtual-router	<u>< virtual-router ></u>
shared network policy-decision-point	<u>< policy-decision-point ></u>
shared sae configuration	<u>< configuration ></u>
shared sae configuration aggregate-services	<u>< aggregate-services ></u>
shared sae configuration driver	<u>< driver ></u>
shared sae configuration driver aaa	<u>< aaa ></u>
shared sae configuration driver aaa session-store	<u>< session-store ></u>
shared sae configuration driver junos	<u>< junos ></u>
shared sae configuration driver junos configuration-checking	<u>< configuration-checking ></u>
shared sae configuration driver junos lsp-tracking	<u>< lsp-tracking ></u>
shared sae configuration driver junos security	<u>< security ></u>
shared sae configuration driver junos session-store	<u>< session-store ></u>
shared sae configuration driver junose	<u>< junose ></u>
shared sae configuration driver junose session-store	<u>< session-store ></u>
shared sae configuration driver pcmm	<u>< pcmm ></u>

shared sae configuration driver pcmm cmts-specific-rks-plug-ins	< cmts-specific-rks-plug-ins >
shared sae configuration driver pcmm session-store	< session-store >
shared sae configuration driver scripts	< scripts >
shared sae configuration driver session-store	< session-store >
shared sae configuration driver simulated	< simulated >
shared sae configuration driver simulated name session-store	< session-store >
shared sae configuration driver snmp	< snmp >
shared sae configuration driver third-party	< third-party >
shared sae configuration driver third-party session-store	< session-store >
shared sae configuration dynamic-radius-server	< dynamic-radius-server >
shared sae configuration external-interface-features	< external-interface-features >
shared sae configuration external-interface-features name CommunityManager	< CommunityManager >
shared sae configuration external-interface-features name EventAPI	< EventAPI >
shared sae configuration external-interface-features name JavaScriptProcessor	< JavaScriptProcessor >
shared sae configuration external-interface-features name PythonScriptProcessor	< PythonScriptProcessor >
shared sae configuration external-interface-features name SAEAccess	< SAEAccess >
shared sae configuration external-interface-features name SAEFeature	< SAEFeature >
shared sae configuration external-interface-features name SAEFeature properties	< properties >
shared sae configuration file-accounting-template	< file-accounting-template >
shared sae configuration file-accounting-template name attributes	< attributes >
shared sae configuration global-radius-udp-port	< global-radius-udp-port >
shared sae configuration idle-timeout	< idle-timeout >

shared sae configuration interim-accounting	<u>< interim-accounting ></u>
shared sae configuration ldap	<u>< ldap ></u>
shared sae configuration ldap directory-eventing	<u>< directory-eventing ></u>
shared sae configuration ldap persistent-login-cache	<u>< persistent-login-cache ></u>
shared sae configuration ldap policy-data	<u>< policy-data ></u>
shared sae configuration ldap service-data	<u>< service-data ></u>
shared sae configuration ldap subscriber-data	<u>< subscriber-data ></u>
shared sae configuration license-manager client	<u>< client ></u>
shared sae configuration license-manager directory-access	<u>< directory-access ></u>
shared sae configuration logger	<u>< logger ></u>
shared sae configuration logger name file	<u>< file ></u>
shared sae configuration logger name syslog	<u>< syslog ></u>
shared sae configuration login-registration	<u>< login-registration ></u>
shared sae configuration nic-proxy-configuration	<u>< nic-proxy-configuration ></u>
shared sae configuration nic-proxy-configuration name cache	<u>< cache ></u>
shared sae configuration nic-proxy-configuration name nic-host-selection	<u>< nic-host-selection ></u>
shared sae configuration nic-proxy-configuration name nic-host-selection blacklisting	<u>< blacklisting ></u>
shared sae configuration nic-proxy-configuration name resolution	<u>< resolution ></u>
shared sae configuration nic-proxy-configuration name test-nic-bindings	<u>< test-nic-bindings ></u>
shared sae configuration nic-proxy-configuration name test-nic-bindings key-values	<u>< key-values ></u>
shared sae configuration plug-ins	<u>< plug-ins ></u>
shared sae configuration plug-ins event-publishers	<u>< event-publishers ></u>
shared sae configuration plug-ins manager	<u>< manager ></u>
shared sae configuration plug-ins name	<u>< name ></u>

shared sae configuration plug-ins name name acp-interface-listener	<u>< acp-interface-listener ></u>
shared sae configuration plug-ins name name custom-radius-accounting	<u>< custom-radius-accounting ></u>
shared sae configuration plug-ins name name custom-radius-accounting peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name custom-radius-authentication	<u>< custom-radius-authentication ></u>
shared sae configuration plug-ins name name custom-radius-authentication peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name ejb-adaptor	<u>< ejb-adaptor ></u>
shared sae configuration plug-ins name name external	<u>< external ></u>
shared sae configuration plug-ins name name file-accounting	<u>< file-accounting ></u>
shared sae configuration plug-ins name name flex-radius-accounting	<u>< flex-radius-accounting ></u>
shared sae configuration plug-ins name name flex-radius-accounting peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition	<u>< radius-packet-definition ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name 26	<u>< 26 ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name 26 name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name 26 name type	<u>< type ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name 26 name type name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific	<u>< vendor-specific ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name attributes	<u>< attributes ></u>

shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name type	<u>< type ></u>
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name type name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-authentication	<u>< flex-radius-authentication ></u>
shared sae configuration plug-ins name name flex-radius-authentication peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition	<u>< radius-packet-definition ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name 26	<u>< 26 ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name 26 name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name 26 name type	<u>< type ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name 26 name type name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific	<u>< vendor-specific ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type	<u>< type ></u>
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type name attributes	<u>< attributes ></u>
shared sae configuration plug-ins name name interface-subscriber-limit	<u>< interface-subscriber-limit ></u>
shared sae configuration plug-ins name name internal	<u>< internal ></u>

shared sae configuration plug-ins name name internal properties	<u>< properties ></u>
shared sae configuration plug-ins name name ldap-authentication	<u>< ldap-authentication ></u>
shared sae configuration plug-ins name name pcmm-rks	<u>< pcmm-rks ></u>
shared sae configuration plug-ins name name pcmm-rks peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name qos-profile-tracking	<u>< qos-profile-tracking ></u>
shared sae configuration plug-ins name name radius-accounting	<u>< radius-accounting ></u>
shared sae configuration plug-ins name name radius-accounting peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name radius-authentication	<u>< radius-authentication ></u>
shared sae configuration plug-ins name name radius-authentication peer-group	<u>< peer-group ></u>
shared sae configuration plug-ins name name schedule-authorization	<u>< schedule-authorization ></u>
shared sae configuration plug-ins state-synchronization	<u>< state-synchronization ></u>
shared sae configuration policy-management-configuration	<u>< policy-management-configuration ></u>
shared sae configuration radius-packet-template	<u>< radius-packet-template ></u>
shared sae configuration radius-packet-template name radius-attributes	<u>< radius-attributes ></u>
shared sae configuration radius-packet-template name radius-attributes name attributes	<u>< attributes ></u>
shared sae configuration radius-packet-template name radius-attributes name 26	<u>< 26 ></u>
shared sae configuration radius-packet-template name radius-attributes name 26 name attributes	<u>< attributes ></u>
shared sae configuration radius-packet-template name radius-attributes name 26 name type	<u>< type ></u>
shared sae configuration radius-packet-template name radius-attributes name 26 name type name attributes	<u>< attributes ></u>

shared sae configuration radius-packet-template name radius-attributes name vendor-specific	<u>< vendor-specific ></u>
shared sae configuration radius-packet-template name radius-attributes name vendor-specific name attributes	<u>< attributes ></u>
shared sae configuration radius-packet-template name radius-attributes name vendor-specific name type	<u>< type ></u>
shared sae configuration radius-packet-template name radius-attributes name vendor-specific name type name attributes	<u>< attributes ></u>
shared sae configuration script-extension	<u>< script-extension ></u>
shared sae configuration service-activation	<u>< service-activation ></u>
shared sae configuration service-schedule	<u>< service-schedule ></u>
shared sae configuration session-job-manager	<u>< session-job-manager ></u>
shared sae configuration subscriber-sessions	<u>< subscriber-sessions ></u>
shared sae configuration time-based-policies	<u>< time-based-policies ></u>
shared sae dhcp-classifier rule	<u>< rule ></u>
shared sae dhcp-classifier rule name condition	<u>< condition ></u>
shared sae group	<u>< group ></u>
shared sae subscriber-classifier rule	<u>< rule ></u>
shared sae subscriber-classifier rule name condition	<u>< condition ></u>
slot number sae	<u>< sae ></u>
slot number sae initial	<u>< initial ></u>
slot number sae initial directory-connection	<u>< directory-connection ></u>
slot number sae initial directory-eventing	<u>< directory-eventing ></u>
slot number sae radius	<u>< radius ></u>

<cached-dhcp-profile> (configuration/shared/auth-cache)

Usage

```

<configuration>
  <shared>
    <auth-cache>
      <cached-dhcp-profile>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <pool-name>pool-name</pool-name>
        <ip-address>ip-address</ip-address>
        <dhcp-options>dhcp-options</dhcp-options>
        <boot-server-name>boot-server-name</boot-server-name>
        <boot-file-name>boot-file-name</boot-file-name>
        <virtual-router>virtual-router</virtual-router>
        <local-interface>local-interface</local-interface>
        <lease-time>lease-time</lease-time>
        <user-name>user-name</user-name>
        <service-bundle>service-bundle</service-bundle>
        <radius-class>radius-class</radius-class>
      </cached-dhcp-profile>
    </auth-cache>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a cached DHCP profile.

Contents

<name>— Name of a cached DHCP profile.

Value— String

<description>—(Optional) Description of the DHCP client device.

Value— String

Default— No value

`<pool-name>`—(Optional) Name of the IP address pool on the JUNOS router from which a DHCP address is selected.

Value— String
Default— No value

`<ip-address>`—(Optional) Fixed IP address that is offered to the DHCP client if the client is part of a network in the configured DHCP pool.

Value— IP address
Default— No value

`<dhcp-options>`—(Optional) Defines DHCP options that are used to configure DHCP clients.

Value— Define DHCP options in the format: option = value [,value...].

where option is the DHCP option name or number (see the customer documentation for a list of supported DHCP options) and values are entered based on the type of option:

- int32, int16, int8—Decimal or hex prefixed by 0x
- string—Optionally surrounded by double quotes
- ip-address—Dotted decimal
- data-string—Sequence of hex-encoded bytes separated by a : (colon) or a string surrounded by double quotes

Separate multiple options by line breaks.

Value is a string containing one or more options defined as 'name = value'. Multiple options are separated by line breaks.

To include nonstandard options in a DHCP profile, use the name option-*nnn*, where *nnn* is the option number, and the value is of type data-string; that is, either a string surrounded in double quotes, or a sequence of hex-encoded bytes, separated by a colon (:).

Default— No value

`<boot-server-name>`—(Optional) Name of the server used to boot the DHCP client.

Value— String, length < 64
Default— No value

`<boot-file-name>`—(Optional) Name of a boot file used to boot the DHCP client.

Value— String, length < 128

Default— No value

`<virtual-router>`—(Optional) Name of the virtual router that holds the IP address pool.

Value— Name of the virtual router in the format `vrname@hostname`.

An * (asterisk) means that the values for the virtual router are ignored when the cached profile is used. Use an * if you do not know the virtual router to which the subscriber will connect.

Default— No value

`<local-interface>`—(Optional) Name of the JUNOSe router interface that will receive the DHCP client device's request for an IP address.

Value— Name of the virtual router in the format `vrname@hostname`.

An * (asterisk) means that the values for local interface are ignored when the cached profile is used. Use an * if you do not know the interface to which the subscriber will connect or if you want to allow the subscriber to connect through multiple interfaces.

Default— No value

`<lease-time>`—(Optional) Length of time the supplied IP address is valid. This parameter is not currently implemented on the JUNOSe router. The DHCP lease time that the SAE sends to the JUNOSe router is ignored.

Value— Number of seconds

Default— No value

`<user-name>`—(Optional) Username of the DHCP subscriber without the domain name.

Value— String that specifies the information to the left of the @ character in `userName@domainName`.

Default— No value

`<service-bundle>`—(Optional) Vendor-specific RADIUS attribute that specifies the SRC service bundle to use.

Value— String

Default— No value

`<radius-class>`—(Optional) RADIUS attribute class.

Value— String

Default— No value

Required Privilege Level

system

<application-manager-group> (configuration/shared/network)

Usage

```

<configuration>
  <shared>
    <network>
      <application-manager-group>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <application-manager-id>application-manager-id</application-manager-
id>
        <connected-sae>connected-sae</connected-sae>
        <pdp-group>pdp-group</pdp-group>
        <local-address-pools>local-address-pools</local-address-pools>
        <managing-sae-ior>managing-sae-ior</managing-sae-ior>
      </application-manager-group>
    </network>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure application managers for the Juniper policy server (JPS).

Contents

<name>— Name of application manager group.

Value— Text string

<description>—(Optional) Information about the SAE community.

Value— Text string

Default— No value

<application-manager-id>— Unique identifier within the domain of the service provider for the application manager that handles the service session; used to specify the application manager identifier (AMID) that is included in all messages sent to and from the policy server.

This option is required. The SAE constructs the AMID value by concatenating two fields: Application Manager Tag (this option) and Application Type (this value is obtained from a service during activation).

Value— 2-byte unsigned integer

Default— No value

<connected-sae>—(Multivalue) SAEs that are connected to the specified policy server group (PDP Group). This list becomes the community of SAEs.

This option is required. When you modify a community, wait for passive session stores of the new community members to be updated before you shut down the current active SAE. Otherwise, a failover from the current active SAE to the new member is triggered immediately, and the new member's session store may not have received all data from the active SAE's session store.

Value— IP address or hostname

Default— No value

<pdp-group>— Name of the policy server group associated with this SAE community.

Value— Text string

Default— No value

<local-address-pools>—(Optional) (Multivalue) List of IP address pools that this PDP group currently manages and stores. You must configure a local address pool if you are using the NIC so that the NIC can resolve the IP-to-SAE mapping.

Value— An address pool is specified by a sequence of zero or more address sets enclosed in parentheses (. An address set can be either a range of addresses or a subnetwork with or without address exclusions.

- Specify a range by entering a start and end address separated by a space and enclosed in square brackets. For example, [10.10.10.5 10.10.10.250] denotes the address set 10.10.10.5 to 10.10.10.250 inclusive.
- Specify a subnet with optional address exclusions in curly brackets. You must include a base address and a mask or prefix length separated by a forward slash. To exclude addresses, follow the forward slash with a comma and a comma-separated list of excluded addresses. For example:
 - { 10.20.20.0/24 } denotes all addresses that start with 10.20.20
 - { 10.21.0.0/255.255.0.0 } denotes all addresses that start with 10.21
 - { 10.20.30.0/24, 10.20.30.0, 10.20.30.255 } denotes all

addresses that start with 10.20.30 except 10.20.30.0 and 10.20.30.255

Default— No value

`<managing-sae-ior>`—(Optional) Common Object Request Broker Architecture (CORBA) reference for the SAE managing this policy server group. The `amlorPublisher` script provides this information when the SAE connects to the policy server. If you do not select this script when configuring initialization scripts, enter a value.

Value— One of the following items:

- The actual CORBA reference for the SAE
- The absolute path to the interoperable object reference (IOR) file
- A corbaloc URL in the form `corbaloc:: < host > :8801/SAE`
 - `< host >` —Name or IP address of the SAE host

The following examples show different CORBA references.

- Absolute path—`/opt/UMC/sae/var/run/sae.ior`
- corbaloc URL—`boston:8801/sae`
- Actual IOR—
IOR:0000000000000002438444C3A736D67742E6A756E697...

Default— No value

Required Privilege Level

system

<device> (configuration/shared/network)

Usage

```
<configuration>
  <shared>
    <network>
      <device>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <management-address>management-address</management-address>
        <device-type>device-type-choice</device-type>
        <qos-profile>qos-profile</qos-profile>
      </device>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a device that the SAE manages.

Contents

<name>— Name of the router or other device that the SAE manages.

Value— Text; must use lowercase characters

<description>—(Optional) Description of the device that the SAE manages.

Value— Text

Default— No value

<management-address>—(Optional) IP address of the device. For networks with JUNOS routers, the redirect component in redundant mode uses this address to send SNMP set messages to set a static route to the new redirect server after a failover.

Value— IP address

Default— No value

`<device-type>`—(Optional) Type of device that you are configuring.

Value

- `junose`— JUNOSe router
- `junos`— JUNOS routing platform
- `pcmm`— CMTS device
- `third-party`— Third-party device

Default— No value

`<qos-profile>`—(Optional) (Multivalue) For JUNOSe routers, specifies quality of service (QoS) profiles that are configured on the router.

Value— Single QoS profile or a list of QoS profiles

Default— No value

Required Privilege Level

system

<rule> (configuration/shared/network/device/interface-classifier)

Usage

```
<configuration>
  <shared>
    <network>
      <device>
        <interface-classifier>
          <rule>
            <name>name</name> <!-- identifier -->
            <target>target</target>
            <script>script</script>
          </rule>
        </interface-classifier>
      </device>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an interface classification rule.

Contents

<name>— Name of the rule in the interface classification script.

Value— Text

<target>—(Optional) Result of the classification script that gets returned to the SAE.

Value— Path to a policy group. For example, /sample/junose/DHCP.

Default— No value

<script>—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Required Privilege Level

system

<condition> (configuration/shared/network/device/interface-classifier/rule)

Usage

```
<configuration>
  <shared>
    <network>
      <device>
        <interface-classifier>
          <rule>
            <condition>
              <name>name</name> <!-- identifier -->
            </condition>
          </rule>
        </interface-classifier>
      </device>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Contents

<name>— Match conditions used to find a target. For more information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC-PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

<virtual-router> (configuration/shared/network/device)

Usage

```
<configuration>
  <shared>
    <network>
      <device>
        <virtual-router>
          <name>name</name> <!-- identifier -->
          <sae-connection>sae-connection</sae-connection>
          <snmp-read-community>snmp-read-community</snmp-read-community>
          <snmp-write-community>snmp-write-community</snmp-write-community>
          <scope>scope</scope>
          <local-address-pools>local-address-pools</local-address-pools>
          <static-address-pools>static-address-pools</static-address-pools>
          <tracking-plug-in>tracking-plug-in</tracking-plug-in>
        </virtual-router>
      </device>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a virtual router object.

Contents

<name>— Name of the virtual router.

Value— One of the following:

- For JUNOSe routers, the name of the VR, which is case sensitive, must exactly match the name of the VR configured on the router.
- For JUNOS routing platforms, CMTS devices, and other third-party devices, use the name default

<sae-connection>—(Optional) (Multivalue) IP addresses of the SAEs that can manage

this device. This option is required for the SAE to work with the router.

Value— IP addresses or a list of IP addresses

Default— No value

`<snmp-read-community>`—(Optional) SNMP community name associated with SNMP read-only operations for this virtual router. Read operations are typically used by router initialization scripts to read information, such as IP address pools, from the router.

Value— Text

Default— No value

`<snmp-write-community>`—(Optional) SNMP community name associated with SNMP write operations for this virtual router. The write community is used only by the redirect server to set a static route.

Value— Text

Default— No value

`<scope>`—(Optional) (Multivalue) The virtual router can be associated with a number of service scopes. The scopes are available for subscribers connected to this virtual router for selecting customized versions of services.

Value— Text

Default— No value

`<local-address-pools>`—(Optional) For JUNOS virtual routers, address of local address pools on the JUNOS virtual router.

- If you do not configure the PoolPublisher router initialization script for a JUNOS virtual router, configure this option for a JUNOS virtual router.
- If you do configure the PoolPublisher router initialization script for a JUNOS virtual router, configure this option if pool data needs to be updated. This data needs to be updated if you change the address pools on a virtual router that is actively being managed by SAE. The reason is that the initialization script is triggered only when the COPS connection is started.

For CMTS devices, You must configure either a local address pool or a static address pool so that the NIC can resolve the IP-to-SAE mapping.

Value— An address pool is specified by a sequence of zero or more address sets enclosed in parentheses (). An address set can be either a range of addresses or a subnetwork with or without address exclusions.

- Specify a range by entering a start and end address separated

by a space and enclosed in square brackets. For example, [10.10.10.5 10.10.10.250] denotes the address set 10.10.10.5 to 10.10.10.250 inclusive.

- Specify a subnet with optional address exclusions in curly brackets. You must include a base address and a mask or prefix length separated by a forward slash. To exclude addresses, follow the forward slash with a comma and a comma-separated list of excluded addresses. For example:
 - { 10.20.20.0/24 } denotes all addresses that start with 10.20.20
 - { 10.21.0.0/255.255.0.0 } denotes all addresses that start with 10.21
 - { 10.20.30.0/24, 10.20.30.0, 10.20.30.255 } denotes all addresses that start with 10.20.30 except 10.20.30.0 and 10.20.30.255

Default— No value

`<static-address-pools>`—(Optional) IP address pools that a JUNOS virtual router manages but does not store on the router because the router is not managing the allocation of these addresses. For CMTS devices, you must configure either a local address pool or a static address pool so that the NIC can resolve the IP-to-SAE mapping.

Value—

Default— No value

`<tracking-plug-in>`—(Optional) (Multivalue) List of plug-ins that are notified of interface events for this virtual router.

Value— IP address. You can include a mask. For example 10.20.20.0/24.

Default— No value

Required Privilege Level

system

<policy-decision-point> (configuration/shared/network)

Usage

```
<configuration>
  <shared>
    <network>
      <policy-decision-point>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <pdp-address>pdp-address</pdp-address>
        <pdp-group>pdp-group</pdp-group>
      </policy-decision-point>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configures the policy server as a policy decision point.

Contents

<name>— Name of policy decision point.

Value— Text string

<description>—(Optional) Information about this policy server.

Value— Text string

Default— No value

<pdp-address>— IP address of the policy server. The SAE uses this address to establish a COPS connection with the policy server.

Value— IP address

Default— No value

<pdp-group>— Name of the policy server group.

Value— Text string

Default— No value

Required Privilege Level

system

<configuration> (configuration/shared/sae)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <substitution-num-engines>substitution-num-engines</substitution-num-
engines>
        <substitution-cache-size>substitution-cache-size</substitution-cache-
size>
        <compress-session-data/>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<substitution-num-engines>—(Optional) Number of Substitution Engines

Value—Integer in the range -2147483648–2147483647

Default—5

<substitution-cache-size>—(Optional) Substitution Engine Cache Size

Value—Integer in the range -2147483648–2147483647

Default—5000

<compress-session-data>—(Optional) Enable or disable compression of the serialized data when saving the state of the SAE. You can use serialized data compression to reduce the size of sessions objects that the SAE sends across the network for the session store feature.

Enabling this option reduces the size of objects, but increases the CPU load on the SAE. We recommend that you do not enable this option because of the increase to the CPU load.

Default— Disabled

Required Privilege Level

system

<aggregate-services> (configuration/shared/sae/configuration)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <aggregate-services>
          <keepalive-time>keepalive-time</keepalive-time>
          <keepalive-retry-time>keepalive-retry-time</keepalive-retry-time>
          <activation-deactivation-time>activation-deactivation-time</
activation-deactivation-time>
          <failed-notification-retry-time>failed-notification-retry-time</
failed-notification-retry-time>
          <reactivation-verification-time>reactivation-verification-time</
reactivation-verification-time>
        </aggregate-services>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure timers and intervals associated with monitoring and activating aggregate sessions.

Contents

<keepalive-time>— Interval at which keepalive messages are sent from an aggregate service session and an associated fragment service session.

Value— Number of seconds in the range 1–2147483647

Default— 86400

<keepalive-retry-time>— Time to wait before resending unacknowledged keepalive messages.

Value— Number of seconds in the range 1–2147483647

Default— 900

<activation-deactivation-time>— Time to wait before retrying failed activation or deactivation of the fragment service session.

Value— Number of seconds in the range 1–2147483647

Default— 900

<failed-notification-retry-time>— Length of time to continue sending failure notifications if an aggregate service cannot reach a fragment service, or a fragment service cannot reach an aggregate service during shutdown of the aggregate service.

Value— Number of seconds in the range 1–2147483647

Default— 86400

<reactivation-verification-time>— Maximum time (in seconds) to verify fragment reactivation

Value— Integer in the range -2147483648–2147483647

Default— 30

Required Privilege Level

system

<driver> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <unauthenticated-subscriber-dn>unauthenticated-subscriber-dn</unauthenticated-subscriber-dn>
          <virtual-portal-address>virtual-portal-address</virtual-portal-address>
          <mac-cache-expiration>mac-cache-expiration</mac-cache-expiration>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<unauthenticated-subscriber-dn>— Transitional profile for subscribers who are not logged in to the SAE. For example, if a subscriber logs out of the SAE using the API method `Subscriber.logout()`, an unauthenticated subscriber session is created. The unauthenticated subscriber profile must exist and can be subscribed to services available for unauthenticated subscribers. The portal implementation determines whether unauthenticated (anonymous) subscribers can access the portal.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *uniqueID= unauthenticated,ou= local,retailerName= default,o= Users,< base>*

<virtual-portal-address>—(Optional) IP address that policies use as a substitution to send traffic to a captive portal.

Value— IP address

Default— No value

<mac-cache-expiration>— Amount of time that a subscriber profile remains in the SAE's in-memory cache. Configure this parameter to be greater than the time required for a DHCP subscriber to transition from an unauthenticated IP address to an authenticated IP address or vice versa. The time required for a DHCP subscriber to transition from one IP address to another depends on the lease times configured on the JUNOS router and the

instructions given to the subscriber on the Web portal, such as reboot your PC now.

Value— Number of seconds in the range 0–2147483647

Default— 1800

Required Privilege Level

system

<aaa> (configuration/shared/sae/configuration/driver)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <aaa>
            <sae-community-manager>sae-community-manager</sae-community-
manager>
            <keep-alive-timeout>keep-alive-timeout</keep-alive-timeout>
            <registry-retry-interval>registry-retry-interval</registry-retry-
interval>
            <reply-timeout>reply-timeout</reply-timeout>
            <sequential-message-timeout>sequential-message-timeout</
sequential-message-timeout>
            <transient-session-timeout>transient-session-timeout</transient-
session-timeout>
            <max-update-interval>max-update-interval</max-update-interval>
            <update-grace-period>update-grace-period</update-grace-period>
            <resume-unrecovered/>
            <thread-pool-size>thread-pool-size</thread-pool-size>
            <thread-idle-timeout>thread-idle-timeout</thread-idle-timeout>
          </aaa>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the SAE to manage AAA NAS groups.

Contents

<sae-community-manager>— Name of the community manager that manages AAA NAS group communities. Active SAEs are selected from this community.

Value— Community name

Default— AAACommunityManager

<keep-alive-timeout>—(Optional) The keep-alive timeout in seconds to expire the registry to a diameter server.

Value— Keep-alive timeout

Default— 60

<registry-retry-interval>—(Optional) The timeout in seconds to retry a failed registry to a diameter server.

Value— Registry-retry timeout

Default— 30

<reply-timeout>—(Optional) The timeout in seconds to expire a request sent to a diameter server.

Value— Reply timeout

Default— 20

<sequential-message-timeout>—(Optional) The timeout in seconds to expire an expected message.

Value— Sequential message timeout

Default— 20

<transient-session-timeout>—(Optional) The timeout in seconds to expire a temporary session.

Value— Transient session timeout

Default— 90

<max-update-interval>—(Optional) The maximum interval of interim updates in seconds for user sessions.

Value— Maximum interval of interim updates

Default— 3600

<update-grace-period>—(Optional) Grace period in seconds to expect an interim update for a user session.

Value— Grace period for an interim update

Default— 900

`<resume-unrecovered>`—(Optional) Specifies whether a user session that has failed to recover from a failover should be resumed.

Value— true or false

Default— true

`<thread-pool-size>`—(Optional) The number of working threads that process requests.

Value— Thread pool size

Default— 50

`<thread-idle-timeout>`—(Optional) The timeout in seconds to kill working threads after they become idle.

Value— Thread idle timeout

Default— 60

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/aaa)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <aaa>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </aaa>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the session store for the AAA NAS groups.

Contents

`<maximum-queue-age>`—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

`<maximum-queued-operations>`—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

`<maximum-queue-size>`—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

`<maximum-file-size>`—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

`<minimum-disk-space-usage>`—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

`<rotation-batch-size>`—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

`<maximum-session-size>`—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

`<disk-load-buffer-size>`—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

`<network-buffer-size>`—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{<size of maximum session size field>}$ –2147483647

Default— 51050

`<retry-interval>`—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

`<communications-timeout>`—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

`<load-timeout>`—(Optional) Amount of time that an active session store waits for a passive session store or, a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<junos> (configuration/shared/sae/configuration/driver)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junos>
            <beep-server-port>beep-server-port</beep-server-port>
            <tls-beep-server-port>tls-beep-server-port</tls-beep-server-port>
            <connection-attempts>connection-attempts</connection-attempts>
            <keepalive-interval>keepalive-interval</keepalive-interval>
            <message-timeout>message-timeout</message-timeout>
            <batch-size>batch-size</batch-size>
            <transaction-batch-time>transaction-batch-time</transaction-batch-
time>
            <sdx-group-name>sdx-group-name</sdx-group-name>
            <sdx-session-group-name>sdx-session-group-name</sdx-session-group-
name>
            <send-commit-check>send-commit-check</send-commit-check>
          </junos>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage JUNOS routing platforms. A JUNOS routing platform interacts with the SAE by using a JUNOS software process called sdx. When the sdx process establishes a TCP/IP connection to the SAE, the SAE begins to manage the router. The JUNOS router driver configuration defines parameters related to the interactions between the SAE and the sdx process.

Contents

<beep-server-port>— TCP port number that is used to communicate with the sdx process on JUNOS routing platforms. This port number must match the port number configured in the sdx process on the router.

Value— TCP port number; if this value is set to zero and the TLS BEEP

server port is set, the SAE accepts only TLS connections.

If you change this port number, you need to restart the SAE before the change takes effect.

Default— 3333

`<tls-beep-server-port>`— TCP port number used to communicate with the `sdx`d process on JUNOS routing platforms using a secure TLS connection.

Value— TLS port number; if this value is set to zero, the SAE does not accept TLS connections.

If you change this port number, you need to restart the SAE before the change takes effect.

Default— 3434

`<connection-attempts>`— Number of outstanding connection attempts before the SAE starts dropping new connection attempts.

Value— Positive value greater than 0; if the value is equal to or less than 0, the default value is used.

Default— 50

`<keepalive-interval>`— Interval between keepalive messages sent from the router. The `sdx`d process on the router monitors the connection to the SAE by sending keepalive messages at one-third the specified interval. If the `sdx`d process does not receive the expected keepalive answer within the specified timeout, it closes the connection.

A short interval results in a high load on the BEEP interface.

A long interval results in a long time before a connection failure is detected.

Value— Number of seconds in the range 0-2147483647. A value of 0 means that timeout is disabled.

Default— 45

`<message-timeout>`— Amount of time that the router driver waits for a response from the `sdx`d process. Under a high load the router may not be able to respond fast enough to requests.

Change this value only if a high number of timeout events appear in the error log.

Value— Number of milliseconds in the range 0–2147483647

Default— 30000

`<batch-size>`— Minimum number of service configuration transactions that are committed at the same time. If any of the transactions in a batch fails, all transactions are aborted, and the associated service activations or deactivations fail.

To control maximum latency for a job when services are activated in parallel, specify 120% of the number of CORBA threads as the batch size.

Value— Integer in the range 0–2147483647

Default— 10

`<transaction-batch-time>`— Maximum time to collect configuration transactions in a batch. The batch is completed if either the batch size or the batch time is reached.

The completion time is calculated from the creation of a batch. Note that the batch time is a function of the total configuration size and not of the number of commands in the configuration transactions.

Value— Number of milliseconds in the range 0–2147483647

Default— 2000

`<sdx-group-name>`— Name of group on the JUNOS routing platform in which provisioning objects are stored.

Value— Name configured on the JUNOS routing platform

Default— sdx

`<sdx-session-group-name>`— Name of group on the JUNOS routing platform in which session objects are stored.

Value— Name configured on the JUNOS routing platform

Default— sdx-sessions

`<send-commit-check>`— Enables or disables commit check. If enabled, a more detailed error message is logged if a batch fails, which lets you verify individual transactions in a batch.

To maximize service activation performance, commit check should be disabled.

Value— true or false

Default— true

Required Privilege Level

system

<configuration-checking> (configuration/shared/sae/configuration/driver/junos)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junos>
            <configuration-checking>
              <configuration-checking-schedule>configuration-checking-
schedule</configuration-checking-schedule>
              <configuration-checking-action>configuration-checking-action-
choice</configuration-checking-action>
            </configuration-checking>
          </junos>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to periodically check the configuration of the JUNOS routing platform.

Contents

<configuration-checking-schedule>—(Optional) Specifies when the SAE checks the router configuration.

Value— The schedule format is modeled on the UNIX crontab Entry Format (see UNIX crontab man pages). It consists of seven fields separated by space or tabs and enclosed in double quotation marks. The fields specify:

- Minute (0-59)
- Hour (0-23)
- Day of month (1-31, or the first three letters of the day of month)
- Month of the year (1-12)

- Day of the week (0-6 with 0 = Sunday, or the first three letters of the name of the day)
- Year (4 digits indicating the year)
- Time Zone ID: An * indicates the SAE local time zone.

For custom time zones, specify the format:

- zone = "GMT" (" + " | "-") (hour : minute | hour minute | hour)
- hour = digit digit
- minute = digit digit
- digit = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

Use the following guidelines when configuring the schedule:

- An asterisk (*) is interpreted as 0 for minutes and hours and as the SAE local time zone for time zone. For all other fields, it stands for "first-last."
- Ranges of numbers and names are allowed. Ranges are two values separated with a hyphen. The specified range is inclusive. For example, 1-5 for the hour field specifies checking at hours 1, 2, 3, 4, and 5.
- Lists are allowed. A list is a set of numbers (or ranges) separated by commas. For example: "1,2,5,9", "0-4,8-12".
- Step values can be used with ranges. Following a range with "/" < number > " specifies skips in the number's value through the range. For example, "0-23/2" in the hours field specifies event execution every other hour. Steps are also permitted after an asterisk, so "* /2" specifies every 2 hours.
- When determining the next event time based on a specific time pattern, the following rules apply: Seconds and milliseconds are ignored (that is, rounded up to the closest minute). If you set both a day of the month and a day of the week, only the day of month is used.

Default— No value

<configuration-checking-action>—(Optional) Action that the SAE takes when it detects disparities between the configuration of the SAE and the configuration on the router.

Value— One of the following:

- detect—Reports disparities through the SAE router driver event trap called routerConfOutOfSynch and through the info log. The SAE does not make any changes on the router.
- enforce—Enforces the state of the session layer on the router. The SAE removes all sessions that have disparities and creates new sessions with the same activation parameters as the original ones

- **synchronize**—Synchronizes the state of the session layer on the router. The SAE removes all sessions that have disparities.

Required Privilege Level

system

<lsp-tracking> (configuration/shared/sae/configuration/driver/junos)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junos>
            <lsp-tracking>
              <match>match</match>
              <file>file</file>
            </lsp-tracking>
          </junos>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure event tracking for JUNOS LSPs to provide information to an application, such as the sample IPTV application, that needs information about LSP status.

LSP tracking can configure the system log on managed JUNOS routing platforms to send notification messages to the managing SAE when LSPs are created and removed, and when bandwidth allocation for an LSP changes.

Contents

<match>—(Optional) A regular expression to identify a set of LSP names. If you do not define an expression, the SAE tracks all LSPs.

Value— Regular expression

Default— No value

<file>—(Optional) Name of the file to store syslog event messages (that provide information about LSP state changes in a JUNOS routing platform).

Value— Filename
Default— mpls4sae

Required Privilege Level

system system

<security> (configuration/shared/sae/configuration/driver/junos)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junos>
            <security>
              <need-client-authentication/>
              <local-certificate>local-certificate</local-certificate>
            </security>
          </junos>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Transport Layer Security (TLS) on the SAE.

Contents

<need-client-authentication>—(Optional) Enables or disables whether or not the SAE requests a client certificate from the router

If enabled, the SAE asks the router for a client certificate when a connection to the router is established.

If disabled, the SAE does not ask the router for a client certificate when a connection to the router is established.

Default— Enabled

<local-certificate>—(Optional) Name of certificate to be used for TLS communications

Value— Name of certificate
Default— No value

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/junos)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junos>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </junos>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the JUNOS driver.

Contents

`<maximum-queue-age>`—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

`<maximum-queued-operations>`—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

`<maximum-queue-size>`—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

`<maximum-file-size>`—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

`<minimum-disk-space-usage>`—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

`<rotation-batch-size>`—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

`<maximum-session-size>`—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

`<disk-load-buffer-size>`—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

`<network-buffer-size>`—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{<size of maximum session size field>}$ –2147483647

Default— 51050

`<retry-interval>`—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

`<communications-timeout>`—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

`<load-timeout>`—(Optional) Amount of time that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<junose> (configuration/shared/sae/configuration/driver)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junose>
            <cops-server-port>cops-server-port</cops-server-port>
            <backlog>backlog</backlog>
            <keepalive-interval>keepalive-interval</keepalive-interval>
            <message-timeout>message-timeout</message-timeout>
            <cops-message-maximum-length>cops-message-maximum-length</cops-
message-maximum-length>
            <cops-message-read-buffer-size>cops-message-read-buffer-size</
cops-message-read-buffer-size>
            <cops-message-write-buffer-size>cops-message-write-buffer-size</
cops-message-write-buffer-size>
            <pending-address-timeout>pending-address-timeout</pending-address-
timeout>
            <cops-handler-threads>cops-handler-threads</cops-handler-threads>
            <cached-driver-expiration>cached-driver-expiration</cached-driver-
expiration>
            <drop-unmanaged-interfaces-xdr-driver/>
            <track-unmanaged-interfaces-xdr-driver/>
          </junose>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage JUNOSE routers. The router driver specifies the COPS connection between the SAE COPS server and the COPS client in the JUNOSE router.

Contents

<cops-server-port>— TCP port number of the COPS server used to communicate with the JUNOSE routers.

Value— Port number that matches the configuration of the SRC client in the JUNOS router.

Default— 3288

`<backlog>`— Maximum number of outstanding connection attempts before connections are dropped.

Value— Integer

Default— 50

`<keepalive-interval>`— Interval between keepalive messages sent from the COPS client (the JUNOS router). The COPS client monitors the COPS connection by sending keepalive messages at random intervals between one-fourth and three-fourths of the specified interval. If the client does not receive the expected keepalive answer within the specified timeout, the client terminates the connection.

A short interval results in a high load on the COPS interface.

A long interval results in a long time before a COPS failure is detected.

Value— Number of seconds in the range 0-32768. A value of 0 means that timeout is disabled.

Default— 45

`<message-timeout>`— Timeout interval in which the COPS server waits for a response to COPS requests. Under a high load the router may not be able to respond fast enough to COPS requests. Change this value only if a high number of COPS timeout events appear in the error log.

Value— Number of milliseconds

Default— 120000

`<cops-message-maximum-length>`— Maximum length of a COPS message. We recommend that you use the default setting.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 200000

`<cops-message-read-buffer-size>`— Buffer size for receiving COPS messages from the JUNOS client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

`<cops-message-write-buffer-size>`— Buffer size for sending COPS messages to the JUNOS client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

`<pending-address-timeout>`— Maximum time that a DHCP address request remains pending.

Value— Number of milliseconds. Typical values are in the range 1000-15000 (1 second to 15 seconds).

Default— 5000

`<cops-handler-threads>`—(Optional) Size of the thread pool for handling unsolicited messages. These threads are shared among all JUNOS router drivers. You may want to set this value higher than the default if you wish to create greater throughput on platforms with multiple processing cores, and you are not achieving full processor resource utilization. Increasing the number of threads increases the ability to use multiple processing cores in parallel.

Value— Number of threads

Default— No value

`<cached-driver-expiration>`— Minimum amount of time to keep the state of a router driver after its COPS connection is closed. You might want to change this value because the SAE can resynchronize more quickly if most of the state is still in memory and it does not need to be reread from the disk.

Value— Number of seconds in the range 0-2147483647

Default— 600

`<drop-unmanaged-interfaces-xdr-driver>`—(Optional) For JUNOS COPS-XDR drivers, enables or disables the driver to keep a record of unmanaged interfaces. You must enable this option if you have unmanaged dynamic interfaces in a virtual router that is managed by COPS-XDR. If the driver does not keep a record of unmanaged interfaces, next-interface actions in policies may not work properly in certain cases. To use RAM more efficiently, enable this option if you have a large number of unmanaged interfaces that are not the target of next-hop policies.

Default— Disabled

`<track-unmanaged-interfaces-xdr-driver>`—(Optional) Enables sending of interface tracking events for unmanaged interfaces of the XDR router driver. Because the COPS-XDR protocol does not include notifications (DRQs) when unmanaged interfaces are disabled, plug-ins will not receive an unmanaged interface's stop events.

Default— Disabled

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/junose)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <junose>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </junose>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the JUNOSe driver.

Contents

<maximum-queue-age>—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

<maximum-queued-operations>—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

<maximum-queue-size>—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

<maximum-file-size>—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

<minimum-disk-space-usage>—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

<rotation-batch-size>—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

`<maximum-session-size>`—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

`<disk-load-buffer-size>`—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

`<network-buffer-size>`—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{<size of maximum session size field>}$ –2147483647

Default— 51050

`<retry-interval>`—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

`<communications-timeout>`—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

`<load-timeout>`—(Optional) Amount of time that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<pcmm> (configuration/shared/sae/configuration/driver)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <pcmm>
            <keepalive-interval>keepalive-interval</keepalive-interval>
            <tcp-connection-timeout>tcp-connection-timeout</tcp-connection-
timeout>
            <application-manager-id>application-manager-id</application-
manager-id>
            <message-timeout>message-timeout</message-timeout>
            <cops-message-maximum-length>cops-message-maximum-length</cops-
message-maximum-length>
            <cops-message-read-buffer-size>cops-message-read-buffer-size</
cops-message-read-buffer-size>
            <cops-message-write-buffer-size>cops-message-write-buffer-size</
cops-message-write-buffer-size>
            <sae-community-manager>sae-community-manager</sae-community-
manager>
            <disable-full-sync/>
            <disable-pcmm-i03-policy/>
            <session-recovery-retry-interval>session-recovery-retry-interval</
session-recovery-retry-interval>
            <element-id>element-id</element-id>
            <default-rks-plug-in>default-rks-plug-in</default-rks-plug-in>
          </pcmm>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage PCMM devices. The SAE connects to the PCMM device by using a COPS-over-TCP connection. The PCMM device driver controls this connection.

Contents

`<keepalive-interval>`— Interval between keepalive messages sent from the COPS client (the PCMM device) to the COPS server (the SAE). The COPS client monitors the COPS connection by sending keepalive messages at random intervals between one-fourth and three-fourths of the specified interval. If the client or the server does not receive the expected keepalive answer within the specified timeout, the client closes the connection.

Value— Number of seconds in the range 0-2147483647. A value of 0 means that the timeout is disabled.

Default— 45

`<tcp-connection-timeout>`— Timeout for opening a TCP connection to the PCMM device.

Value— Number of seconds in the range 0-2147483647.

Default— 5

`<application-manager-id>`— Identifier of the application manager when this SAE is configured as the application manager. The application manager includes this identifier in all messages that it sends to the policy server. The policy server passes this ID to the CMTS device in Gate Control messages. The CMTS device returns the ID associated with the gate to the policy server. The policy server uses this information to associate gate messages with a particular application manager.

Value— 4-byte unsigned integer that is unique in a service provider network.

Default— 1

`<message-timeout>`— Amount of time that the COPS server (the SAE) waits for a response to COPS requests from the COPS client (the PCMM device). Under a high load the PCMM device may not be able to respond fast enough to COPS requests. Change this value only if a high number of COPS timeout events appear in the error log.

Value— Number of milliseconds in the range 0-2147483647

Default— 120000

`<cops-message-maximum-length>`— Maximum length of a COPS message. We recommend that you use the default setting.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 204800

`<cops-message-read-buffer-size>`— Buffer size for receiving COPS messages from the PCMM client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

`<cops-message-write-buffer-size>`— Buffer size for sending COPS messages to the PCMM client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

`<sae-community-manager>`— Name of the community manager that manages PCMM driver communities. Active SAEs are selected from this community.

Value— Community name

Default— PCMMCommunityManager

`<disable-full-sync>`—(Optional) Disables state synchronization with PCMM policy servers. State synchronization is achieved when the SAE is required to communicate with the policy server over the COPS connection.

Default—false

`<disable-pcmm-i03-policy>`—(Optional) Disables the SAE to send classifiers to the router that comply with PCMM I03. Use this option if your network deployment has CMTS devices that do not support PCMM I03.

Default—true

`<session-recovery-retry-interval>`— Time interval between attempts by the SAE to restore service sessions that are still being recovered in the background when state synchronization is completed with a state-data-incomplete error. The SAE attempts to restore a service session if it receives a service modification or deactivation request for an unrecovered service session before the next interval.

We recommend setting this value to 3600000 (1 hour) or longer.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<element-id>`—(Optional) Unique identifier that the SAE uses to identify itself when it originates RKS events.

Value— 8-byte unsigned integer in the range 0–99999; must be unique within a PCMM network

Default— 1

`<default-rks-plug-in>`—(Optional) RKS plug-in to which the SAE sends event messages if you do not configure a CMTS-specific plug-in.

Value— Name of an RKS plug-in

Default— No value

Required Privilege Level

system

<cmts-specific-rks-plug-ins> (configuration/shared/sae/configuration/driver/pcmm)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <pcmm>
            <cmts-specific-rks-plug-ins>
              <name>name</name> <!-- identifier -->
              <rks-plug-in>rks-plug-in</rks-plug-in>
            </cmts-specific-rks-plug-ins>
          </pcmm>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a CMTS-specific RKS plug-in.

Contents

<name>— Name of the RKS plug-in.

Value—Text

<rks-plug-in>—(Optional) Name of the plug-in to which the SAE sends events for this CMTS device.

Value— Name of an RKS plug-in

Default— No value

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/pcmm)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <pcmm>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </pcmm>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the PCMM driver.

Contents

`<maximum-queue-age>`—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

`<maximum-queued-operations>`—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

`<maximum-queue-size>`—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

`<maximum-file-size>`—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

`<minimum-disk-space-usage>`—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

`<rotation-batch-size>`—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

`<maximum-session-size>`—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

`<disk-load-buffer-size>`—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

`<network-buffer-size>`—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{<size of maximum session size field>}$ –2147483647

Default— 51050

`<retry-interval>`—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

`<communications-timeout>`—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

`<load-timeout>`—(Optional) Amount of time that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<scripts> (configuration/shared/sae/configuration/driver)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <scripts>
            <extension-path>extension-path</extension-path>
            <general>general</general>
            <junos>junos</junos>
            <junose-pr>junose-pr</junose-pr>
            <junose-xdr>junose-xdr</junose-xdr>
            <pcmm>pcmm</pcmm>
            <third-party>third-party</third-party>
          </scripts>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure device scripts. When the SAE establishes a connection with a router, PCMM device, or other network device, it can run a script to customize the setup of the connection. These scripts are run when the connection is established and again when the connection is dropped.

Contents

<extension-path>—(Optional) Path to scripts that are not in the default location, */opt/UMC/sae/lib*.

Value— List of paths separated by semicolons (;)

Default— No value

<general>—(Optional) Script that can be used for all types of routers, PCMM devices, and other network devices that the SRC software supports. The script is run when the connection between a router or other network device and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

<junos>—(Optional) Initialization script for JUNOS routing platforms. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

<junose-pr>—(Optional) Initialization script for JUNOSe routers when the JUNOSe driver uses COPS-PR mode when connecting to the SAE. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

Value— Name of the file that contains the script without including the .py extension.

Default— No value

<junose-xdr>—(Optional) Initialization script for JUNOSe routers when the JUNOSe driver uses XDR mode when connecting to the SAE. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

In COPS XDR mode, the router does not send the network access server (NAS) IP address to the SAE. If your configuration requires this value, add the following line to a JUNOSe script:

```
import ERXnasip
```

When you add the import ERXnasip entry, the script obtains the NAS-IP address from the router through SNMP. This mechanism can affect performance, especially when the SAE manages a large number of virtual routers.

Value— Name of a script. For example, iorPublisher, poolPublisher.

Default— No value

<pcmm>—(Optional) Initialization script for the Juniper Policy Server in a PCMM environment. The script is run when the connection between a policy server and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

<third-party>—(Optional) Initialization script for third-party device drivers. The script

is run when the third-party device driver is activated or deactivated.

Value— Name of a script. For example, iorPublisher.

Default— No value

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <session-store>
            <ip-address>ip-address</ip-address>
            <port>port</port>
            <root-directory>root-directory</root-directory>
          </session-store>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure global session store parameters that are shared by all session store instances (active or passive) on the SAE. You can also configure session store parameters within a router or other device driver configuration.

Contents

<ip-address>—(Optional) IP address that the session store infrastructure on this SAE uses to listen for incoming TCP connections from active session stores.

Value— IP address. The address must be an IP address configured for the SAE host. If you do not enter an address or if you disable this field, active session stores cannot create passive session stores on this SAE. We recommend that you enter an address that is configured in a list of connected SAEs.

Default— No value

<port>—(Optional) TCP port number on which the session store infrastructure on this SAE listens for incoming connections from active session stores. This option has no effect if you have not configured a session store IP address.

Value— Port number in the range 1027–65535

Default— No value

`<root-directory>`—(Optional) Root directory in which the session store creates files.
This option has no effect if you have not configured a session store IP address.

Value— Directory name

Default— *No value*

Required Privilege Level

system

<simulated> (configuration/shared/sae/configuration/driver)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <simulated>
            <name>name</name> <!-- identifier -->
            <driver-type>driver-type-choice</driver-type>
            <router-version>router-version</router-version>
            <router-address>router-address</router-address>
            <transport-router>transport-router</transport-router>
          </simulated>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure simulated router drivers. Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can then use the simulated subscriber sessions to test SAE applications.

Contents

<name>— Name of the simulated router driver.

Value—Text

<driver-type>— Type of device that the simulated driver simulates

Value— One of the following:

- junos
- junose
- pcmm

Default— JUNOS

`<router-version>`—(Optional) Version of the device software to simulate.

Value— Valid software version for the device that is being simulated.

Default— No value

`<router-address>`— Address of the router that is available for router initialization scripts.

Value— IP address

Default— 10.0.0.1

`<transport-router>`—(Optional) Name of a virtual router that is used to connect to the SAE. This value is passed to the router initialization script. It is not supported on JUNOS routing platforms.

Value— Name of a virtual router

Default— No value

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/simulated)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <simulated>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </simulated>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the simulated driver.

Contents

`<maximum-queue-age>`—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

`<maximum-queued-operations>`—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

`<maximum-queue-size>`—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

`<maximum-file-size>`—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

`<minimum-disk-space-usage>`—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

`<rotation-batch-size>`—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

<maximum-session-size>—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

<disk-load-buffer-size>—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

<network-buffer-size>—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{< size of maximum session size field >}$ –2147483647

Default— 51050

<retry-interval>—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

<communications-timeout>—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

<load-timeout>—(Optional) Amount of time that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<snmp> (configuration/shared/sae/configuration/driver)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <snmp>
            <read-only-community-string>read-only-community-string</read-only-
community-string>
            <read-write-community-string>read-write-community-string</read-
write-community-string>
          </snmp>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure global default SNMP communities for use with JUNOS routers and JUNOS routing platforms. Global default SNMP communities are used if a virtual router does not exist on the router or the community strings have not been configured for the VR.

Contents

<read-only-community-string>— Default SNMP community string used for read access to the router.

Value— SNMP community string that matches a read-only community string configured on the router.

Default— public

<read-write-community-string>— Default SNMP community string used for write access to the router.

Value— SNMP community string that matches a read-write community string configured on the router.

Default— private

Required Privilege Level

system

<third-party> (configuration/shared/sae/configuration/driver)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <third-party>
            <sae-community-manager>sae-community-manager</sae-community-
manager>
          </third-party>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the community manager for third-party devices that the SAE manages.

Contents

<sae-community-manager>— Name of the community manager that manages network device communities. Active SAEs are selected from this community.

Value— Community name

Default— PROXYCommunityManager

Required Privilege Level

system

<session-store> (configuration/shared/sae/configuration/driver/third-party)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <driver>
          <third-party>
            <session-store>
              <maximum-queue-age>maximum-queue-age</maximum-queue-age>
              <maximum-queued-operations>maximum-queued-operations</maximum-
queued-operations>
              <maximum-queue-size>maximum-queue-size</maximum-queue-size>
              <maximum-file-size>maximum-file-size</maximum-file-size>
              <minimum-disk-space-usage>minimum-disk-space-usage</minimum-
disk-space-usage>
              <rotation-batch-size>rotation-batch-size</rotation-batch-size>
              <maximum-session-size>maximum-session-size</maximum-session-
size>
              <disk-load-buffer-size>disk-load-buffer-size</disk-load-buffer-
size>
              <network-buffer-size>network-buffer-size</network-buffer-size>
              <retry-interval>retry-interval</retry-interval>
              <communications-timeout>communications-timeout</communications-
timeout>
              <load-timeout>load-timeout</load-timeout>
              <idle-timeout>idle-timeout</idle-timeout>
              <maximum-backlog-ratio>maximum-backlog-ratio</maximum-backlog-
ratio>
              <minimum-backlog>minimum-backlog</minimum-backlog>
            </session-store>
          </third-party>
        </driver>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the third-party device driver.

Contents

`<maximum-queue-age>`—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

`<maximum-queued-operations>`—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

`<maximum-queue-size>`—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

`<maximum-file-size>`—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

`<minimum-disk-space-usage>`—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30–50

Default— 25

`<rotation-batch-size>`—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at

the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

`<maximum-session-size>`—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

`<disk-load-buffer-size>`—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

`<network-buffer-size>`—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range $21 + \text{<size of maximum session size field>}$ –2147483647

Default— 51050

`<retry-interval>`—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

`<communications-timeout>`—(Optional) Amount of time that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk.

Value— Number of milliseconds in the range 0–2147483647

Default— 60000

`<load-timeout>`—(Optional) Amount of time that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store.

Value— Number of milliseconds in the range 0–2147483647

Default— 420000

`<idle-timeout>`—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

`<maximum-backlog-ratio>`—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

`<minimum-backlog>`—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Required Privilege Level

system

<dynamic-radius-server> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <dynamic-radius-server>
          <maximum-cached-peer>maximum-cached-peer</maximum-cached-peer>
        </dynamic-radius-server>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of peers that the dynamic RADIUS server can maintain.

Contents

<maximum-cached-peer>— Maximum number of peers maintained by the dynamic RADIUS server.

Value— Integer

Default— 100

Required Privilege Level

system

<external-interface-features> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <name>name</name> <!-- identifier -->
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an external interface configuration.

Contents

<name>— Name of the external interface configuration.

Value—Text

Required Privilege Level

system

<CommunityManager> (configuration/shared/sae/configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <CommunityManager>
            <keepalive-interval>keepalive-interval</keepalive-interval>
            <threads>threads</threads>
            <acquire-timeout>acquire-timeout</acquire-timeout>
            <blackout-time>blackout-time</blackout-time>
          </CommunityManager>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE community manager that manages PCMM and third-party device communities.

Contents

<keepalive-interval>— Interval between keepalive messages sent from the active SAE to the passive members of the community.

Value— Number of seconds in the range 0–2147483647

Default— 30

<threads>— Number of threads that are allocated to manage the community. You generally do not need to change this property.

Value— Integer in the range 1–50

Default— 5

`<acquire-timeout>`— Amount of time an SAE waits for a remote member of the community when it is acquiring a distributed lock. To avoid race conditions when the SAE community is determining which SAE is the active SAE, the community manager has a distributed lock. When an SAE attempts to become the active SAE, it needs to acquire the distributed lock. You generally do not need to change this property.

Value— Number of seconds in the range 0–2147483647

Default— 15

`<blackout-time>`— Amount of time that an active SAE must wait after it shuts down before it can try to become the active SAE of the community again.

Value— Number of seconds in the range 0–2147483647

Default— 30

Required Privilege Level

system

<EventAPI> (configuration/shared/sae/configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <EventAPI>
            <retry-time>retry-time</retry-time>
            <retry-limit>retry-limit</retry-limit>
            <threads>threads</threads>
          </EventAPI>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for the Event Notification API.

Contents

<retry-time>— Amount of time between attempts to send router events that could not be delivered.

Value— Number of seconds in the range 0–2147483647

Default— 300

<retry-limit>— Maximum number of times an event fails to be delivered before it is discarded.

Value— Integer in the range 0–2147483647

Default— 5

<threads>— Number of threads allocated to process events.

Value— Integer in the range 0–2147483647

Default— 5

Required Privilege Level

system

<JavaScriptProcessor> (configuration/shared/sae/ configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <JavaScriptProcessor>
            <script-directory>script-directory</script-directory>
            <scan-interval>scan-interval</scan-interval>
            <compiler-classpath>compiler-classpath</compiler-classpath>
            <character-encoding>character-encoding</character-encoding>
            <compiler-debug/>
            <java-compiler>java-compiler</java-compiler>
          </JavaScriptProcessor>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE properties that activate and configure the Java script interface module.

Contents

<script-directory>—(Optional) Storage location for Java scripts; defined relative to the SAE installation directory. If you store the scripts in the /opt/UMC/sae/var/javaScripts directory on the SRC system, you do not need to specify this property.

Do not specify a directory that is part of the class path of the JVM running the SAE. If you do so, unloading of Java scripts will fail.

Value— Path that can be read by a URL class loader, in one of the following formats:

- file: // < path > < filename >
- http: // < hostName > . < portNumber > < path > < filename >

- path—List of directories separated by forward slashes
- filename—Name of the JAR file
- hostName—Name of the host on which the script is stored
- portNumber—Number of the TCP/IP port

Default— *var/javaScripts*

<scan-interval>— Time interval between scans in the script directory for new or modified .java source files. At each scan, the interface module compiles new and modified files. If the scripts conform to Java script requirements, the interface module installs them on the SAE as Java scripts. It also removes deleted scripts from the SAE.

Value— Number of seconds in the range 0–2147483647; 0 (zero) means that the interface module does not scan the directories.

Default— 0

<compiler-classpath>— Class path that the compiler uses to load source files.

Value— Path that can be read by a URL class loader, in one of the following formats:

- file: // < path > < filename >
- http:// < hostName > . < portNumber > < path > < filename >
- path—List of directories separated by forward slashes
- filename—Name of the JAR file
- hostName—Name of the host on which the script is stored
- portNumber—Number of the TCP/IP port

If you clear this value, the value defaults to the Java script directory specified by the script-directory option.

Default— *var/javaScripts:lib/sae.jar*

<character-encoding>—(Optional) Character encoding that the compiler uses when it loads Java source files.

Value— See <http://java.sun.com/j2se/1.4/docs/guide/intl/encoding.doc.html>

Default— Default encoding for the platform on which you are working

<compiler-debug>—(Optional) Enables or disables whether the compiler places debug information into .class files

Default— Disabled`<java-compiler>`—(Optional)

If you do not specify an external compiler, the interface module compiles the scripts-in-process with the `com.sun.tools.javac.Main` compiler from Sun Microsystems's `tools.jar`. The information specified in the Character Encoding, Compiler Classpath, and Compiler Debug fields is passed to the compiler.

If you specify an external compiler, an external process is created to perform the compilation using the specified command, and the information specified in the Character Encoding, Compiler Classpath, and Compiler Debug fields is ignored. Assumptions:

- The specified shell command will invoke an appropriate Java compiler without error.
- The specified shell command uses a class path that includes both the Java script directory specified in the Script Directory field and the SAE's public APIs.
- The compiler outputs its `.class` files to the directory specified in the Script Directory field.

Value— Command string with the class path that identifies both the Java script directory and the public APIs for the SAE.

Default— `javac -classpath var/javaScripts:lib/sae.jar -d var/javaScripts`

Required Privilege Level

system

<PythonScriptProcessor> (configuration/shared/sae/ configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <PythonScriptProcessor>
          </PythonScriptProcessor>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an instance of the Python script processor.

Contents

Required Privilege Level

system

<SAEAccess> (configuration/shared/sae/configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <SAEAccess>
            <cache-size>cache-size</cache-size>
            <cache-timeout>cache-timeout</cache-timeout>
            <cache-clean>cache-clean</cache-clean>
          </SAEAccess>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for the SAE access interface module.

Contents

<cache-size>— Maximum number of subscriber objects kept in the cache.

Value— Integer in the range 0–2147483647

Default— 1024

<cache-timeout>— Maximum time that idle subscriber objects are kept in the cache.

Value— Number of seconds in the range 0–2147483647

Default— 30

<cache-clean>— Number of subscriber objects removed from the cache when the maximum number is reached.

Value— Integer in the range 1– < cache size >

Default— 1

Required Privilege Level

system

<SAEFeature> (configuration/shared/sae/configuration/external-interface-features)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <SAEFeature>
            <java-class>java-class</java-class>
            <additional-classpath>additional-classpath</additional-classpath>
          </SAEFeature>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SAE properties for customized interface modules.

Contents

<java-class>— Name of the Java class that implements the interface module.

Value— Fully qualified Java class name. For example,net.juniper.smg.
sae.saeimpl.SAEAccessImpl.

Default— No value

<additional-classpath>—(Optional) Path to the location where libraries are stored.
If you store the libraries in the /opt/UMC/sae/lib directory on the host where you installed the SAE software, you do not need to specify a class path.

Value— Comma-separated list of URLs that can be read by a URL class loader in one of the following formats:

- file:// < path > < filename >
- http:// < hostName > < portNumber > < path > < filename >

where

- path is a list of directories separated by backslashes
- filename is the name of the JAR file
- hostName is the name of the host on which the script is stored
- portNumber is the number of the TCP/IP port

Default— No value

Required Privilege Level

system

<properties> (configuration/shared/sae/configuration/external-interface-features/SAEFeature)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <external-interface-features>
          <SAEFeature>
            <properties>
              <name>name</name> <!-- identifier -->
              <value>value</value>
            </properties>
          </SAEFeature>
        </external-interface-features>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define properties for an SAE customized interface module.

Contents

<name>— Name of the property for which you want to define a value.

Value—Text

<value>— Value for the property.

Value— Value for the property.

Default— No value

Required Privilege Level

system

<file-accounting-template> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <file-accounting-template>
          <name>name</name> <!-- identifier -->
        </file-accounting-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a template that defines header names for attributes listed in accounting files. When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. For example, in the following accounting file, the first line lists headers for all attribute fields in the file, and the following lines list the actual data in each field:

Accounting Status,NAS ID,SAE Host,Router Name,Interface Name,Interface Alias

start,SSP.uelmo,uelmo,default@erx7_ssp57,FastEthernet1/1.1.

You can assign your own names to the headers that appear in the file. To do so, you define the header names in a template and then set up file accounting plug-ins to use the template. The default template, FileAccounting.std, defines header names for all possible attributes. You can use the default template or create your own templates.

Contents

<name>— Name of the file-accounting template.

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/file-accounting-template)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <file-accounting-template>
          <attributes>
            <name>name-choice</name> <!-- identifier -->
            <value>value</value>
          </attributes>
        </file-accounting-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure the values for the attribute headers that will appear in accounting files.

Contents

Name of the accounting attribute for which you want to define a header.

Value

- status
- nas-id
- host
- router-name
- interface-name
- interface-alias
- interface-descr
- port-id
- user-ip-address
- login-name
- accounting-id
- auth-user-id
- if-radius-class
- if-session-id
- service-name
- radius-class

- event-time
- session-id
- terminate-cause
- session-time
- in-octets
- out-octets
- in-packets
- out-packets
- nas-ip
- user-mac-address
- service-session-name
- service-session-tag
- user-type
- user-radius-class
- user-session-id
- primary-user-name
- subscription-name
- login-id
- if-index
- event-time-millisecond
- nas-port
- operational
- user-inet-address
- nas-inet-address
- router-type
- interface-speed
- service-bundle
- user-dn
- uid
- domain
- retailer-dn
- password
- service-scope
- session-timeout
- downstream-bandwidth
- upstream-bandwidth
- dhcp-packet
- aggr-session-id
- aggr-login-name
- aggr-user-dn
- aggr-user-inet-address
- aggr-accounting-id
- aggr-auth-user-id

<value>— Header text that appears in the accounting file.

Value— Text that you want to appear as the header in the property file.
If the header contains spaces, enclose the header in quotation marks.

Default— No value

Required Privilege Level

system

<global-radius-udp-port> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <global-radius-udp-port>
          <udp-port>udp-port</udp-port>
        </global-radius-udp-port>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a global source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers.

In RADIUS packets that RADIUS plug-ins send to a RADIUS server, the plug-in uses an identifier field to match requests to replies. This field provides for a maximum of 256 identifiers. Once all identifiers are used, the plug-in cannot send any more requests until it receives replies that match the requests already sent. In high-load systems, this limit can slow performance.

To overcome this limitation, you can configure a pool of UDP ports for RADIUS plug-ins. Having a pool of ports allows RADIUS plug-ins to create one queue per port to wait for RADIUS replies. Each queue can wait for 256 RADIUS packets. The RADIUS plug-ins send RADIUS packets through the pool of ports in a round-robin mode.

Contents

<udp-port>— Global source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers. You can also configure UDP ports for each plug-in instance. If you do not configure a UDP port for a plug-in instance, the plug-in uses the global UDP port.

Value— You can enter a single port number, a pool of port numbers, or a list of port numbers and port ranges:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003

Default— 18130

Required Privilege Level

system

<idle-timeout> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <idle-timeout>
          <adjust-session-time/>
        </idle-timeout>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify whether or not the SAE reduces the session time reported in the accounting stop message by the idle time. This way the session time is accurately reported to avoid overcharges for the session.

Contents

<adjust-session-time>—(Optional) If enabled, when an idle timeout terminates a session, the session time reported in the accounting stop message is reduced by the idle time.

Default— No value

Required Privilege Level

system

<interim-accounting> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <interim-accounting>
          <service-interim-accounting/>
          <service-interim-interval>service-interim-interval</service-interim-
interval>
          <subscriber-interim-accounting/>
          <subscriber-interim-interval>subscriber-interim-interval</
subscriber-interim-interval>
        </interim-accounting>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable interim accounting and set intervals between interim accounting messages for services and subscribers. These settings apply to all subscriber sessions and service sessions. You can override these settings for specific services by configuring an accounting interim interval in the service configuration.

Contents

<service-interim-accounting>—(Optional) Enable interim accounting for services. You can override this setting for specific services by configuring an accounting interim interval in the service configuration.

Default— Enabled

<service-interim-interval>— Interval between service interim accounting messages. A short interval causes the SAE to send many messages to the router and to the RADIUS servers. A long interval can result in a large loss of accounting information in the event of a system failure.

Value— Number of seconds in the range 900–86400

Default— 900

`<subscriber-interim-accounting>`—(Optional) Enable interim accounting for subscribers. If enabled, the SAE continually generates Interim-Update accounting requests for all active subscribers at the interval specified with the **subscriber-interim-interval** option.

Default— Enabled

`<subscriber-interim-interval>`— Interval between subscriber interim accounting messages. A short interval causes the SAE to send many messages to any configured accounting servers. A long interval can result in a large loss of accounting information in the event of a system failure.

Value— Number of seconds in the range 900–86400

Default— 900

Required Privilege Level

system

<ldap> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <network-dn>network-dn</network-dn>
          <enable-directory-eventing/>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure the LDAP connection from the SAE to the directory in which network device data is stored.

Contents

<network-dn>— Subtree in the directory in which network device data is stored.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *o= Network, < base>*

<enable-directory-eventing>—(Optional) Enables or disables automatic discovery of changes in the SAE configuration data.

Default— Enabled

Required Privilege Level

system

<directory-eventing> (configuration/shared/sae/configuration/ldap)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <directory-eventing>
            <timeout>timeout</timeout>
            <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
          </directory-eventing>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a timeout for SAE directory eventing, and specify the number of events that the SAE can receive from the directory simultaneously.

Contents

<timeout>— Maximum time that the directory eventing system waits for the directory to respond.

Value— Number of seconds in the range 1–2147483647

Default— No value

<dispatcher-pool-size>— Number of events that the SAE can receive from the directory simultaneously.

Value— Integer in the range 1–2147483647

Default— No value

Required Privilege Level

system

<persistent-login-cache> (configuration/shared/sae/configuration/ldap)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <persistent-login-cache>
            <dn>dn</dn>
            <server-address>server-address</server-address>
            <port-number>port-number</port-number>
            <authentication-dn>authentication-dn</authentication-dn>
            <password>password</password>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
            <blacklist/>
            <ldaps/>
          </persistent-login-cache>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which persistent login cache data is stored.

Contents

<dn>— Subtree in the directory in which persistent login cache data is stored.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— o = authCache, <base>

<server-address>—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

<port-number>—(Optional) Directory port number

Value— Integer in the range -2147483648–2147483647

Default— 389

<authentication-dn>—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

<password>—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the userPassword attribute of the authentication DN.

Default— No value

<directory-eventing>—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.
- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

`<polling-interval>`— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

Required Privilege Level

system

<policy-data> (configuration/shared/sae/configuration/ldap)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <policy-data>
            <policy-dn>policy-dn</policy-dn>
            <parameter-dn>parameter-dn</parameter-dn>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
          </policy-data>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which service data is stored.

Contents

<policy-dn>— Subtree in the directory in which policy data is stored.

Value— <DN> . You can use the special value < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— *o= Policies, < base >*

<parameter-dn>— Subtree in the directory in which policy parameter data is stored.

Value— <DN> . You can use the special value < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— *o= Parameters, < base >*

`<directory-eventing>`—(Optional) Enables or disables automatic discovery of changes to directory data.

- If enabled, changes in policy definitions take effect automatically. If a changed policy is in use, all policy instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in when the change is made.
- If disabled, changes in policy definitions do not take effect until you restart the SAE.

Default— Disabled

`<polling-interval>`— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

Required Privilege Level

system

<service-data> (configuration/shared/sae/configuration/ldap)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <service-data>
            <dn>dn</dn>
            <server-address>server-address</server-address>
            <port-number>port-number</port-number>
            <authentication-dn>authentication-dn</authentication-dn>
            <password>password</password>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
            <blacklist/>
            <ldaps/>
          </service-data>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which service data is stored.

Contents

<dn>— Subtree in the directory in which service data is stored.

The SAE loads service definitions on startup and when service reloading is requested.

Value— <DN> . You can use the special value < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— < base >

<server-address>—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

<port-number>—(Optional) Directory port number

Value—Integer in the range -2147483648–2147483647

Default— 389

<authentication-dn>—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

<password>—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the userPassword attribute of the authentication DN.

Default— No value

<directory-eventing>—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.
- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

`<polling-interval>`— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

Required Privilege Level

system

<subscriber-data> (configuration/shared/sae/configuration/ldap)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <ldap>
          <subscriber-data>
            <subscription-loading-filter>subscription-loading-filter-choice</
subscription-loading-filter>
            <load-subscriber-schedules/>
            <persistent-sessions/>
            <login-cache-dn>login-cache-dn</login-cache-dn>
            <session-cache-dn>session-cache-dn</session-cache-dn>
            <dn>dn</dn>
            <server-address>server-address</server-address>
            <port-number>port-number</port-number>
            <authentication-dn>authentication-dn</authentication-dn>
            <password>password</password>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
            <blacklist/>
            <ldaps/>
          </subscriber-data>
        </ldap>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which subscriber data is stored.

Contents

<subscription-loading-filter>— Filter that the SAE uses to search for subscriptions in the directory when the SAE loads a subscription.

Value— One of the following:

- **subscriberRefFilter**—Subscriber reference filter. The SAE runs a search based on the subscriberRef attribute in the umcServiceProfile object, which is the base object class of the service profile hierarchy. The subscriberRef attribute contains a DN that points to the parent of the subscriber object.
- **objectClassFilter**—Subscription Objectclass filter. The SAE performs a one-level search with the directory entry, which represents the subscriber folder as the base DN. The search filter is (objectClass = sspServiceProfile). This method can be slow if you have a large number of subscription entries within the subscriber folder subtree.

Default— objectClassFilter

`<load-subscriber-schedules>`—(Optional) Enable or disable loading of subscriber schedules.

Default— Enabled

`<persistent-sessions>`—(Optional) Load existing persistent sessions and schedules when starting or recovering a user session.

Default—false

`<login-cache-dn>`— Subtree in the directory where subscriber login information is cached. When a subscriber logs in to a residential portal, the SAE searches subscriber profiles by mapping the realm of the login name to a retailer object found below the search base.

Value— `<DN>` . You can use the special value `<base>` to refer to the globally configured base DN. The string `<base>` is replaced with the directory base DN.

Default— `o= userProfileCache,< base>`

`<session-cache-dn>`— Subtree in the directory where persistent session data is cached.

Value— `<DN>` . You can use the special value `<base>` to refer to the globally configured base DN. The string `<base>` is replaced with the directory base DN.

Default— `o= PersistentSessions,< base>`

`<dn>`— Subtree in the directory in which subscriber data is stored.

When a subscriber logs in to a residential portal, the SAE searches subscriber profiles by mapping the realm of the login name to a retailer object found below the DN.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— o = Users, <base>

<server-address>—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

<port-number>—(Optional) Directory port number

Value— Integer in the range -2147483648–2147483647

Default— 389

<authentication-dn>—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN> . You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

<password>—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the userPassword attribute of the authentication DN.

Default— No value

`<directory-eventing>`—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.
- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

`<polling-interval>`— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

Required Privilege Level

system

<client> (configuration/shared/sae/configuration/license-manager)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <license-manager>
          <client>
            <type>type</type>
            <cache>cache</cache>
          </client>
        </license-manager>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the license manager client.

Contents

<type>— Type of the license client.

Value— SDX is currently the only valid value

Default— SDX

<cache>— Path to a cache file.

Value— Valid path

Default— var/run/lic_cache

Required Privilege Level

system

<directory-access> (configuration/shared/sae/configuration/license-manager)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <license-manager>
          <directory-access>
            <server-address>server-address</server-address>
            <server-port>server-port</server-port>
            <license-dn>license-dn</license-dn>
            <authentication-dn>authentication-dn</authentication-dn>
            <password>password</password>
            <ldaps/>
            <connection-manager-id>connection-manager-id</connection-manager-
id>
            <event-base-dn>event-base-dn</event-base-dn>
            <signature-dn>signature-dn</signature-dn>
            <snmp-agent/>
          </directory-access>
        </license-manager>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure directory access to the license manager.

Contents

<server-address>—(Optional) IP addresses or hostnames of the directory server that stores licensing data.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space.

Default— No value

`<server-port>`—(Optional) Port number of the LDAP connection to the directory server that stores licensing data.

Value— Port number in the range 0–65535

Default— 389

`<license-dn>`—(Optional) Subtree in the directory where licensing information is stored. The SAE searches for the license key below this path.

Value— `<DN>`. The string `<base>` is replaced with the directory base DN

Default— `ou = Licenses, o = Management, < base >`

`<authentication-dn>`—(Optional) DN the SAE uses to authenticate access to the directory server.

Value— `<DN>`. The string `<base>` is replaced with the directory base DN

Default— No value

`<password>`—(Optional) Password used to authenticate access to the directory.

Value— Text string or Base64 string

Default— No value

Enables or disables LDAPS as the secure protocol for connections to the directory server that stores license data.

Value

- `ldaps`—

Default— Disabled

`<connection-manager-id>`— DES connection manager within the Java Naming and Directory Interface (JNDI) framework.

Value— Text

Default— `LICENSE_MANAGER`

`<event-base-dn>`—(Optional) Directory eventing base DN for the license manager data.

Value— `<DN>` . The string `<base>` is replaced with the directory base DN

Default— No value

`<signature-dn>`—(Optional) DN of the entry that specifies the LDAP schema attribute usedDirectory. This attribute identifies the type of directory, such as openLDAP or DirX, on which the license data is stored.

Value— `<DN>` . The string `<base>` is replaced with the directory base DN

Default— No value

`<snmp-agent>`—(Optional) Specifies whether the SRC SNMP agent exports MIBs for this directory connection.

Default— Disabled

Required Privilege Level

system

<logger> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <logger>
          <name>name</name> <!-- identifier -->
        </logger>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create a logging configuration for the SAE.

Contents

<name>— Name of the logging configuration.

Value—Text

Required Privilege Level

system

<file> (configuration/shared/sae/configuration/logger)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <logger>
          <file>
            <filter>filter</filter>
            <filename>filename</filename>
            <rollover-filename>rollover-filename</rollover-filename>
            <maximum-file-size>maximum-file-size</maximum-file-size>
          </file>
        </logger>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— No value

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system

<syslog> (configuration/shared/sae/configuration/logger)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <logger>
          <syslog>
            <filter>filter</filter>
            <host>host</host>
            <facility>facility</facility>
            <format>format</format>
          </syslog>
        </logger>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Default— None

Required Privilege Level

system

<login-registration> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <login-registration>
          <registration-authentication/>
        </login-registration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the authentication of registered username/password pairs.

Contents

`<registration-authentication>`—(Optional) Enables the authentication of registered username/password pairs. Enable this option if your authentication server does not allow authentication while a session for the authenticated username is active.

Default—

Required Privilege Level

system

<nic-proxy-configuration> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <name>name</name> <!-- identifier -->
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC proxy.

Contents

<name>— Name of the NIC proxy configuration.

Value—Text

Required Privilege Level

system

<cache> (configuration/shared/sae/configuration/nic-proxy-configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <cache>
            <cache-size>cache-size</cache-size>
            <cache-cleanup-interval>cache-cleanup-interval</cache-cleanup-
interval>
            <cache-entry-age>cache-entry-age</cache-entry-age>
          </cache>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure the NIC Proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

Contents

<cache-size>—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default— 10000

<cache-cleanup-interval>— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default— 15

<cache-entry-age>—(Optional) Maximum time that the NIC proxy can cache an entry.

The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Required Privilege Level

system

<nic-host-selection> (configuration/shared/sae/configuration/nic-proxy-configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <nic-host-selection>
            <groups>groups</groups>
            <selection-criteria>selection-criteria-choice</selection-
criteria>
          </nic-host-selection>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

Contents

<groups>—(Optional) (Multivalue) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

<selection-criteria>— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest

priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default—round-

Required Privilege Level

system

<blacklisting> (configuration/shared/sae/configuration/nic-proxy-configuration/nic-host-selection)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <nic-host-selection>
            <blacklisting>
              <try-next-system-on-error/>
              <number-of-retries-before-blacklisting>number-of-retries-before-
blacklisting</number-of-retries-before-blacklisting>
              <blacklist-retry-interval>blacklist-retry-interval</blacklist-
retry-interval>
            </blacklisting>
          </nic-host-selection>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Contents

<try-next-system-on-error>—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

<number-of-retries-before-blacklisting>— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the NIC host for a period of time.

Value—Integer in the range 0–2147483647
Default—3

<blacklist-retry-interval>— Interval at which the NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s
Default—15

Required Privilege Level

system

<resolution> (configuration/shared/sae/configuration/nic-proxy-configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <resolution>
            <resolver-name>resolver-name</resolver-name>
            <key-type>key-type</key-type>
            <value-type>value-type</value-type>
            <expect-multiple-values/>
            <constraints>constraints</constraints>
          </resolution>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

<key-type>— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<value-type>— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaeId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<expect-multiple-values>—(Optional) Specifies whether or not the key can have multiple corresponding values.

<constraints>—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution. Separate data types with commas.

Default— No value

Required Privilege Level

system

<test-nic-bindings> (configuration/shared/sae/configuration/nic-proxy-configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <test-nic-bindings>
            <use-test-bindings/>
          </test-nic-bindings>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure key-value mappings to be used to test a NIC resolution.

Contents

<use-test-bindings>—(Optional) Test the NIC resolutions without having to configure or run a NIC host. The values returned are those configured in the key-values property.

Default—false

Required Privilege Level

system

<key-values> (configuration/shared/sae/configuration/nic-proxy-configuration/test-nic-bindings)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <nic-proxy-configuration>
          <test-nic-bindings>
            <key-values>
              <name>name</name> <!-- identifier -->
              <value>value</value>
            </key-values>
          </test-nic-bindings>
        </nic-proxy-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure keys and associated values to use for testing. Define all of values to be returned for specified keys.

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<plug-ins> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <plugin-publisher-auth-queue>plugin-publisher-auth-queue</plugin-
publisher-auth-queue>
          <plugin-publisher-tracking-queue>plugin-publisher-tracking-queue</
plugin-publisher-tracking-queue>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<plugin-publisher-auth-queue>—

Value—Integer in the range -2147483648–2147483647

Default—20

<plugin-publisher-tracking-queue>—

Value—Integer in the range -2147483648–2147483647

Default—20

Required Privilege Level

system

<event-publishers> (configuration/shared/sae/configuration/plugin-ins)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-ins>
          <event-publishers>
            <subscriber-authorization>subscriber-authorization</subscriber-
authorization>
            <default-retailer-authentication>default-retailer-authentication</
default-retailer-authentication>
            <default-retailer-dhcp-authentication>default-retailer-dhcp-
authentication</default-retailer-dhcp-authentication>
            <dhcp-authorization>dhcp-authorization</dhcp-authorization>
            <service-authorization>service-authorization</service-
authorization>
            <subscription-authorization>subscription-authorization</
subscription-authorization>
            <subscriber-tracking>subscriber-tracking</subscriber-tracking>
            <service-tracking>service-tracking</service-tracking>
            <interface-tracking>interface-tracking</interface-tracking>
            <embedded-admin-server-authorization>embedded-admin-server-
authorization</embedded-admin-server-authorization>
          </event-publishers>
        </plugin-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure event publishers. Event publishers tell the SAE which events to send to which plug-in.

Contents

<subscriber-authorization>—(Optional) (Multivalue) Authorize all subscriber sessions. These plug-in instances are called after a subscriber profile is loaded but before a subscriber session is started. The SAE calls these plug-ins for each subscriber who logs in to

a portal.

These plug-in instances cannot perform authentication because passwords are not available at this point in the login process. Therefore if you specify plug-ins that perform authentication, the login process will fail.

Value— List of plug-ins

Default— No value

Introduced in— 1.0.0

`<default-retailer-authentication>`—(Optional) (Multivalue) Authenticate subscribers who are assigned to retailer objects that do not specify a an authentication plug-in. These plug-ins are called when the subscriber logs in to a domain. The authentication process for portal logins maps the supplied domain name to a retailer object.

If you do not specify default retailer authentication plug-ins or retailer-specific plug-ins, subscribers are admitted without authentication.

Value— List of plug-ins

Default— No value

`<default-retailer-dhcp-authentication>`—(Optional) (Multivalue) Authenticate DHCP address requests for subscribers who are assigned to retailer objects that do not specify a DHCP authentication plug-in. These plug-ins are called when the SAE receives a DHCP discover request from a client that has its username and password cached in the SAE. The username and password can either be cached persistently in the directory or temporarily in memory during a switch from an unauthenticated to an authenticated address.

Value— List of plug-ins

Default— No value

`<dhcp-authorization>`—(Optional) (Multivalue) Authorize all DHCP address requests for all DHCP subscribers who log in to a portal. These plug-ins are called for both authenticated and unauthenticated address requests.

Value— List of plug-ins

Default— No value

`<service-authorization>`—(Optional) (Multivalue) Authorize all service sessions. These plug-ins are called before a service session is started, and are called for every service session started by any subscriber.

Value— List of plug-ins

Default— No value

`<subscription-authorization>`—(Optional) (Multivalue) Authorize subscribers to change their subscriptions. These plug-ins are called when a subscriber tries to modify, subscribe to, or unsubscribe from a subscription.

Value— List of plug-ins

Default— No value

`<subscriber-tracking>`—(Optional) (Multivalue) Collect accounting data for all subscriber sessions. These plug-ins are called for every subscriber session that is started and stopped. They are called after a subscriber session has started and when the session is stopped.

Value— List of plug-ins

Default— No value

`<service-tracking>`—(Optional) (Multivalue) Collect accounting data for all service sessions. These plug-ins are called for every service session that is started and stopped. They are called after a service session starts, when the service session stops, and during interim updates.

Value— List of plug-ins

Default— No value

`<interface-tracking>`—(Optional) (Multivalue) Collect accounting data for all interfaces that the SAE manages. These plug-ins are called for every managed interface that is started and stopped. They are called after an interface comes up, when new policies are installed on the interface, and when the interface goes down. You can include NIC SAE plug-ins, which cause the SAE to send interface tracking events to the NIC SAE plug-in agent.

Value— List of plug-ins

Default— No value

`<embedded-admin-server-authorization>`—(Optional) (Multivalue) Authorize administrators to connect to the embedded Web server, which is used to access SAE Web Admin.

Value— List of plug-ins

Default— No value

Required Privilege Level

system

<manager> (configuration/shared/sae/configuration/plugin-ins)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-ins>
          <manager>
            <threads>threads</threads>
          </manager>
        </plugin-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of threads used for plug-in synchronization.

Contents

<threads>— Number of threads that the SAE maintains for plug-in synchronization.

Value— Integer in the range 0–100

Default— 5

Required Privilege Level

system

<name> (configuration/shared/sae/configuration/plugin)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <name>name</name> <!-- identifier -->
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a plug-in. A plug-in configuration describes a particular plug-in that can handle events that it receives from the SAE.

- An authorization plug-in configuration might perform RADIUS authentication when it receives a subscriber login event.
- A tracking plug-in might write accounting information to a file when it receives service session events.

For each type of plug-in you can create multiple instances that contain different configurations of the plug-in.

Contents

<name>— Name of the plug-in configuration.

Value—Text

Required Privilege Level

system

<acp-interface-listener> (configuration/shared/sae/ configuration/plugin-ins/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <acp-interface-listener>
              <ldap-server>ldap-server</ldap-server>
              <bind-dn>bind-dn</bind-dn>
              <bind-password>bind-password</bind-password>
              <ldaps/>
              <congestion-points-base-dn>congestion-points-base-dn</
congestion-points-base-dn>
              <admission-control-base-dn>admission-control-base-dn</admission-
control-base-dn>
              <timeout>timeout</timeout>
              <acp-remote-corba-ior>acp-remote-corba-ior</acp-remote-corba-
ior>
            </acp-interface-listener>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a hosted internal plug-in for SRC-ACP that the SAE uses to monitor the state of interfaces on a VR for backbone congestion points.

Contents

<ldap-server>— IP address or name of the host that supports the directory that contains backbone service definitions and network interfaces.

Value— IP address or name of the host optionally followed by a port number. Use the format < host > : < port number > . For example,

10.227.0.0:389

Default— No value

`<bind-dn>`— DN of the directory entry that defines the username with which the plug-in accesses the directory.

Value— `<DN>` . You can use the special value `<base>` to refer to the globally configured base DN. The string `<base>` is replaced with the directory base DN.

Default— No value

`<bind-password>`— Password with which the plug-in accesses the directory.

Value— Text string

Default— No value

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

`<congestion-points-base-dn>`— DN at which SRC-ACP stores backbone congestion points.

Value— `<DN>` . You can use the special value `<base>` to refer to the globally configured base DN. The string `<base>` is replaced with the directory base DN.

Default— No value

`<admission-control-base-dn>`— DN at which SRC-ACP stores edge congestion points.

Value— `<DN>` . You can use the special value `<base>` to refer to the globally configured base DN. The string `<base>` is replaced with the directory base DN.

Default— No value

`<timeout>`—(Optional) Maximum time that the plug-in waits for the router to respond.

Value— Number of milliseconds in the range 0–2147483647. A zero means there is no timeout.

Default— 5000

`<acp-remote-corba-ior>`— Object reference for the ACP plug-in.

Value— ACP CORBA reference that is defined with the **edit shared acp configuration corba acp-ior** statement.

Default— No value

Required Privilege Level

system

<custom-radius-accounting> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <custom-radius-accounting>
            <java-class-radius-packet-handler>java-class-radius-packet-
handler</java-class-radius-packet-handler>
            <class-path-radius-packet-handler>class-path-radius-packet-
handler</class-path-radius-packet-handler>
            <append-acct-status-type-attribute/>
            <require-mandatory-attributes/>
            <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>
            <failback-timer>failback-timer</failback-timer>
            <timeout>timeout</timeout>
            <retry-interval>retry-interval</retry-interval>
            <maximum-queue-length>maximum-queue-length</maximum-queue-
length>
            <bind-address>bind-address</bind-address>
            <udp-port>udp-port</udp-port>
            <default-peer>default-peer</default-peer>
          </custom-radius-accounting>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a custom RADIUS accounting plug-in.

Contents

<java-class-radius-packet-handler>— Name of the Java class that implements

the RadiusPacketHandler interface in the RADIUS client library.

Value— Java class name. For example, net.juniper.smgmt.radius.
RadiusPacketHandlerImpl

Default— No value

`<class-path-radius-packet-handler>`—(Optional) List of URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

Value— Comma-separated list of URLs

Default— No value

`<append-acct-status-type-attribute>`—(Optional) Enable or disable whether or not the plug-in includes the Acct-Status-Type attribute in a RADIUS accounting request packet.

Default— Enabled

`<require-mandatory-attributes>`—(Optional) Enable or disable whether or not a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

Default— Enabled

`<load-balancing-mode>`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- Failover—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- Round-robin—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<timeout>`— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0–9223372036854775807.

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

`<bind-address>`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

`<udp-port>`—(Optional) Source UDP port used for communication with the RADIUS server. If not specified, the global default is used.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

`<default-peer>`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* custom-radius-accounting peer-group** command.

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/custom-radius-accounting)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <custom-radius-accounting>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </custom-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

`<server-address>`— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

`<server-port>`— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

`<secret>`— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<custom-radius-authentication> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <custom-radius-authentication>
            <java-class-radius-packet-handler>java-class-radius-packet-
handler</java-class-radius-packet-handler>
            <class-path-radius-packet-handler>class-path-radius-packet-
handler</class-path-radius-packet-handler>
            <require-mandatory-attributes/>
            <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>
            <failback-timer>failback-timer</failback-timer>
            <timeout>timeout</timeout>
            <retry-interval>retry-interval</retry-interval>
            <maximum-queue-length>maximum-queue-length</maximum-queue-
length>
            <bind-address>bind-address</bind-address>
            <udp-port>udp-port</udp-port>
            <default-peer>default-peer</default-peer>
          </custom-radius-authentication>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a custom RADIUS authentication plug-in.

Contents

<java-class-radius-packet-handler>— Name of the Java class that implements the RadiusPacketHandler interface in the RADIUS client library.

Value— Java class name. For example, net.juniper.smgd.radius.
RadiusPacketHandlerImpl

Default— No value

`<class-path-radius-packet-handler>`—(Optional) List of URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

Value— Comma-separated list of URLs

Default— No value

`<require-mandatory-attributes>`—(Optional) Specifies whether or not a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

Value— true or false

Default— true

`<load-balancing-mode>`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- Failover—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- Round-robin—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<timeout>`— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

`<bind-address>`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

`<udp-port>`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, 7000-7003,

7006, 7007-7009

Default— No value

`<default-peer>`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* custom-radius-authentication peer-group** command.

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/custom-radius-authentication)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <custom-radius-authentication>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </custom-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

`<server-address>`— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

`<server-port>`— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

`<secret>`— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<ejb-adaptor> (configuration/shared/sae/configuration/plugins/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <ejb-adaptor>
              <jndi-service-provider>jndi-service-provider</jndi-service-
provider>
              <application-server-url>application-server-url</application-
server-url>
              <jndi-sae-event-listener>jndi-sae-event-listener</jndi-sae-
event-listener>
              <event-admitter>event-admitter</event-admitter>
              <use-ejb-cluster/>
              <ejb-clustering-strategy>ejb-clustering-strategy-choice</ejb-
clustering-strategy>
              <attributes>attributes-choice</attributes>
            </ejb-adaptor>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Note that the EJB adapter plug-in works only with the SRC-VTA, which is not yet supported on the C-series platform.

Configure an EJB adapter plug-in that the SRC-VTA uses to communicate with the SAE. The plug-in performs the following functions:

- Filters SAE plug-in events for the SRC-VTA.
- Adapts internal SAE events to EJB-compatible methods.
- Sends SAE tracking events to the SRC-VTA.

Contents

`<jndi-service-provider>`— Class name of the J2EE application server's JNDI service provider

Value— Depends on the type of J2EE application server. Consult documentation for the J2EE application server.

Default— `org.jnp.interfaces.NamingContextFactory`

`<application-server-url>`— URL of J2EE application server that is running the JNDI service.

Value— Depends on the type of J2EE application server. Consult the documentation for the J2EE application server.

Default— `jnp://127.0.0.1:1099`

`<jndi-sae-event-listener>`— JNDI name of `SAEEventListener` EJB of the peer SRC-VTA.

Value— JNDI name. For example, `Quota/SAEEventListenerBean`.

Default— No value

`<event-admitter>`—(Optional) LDAP filter that determines the subscriber and service events that the EJB adapter plug-in sends to the SRC-VTA.

Value— See *Installing and Initially Configuring the SRC-VTA* in the *SRC Application Library Guide*.

Default— No value

`<use-ejb-cluster>`—(Optional) Property that specifies whether or not the J2EE application server uses EJB cluster.

Default— Disabled

`<ejb-clustering-strategy>`— Load-balancing scheme of the J2EE application server that hosts the SRC-VTA. See the documentation for the J2EE application server to determine which load-balancing scheme it supports.

Value— One of the following:

- `EJBObjectClustering`—load balancing by means of object stubs.
- `EJBHomeClustering`—load balancing by means of home interface.

- JNDIClustering—Load balancing by means of JNDI

Default— EJBOBJECTClustering

<attributes>—(Optional) (Multivalue) Attributes that are sent to the plug-in. We recommend that you configure only the required attributes. If you do not specify attributes, all attributes are sent. Specifying fewer attributes improves the performance of the SRC network.

Value

- host—Name of the SAE host
- router-name—Name of the virtual router
- interface-name—Name of the router interface
- interface-alias—Alias of the router interface
- interface-descr—Description of the router interface
- port-id—NAS port ID of the physical interface
- user-ip-address—IP address of the subscriber
- login-name—Login name of the subscriber
- accounting-id—Accounting ID attribute
- auth-user-id—Subscriber ID used for service authentication
- if-radius-class—RADIUS class of the router interface
- if-session-id—Interface session ID assigned by the router
- service-name—Name of the service
- radius-class—RADIUS class attribute
- event-time—Timestamp when the event was created
- session-id—Session ID assigned by the SAE
- terminate-cause—RADIUS termination cause
- session-time—Length of the session in seconds
- in-octets—Number of octets received from the subscriber
- out-octets—Number of octets sent to the subscriber
- in-packets—Number of packets received from the subscriber
- out-packets—Number of packets sent to the subscriber
- nas-ip—NAS IP address that router uses for accounting messages
- user-mac-address—MAC address of subscriber session
- service-session-name—Name of the service session
- service-session-tag—Tag assigned to the service session
- user-type—Subscriber session type
- user-radius-class— RADIUS class of the subscriber session that is associated with the service session
- user-session-id—RADIUS session ID for the subscriber session
- primary-user-name— pppLoginName or public Dhcp userName
- session-volume-quota—Session volume quota

- `subscription-name`—Name of the subscription
- `login-id`—Login ID of the subscriber
- `if-index`—SNMP index of the router interface
- `event-time-millisecond`—Event time in milliseconds
- `nas-port`—ID that the router uses to identify interface to RADIUS
- `operational`—Flag that identifies whether an interface was operational at the time of the tracking event
- `idle-timeout`—Idle timeout
- `user-inet-address`—Subscriber INET address
- `nas-inet-address`—NAS INET address of the router
- `router-type`—Type of device driver
- `interface-speed`—Speed of the interface
- `service-bundle`—RADIUS vendor-specific attribute that a subscriber authorization plug-in returns to the SAE
- `user-dn`—DN of the subscriber profile
- `uid`—Subscriber ID used for secondary authentication
- `domain`—Subscriber domain used for secondary authentication
- `retailer-dn`—Retailer DN associated with the domain
- `password`—Password used for secondary authentication
- `service-scope`—List of service scopes
- `session-timeout`—Session timeout in seconds
- `downstream-bandwidth`—Downstream bandwidth for the service
- `upstream-bandwidth`—Upstream bandwidth for the service
- `dhcp-packet`—Contents of the DHCP discover request
- `aggr-session-id`—Accounting session ID of the aggregate service session
- `aggr-login-name`—Login name of the subscriber who started the session
- `aggr-user-dn`—Aggregate service subscriber DN
- `aggr-user-inet-address`—Aggregate service subscriber INET address
- `aggr-accounting-id`—Aggregate service accounting ID
- `aggr-auth-user-id`—Aggregate service subscriber ID
- `accounting-interim-time`—Accounting interim time
- `substitution`—Substitution
- `pcmm-request-type`—PCMM request type
- `pcmm-application-manager-id`—PCMM application manager ID
- `pcmm-billing-correlation-id`—PCMM billing correlation ID
- `l2c-access-mode`—L2C access mode
- `l2c-upstream-rate`—L2C upstream rate
- `l2c-downstream-rate`—L2C downstream rate

Default—List of all attributes

Required Privilege Level

system

<external> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <external>
            <corba-object-reference>corba-object-reference</corba-object-
reference>
            <attributes>attributes-choice</attributes>
          </external>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SAE external plug-ins. You need to configure external plug-ins for SAE plug-in agents for the NIC, for Admission Control Plug-Ins, and for custom plug-ins developed in Common Object Request Broker Architecture (CORBA).

Contents

<corba-object-reference>— Object reference of the external plug-in that is exported to the SAE. When the SAE sends the first event to a registered plug-in, it resolves the object reference.

Value— Object reference in one of the following formats:

- The absolute path to the interoperable object reference (IOR) file in the format: "file:// < absolute path > "
- The corbaloc URL in the format corbaloc:: < host > : < portNumber > / < path > where:
 - host is the name or IP address of the host that supports the plug-in

- portNumber is the port number of the host
 - path is the absolute path to the plug-in
- Common Object Services (COS) in the format corbaname::
 < host > [: < port >][/serviceName]# < key > where the key is
 provided by the publisher of the IOR to the COS naming service.
- The actual IOR in the form IOR: < objectReference >

Default— No value

<attributes>—(Optional) (Multivalue) Attributes that are sent to the plug-in. We recommend that you configure only the required attributes. If you do not specify attributes, all attributes are sent. Specifying fewer attributes improves the performance of the SRC network.

Value

- host—Name of the SAE host
- router-name—Name of the virtual router
- interface-name—Name of the router interface
- interface-alias—Alias of the router interface
- interface-descr—Description of the router interface
- port-id—NAS port ID of the physical interface
- user-ip-address—IP address of the subscriber
- login-name—Login name of the subscriber
- accounting-id—Accounting ID attribute
- auth-user-id—Subscriber ID used for service authentication
- if-radius-class—RADIUS class of the router interface
- if-session-id—Interface session ID assigned by the router
- service-name—Name of the service
- radius-class—RADIUS class attribute
- event-time—Timestamp when the event was created
- session-id—Session ID assigned by the SAE
- terminate-cause—RADIUS termination cause
- session-time—Length of the session in seconds
- in-octets—Number of octets received from the subscriber
- out-octets—Number of octets sent to the subscriber
- in-packets—Number of packets received from the subscriber
- out-packets—Number of packets sent to the subscriber
- nas-ip—NAS IP address that router uses for accounting messages
- user-mac-address—MAC address of subscriber session
- service-session-name—Name of the service session
- service-session-tag—Tag assigned to the service session
- user-type—Subscriber session type
- user-radius-class— RADIUS class of the subscriber session that is associated with the service session

- `user-session-id`—RADIUS session ID for the subscriber session
- `primary-user-name`— `pppLoginName` or public `Dhcp userName`
- `session-volume-quota`—Session volume quota
- `subscription-name`—Name of the subscription
- `login-id`—Login ID of the subscriber
- `if-index`—SNMP index of the router interface
- `event-time-millisecond`—Event time in milliseconds
- `nas-port`—ID that the router uses to identify interface to RADIUS
- `operational`— Flag that identifies whether an interface was operational at the time of the tracking event
- `idle-timeout`—Idle timeout
- `user-inet-address`—Subscriber INET address
- `nas-inet-address`—NAS INET address of the router
- `router-type`—Type of device driver
- `interface-speed`—Speed of the interface
- `service-bundle`— RADIUS vendor-specific attribute that a subscriber authorization plug-in returns to the SAE
- `user-dn`—DN of the subscriber profile
- `uid`—Subscriber ID used for secondary authentication
- `domain`—Subscriber domain used for secondary authentication
- `retailer-dn`—Retailer DN associated with the domain
- `password`—Password used for secondary authentication
- `service-scope`—List of service scopes
- `session-timeout`—Session timeout in seconds
- `downstream-bandwidth`—Downstream bandwidth for the service
- `upstream-bandwidth`—Upstream bandwidth for the service
- `dhcp-packet`—Contents of the DHCP discover request
- `aggr-session-id`—Accounting session ID of the aggregate service session
- `aggr-login-name`—Login name of the subscriber who started the session
- `aggr-user-dn`—Aggregate service subscriber DN
- `aggr-user-inet-address`—Aggregate service subscriber INET address
- `aggr-accounting-id`—Aggregate service accounting ID
- `aggr-auth-user-id`—Aggregate service subscriber ID
- `accounting-interim-time`—Accounting interim time
- `substitution`—Substitution
- `pcmm-request-type`—PCMM request type
- `pcmm-application-manager-id`—PCMM application manager ID
- `pcmm-billing-correlation-id`—PCMM billing correlation ID
- `l2c-access-mode`—L2C access mode
- `l2c-upstream-rate`—L2C upstream rate
- `l2c-downstream-rate`—L2C downstream rate

Default— List of all attributes

Required Privilege Level

system

<file-accounting> (configuration/shared/sae/configuration/plugin-name)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <file-accounting>
              <filename>filename</filename>
              <template>template</template>
              <interval>interval</interval>
              <fields>fields-choice</fields>
            </file-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a file accounting plug-in, which writes information to a file in a comma-separated format.

Contents

<filename>— Name and location of the file to which the SAE writes accounting information. The SAE names accounting files by appending the timestamp for the start of the accounting period.

Value— Path and name of file

Default— /var/acct/log

<template>— Name of the template that defines header names for the attributes written to the accounting file.

Value— Template name

Default— std

<interval>— Number of hours of information stored in each accounting file. When the interval expires, the SAE closes the file, renames it to the archive name, and creates a new file.

Accounting files are aligned with midnight of the day the SAE process starts. If the interval is 24 hours, the SAE starts a new file at midnight every day beginning on the day the SAE process starts.

- If the interval is a divisor of 24 hours (for example, 15 minutes, 30 minutes, 1 hour), there is a repeatable pattern of file starts. For example, if the interval is set to 6 hours, the SAE creates a new file at midnight, 6 am, 12 pm, and 6 pm every day.
- If the interval is not a divisor of 24 hours, then the file start times shift each day to different times of the day.

If the SAE is restarted, the schedule for creating accounting files is reset to start at midnight.

Value— Interval in the format hour:minutes

Default— 24

<fields>—(Optional) (Multivalue) List of accounting attributes that are written to the accounting file.

Value

- status—Accounting status
- nas-id—NAS identifier
- host—Hostname of the SAE
- router-name—Router name
- interface-name—Interface name
- interface-alias—Interface alias
- interface-descr—Interface description
- port-id—NAS port ID
- user-ip-address—Subscriber IP address
- login-name—Login name
- accounting-id—Accounting ID
- auth-user-id—User authentication ID
- if-radius-class—Interface RADIUS class
- if-session-id—Interface session ID
- service-name—Service name
- radius-class—RADIUS class
- event-time—Event time (s)
- session-id—Session ID
- terminate-cause—Terminate cause

- session-time—Session time
- in-octets—Number of input octets
- out-octets—Number of output octets
- in-packets—Number of input packets
- out-packets—Number of output packets
- nas-ip—NAS IP address
- user-mac-address—Subscriber MAC address
- service-session-name—Service session name
- service-session-tag—Service session tag
- user-type—Subscriber session type
- user-radius-class—Subscriber session RADIUS class
- user-session-id—Subscriber session ID
- primary-user-name—Primary subscriber name
- subscription-name—Subscription name
- login-id—Login ID
- if-index—Interface index
- event-time-millisecond—Event time (ms)
- nas-port—NAS port
- operational—Operational flag
- user-inet-address—Subscriber INET address
- nas-inet-address—NAS INET address
- router-type—Router type
- interface-speed—Interface speed

Default— status,nas-id,host,router-name,interface-name,interface-alias,interface-descr,port-id,user-ip-address, login-name,accounting-id,auth-user-id,if-radius-class,if-session-id,service-name,radius-class,event-time,session-id, terminate-cause,session-time,in-octets,out-octets,in-packets,out-packets,nas-ip,user-mac-address,service-session-name,service-session-tag,user-type,user-radius-class,user-session-id

Required Privilege Level

system

<flex-radius-accounting> (configuration/shared/sae/configuration/plugin/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>

              <failback-timer>failback-timer</failback-timer>
              <timeout>timeout</timeout>
              <retry-interval>retry-interval</retry-interval>
              <maximum-queue-length>maximum-queue-length</maximum-queue-
length>

              <bind-address>bind-address</bind-address>
              <udp-port>udp-port</udp-port>
              <error-handling>error-handling-choice</error-handling>
              <default-peer>default-peer</default-peer>
              <template>template</template>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a flexible RADIUS accounting plug-in.

Contents

<load-balancing-mode>— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<timeout>`— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range -1-9223372036854775807. -1 means that there is no timeout.

Default— 15000

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0-9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0-2147483647

Default— 10000

<bind-address>—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

<udp-port>—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

<error-handling>— Configures the way the SAE handles errors.

Value— One of the following:

- 0—Ignores incorrect definitions and logs them for debugging purposes
- 1—Logs errors and discards the affected RADIUS packet

Default— 0 (Ignore)

<default-peer>— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool name flex-radius-accounting peer-group** command.

Default— No value

<template>— Name of RADIUS packet template.

Value— Name of template

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/flex-radius-accounting)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

`<server-address>`— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

`<server-port>`— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

`<secret>`— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<radius-packet-definition> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <name>name</name> <!-- identifier -->
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet definition for the plug-in.

Contents

<name>— Name of the RADIUS attribute instance.

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting/radius-packet-definition)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <attributes>
                  <name>name</name> <!-- identifier -->
                  <value>value</value>
                </attributes>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plugin>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure a RADIUS packet definition within a plug-in.

Contents

<name>— Name of the RADIUS attribute.

Value—Text

<value>— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins with the SRC CLI* in the *SRC-PE Subscribers and Subscriptions Guide*.

Default— No value

Required Privilege Level

system

<26> (configuration/shared/sae/configuration/plugin-name/ flex-radius-accounting/radius-packet-definition)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <26>
                  <name>name</name> <!-- identifier -->
                </26>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting/radius-packet-definition/26)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <26>
                  <attributes>
                    <name>name</name> <!-- identifier -->
                    <value>value</value>
                  </attributes>
                </26>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/plugin-name/ flex-radius-accounting/radius-packet-definition/26)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <flex-radius-accounting>
            <radius-packet-definition>
              <26>
                <type>
                  <name>name</name> <!-- identifier -->
                </type>
              </26>
            </radius-packet-definition>
          </flex-radius-accounting>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting/radius-packet-definition/26/type)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <26>
                  <type>
                    <attributes>
                      <name>name</name> <!-- identifier -->
                      <value>value</value>
                    </attributes>
                  </type>
                </26>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<vendor-specific> (configuration/shared/sae/configuration/ plug-ins/name/flex-radius-accounting/radius-packet-definition)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <vendor-specific>
                  <name>name</name> <!-- identifier -->
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting/radius-packet-definition/vendor-specific)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <vendor-specific>
                  <attributes>
                    <name>name</name> <!-- identifier -->
                    <value>value</value>
                  </attributes>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/plugin-name/ flex-radius-accounting/radius-packet-definition/vendor- specific)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <vendor-specific>
                  <type>
                    <name>name</name> <!-- identifier -->
                  </type>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-accounting/radius-packet-definition/vendor-specific/type)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-accounting>
              <radius-packet-definition>
                <vendor-specific>
                  <type>
                    <attributes>
                      <name>name</name> <!-- identifier -->
                      <value>value</value>
                    </attributes>
                  </type>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<flex-radius-authentication> (configuration/shared/sae/configuration/plugin/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>

              <failback-timer>failback-timer</failback-timer>
              <timeout>timeout</timeout>
              <retry-interval>retry-interval</retry-interval>
              <maximum-queue-length>maximum-queue-length</maximum-queue-
length>

              <bind-address>bind-address</bind-address>
              <udp-port>udp-port</udp-port>
              <error-handling>error-handling-choice</error-handling>
              <default-peer>default-peer</default-peer>
              <template>template</template>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a flexible RADIUS authentication plug-in.

Contents

<load-balancing-mode>— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<timeout>`— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range -1-9223372036854775807. -1 means that there is no timeout.

Default— 15000

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0-9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0-2147483647

Default— 10000

`<bind-address>`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

`<udp-port>`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

`<error-handling>`— Configure the way the SAE handles errors.

Value— One of the following:

- 0—Ignores incorrect definitions and logs them for debugging purposes
- 1—Logs errors and discards the affected RADIUS packet

Default— 0 (Ignore)

`<default-peer>`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool name flex-radius-authentication peer-group** command.

Default— No value

<template>— Name of RADIUS packet template.

Value— Name of template

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/flex-radius-authentication)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

<server-address>— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

<server-port>— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

<secret>— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<radius-packet-definition> (configuration/shared/sae/ configuration/plugin-ins/name/flex-radius-authentication)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <name>name</name> <!-- identifier -->
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet definition for the plug-in.

Contents

<name>— Name of the RADIUS attribute instance.

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin/name/flex-radius-authentication/radius-packet-definition)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <attributes>
                  <name>name</name> <!-- identifier -->
                  <value>value</value>
                </attributes>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure a RADIUS packet definition within a plug-in.

Contents

<name>— Name of the RADIUS attribute.

Value—Text

<value>— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins with the SRC CLI* in the *SCR-PE Subscribers and Subscriptions Guide*.

Default— No value

Required Privilege Level

system

<26> (configuration/shared/sae/configuration/plugin-name/ flex-radius-authentication/radius-packet-definition)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <26>
                  <name>name</name> <!-- identifier -->
                </26>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-/name/flex-radius-authentication/radius-packet-definition/26)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <26>
                  <attributes>
                    <name>name</name> <!-- identifier -->
                    <value>value</value>
                  </attributes>
                </26>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/plugin/name/flex-radius-authentication/radius-packet-definition/26)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <26>
                  <type>
                    <name>name</name> <!-- identifier -->
                  </type>
                </26>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin-name/flex-radius-authentication/radius-packet-definition/26/type)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <26>
                  <type>
                    <attributes>
                      <name>name</name> <!-- identifier -->
                      <value>value</value>
                    </attributes>
                  </type>
                </26>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<vendor-specific> (configuration/shared/sae/configuration/ plug-ins/name/flex-radius-authentication/radius-packet- definition)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <vendor-specific>
                  <name>name</name> <!-- identifier -->
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin/ name/flex-radius-authentication/radius-packet-definition/ vendor-specific)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <vendor-specific>
                  <attributes>
                    <name>name</name> <!-- identifier -->
                    <value>value</value>
                  </attributes>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/plugin-name/ flex-radius-authentication/radius-packet-definition/vendor- specific)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <vendor-specific>
                  <type>
                    <name>name</name> <!-- identifier -->
                  </type>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/plugin- name/flex-radius-authentication/radius-packet-definition/ vendor-specific/type)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <flex-radius-authentication>
              <radius-packet-definition>
                <vendor-specific>
                  <type>
                    <attributes>
                      <name>name</name> <!-- identifier -->
                      <value>value</value>
                    </attributes>
                  </type>
                </vendor-specific>
              </radius-packet-definition>
            </flex-radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<interface-subscriber-limit> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <interface-subscriber-limit>
            <concurrent-subscribers>concurrent-subscribers</concurrent-
subscribers>
          </interface-subscriber-limit>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a plug-in that limits the number of authenticated subscribers who connect to an IP interface on the router.

Contents

<concurrent-subscribers>— Number of authenticated subscribers who can connect to an IP interface on the router simultaneously.

Value— Integer in the range 0–2147483647

Default— 1

Required Privilege Level

system

<internal> (configuration/shared/sae/configuration/plugin-name)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin>
          <name>
            <internal>
              <plugin-class>plugin-class</plugin-class>
            </internal>
          </name>
        </plugin>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an internal plug-in.

Contents

<plugin-class>— Class name of the plug-in.

Value— Fully qualified name of the Java class

Default— No value

Required Privilege Level

system

<properties> (configuration/shared/sae/configuration/plugin/name/internal)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <internal>
              <properties>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </properties>
            </internal>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Description

Configure the property name and value pairs that make up the plug-in.

Contents

<name>— Name of the property for which you want to define a value.

Value—Text

<value>— Value for the property.

Value— Value for the property.

Default— No value

Required Privilege Level

system

<ldap-authentication> (configuration/shared/sae/configuration/plugin/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <ldap-authentication>
              <method>method-choice</method>
              <server>server</server>
              <bind-dn>bind-dn</bind-dn>
              <bind-password>bind-password</bind-password>
              <search-filter>search-filter</search-filter>
              <ldaps/>
              <search-base-dn>search-base-dn</search-base-dn>
              <name-attribute>name-attribute</name-attribute>
              <password-attribute>password-attribute</password-attribute>
              <service-bundle-attribute>service-bundle-attribute</service-
bundle-attribute>
              <session-volume-quota>session-volume-quota</session-volume-
quota>
              <timeout>timeout</timeout>
              <signature-dn>signature-dn</signature-dn>
              <blacklist/>
            </ldap-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an LDAP authentication plug-in. This plug-in performs authentication against different directories using different authentication methods.

Contents

<method>— LDAP authentication method that the SAE uses. Both search and bind have different implications for system security and performance. When you design the system, consider:

- Search—Because the SAE retrieves passwords from the directory, the directory must allow read access to the password. Allowing read access can be a security risk because an attacker may be able to read passwords in subscriber profiles. However, to lower the risk of password exposure, you can store passwords in encrypted (hashed) form.
- Bind—The SAE sends the password to the directory for authentication. The advantage is that passwords never need to be read from the directory. However, passwords are sent in clear text, and an attacker could intercept them. Bind is a relatively expensive operation that can affect system performance.

Value— One of the following:

- Search—The SAE searches the directory for the username that the subscriber enters, retrieves the found object, and compares the password stored in the object with the provided password. You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX /etc/passwd), SHA, or MD5 algorithms. The format for a hashed password is: {crypt} *hashed password*, {sha} *base64 SHA password*, or {md5} *base64 MD5 password*.
- Bind—The SAE performs a directory search, retrieves the DN of the found object, and tries to bind this DN and the password that the subscriber provides. If you specify the bind method, the plug-in uses the provided username and password to authenticate the directory (bind). You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX /etc/passwd), SHA, or MD5 algorithms. You must use an encryption method that the directory supports.

Default— Search

<server>—(Optional) List of IP addresses of the LDAP authentication server(s).

Value— Comma-separated list of IP addresses

Default— 127.0.0.1

<bind-dn>—(Optional) DN used to authenticate access to the directory.

Value— DN

Default— cn = ssp, ou = Components, o = Operators, < base >

<bind-password>—(Optional) Password that the SAE uses to authenticate its access to the directory to search for the subscriber profile. If you do not specify a bind DN or bind password, the SAE uses anonymous access.

Value— Characters that make up the password. The SRC software encodes the secret using base64.

Default— ssp

`<search-filter>`—(Optional) Additional LDAP search filter that the SAE uses to search the directory for the subscriber profile. The initial search uses a search filter in the form (&(nameAttribute = userName) filter). The search is successful when the username and the filter match.

Value— Search filter syntax defined in RFC 2254—The String Representation of LDAP Search Filters (December 1997)

Default— (objectClass = umcSubscriber)

`ldaps`—Enables LDAPS as the secure protocol used for LDAP connections with the directory. Enabling LDAPS causes communication with the directory to be encrypted with Secure Sockets Layer (SSL).

Value— `ldaps`—Enable LDAPS

Default— Disabled

`<search-base-dn>`—(Optional) Base DN for searching entries in the directory. If you do not specify a base DN, the SAE uses the DN of the associated retailer object.

Also, if you do not specify the base DN, the SAE takes a username in the form `subscriber@domain` and maps domain to a retailer object by comparing domain with the domain names stored in the retailer object. There are two special cases:

- If domain is empty, first the virtual router name and then the name default are tried.
- If a retailer defines * (asterisk) as a domain name, it is used to map all domains that cannot be mapped directly.

Value— DN

Default— No value

`<name-attribute>`—(Optional) Name of the directory attribute that holds the username.

Value— Attribute name

Default— `uniqueID`

`<password-attribute>`—(Optional) Name of the directory attribute that stores the password.

Value— Directory attribute name
Default— userPassword

<service-bundle-attribute>—(Optional) Name of the directory attribute that contains the name of the service bundle that is used for subscriber authentication. This value is made available to the subscriber classification process and can be used to select the subscriber profile to load.

Value— Directory attribute name
Default— No value

<session-volume-quota>—(Optional) Name of the LDAP attribute that contains the value of the session volume quota. The LDAP plug-in sets the session volume quota to this value.

Value— Name of LDAP attribute
Default— No value

<timeout>—(Optional) Maximum time the SAE waits for a response from a directory server. If the directory server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range 0–2147483647
Default— 5000

<signature-dn>—DES Signature DN

Value—Text
Default— < base >

<blacklist>—Directory blacklisting

Default—true

Required Privilege Level

system

<pcmm-rks> (configuration/shared/sae/configuration/plugin/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin>
          <name>
            <pcmm-rks>
              <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>
              <failback-timer>failback-timer</failback-timer>
              <retry-interval>retry-interval</retry-interval>
              <maximum-queue-length>maximum-queue-length</maximum-queue-
length>
              <bind-address>bind-address</bind-address>
              <udp-port>udp-port</udp-port>
              <feid-mso-data>feid-mso-data</feid-mso-data>
              <feid-mso-domain-name>feid-mso-domain-name</feid-mso-domain-
name>
              <trusted-element/>
              <default-peer>default-peer</default-peer>
            </pcmm-rks>
          </name>
        </plugin>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a PCMM record-keeping server plug-in.

Contents

<load-balancing-mode>— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- Failover—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- Round-robin—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0-9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0-2147483647

Default— 10000

`<bind-address>`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

`<udp-port>`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

`<feid-mso-data>`—(Optional) MSO-defined data in the financial entity ID (FEID) attribute, which is included in event messages.

Value— First eight bytes of the FEID attribute

Default— The first eight bytes are filled with zeros.

`<feid-mso-domain-name>`— The MSO domain name that uniquely identifies the MSO for billing and settlement purposes.

Value— Domain name up to 239 bytes; begins at the ninth byte of the FEID attribute

Default— No value

`<trusted-element>`—(Optional) When the SAE is running as a policy server—which means that the SAE sends event messages directly to the RKS—enables the SAE as a trusted network element.

Default— Enabled

`<default-peer>`— Configure an RKS peer, which is an instance of an RKS. You must configure at least one RKS peer.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool PccmRKSPugin peer-group** command.

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/pcmm-rks)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <pcmm-rks>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
              </peer-group>
            </pcmm-rks>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

<server-address>— IP address of the RKS server to which the SAE sends accounting

data

Value— IP address

Default— No value

<server-port>— Port used for sending accounting packets.

Value— Port number in the range 0–65535

Default— 1813

Required Privilege Level

system

<qos-profile-tracking> (configuration/shared/sae/ configuration/plugin-ins/name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <qos-profile-tracking>
              <threads>threads</threads>
              <default-qos-profile>default-qos-profile</default-qos-profile>
              <separator>separator</separator>
              <qos-profile-prefix>qos-profile-prefix</qos-profile-prefix>
              <service-selection-attribute>service-selection-attribute</
service-selection-attribute>
              <search-filter>search-filter</search-filter>
              <invisible-qos-service>invisible-qos-service</invisible-qos-
service>
              <qos-profile-parameter-name>qos-profile-parameter-name</qos-
profile-parameter-name>
            </qos-profile-tracking>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a QoS-tracking plug-in that you can use to ensure that, as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface.

Contents

<threads>— Number of working threads that all QTP instances share when they process QTP events.

Value— Integer in the range 1–100.

Default— 1

`<default-qos-profile>`—(Optional) Name of the QoS profile that is attached to the interface when QoS services have been deactivated.

Value— Name of QoS profile

Default— No value

`<separator>`— Character that is placed between QoS profile input values when the system concatenates the values during the process of creating QoS profile names.

Value— Any character that is valid in QoS profile names on the router.

Default— A single hyphen (-)

`<qos-profile-prefix>`— Prefix added to the QoS service name as part of the process to determine the name of the QoS profile that needs to be attached to an interface for a particular service.

Value— Prefix that, when combined with QoS profile input values, matches a QoS profile on the router.

Default— qos-profile

`<service-selection-attribute>`— Name of the attribute in the service definition that you want the QTP to use as QoS profile input values. The QTP uses these values to determine the name of the QoS profile that needs to be attached to an interface for a group of QoS services.

Value— Name of any attribute in the service object; for example, `serviceCategory`, `sspDesignAndGraphics`. For a list of attribute names for the `sspService` object class, see the documentation for the LDAP schema in the SRC software distribution in the folder *SDK/doc/ldap* or on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/sdx>

Default— serviceName

`<search-filter>`— Search filter that the SAE uses to search service objects in the directory to find QoS services. You can set up the filter to search the values of any attribute in the service object, such as service name, category, or tracking plug-in. The search is successful when a value matches the filter.

Value— Search filter in a format similar to the LDAP search filter. See *Managing Tiered and Premium Services with QoS on JUNOS Routers* in the

SRC Solutions Guide for a list of the values that you can use for filters.

Default— (attribute.trackPlugin =) Note that you must add a search value after the equal sign.

`<invisible-qos-service>`— Name of the hidden QoS profile attachment service that the QTP uses to attach QoS profiles to and remove QoS profiles from a router interface.

Value— Name of the configured service

Default— svc-qos-attach

`<qos-profile-parameter-name>`— Name of the variable parameter used in the QoS profile name field in the QoS profile attachment action of the policy group that is assigned to the hidden QoS service. When the QTP obtains the name of the required QoS profile, it substitutes that value for the variable parameter.

Value— Valid parameter name

Default— qpName

Required Privilege Level

system

<radius-accounting> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <radius-accounting>
            <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>

            <failback-timer>failback-timer</failback-timer>
            <nas-ip>nas-ip-choice</nas-ip>
            <retry-interval>retry-interval</retry-interval>
            <maximum-queue-length>maximum-queue-length</maximum-queue-
length>

            <bind-address>bind-address</bind-address>
            <udp-port>udp-port</udp-port>
            <username>username-choice</username>
            <calling-station-id>calling-station-id-choice</calling-station-
id>

            <default-peer>default-peer</default-peer>
          </radius-accounting>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a basic RADIUS accounting plug-in. This plug-in sends accounting information to an external RADIUS accounting server or a group of accounting servers.

Contents

<load-balancing-mode>— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- Failover—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- Round-robin—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<nas-ip>`—(Optional) Value of the NAS-Ip attribute.

Value— One of the following:

- SSP local IP—IP address of the SAE
- RADIUS client IP—IP address of the virtual router

Default— No value

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0-9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages

that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

<bind-address>—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

<udp-port>—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

<username>— Value of the User-Name attribute (RADIUS attribute [1]).

Value— One of the following:

- login-name—Name used for login
- accounting-id—Value stored in the subscriber profile
- auth-user-name—Name used to authenticate a service
- manager-id—Value of the manager ID in the service subscription; use this setting to identify subscribers to enterprise services. Manager ID is the value of modifiersName (DN of the administrator who last modified the entry in the directory) in the subscription. If modifiersName does not exist, manager ID is the value of creatorsName (DN of the administrator who created the entry in the directory).

Default— login-name

`<calling-station-id>`— Specifies whether the SAE sends the MAC address of the subscriber in the Calling-Station-Id attribute.

Value— One of the following:

- `mac`—Sends the MAC address in the Calling-Station-Id attribute
- `no`—Does not send the MAC address in the Calling-Station-Id attribute

Default— `no`

`<default-peer>`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool RadiusAcctPlugin peer-group** command.

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/radius-accounting)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <radius-accounting>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </radius-accounting>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

`<server-address>`— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

`<server-port>`— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

`<secret>`— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<radius-authentication> (configuration/shared/sae/configuration/plugin-name)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-name>
          <radius-authentication>
            <load-balancing-mode>load-balancing-mode-choice</load-balancing-
mode>

            <failback-timer>failback-timer</failback-timer>
            <nas-ip>nas-ip-choice</nas-ip>
            <retry-interval>retry-interval</retry-interval>
            <maximum-queue-length>maximum-queue-length</maximum-queue-
length>

            <bind-address>bind-address</bind-address>
            <udp-port>udp-port</udp-port>
            <default-peer>default-peer</default-peer>
          </radius-authentication>
        </plugin-name>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a basic RADIUS accounting plug-in. This plug-in sends authentication information to an external RADIUS authentication server or a group of redundant servers.

Contents

<load-balancing-mode>— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

`<failback-timer>`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1-2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

`<nas-ip>`—(Optional) Value of the NAS-IP attribute.

Value— One of the following:

- SSP local IP—IP address of the SAE
- RADIUS client IP—IP address of the virtual router

Default— No value

`<retry-interval>`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.

Value— Number of milliseconds in the range 0-9223372036854775807

Default— 3000

`<maximum-queue-length>`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

`<bind-address>`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

`<udp-port>`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

`<default-peer>`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool RadiusAuthPlugin peer-group** command.

Default— No value

Required Privilege Level

system

<peer-group> (configuration/shared/sae/configuration/plugins/name/radius-authentication)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <radius-authentication>
              <peer-group>
                <name>name</name> <!-- identifier -->
                <server-address>server-address</server-address>
                <server-port>server-port</server-port>
                <secret>secret</secret>
              </peer-group>
            </radius-authentication>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Contents

<name>— Name of the RADIUS peer.

Value—Text

<server-address>— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

<server-port>— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default— 1812

<secret>— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Required Privilege Level

system

<schedule-authorization> (configuration/shared/sae/configuration/plugin-ins/name)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plug-ins>
          <name>
            <schedule-authorization>
            </schedule-authorization>
          </name>
        </plug-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an authorization plug-in that authorizes a scheduled service.

Contents

Required Privilege Level

system

<state-synchronization> (configuration/shared/sae/ configuration/plugin-ins)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <plugin-ins>
          <state-synchronization>
            <fail-queue-size>fail-queue-size</fail-queue-size>
            <fail-queue-age>fail-queue-age</fail-queue-age>
            <batch-time>batch-time</batch-time>
            <keepalive-time>keepalive-time</keepalive-time>
          </state-synchronization>
        </plugin-ins>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a state synchronization plug-in. Some plug-ins, such as the ACP plug-in and the SAE plug-in agent for the NIC, support state synchronization with the SAE. The state synchronization plug-in allows external plug-ins to maintain the state of active subscriber, service, and interface sessions without having to store intermediate versions of the state locally.

Contents

<fail-queue-size>— Maximum number of plug-in events that are stored while the communication with a state synchronization plug-in is interrupted.

Value— Integer in the range -1-2147483647. -1 means unlimited.

Default— 5000

<fail-queue-age>— Mximum time for which plug-in events are stored while the communication with a state synchronization plug-in is interrupted.

Value— Integer in the range -1-2147483647. -1 means unlimited.

Default— -1

`<batch-time>`— Time the SAE waits for other plug-ins to become ready before starting a synchronization sequence.

Value— Number of seconds in the range 0–2147483647

Default— 60

`<keepalive-time>`— Time the SAE waits after an event before sending a ping to the remote plug-in.

Value— Number of seconds in the range 0–2147483647

Default— 60

Required Privilege Level

system

<policy-management-configuration> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <policy-management-configuration>
          <enable-junose-classifier-expansion/>
        </policy-management-configuration>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify whether or not the SAE expands the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

Contents

<enable-junose-classifier-expansion>—(Optional) Enables or disables the expansion of JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

You would use this feature in policies that are used in IP multimedia subsystem (IMS) environments. You can also use it to simplify the configuration of JUNOSe policies.

Because classifier expansion uses processing resources when the policy is created, you should set this property to true only if you are going to use the feature.

Default— Disabled

Required Privilege Level

system

<radius-packet-template> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <name>name</name> <!-- identifier -->
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet template that contains the definition of RADIUS packets. You can use the template to define the content of RADIUS packets that the SAE sends to RADIUS servers. You can then apply the template to flexible RADIUS plug-ins.

Contents

<name>— Name of the RADIUS packet template.

Value—Text

Required Privilege Level

system

<radius-attributes> (configuration/shared/sae/configuration/radius-packet-template)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <name>name</name> <!-- identifier -->
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create a RADIUS attribute instance.

Contents

<name>— Name of the file-accounting template. RADIUS attribute instance. The name you assign to the RADIUS attribute instance must match a RADIUS attribute instance name listed in *Configuring Accounting and Authentication Plug-Ins with the SRC CLI* in the *SCR-PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <attributes>
              <name>name</name> <!-- identifier -->
              <value>value</value>
            </attributes>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Description

Configure a RADIUS packet definition within a plug-in.

Contents

<name>— Name of the RADIUS attribute.

Value—Text

<value>— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins with the SRC CLI* in the *SRC-PE Subscribers and Subscriptions Guide*.

Default— No value

Required Privilege Level

system

<26> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <26>
              <name>name</name> <!-- identifier -->
            </26>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/26)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <26>
              <attributes>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </attributes>
            </26>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/26)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <26>
              <type>
                <name>name</name> <!-- identifier -->
              </type>
            </26>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/26/type)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <26>
              <type>
                <attributes>
                  <name>name</name> <!-- identifier -->
                  <value>value</value>
                </attributes>
              </type>
            </26>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<vendor-specific> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <vendor-specific>
              <name>name</name> <!-- identifier -->
            </vendor-specific>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/vendor-specific)

Usage

```

<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <vendor-specific>
              <attributes>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </attributes>
            </vendor-specific>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>

```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<type> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/vendor-specific)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <vendor-specific>
              <type>
                <name>name</name> <!-- identifier -->
              </type>
            </vendor-specific>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

Required Privilege Level

system

<attributes> (configuration/shared/sae/configuration/radius-packet-template/radius-attributes/vendor-specific/type)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <radius-packet-template>
          <radius-attributes>
            <vendor-specific>
              <type>
                <attributes>
                  <name>name</name> <!-- identifier -->
                  <value>value</value>
                </attributes>
              </type>
            </vendor-specific>
          </radius-attributes>
        </radius-packet-template>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<script-extension> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <script-extension>
          <flexible-radius-script>flexible-radius-script</flexible-radius-
script>
          <dynamic-radius-script>dynamic-radius-script</dynamic-radius-script>
        </script-extension>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<flexible-radius-script>— Python script name of flexible radius plug-in

Value—

Default— flexRadius

<dynamic-radius-script>— Python script name of local dynamic radius server

Value—

Default— dynRadius

Required Privilege Level

system

<service-activation> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <service-activation>
          <retry-time>retry-time</retry-time>
          <retry-limit>retry-limit</retry-limit>
        </service-activation>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure session reactivation behavior. If a service session fails unexpectedly, the SAE tries to start the session again in the background. You can change how many times the SAE tries to activate the session and the interval between these attempts. In most instances, the default values do not need to be changed.

Contents

<retry-time>— Time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background.

Value— Number of seconds in the range -1-9223372036854775807; -1 indicates no limit

Default— 60

<retry-limit>— Number of times the SAE tries to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background. Limit number of times to retry service failed background activation.

Value— Integer in the range -1-2147483647; -1 indicates no limit

Default— -1

Required Privilege Level

system

<service-schedule> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <service-schedule>
          <years-in-future>years-in-future</years-in-future>
          <years-in-past>years-in-past</years-in-past>
        </service-schedule>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure parameters related to service schedules.

Contents

<years-in-future>—(Optional) Amount of time in the future from the year that the SRC system is started, that the scheduler can see.

Value— Integer in the range 1–100

Default— No value

<years-in-past>—(Optional) Amount of time in the past, from the year that the SRC system is started, that the scheduler can see.

Value— Integer in the range 1–100

Default— No value

Required Privilege Level

system

<session-job-manager> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <session-job-manager>
          <number-of-threads>number-of-threads</number-of-threads>
        </session-job-manager>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of threads used for session-related activity; for example, interim accounting, subscriber and service session timeout, idle timeouts, aggregate service keepalives, and remote session monitoring.

Contents

<number-of-threads>— Number of threads used for session-related activity.

Value— Integer in the range 1–50

Default— 10

Required Privilege Level

system

<subscriber-sessions> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <subscriber-sessions>
          <assigned-ip-idle-timeout>assigned-ip-idle-timeout</assigned-ip-
idle-timeout>
          <allow-same-ip-login/>
        </subscriber-sessions>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an idle timeout for sessions of assigned IP subscribers, and specify whether or not the SAE allows multiple logins from the same IP address.

Contents

<assigned-ip-idle-timeout>— Interval after which assigned IP subscriber sessions are deactivated if no service session is active.

Value— Number of seconds in the range 0–2147483647

Default— 900

<allow-same-ip-login>—(Optional) Enables or disables whether the SAE allows a login from the same IP address without requiring that the previous session logs out first.

- If enabled, the SAE logs in the new subscriber session and automatically logs out the previous session.
- If disabled, the SAE denies login requests if a subscriber session for an IP address is active.

Default— Disabled

Required Privilege Level

system

<time-based-policies> (configuration/shared/sae/configuration)

Usage

```
<configuration>
  <shared>
    <sae>
      <configuration>
        <time-based-policies>
          <action-threshold>action-threshold</action-threshold>
          <preparation-time>preparation-time</preparation-time>
          <max-worker-threads>max-worker-threads</max-worker-threads>
        </time-based-policies>
      </configuration>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the action threshold and preparation time for all schedules. You cannot set these values for individual schedules.

Contents

<action-threshold>— Maximum delay that the service allows for a time-related change to occur.

Value— Number of milliseconds in the range 0–9223372036854775807. The recommended range is 60000-300000 milliseconds

Default— 300000 (5 minutes)

<preparation-time>— Preparation time allowed for a state transition. When you set the preparation time, take into consideration system load and performance. Factors such as the number of subscribers, the number of active services, the number of schedule services, the speed of the processor on the system, as well as other conditions might affect the amount of time to process all the scheduled actions at a specified scheduled time.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 300000 (5 minutes)

`<max-worker-threads>`—(Optional) The maximum number of worker threads for service scheduling.

Value— Integer in the range 0–2147483647

Default—

Required Privilege Level

system

<rule> (configuration/shared/sae/dhcp-classifier)

Usage

```
<configuration>
  <shared>
    <sae>
      <dhcp-classifier>
        <rule>
          <name>name</name> <!-- identifier -->
          <target>target</target>
          <script>script</script>
        </rule>
      </dhcp-classifier>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a rule in a classifier script.

Contents

<name>— Name of a classification script.

Value—Text

<target>—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

`<script>`—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Required Privilege Level

system

<condition> (configuration/shared/sae/dhcp-classifier/rule)

Usage

```
<configuration>
  <shared>
    <sae>
      <dhcp-classifier>
        <rule>
          <condition>
            <name>name</name> <!-- identifier -->
          </condition>
        </rule>
      </dhcp-classifier>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Contents

<name>— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC-PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

<group> (configuration/shared/sae)

Usage

```
<configuration>
  <shared>
    <sae>
      <group>
        <name>name</name> <!-- identifier -->
      </group>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a group of SAE configuration properties.

Contents

<name>— Name of a shared SAE configuration.

Value— Text

Required Privilege Level

system

<rule> (configuration/shared/sae/subscriber-classifier)

Usage

```
<configuration>
  <shared>
    <sae>
      <subscriber-classifier>
        <rule>
          <name>name</name> <!-- identifier -->
          <target>target</target>
          <script>script</script>
        </rule>
      </subscriber-classifier>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a rule in a classifier script.

Contents

<name>— Name of a classification script.

Value—Text

<target>—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

`<script>`—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Required Privilege Level

system

<condition> (configuration/shared/sae/subscriber-classifier/rule)

Usage

```
<configuration>
  <shared>
    <sae>
      <subscriber-classifier>
        <rule>
          <condition>
            <name>name</name> <!-- identifier -->
          </condition>
        </rule>
      </subscriber-classifier>
    </sae>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Contents

<name>— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC-PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

<sae> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <sae>
      <base-dn>base-dn</base-dn>
      <real-portal-address>real-portal-address</real-portal-address>
      <java-runtime-environment>java-runtime-environment</java-runtime-
environment>
      <java-heap-size>java-heap-size</java-heap-size>
      <java-new-size>java-new-size</java-new-size>
      <java-garbage-collection-options>java-garbage-collection-options</java-
garbage-collection-options>
      <port-offset>port-offset</port-offset>
      <snmp-agent />
      <shared>shared</shared>
    </sae>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local properties for the SAE, including the base DN, interface the SAE uses to communicate with the router, path to the JRE, Java heap size, Java garbage collection options, and port offset. The statement also specifies the shared configuration object that holds the shared SAE configuration, and it enables or disables SNMP.

Contents

<base-dn>— Distinguished name (DN) of the root directory for the SAE. You must set this attribute if you use a directory-naming scheme different from the default.

Value— DN of the root directory for the SAE.

Default— *o= umc*

<real-portal-address>— Interface on the SAE that the SAE uses for communication with the router. If you clear this field, the interface is assumed to be the interface that was used to connect the router driver to the SAE. If the SAE has multiple network interfaces, you must specify the interfaces that are used to communicate with the router.

Value— IP address of the interface

Default— One of the IP addresses configured on the host (except 127.0.0.1)

`<java-runtime-environment>`— Path to the Java runtime environment (JRE) The SRC software requires a JRE that conforms to the Java 2 specification. The SRC software has been tested with Sun's JRE. See the SRC Release Notes for information about which version of the Sun JRE is distributed with the SRC software. We expect other JREs to work, but have not verified whether they do.

Value— Absolute or relative directory path. This path is the default installation path for the JRE that is distributed with the SRC software and installed with the other SRC components.

Default— `../jre/bin/java`

`<java-heap-size>`— Maximum Java heap (memory) size available to the JRE.

Value— Number of megabytes followed by m. For example, 896m. Change this value if you experience problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping. See the documentation for the JRE for valid values.

Default— The value is calculated dynamically to 70 % of the available real memory.

`<java-new-size>`— Maximum Java new generation heap (memory) size available to the JRE when the SAE starts.

Value— Integer in the range 0– `<Java heap size >` . Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 24m. See the documentation for the JRE for valid values.

Default— 24m

`<java-garbage-collection-options>`— Garbage collection functionality of the Java Virtual Machine.

Value—

Default— `-Xbatch -XX: + UseConcMarkSweepGC -XX: CMSInitiatingOccupancyFraction = 80 -XX: + UseParNewGC -XX: SurvivorRatio = 1 -XX:InitialTenuringThreshold = 8 -XX: MaxTenuringThreshold = 10 -XX:TargetSurvivorRatio = 90 -XX: + UseCMSCompactAtFullCollection -XX: CMSFullGCsBeforeCompaction = 0 -XX: + CMSClassUnloadingEnabled -XX: + CMSParallelRemarkEnabled`

`<port-offset>`— Port offset for SAE instances. The offset is added to the OA port, RADIUS socket, and administration HTTPS server ports.

Value— Integer in the range 0–65535. Set to 0 if you install multiple SAE instances on the same host.

Default— 0

`<snmp-agent>`—(Optional) Enables the SAE to communicate with the SNMP agent.

`<shared>`— Shared configuration object that holds most of the SAE specific configuration.

Value— Name of the object in the format `"/SAE/< path > "`. The `< path >` is separated by `/` and can contain multiple levels. The effective configuration is combined by all configuration objects in the path, with more specific configuration in the lower levels of the path.

Default— `/SAE/POP-ID;`

Required Privilege Level

system

<initial> (configuration/slot/sae)

Usage

```
<configuration>
  <slot>
    <sae>
      <initial>
        <static-dn>static-dn</static-dn>
        <dynamic-dn>dynamic-dn</dynamic-dn>
      </initial>
    </sae>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for SRC components.

Contents

<static-dn>—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—ou = staticConfiguration,ou = Configuration,o = Management,
o = umc

<dynamic-dn>—(Optional) Location of programmatically-defined configuration data in the directory.

Value—Text

Default—ou = dynamicConfiguration,ou = Configuration,
o = Management,o = umc

Required Privilege Level

system

<directory-connection> (configuration/slot/sae/initial)

Usage

```

<configuration>
  <slot>
    <sae>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </sae>
  </slot>
</configuration>

```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default— 10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

system

<directory-eventing> (configuration/slot/sae/initial)

Usage

```
<configuration>
  <slot>
    <sae>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </sae>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

<polling-interval>—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s
Default—30

<event-base-dn>—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN
Default—o = UMC

<dispatcher-pool-size>—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default— 1

Required Privilege Level

system

<radius> (configuration/slot/sae)

Usage

```
<configuration>
  <slot>
    <sae>
      <radius>
        <local-address>local-address</local-address>
        <local-nas-id>local-nas-id</local-nas-id>
      </radius>
    </sae>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the local address that the SAE uses to communicate with RADIUS servers, the network access server (NAS) ID that identifies the SAE when it sends RADIUS messages, and the real portal address that the SAE uses to communicate with the router.

Contents

<local-address>— Local IP address on the SAE host used for communication with RADIUS servers.

Value— IP address; should be a unique NAS IP address.

In an installation in which the SAE is equipped with multiple network interfaces, you must specify the interface that communicates with external RADIUS servers. Typically, you must configure the RADIUS server to accept requests from a client; use this IP address for the RADIUS client configuration. Even if the RADIUS server is running on the same server as the SAE, do not use 127.0.0.1 as the local address, because this address is typically the loopback address for a server.

<local-nas-id>— String that identifies the SAE when it sends RADIUS authentication and accounting messages.

Value— Text string that identifies the SAE. Typically, the string is the

name of the SAE host.

Required Privilege Level

system

Network Information Collector (NIC) Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the network information collector (NIC). The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
shared nic scenario	<u>< scenario ></u>
shared nic scenario name agents	<u>< agent ></u>
shared nic scenario name agents name configuration consolidator	<u>< consolidator ></u>
shared nic scenario name agents name configuration directory	<u>< directory ></u>
shared nic scenario name agents name configuration properties	<u>< properties ></u>
shared nic scenario name agents name configuration sae-client	<u>< sae-client ></u>
shared nic scenario name agents name configuration sae-plug-in	<u>< sae-plug-in ></u>
shared nic scenario name agents name configuration xml	<u>< xml ></u>
shared nic scenario name hosts	<u>< host ></u>
shared nic scenario name hosts logger	<u>< logger ></u>
shared nic scenario name hosts logger name file	<u>< file ></u>
shared nic scenario name hosts logger name syslog	<u>< syslog ></u>
shared nic scenario name hosts name configuration	<u>< configuration ></u>
shared nic scenario name hosts name configuration logger	<u>< logger ></u>
shared nic scenario name hosts name configuration logger name file	<u>< file ></u>
shared nic scenario name hosts name configuration logger name syslog	<u>< syslog ></u>
shared nic scenario name nic-locators	<u>< nic-locator-configuration ></u>
shared nic scenario name nic-locators name resolution	<u>< resolution ></u>
shared nic scenario name realms	<u>< realm ></u>

shared nic scenario name realms name configuration custom-resolver classname	<u>< classname ></u>
shared nic scenario name realms name configuration transitions	<u>< transitions ></u>
shared nic scenario name realms name resolvers	<u>< resolvers ></u>
shared nic scenario name realms name resolvers name configuration	<u>< configuration ></u>
slot number network-publisher directory-connection	<u>< directory-connection ></u>
slot number network-publisher logger	<u>< logger ></u>
slot number network-publisher logger name file	<u>< file ></u>
slot number network-publisher logger name syslog	<u>< syslog ></u>
slot number network-publisher routers	<u>< routers ></u>
slot number network-publisher routers authentication	<u>< authentication ></u>
slot number network-publisher routers router	<u>< router ></u>
slot number network-publisher routers router router-name authentication	<u>< authentication ></u>
slot number network-publisher routers router router-name test-mode	<u>< test-mode ></u>
slot number network-publisher routers test-mode	<u>< test-mode ></u>
slot number network-publisher select	<u>< select ></u>
slot number nic	<u>< nic ></u>
slot number nic initial	<u>< initial ></u>
slot number nic initial directory-connection	<u>< directory-connection ></u>
slot number nic initial directory-eventing	<u>< directory-eventing ></u>

<scenario> (configuration/shared/nic)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <name>name</name> <!-- identifier -->
      </scenario>
    </nic>
  </shared>
</configuration>
```

Description

Configure a NIC configuration scenario to use. A configuration scenario defines the type of resolution to be performed.

Contents

<name>— Name of a NIC configuration scenario.

Value— Name of a configuration scenario that has been established for the NIC.

Required Privilege Level

system

<agent> (configuration/shared/nic/scenario)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <name>name</name> <!-- identifier -->
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC agent in a NIC configuration scenario.

Contents

<name>— Name of a NIC agent in a configuration scenario.

Value—Text

Required Privilege Level

system

<consolidator> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <consolidator>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
                <source-agent>source-agent</source-agent>
                <agent-processor>agent-processor</agent-processor>
                <network-data-types>network-data-types</network-data-types>
                <publishingInterval>publishingInterval</publishingInterval>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
              </consolidator>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for consolidator agents. When you use a configuration scenario, you typically change the source-agent option.

Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Contents

<resolvers-list>—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName : roleName* . Use commas to separate one role from another in the list.

Default— No value

`<source-agent>`— Path to the agent for which this consolidator agent publishes data.

Value— Text

Example—`/agents/InterfaceIdInterface`

Default— No value

`<agent-processor>`— Name of the Java class that the NIC agent uses to generate the data value object.

Value— Path to Java class

Default— No value

`<network-data-types>`— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key* , *value* . Use commas to separate entries.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—`IpPool, InterfaceId`

Default— No value

`<publishingInterval>`—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647

Default—60

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0

Required Privilege Level

system

<directory> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <directory>
                <principal>principal</principal>
                <credentials>credentials</credentials>
                <key-attribute-processor>key-attribute-processor</key-
attribute-processor>
                <value-attribute-processor>value-attribute-processor</value-
attribute-processor>
                <mapping-attribute-processor>mapping-attribute-processor</
mapping-attribute-processor>
                <publishing-interval>publishing-interval</publishing-interval>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
                <search-base>search-base</search-base>
                <search-filter>search-filter</search-filter>
                <search-scope>search-scope-choice</search-scope>
                <server-url>server-url</server-url>
                <directory-backup-urls>directory-backup-urls</directory-
backup-urls>
                <key-attribute-name>key-attribute-name</key-attribute-name>
                <value-attribute-name>value-attribute-name</value-attribute-
name>
                <network-data-types>network-data-types</network-data-types>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
                <enable-directory-eventing/>
                <directory-connection-id>directory-connection-id</directory-
connection-id>
                <snmp-agent/>
                <share-directory-connection/>
                <polling-interval>polling-interval</polling-interval>
                <retry-interval>retry-interval</retry-interval>
              </directory>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

```
</shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for directory agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- search-base
- search-filter
- search-scope
- server-url
- authentication-dn
- password

Contents

`<principal>`— DN that the NIC agent uses for authentication to access the directory.

Value— *DN, base*

Example—*cn= nic,ou= Components,o= Operators,base*

Default— *cn = nic, ou = Components, o = Operators, < base >*

`<credentials>`— Password with which the NIC agent accesses the directory.

Value— *password*

Default— *nic*

`<key-attribute-processor>`—(Optional) Java class that the NIC agent uses to generate the network data object named key.

The object includes a list of attributes from the directory. If no class is specified, there can be only one key attribute (in the `key.attrNames` property).

This value is ignored if a mapping processor is specified.

Before you change the value of this option, contact Juniper Networks Professional Services

or Juniper Networks Customer Support.

Value— Path to Java class

Example—net.juniper.smgmt.gateway.nic.agent.dir. DnAttributeProcessor

Default— No value

`<value-attribute-processor>`—(Optional) Name of the Java class that the NIC agent uses to generate the data value object. Specify only if the agent publishes mappings.

If no class is specified, there can be only one value attribute (in the `value.attrNames` property).

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Default— No value

`<mapping-attribute-processor>`—(Optional) Name of the Java class that the NIC agent uses to process the key object and the value object, and to produce the mapping object `DataPair`. If no class is specified, NIC uses the key and value attribute processors.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Default— No value

`<publishing-interval>`—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–2147483647

Default— 60

`<resolvers-list>`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—`/realms/ip/B1, /realms/sharedIp/B1, /realms/login/D1`

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events. If you do not define the names of the NIC roles, you must define a list of resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Names of NIC roles in the format *realmName:roleName*. Use commas to separate one role from another in the list.

Default— No value

`<search-base>`— DN of the location in the directory from which the agent should read information.

Value— *DN, base*

Default— No value

`<search-filter>`—(Optional) Directory search filter that the agent should use.

Value— LDAP search filter

Default— No value

`<search-scope>`—(Optional) Location in the directory relative to the base DN from which the NIC agent can retrieve information.

Value— One of the following options:

- 0—Object; entry specified in the Search Base field only
- 1—One level; entry specified in the Search Base field and objects that are subordinate by one level
- 2—Subtree of entry specified in the Search Base field

Default— sub-tree

`<server-url>`— URL that identifies the location of the primary directory server to which this NIC agent connects.

Value— Location of the directory that stores configuration information in URL string format `protocol:// host :portNumber` where:

- *protocol* —ldap or ldaps
- *host* —IP address or name of directory host
- *portNumber* —Number of TCP/IP port

Example—`ldap://127.0.0.1:389/`

Default— No value

`<directory-backup-urls>`—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— URLs of redundant directories separated by semicolons.

Example—`ldap://127.0.0.1:389/`

Default— No value

`<key-attribute-name>`— Name of the directory attribute that the NIC agent uses for the network data object called key. You can define these attribute names if you use a customized key attribute processor.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas to separate attribute names.

Example—`virtualRouterName`

Default— No value

`<value-attribute-name>`—(Optional) Directory attribute that the NIC agent uses for

the network data object called `value`. Specify only if the agent publishes mappings.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of an attribute in the directory.

Example—`SaeId`

Default— No value

`<network-data-types>`— Names of the data types that this NIC agent publishes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the form *key*, *value*. If there is more than one data type, separate entries with commas.

Example

- Agent to publish IP pools—`networkDataTypes = IpPool`
- Agent is to publish mappings between IP pools and VRs—`networkDataTypes = IpPool, Vr`

Default— No value

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0

`<enable-directory-eventing>`—(Optional) Specifies whether NIC polls the directory

for changes.

Value—

- true—Enable polling.
- false—Disable polling

Default—true

`<directory-connection-id>`— Name for directory connection in SNMP agent view.

Value— ID for connection manager.

Example—DIRAGENT_POOL_VR

Default— No value

`<snmp-agent>`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory connection.

`<share-directory-connection>`—(Optional) Enable DES listeners of NIC agents to share a connection to the directory.

Do not change this value unless instructed to do so by Juniper Networks.

`<polling-interval>`— Time interval at which the SRC component polls the directory.

Value— Integer in the range 30–2147483647

Default— 30

`<retry-interval>`— Length of time that the directory monitoring system waits to initiate a directory connection after an unsuccessful attempt to connect to the directory.

Value— Integer in the range -2147483648–2147483647 s

Default— No value

Required Privilege Level

system

<properties> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <properties>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
                <data-sources>data-sources</data-sources>
                <network-data-types>network-data-types</network-data-types>
                <publishing-interval>publishing-interval</publishing-interval>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
                <reverse-values/>
              </properties>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties agents. A properties agent retrieves information from one or more specified property files and makes event information based on the information in the file available to the NIC.

Although a properties agent may be used by an SRC application, typically you do not need to configure it. Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Contents

<resolvers-list>—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName* : *roleName* . Use commas to separate one role from another in the list.

Default— No value

`<data-sources>`— List of URIs or filenames of property files that provides information about NIC events to the NIC system. You must provide at least one URI or filename.

At this time, the only supported format for the data source is a property file.

Value— URIs or filenames separated by commas

Default— No value

`<network-data-types>`— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key* , *value* . Use commas to separate entries.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—IpPool, InterfaceId

Default— No value

`<publishing-interval>`—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647

Default—60

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0

`<reverse-values>`—(Optional) Specifies whether a property name is made available as a NIC key or a NIC value. If enabled, properties are published as keys.

Required Privilege Level

system

<sae-client> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <sae-client>
                <principal>principal</principal>
                <credentials>credentials</credentials>
                <subscriber-id>subscriber-id-choice</subscriber-id>
                <sae-connection-threads>sae-connection-threads</sae-
connection-threads>
                <sae-retry-interval>sae-retry-interval</sae-retry-interval>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
                <search-base>search-base</search-base>
                <search-filter>search-filter</search-filter>
                <search-scope>search-scope-choice</search-scope>
                <server-url>server-url</server-url>
                <directory-backup-urls>directory-backup-urls</directory-
backup-urls>
                <key-attribute-name>key-attribute-name</key-attribute-name>
                <value-attribute-name>value-attribute-name</value-attribute-
name>
                <network-data-types>network-data-types</network-data-types>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
                <enable-directory-eventing/>
                <directory-connection-id>directory-connection-id</directory-
connection-id>
                <snmp-agent/>
                <share-directory-connection/>
                <polling-interval>polling-interval</polling-interval>
                <retry-interval>retry-interval</retry-interval>
              </sae-client>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for SAE client agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- `search-base`
- `search-filter`
- `search-scope`
- `server-url`
- `backup-servers-url`
- `principal`
- `credentials`

Contents

`<principal>`— DN that the NIC agent uses for authentication to access the directory.

Value— *DN, base*

Example—*cn= umcadmin, base*

Default— *cn = umcadmin, < base >*

`<credentials>`— Password with which the NIC agent accesses the directory.

Value— *password*

Default—*admin123*

`<subscriber-id>`— The SAE subscriber type. The NIC passes subscriber ID of the specified type to the SAE external interface of active SAEs to determine which SAE has a user session for the subscriber.

Value— One of the following options:

- *user-ip-address* —Subscriber's IP address
- *dn* —DN that identifies the subscriber in the directory
- *login-name* —Login name that identifies the subscriber
- *interface-name* —Name of the interface through which the subscriber traffic passes

- *primary-user-name* —User name that identifies the subscriber

Default— No value

`<sae-connection-threads>`—(Optional) Size of the thread pool for contacting SAEs during resolution. These threads are shared among all resolution requests and are spanned in parallel one thread per SAE per resolution request. You may want to set this value higher than the default if you have multiple SAEs in your network and a high resolution rate.

Value— Number of threads

Default— 5

`<sae-retry-interval>`—(Optional) Min. length of time that the agent waits before it sends a resolution request to a particular SAE after an unsuccessful attempt to contact it.

Value— Retry interval in seconds

Default— 30

`<resolvers-list>`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—`/realms/ip/B1, /realms/sharedIp/B1, /realms/login/D1`

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events. If you do not define the names of the NIC roles, you must define a list of resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Names of NIC roles in the format *realmName:roleName*. Use commas to separate one role from another in the list.

Default— No value

<search-base>— DN of the location in the directory from which the agent should read information.

Value— *DN, base*

Default— No value

<search-filter>—(Optional) Directory search filter that the agent should use.

Value— LDAP search filter

Default— No value

<search-scope>—(Optional) Location in the directory relative to the base DN from which the NIC agent can retrieve information.

Value— One of the following options:

- 0—Object; entry specified in the Search Base field only
- 1—One level; entry specified in the Search Base field and objects that are subordinate by one level
- 2—Subtree of entry specified in the Search Base field

Default— sub-tree

<server-url>— URL that identifies the location of the primary directory server to which this NIC agent connects.

Value— Location of the directory that stores configuration information in URL string format *protocol:// host :portNumber* where:

- *protocol* —ldap or ldaps
- *host* —IP address or name of directory host
- *portNumber* —Number of TCP/IP port

Example—ldap://127.0.0.1:389/

Default— No value

<directory-backup-urls>—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— URLs of redundant directories separated by semicolons.

Example—`ldap://127.0.0.1:389/`

Default— No value

`<key-attribute-name>`— Name of the directory attribute that the NIC agent uses for the network data object called key. You can define these attribute names if you use a customized key attribute processor.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas to separate attribute names.

Example—`virtualRouterName`

Default— No value

`<value-attribute-name>`—(Optional) Directory attribute that the NIC agent uses for the network data object called value. Specify only if the agent publishes mappings.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of an attribute in the directory.

Example—`SaeId`

Default— No value

`<network-data-types>`— Names of the data types that this NIC agent publishes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the form *key*, *value*. If there is more than one data type, separate entries with commas.

Example

- Agent to publish IP pools—`networkDataTypes = IpPool`
- Agent is to publish mappings between IP pools and VRs—`networkDataTypes = IpPool, Vr`

Default— No value

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0

`<enable-directory-eventing>`—(Optional) Specifies whether NIC polls the directory for changes.

Value—

- `true`—Enable polling.
- `false`—Disable polling

Default—`true`

`<directory-connection-id>`— Name for directory connection in SNMP agent view.

Value— ID for connection manager.Example—`DIRAGENT_POOL_VR`**Default**— No value

`<snmp-agent>`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory connection.

`<share-directory-connection>`—(Optional) Enable DES listeners of NIC agents to share a connection to the directory.

Do not change this value unless instructed to do so by Juniper Networks.

`<polling-interval>`— Time interval at which the SRC component polls the directory.

Value—Integer in the range 30–2147483647

Default— 30

`<retry-interval>`— Length of time that the directory monitoring system waits to initiate a directory connection after an unsuccessful attempt to connect to the directory.

Value—Integer in the range -2147483648–2147483647 s

Default— No value

Required Privilege Level

system

<sae-plug-in> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <sae-plug-in>
                <resolvers-list>resolvers-list</resolvers-list>
                <plug-in-event-type>plug-in-event-type-choice</plug-in-event-
type>
                <key-attribute-name>key-attribute-name</key-attribute-name>
                <key-attribute-processor>key-attribute-processor</key-
attribute-processor>
                <value-attribute-name>value-attribute-name</value-attribute-
name>
                <value-attribute-processor>value-attribute-processor</value-
attribute-processor>
                <naming-context>naming-context</naming-context>
                <event-filter>event-filter</event-filter>
                <share-the-event-system/>
                <number-of-events>number-of-events</number-of-events>
                <network-data-types>network-data-types</network-data-types>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
              </sae-plug-in>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for SAE plug-in agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- event-filter
- number-of-events

Contents

`<resolvers-list>`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—/realms/dB/E1

Default— No value

`<plug-in-event-type>`—(Optional) Types of plug-in events that the agent supports.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— One of the following:

- User—Agent supports user-tracking plug-in events.
- Interface—Agent supports interface-tracking plug-in events.

Default—User

`<key-attribute-name>`— Names of the plug-in attributes that provide information for the data key. You can define these attribute names if you use a customized key attribute processor.

The list can contain one or more plug-in attributes. If the format of the single plug-in attribute is not a string or you specify multiple plug-in attributes, the agent passes the data to the key processor to construct the data value in string format. In this case, you must specify the processor in the Key Attribute Processor field.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas

to separate attribute names.

Example—PA_USER_DN,PA_ROUTER_NAME

Default— No value

`<key-attribute-processor>`—(Optional) Name of the Java class that the agent uses to generate the data key object. If no class is specified, there can be only one key event attribute.

Configure a key attribute processor if the agent acquires for the key value either a single plug-in attribute that is not in string format or multiple plug-in attributes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Example—net.juniper.smgmt.gateway.nic.agent.saeplugin.
InterfaceIdProcessor

Default— No value

`<value-attribute-name>`— List of plug-in attributes that provide information for the data value.

The list can contain one or more plug-in attributes. If the format of the single plug-in attribute is not a string or you specify multiple plug-in attributes, the agent passes the data to the value processor to construct the data value in string format. In this case, you must specify the processor for the value attribute processor option.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of comma-separated plug-in attributes.

Example—PA_USER_DN, PA_ROUTER_NAME

Default— No value

`<value-attribute-processor>`—(Optional) Name of the Java class that the agent uses to generate the data value object. If no class is specified, there can be only one value

event attribute.

Configure a value attribute processor if the agent acquires for the data value either a single plug-in attribute that is not in string format or multiple plug-in attributes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Example—`net.juniper.smgmt.gateway.nic.agent.saeplugin.
InterfaceProcessor`

Default— No value

`<naming-context>`— CORBA naming context in which the agent publishes references.

If you configure event sharing for multiple SAE plug-in agents, this setting must be identical for all those agents.

The incoming interface is bound under the specified context with the name `saePort`. The mirror interface has the name `mirrorPort`.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— String that must match the context name in the `objectref` property for this SAE plug-in. For more information, see the documentation for the NIC resolution process.

Example—`nicstestDNottawa`

This example matches the context name of the following `objectref` property:

`corbaname::10.10.10.10:900/NameService#nicstestDNottawa/saePort`

In this property:

- 10.10.10.10—Address of the machine running the CORBA naming server
- 900—TCP/IP port
- `saePort`—Name of plug-in (in this case, the agent eventing system)

Default— No value

`<event-filter>`— LDAP filter that restricts the events that the agent collects.

Value— *pluginAttribute* = *attributeValue*

where

- *pluginAttribute* — Plug-in attribute name
- *attributeValue* — Value of filter

Example—PA_USER_TYPE = INTF

Default— No value

`<share-the-event-system>`—(Optional) Enable an agent to share the event system with other agents in the same host. If you configure event sharing for multiple SAE plug-in agents, this setting must be identical for all those agents.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

`<number-of-events>`—(Optional) Number of events that the SAE sends to the agent at one time during state synchronization. This value is used if state synchronization is enabled.

Value— Integer in the range 1–2147483647

Default—50

`<network-data-types>`— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key*, *value* . Use commas to separate entries.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—Dn, Vr

Default— No value

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0

Required Privilege Level

system

<xml> (configuration/shared/nic/scenario/agents/agent/configuration)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <agents>
          <agent>
            <configuration>
              <xml>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
                <data-source>data-source</data-source>
                <search-base>search-base</search-base>
                <search-filter>search-filter</search-filter>
                <search-scope>search-scope-choice</search-scope>
                <mapping-file>mapping-file</mapping-file>
                <root-tag-name>root-tag-name</root-tag-name>
                <key-attribute-name>key-attribute-name</key-attribute-name>
                <key-attribute-processor>key-attribute-processor</key-
attribute-processor>
                <value-attribute-name>value-attribute-name</value-attribute-
name>
                <value-attribute-processor>value-attribute-processor</value-
attribute-processor>
                <network-data-types>network-data-types</network-data-types>
                <publishing-interval>publishing-interval</publishing-interval>
                <event-life-expectancy>event-life-expectancy</event-life-
expectancy>
                <enable-eventing/>
              </xml>
            </configuration>
          </agent>
        </agents>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an XML agent. An XML agent retrieves information from a specified XML document and makes information available to the NIC based on specified tags in the file. An XML agent provides information about one type of data or mappings.

Although an XML agent may be used by an SRC application, typically you do not need to configure it. Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Contents

`<resolvers-list>`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName : roleName* .

Use commas to separate one role from another in the list.

Default— No value

`<data-source>`— URI of the XML document that provides information about NIC events to the NIC system. You must provide a URI for the XML document.

At this time, the only supported schema is a file.

Value— URI

Default— No value

`<search-base>`—(Optional) Root XML element in the specified XML document at which the agent starts to search the XML document. If you do not specify an element for the search base, the agent starts searching at the top of the file.

Value— XML element

Default— No value

`<search-filter>`—(Optional) Search filter that the agent uses to read entries in an XML document.

Value— Search filter syntax defined in RFC 2254— The String Representation of LDAP Search Filters (December 1997)

Default— No value

<search-scope>—(Optional) Level at which the agent searches the XML document.

Value— Search level:

- Object—Searches the object defined by the search base entry.
- One level—Specifies objects at the same level as the object defined by the search base entry.
- Subtree—Searches objects subordinate to the object defined by the search base entry.

Default— No value

<mapping-file>—(Optional) Name of the property file that maps XML tag names to corresponding Java class names. Enter a value if the XML document does not conform to the SDX XML schema.

Value— Filename

Default— No value

<root-tag-name>—(Optional) Tag name of the root XML element in the data source. Enter a value if the XML document does not follow the SDX XML schema.

Value— Tag name

Default— No value

<key-attribute-name>— List of XML attribute names to be used in constructing the key network data object for a custom processor.

Value—Text

<key-attribute-processor>—(Optional) The name of the Java class for processing the key object.

If specified, it will be used to produce the key network data object by using the list of attributes read from the directory. If no class is specified, there must be only one key LDAP attribute (in the key.attrNames property), and the attribute value must be in the proper format expected by the data type.

Value—Text

`<value-attribute-name>`—(Optional) List of LDAP attribute names to be used in constructing a value for the network data object. Specified attribute names if the agent publishes mappings or if you use a custom processor.

Value— List of attribute names. Use commas to separate entries.

`<value-attribute-processor>`—(Optional) The name of the Java class for processing the value object.

If specified, it will be used to produce the value network data object by using the list of attributes read from the directory. If no class is specified, there must be only one value attribute (in the `value.attrNames` property), and the attribute value must be in the proper format expected by the data type.

Value—Text

`<network-data-types>`— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key* , *value* . Use commas to separate entries.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—IpPool, InterfaceId

Default— No value

`<publishing-interval>`—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647

Default—60

`<event-life-expectancy>`—(Optional) Length of time that data is valid after the NIC

proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0

`<enable-eventing>`—(Optional) Enable Eventing

Default—true

Required Privilege Level

system

<host> (configuration/shared/nic/scenario)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <host>
            <name>name</name> <!-- identifier -->
          </host>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Description

Configure a NIC host for a specified NIC configuration scenario.

Contents

<name>— Name of the NIC host.

Value—Text

Required Privilege Level

system

<logger> (configuration/shared/nic/scenario/hosts)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <logger>
            <name>name</name> <!-- identifier -->
          </logger>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a logging component for NIC. Logging can be to a file or to the system logging utility.

Contents

<name>— Name of a NIC logging component.

Value—Text

Required Privilege Level

system

<file> (configuration/shared/nic/scenario/hosts/logger)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <logger>
            <file>
              <filter>filter</filter>
              <filename>filename</filename>
              <rollover-filename>rollover-filename</rollover-filename>
              <maximum-file-size>maximum-file-size</maximum-file-size>
            </file>
          </logger>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the

user has write access.

Value— Filename

Default— No value

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system

<syslog> (configuration/shared/nic/scenario/hosts/logger)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <logger>
            <syslog>
              <filter>filter</filter>
              <host>host</host>
              <facility>facility</facility>
              <format>format</format>
            </syslog>
          </logger>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings `{#}` are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Default— None

Required Privilege Level

system

<configuration> (configuration/shared/nic/scenario/hosts/host)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <host>
            <configuration>
              <hosted-resolvers>hosted-resolvers</hosted-resolvers>
              <hosted-agents>hosted-agents</hosted-agents>
            </configuration>
          </host>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC hosts.

Contents

<hosted-resolvers>— List of resolvers that should run on this host.

Value— Names of NIC resolvers which include the path of the locations of the NIC resolvers relative to the static configuration object. A forward slash (/) separates components in a path.

Example—/realms/sharedIp/A1,/realms/sharedIp/B1,/realms/sharedIp/C1,/realms/ip/A1,/realms/ip/B1,/realms/ip/C1,/realms/dn/A1,/realms/dn/B1,/realms/dn/C1,/realms/login/A1,/realms/login/B1,/realms/login/C1,/realms/login/D1

Default— No value

<hosted-agents>— List of paths to NIC agents that this host supports.

Value— Names of NIC agents that include the path of the locations of the NIC agents relative to the static configuration object. A forward slash (/) separates components in a path.

Example—/agents/VrSaeId,/agents/Router, /agents/PoolInterfaceId,/agents/InterfaceIdInterface

Default— No value

Required Privilege Level

system

<logger> (configuration/shared/nic/scenario/hosts/host/configuration)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <host>
            <configuration>
              <logger>
                <name>name</name> <!-- identifier -->
              </logger>
            </configuration>
          </host>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<name>—

Value—Text

Required Privilege Level

system

<file> (configuration/shared/nic/scenario/hosts/host/configuration/logger)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <host>
            <configuration>
              <logger>
                <file>
                  <filter>filter</filter>
                  <filename>filename</filename>
                  <rollover-filename>rollover-filename</rollover-filename>
                  <maximum-file-size>maximum-file-size</maximum-file-size>
                </file>
              </logger>
            </configuration>
          </host>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

`<filename>`— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— No value

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system

<syslog> (configuration/shared/nic/scenario/hosts/host/configuration/logger)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <hosts>
          <host>
            <configuration>
              <logger>
                <syslog>
                  <filter>filter</filter>
                  <host>host</host>
                  <facility>facility</facility>
                  <format>format</format>
                </syslog>
              </logger>
            </configuration>
          </host>
        </hosts>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

`<host>`— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Default— None

Required Privilege Level

system

<nic-locator-configuration> (configuration/shared/nic/scenario/nic-locators)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <nic-locators>
          <nic-locator-configuration>
            <name>name</name> <!-- identifier -->
          </nic-locator-configuration>
        </nic-locators>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC locator or NIC proxy, a NIC component that requests data resolution.

Contents

<name>— Name of the NIC locator.

Value—Text

Required Privilege Level

system

<resolution> (configuration/shared/nic/scenario/nic-locators/nic-locator-configuration)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <nic-locators>
          <nic-locator-configuration>
            <resolution>
              <resolver-name>resolver-name</resolver-name>
              <key-type>key-type</key-type>
              <value-type>value-type</value-type>
              <expect-multiple-values/>
              <constraints>constraints</constraints>
            </resolution>
          </nic-locator-configuration>
        </nic-locators>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

<key-type>— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<value-type>— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaeId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<expect-multiple-values>—(Optional) Specifies whether or not the key can have multiple corresponding values.

<constraints>—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Required Privilege Level

system

<realm> (configuration/shared/nic/scenario)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <realms>
          <realm>
            <name>name</name> <!-- identifier -->
          </realm>
        </realms>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Description

Configure a NIC realm, the NIC component that consists of a group of resolvers that perform a series of resolution tasks to provide a mapping from a specified key to a specified data type.

Typically, you use the default realm configuration for the NIC configuration scenarios in the SRC software.

Contents

<name>— Name of the NIC realm.

Value—Text

Required Privilege Level

system

<classname> (configuration/shared/nic/scenario/realms/realm/configuration/custom-resolver)

Usage

```

<configuration>
  <shared>
    <nic>
      <scenario>
        <realms>
          <realm>
            <configuration>
              <custom-resolver>
                <classname>
                  <name>name</name> <!-- identifier -->
                  <value>value</value>
                </classname>
              </custom-resolver>
            </configuration>
          </realm>
        </realms>
      </scenario>
    </nic>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an identifier to distinguish between different instances of the same data type in a resolution sequence. For the value enter the name of the data type.

Contents

<name>— Identifier to append to data type

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<transitions> (configuration/shared/nic/scenario/realms/realm/configuration)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <realms>
          <realm>
            <configuration>
              <transitions>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </transitions>
            </configuration>
          </realm>
        </realms>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a set of resolution sequences that map a property to a value.

Contents

<name>— Identifier for a resolution that represents one transition, or step, in the resolution process. Use ? to view the list of transitions for this realm, a group of resolvers that perform a series of resolution tasks to provide a mapping from a specified key to a specified data type.

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<resolvers> (configuration/shared/nic/scenario/realms/realms)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <realms>
          <realm>
            <resolvers>
              <name>name</name> <!-- identifier -->
            </resolvers>
          </realm>
        </realms>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC resolvers— the components that process NIC resolution requests.

Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Contents

<name>— Name of the NIC resolver.

Value—Text

Required Privilege Level

system

<configuration> (configuration/shared/nic/scenario/realms/realms/resolvers)

Usage

```
<configuration>
  <shared>
    <nic>
      <scenario>
        <realms>
          <realm>
            <resolvers>
              <configuration>
                <resolver-role>resolver-role</resolver-role>
                <resolvers-list>resolvers-list</resolvers-list>
                <roles-list>roles-list</roles-list>
              </configuration>
            </resolvers>
          </realm>
        </realms>
      </scenario>
    </nic>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure resolution from a NIC key to a NIC value.

Contents

<resolver-role>— Configure a transition that defines a key to value mapping.

Value—Text

<resolvers-list>—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—/realms/ip/A1, /realms/ip/B1

Default— No value

`<roles-list>`—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName* : *roleName* .
Use commas to separate one role from another in the list.

Default— No value

Required Privilege Level

system

<directory-connection> (configuration/slot/network-publisher)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <directory-connection>
        <url>url</url>
        <base-dn>base-dn</base-dn>
        <principal>principal</principal>
        <credentials>credentials</credentials>
      </directory-connection>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure directory connection properties that the network publisher uses to connect to the Juniper Networks database.

Contents

<url>—(Optional) URL that the network publisher uses to connect to the Juniper Networks database.

Value— URL

Default—ldap://127.0.0.1:389

<base-dn>—(Optional) Specify the distinguished name (DN) of the subtree in the Juniper Networks database that stores data collected from JUNOS routing platforms.

Value— DN

Default—o = Network, < base >

<principal>—(Optional) Specify the DN that defines the username with which the network publisher accesses the Juniper Networks database.

Value— DN

Default—cn = cli,ou = Components,o = Operators, < base >

<credentials>—(Optional) Specify the password with which the network publisher accesses the Juniper Networks database.

Value— *password*

Default—cli

Required Privilege Level

No specific privilege required.

<logger> (configuration/slot/network-publisher)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <logger>
        <name>name</name> <!-- identifier -->
      </logger>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to a file or to a system log server.

Contents

<name>— Configure logging to a file or to a system log server.

Value—Text

Required Privilege Level

No specific privilege required.

<file> (configuration/slot/network-publisher/logger)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <logger>
        <file>
          <filter>filter</filter>
          <filename>filename</filename>
          <rollover-filename>rollover-filename</rollover-filename>
          <maximum-file-size>maximum-file-size</maximum-file-size>
        </file>
      </logger>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to save messages in a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

No specific privilege required.

<syslog> (configuration/slot/network-publisher/logger)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <logger>
        <syslog>
          <filter>filter</filter>
          <host>host</host>
          <facility>facility</facility>
          <format>format</format>
        </syslog>
      </logger>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to send messages to the system log server.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

<facility>—(Optional) Type of system log in accordance with the system logging

protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Required Privilege Level

No specific privilege required.

<router> (configuration/slot/network-publisher)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <router>
        <router-release-number>router-release-number</router-release-number>
        <router-script-version>router-script-version</router-script-version>
      </router>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure connections between JUNOS routing platforms and the network publisher. The network publisher connects to the JUNOScript server on a JUNOS routing platform. Properties defined at this hierarchy level are applied by all the configured JUNOS routing platforms unless you specify different properties for a particular device.

<router-release-number>—(Optional) The release number of the JUNOS software running on the JUNOS routing platforms.

Value—Text

Default— No value

<router-script-version>—(Optional) Version of JUNOScript running on the JUNOS routing platforms.

Value—Text

Default— 1.0

Required Privilege Level

No specific privilege required.

<authentication> (configuration/slot/network-publisher/routers)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <routers>
        <authentication>
          <login-name>login-name</login-name>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
        </authentication>
      </routers>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure authentication properties for the JUNOS routing platforms to which the network publisher connects. Properties defined at this hierarchy level are applied to all the configured JUNOS routing platforms unless you specify different properties for a particular device.

Contents

<login-name>—(Optional) Username to log in to the JUNOS software.

Value—Text

Default— No value

<credentials>—(Optional) Password to log in to the JUNOS software.

Value— *password*

Default— No value

<protocol>—(Optional) Authentication protocol that network publisher uses to access a JUNOS routing platform.

Value

- `telnet`— Use JUNOScript over a Telnet connection.
- `ssh`— (Recommended) Use JUNOScript over an SSH connection.

Default—`ssh`

Required Privilege Level

No specific privilege required.

<router> (configuration/slot/network-publisher)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <routers>
        <router>
          <router-name>router-name</router-name> <!-- identifier -->
          <address>address</address>
          <router-release-number>router-release-number</router-release-number>
          <router-script-version>router-script-version</router-script-version>
        </router>
      </routers>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the connection between a particular JUNOS routing platform and the network publisher. The network publisher connects to the JUNOScript server on a JUNOS routing platform. Properties defined at this hierarchy level take precedence over those defined at the slot 0 network-publisher routers hierarchy level.

Contents

<router-name>— Configure properties for a specific JUNOS routing platform. Properties that you configure at this hierarchy level have precedence over properties defined at the slot 0 network-publisher routers level.

Value—Text

<address>— IP address of a JUNOS routing platform.

Value—IP address

<router-release-number>—(Optional) The release number of the JUNOS software running on the JUNOS routing platforms.

Value—Text

Default— No value

`<router-script-version>`—(Optional) Version of JUNOScript running on the JUNOS routing platforms.

Value—Text

Default— 1.0

Required Privilege Level

No specific privilege required.

<authentication> (configuration/slot/network-publisher/routers/router)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <routers>
        <router>
          <authentication>
            <login-name>login-name</login-name>
            <credentials>credentials</credentials>
            <protocol>protocol-choice</protocol>
          </authentication>
        </router>
      </routers>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure authentication properties for a particular JUNOS routing platform to which the network publisher connects. Properties defined at this hierarchy level take precedence over those defined at the slot 0 network-publisher routers authentication hierarchy level.

Contents

<login-name>—(Optional) Username to log in to the JUNOS software.

Value—Text

Default— No value

<credentials>—(Optional) Password to log in to the JUNOS software.

Value— *password*

Default— No value

<protocol>—(Optional) Authentication protocol that network publisher uses to access a

JUNOS routing platform.

Value

- `telnet`— Use JUNOScript over a Telnet connection.
- `ssh`— (Recommended) Use JUNOScript over an SSH connection.

Default—`ssh`

Required Privilege Level

No specific privilege required.

<test-mode> (configuration/slot/network-publisher/routers/router)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <routers>
        <router>
          <test-mode>
            <enable-file-input/>
            <enable-file-output/>
            <input-location>input-location</input-location>
            <output-location>output-location</output-location>
          </test-mode>
        </router>
      </routers>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure information to test the network publisher.

Use an input file to test a configuration before routes to the NIC are available or before VPNs are configured. You can also use an input file to set up a test configuration for demonstration purposes.

Use an output file to review the information that the network publisher has gathered.

Contents

<enable-file-input>—(Optional) Configure the network publisher to use data in a file, rather than in the directory, when you run the network publisher.

<enable-file-output>—(Optional) Configure the network publisher to collect data from JUNOS routing platforms and store that information in a file, rather than in the directory.

`<input-location>`—(Optional) Location in the directory where input files are located. In most cases, you do not need to change the value of this option.

Note: Input filenames should be in the format `router_name_1.xml`. where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`sample/junos/rt`

`<output-location>`—(Optional) Location in the directory where output files are located. In most cases, you do not need to change the value of this option.

Note: Output filenames should be in the format `router_name_1.xml` where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`var/junos/rt`

Required Privilege Level

No specific privilege required.

<test-mode> (configuration/slot/network-publisher/routers)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <routers>
        <test-mode>
          <enable-file-input/>
          <enable-file-output/>
          <input-location>input-location</input-location>
          <output-location>output-location</output-location>
        </test-mode>
      </routers>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure information to test the network publisher.

Use an input file to test a configuration before routes to the NIC are available or before VPNs are configured. You can also use an input file to set up a test configuration for demonstration purposes.

Use an output file to review the information that the network publisher has gathered.

Contents

<enable-file-input>—(Optional) Configure the network publisher to use data in a file, rather than in the directory, when you run the network publisher.

<enable-file-output>—(Optional) Configure the network publisher to collect data from JUNOS routing platforms and store that information in a file, rather than in the directory.

<input-location>—(Optional) Location in the directory where input files are located. In most cases, you do not need to change the value of this option.

Note: Input filenames should be in the format `router_name_1.xml`, where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`sample/junos/rt`

`<output-location>`—(Optional) Location in the directory where output files are located. In most cases, you do not need to change the value of this option.

Note: Output filenames should be in the format `router_name_1.xml` where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`var/junos/rt`

Required Privilege Level

No specific privilege required.

<select> (configuration/slot/network-publisher)

Usage

```
<configuration>
  <slot>
    <network-publisher>
      <select>
        <route-table-filter>route-table-filter</route-table-filter>
        <route-entry-filter>route-entry-filter</route-entry-filter>
      </select>
    </network-publisher>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Specify the routing tables and the entries in the routing tables from which the network publisher collects routing information.

The network publisher can collect information from JUNOS IPv4 and IPv6 routing tables. By default, it collects information from all IPv4 routing tables, including tables for VPNs, and entries for all protocols. Based on your network configuration, consider which protocols to exclude from the configuration for network publisher.

The network publisher saves the information collected in the Juniper Networks database.

Contents

<route-table-filter>—(Optional) Routing table from which the network publisher collects information.

Value— Routing table name

<route-entry-filter>—(Optional) Routing table entry from which the network publisher collects information.

Value— Name of routing table entry

Required Privilege Level

No specific privilege required.

<nic> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <nic>
      <base-dn>base-dn</base-dn>
      <java-runtime-environment>java-runtime-environment</java-runtime-
environment>
      <java-heap-size>java-heap-size</java-heap-size>
      <java-new-size>java-new-size</java-new-size>
      <java-garbage-collection-options>java-garbage-collection-options</java-
garbage-collection-options>
      <java-64bit/>
      <snmp-agent/>
      <hostname>hostname</hostname>
      <scenario-name>scenario-name</scenario-name>
      <runtime-group>runtime-group</runtime-group>
    </nic>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC local operating properties.

Contents

<base-dn>— Distinguished name (DN) of the root directory for the NIC.

Value— DN

Default— o = umc

<java-runtime-environment>— Path to the Java runtime environment (JRE).

Value— Directory path

Default— ../jre/bin/java

<java-heap-size>— Maximum Java heap (memory) size available to the JRE. The value

is inserted when the JRE starts. See documentation for the Java runtime environment for valid values.

Value— Number of megabytes in the format ###m

Default— 128m

<java-new-size>— Maximum Java new generation heap (memory) size available to the JRE when the NIC starts.

Value— Integer in the range 0– < Java heap size > . Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 64m. See the documentation for the JRE for valid values.

Default— 24m

<java-garbage-collection-options>— Garbage collection functionality of the Java Virtual Machine.

Value—

Default— -Xbatch -XX:CMSInitiatingOccupancyFraction = 80 -XX:

+ UseParNewGC -XX:SurvivorRatio = 1 -XX:

InitialTenuringThreshold = 8 -XX:MaxTenuringThreshold = 10 -XX:

+ UseCMSCompactAtFullCollection -XX:

CMSEFullGCsBeforeCompaction = 0 -XX: + CMSClassUnloadingEnabled -

XX: + CMSParallelRemarkEnabled -XX: + UseConcMarkSweepGC

<java-64bit>—(Optional) Start the java virtual machine in 64 bit mode

<snmp-agent>—(Optional) Enable the NIC to communicate with the SNMP agent. By using SNMP, you can view SNMP counters with an SNMP browser.

Default—false

<hostname>— Name of the NIC host. In most cases, use the name DemoHost because this is the hostname used in most NIC configuration scenarios. Refer to the documentation to verify that the NIC configuration scenario you use includes DemoHost as the NIC host.

Value— NIC hostname

Default— DemoHost for most configuration scenarios

<scenario-name>— Name of the NIC scenario under the static configuration namespace.

Value— NIC hostname

Default— DemoHost for most configuration scenarios

`<runtime-group>`—(Optional) Group to which this NIC host belongs for use with NIC replication. NIC hosts that run in the same system must specify the same runtime group. If you do not specify a value for the group, the NIC host creates the configuration.

Value— Group name

Default— No value

Required Privilege Level

No specific privilege required.

<initial> (configuration/slot/nic)

Usage

```
<configuration>
  <slot>
    <nic>
      <initial>
        <static-dn>static-dn</static-dn>
        <dynamic-dn>dynamic-dn</dynamic-dn>
      </initial>
    </nic>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for the NIC.

Contents

<static-dn>—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—l = NIC, ou = staticConfiguration, ou = Configuration,
o = Management, o = umc

<dynamic-dn>—(Optional) Location of programmatically defined configuration data in the directory.

Value—DN

Default— ou = dynamicConfiguration, ou = Configuration,
o = Management, < base >

Required Privilege Level

No specific privilege required.

<directory-connection> (configuration/slot/nic/initial)

Usage

```
<configuration>
  <slot>
    <nic>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </nic>
  </slot>
</configuration>
```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default— 10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

No specific privilege required.

<directory-eventing> (configuration/slot/nic/initial)

Usage

```
<configuration>
  <slot>
    <nic>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </nic>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

<polling-interval>—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30

<event-base-dn>—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default—o = UMC

<dispatcher-pool-size>—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

Default—1

Required Privilege Level

No specific privilege required.

SNMP Agent Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for configuring the SNMP agent. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
snmp	snmp
snmp agent	< agent >
snmp agent initial	< initial >
snmp agent initial directory-connection	< directory-connection >
snmp agent initial directory-eventing	< directory-eventing >
snmp agent java	< java >
snmp agent logger	< logger >
snmp agent logger name file	< file >
snmp agent logger name syslog	< syslog >
snmp community	< community >
snmp monitor	< monitor >
snmp monitor alarm	< alarm >
snmp monitor alarm name boolean-test	< boolean-test >
snmp monitor alarm name delta-discontinuity-check	< delta-discontinuity-check >
snmp monitor alarm name existence-test	< existence-test >
snmp monitor alarm name threshold-test	< threshold-test >
snmp monitor event	< event >
snmp monitor event name notification	< notification >
snmp monitor event name snmp-set	< snmp-set >
snmp notify alarm category	< category >

snmp notify alarm category category-name alarm	<u>< alarm ></u>
snmp notify event category	<u>< category ></u>
snmp notify event category category-name event	<u>< event ></u>
snmp notify target	<u>< target ></u>
snmp v3 snmp-community	<u>< snmp-community ></u>
snmp v3 usm local-engine user	<u>< user ></u>
snmp v3 usm local-engine user username authentication-md5	<u>< authentication-md5 ></u>
snmp v3 usm local-engine user username authentication-sha	<u>< authentication-sha ></u>
snmp v3 usm local-engine user username privacy-aes	<u>< privacy-aes ></u>
snmp v3 usm local-engine user username privacy-des	<u>< privacy-des ></u>
snmp v3 vacm access group	<u>< group ></u>
snmp v3 vacm access group group-name default-context-prefix security-model	<u>< security-model ></u>
snmp v3 vacm access group group-name default-context-prefix security-model security-level	<u>< security-level ></u>
snmp v3 vacm security-to-group security-model	<u>< security-model ></u>
snmp v3 vacm security-to-group security-model security-name	<u>< security-name ></u>
snmp view	<u>< view ></u>
snmp view view-name oid	<u>< oid ></u>

<snmp> (configuration)

Usage

```
<configuration>  
  <snmp>  
    <contact>contact</contact>  
    <name>name</name>  
    <location>location</location>  
    <description>description</description>  
    <address>address</address>  
  </snmp>  
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SNMP system information.

Contents

<contact>—(Optional) Administrative contact for the system being managed by SNMP.

Value—Text

<name>—(Optional) Name of the system being managed by SNMP.

Value—Text

<location>—(Optional) Location of the system being managed by SNMP.

Value—Text

<description>—(Optional) Description of the system being managed by SNMP.

Value—Text

`<address>`—(Optional) (Multivalue) Listening address on which to receive incoming SNMP requests.

Value— IP address; list of addresses.

Default— The SNMP agent listens on all IPv4 interfaces.

Required Privilege Level

snmp

<agent> (configuration/snmp)

Usage

```
<configuration>
  <snmp>
    <agent>
      <trap-history-limit>trap-history-limit</trap-history-limit>
      <component-polling-interval>component-polling-interval</component-
polling-interval>
      <protocol-log-level>protocol-log-level</protocol-log-level>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SDX SNMP agent.

Contents

<trap-history-limit>—(Optional) Maximum number of elements stored in the SNMP trap history table.

Value—Integer in the range 1–2147483647

Default—800

<component-polling-interval>—(Optional) Interval at which the SDX component is polled to determine whether it is running and to generate up and down event traps.

Value—Integer in the range 10–2147483647 seconds

Default—60

<protocol-log-level>—(Optional) The log level for SNMP requests received from the master agent and responses to the requests. To enable packet-level logging, set it to 9 or less.

Value—Integer in the range 0–100

Default—20

Required Privilege Level

snmp

<initial> (configuration/snmp/agent)

Usage

```
<configuration>
  <snmp>
    <agent>
      <initial>
        <base-dn>base-dn</base-dn>
        <host-id>host-id</host-id>
      </initial>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for the SDX SNMP agent.

Contents

<base-dn>— DN of the directory used for the SNMP agent configuration data.

Value— DN

Default—\${system ldap client base-dn}

<host-id>— Identifier of the system management configuration in the directory server that provides the remaining configuration for the SNMP agent. If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

Value— DN

Default—ou = POP-ID,ou = System Management,ou = Configuration,
o = Management,o = umc

Required Privilege Level

snmp

<directory-connection> (configuration/snmp/agent/initial)

Usage

```
<configuration>
  <snmp>
    <agent>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </agent>
  </snmp>
</configuration>
```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default— 10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

snmp

<directory-eventing> (configuration/snmp/agent/initial)

Usage

```
<configuration>
  <snmp>
    <agent>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

<polling-interval>—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30

<event-base-dn>—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default—o = UMC

<dispatcher-pool-size>—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

Default— 1

Required Privilege Level

snmp

<java> (configuration/snmp/agent)

Usage

```
<configuration>
  <snmp>
    <agent>
      <java>
        <heap-size>heap-size</heap-size>
      </java>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local Java Runtime Environment (JRE) properties for the SDX SNMP agent.

Contents

<heap-size>—(Optional) Maximum amount of Java heap (memory) available to the JRE.
Do not change this value unless instructed to do so by Juniper Networks.

Value— Number of megabytes in the format *integer*m

Default— 160m

Required Privilege Level

snmp

<logger> (configuration/snmp/agent)

Usage

```
<configuration>
  <snmp>
    <agent>
      <logger>
        <name>name</name> <!-- identifier -->
      </logger>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination.

Contents

<name>— Name used to group parameters for the logging destination.

Value—Text

Required Privilege Level

snmp

<file> (configuration/snmp/agent/logger)

Usage

```
<configuration>
  <snmp>
    <agent>
      <logger>
        <file>
          <filter>filter</filter>
          <filename>filename</filename>
          <rollover-filename>rollover-filename</rollover-filename>
          <maximum-file-size>maximum-file-size</maximum-file-size>
        </file>
      </logger>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination for file-based logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

snmp

<syslog> (configuration/snmp/agent/logger)

Usage

```
<configuration>
  <snmp>
    <agent>
      <logger>
        <syslog>
          <filter>filter</filter>
          <host>host</host>
          <facility>facility</facility>
          <format>format</format>
        </syslog>
      </logger>
    </agent>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination for syslog-based logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

<facility>—(Optional) Type of system log in accordance with the system logging

protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Required Privilege Level

snmp

<community> (configuration/snmp)

Usage

```
<configuration>
  <snmp>
    <community>
      <community>community</community> <!-- identifier -->
      <authorization>authorization-choice</authorization>
      <clients>clients</clients>
      <oid>oid</oid>
    </community>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a community string, which defines the access control for client systems.

Contents

<community>— Community name.

Value—Text

<authorization>—(Optional) Authorization type.

Value

- read-only— Allow read-only access
- read-write— Allow read and write access

Default—read-only

<clients>— IP address or subnet of the SNMP client hosts that are authorized to use this community. By default, all clients are allowed.

Value—Text

Default—0.0.0.0/0

<oid>—(Optional) Object identifier (OID) used to represent a subtree of MIB objects to which access is allowed.

Value—Text

Default— Access to the full OID tree

Required Privilege Level

snmp

<monitor> (configuration/snmp)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <security-name>security-name</security-name>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Provide active monitoring of SRC MIB objects as configured. The software generates associated notification events when specified criteria are met.

Contents

<security-name>— SNMPv3 username to access a monitored MIB object. SNMPv3 provides security by controlling access to the objects.

Value— *username*

Default— No value

Required Privilege Level

snmp

<alarm> (configuration/snmp/monitor)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <alarm>
        <name>name</name> <!-- identifier -->
        <interval>interval</interval>
        <sample-type>sample-type-choice</sample-type>
        <ignore-startup-alarm/>
        <event>event</event>
        <variable>variable</variable>
        <strict-oid/>
      </alarm>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Monitor the value of a MIB object. You can configure how often to sample a value, the type of sampling to perform, the type of alarm or trigger to use the sampled value, and the event to generate in response to a specified condition.

Note: Configure one alarm condition at a time.

Contents

<name>— Name of the alarm (also referred to as a trigger).

Value—Text

<interval>— Interval between monitoring samples.

Value—Integer in the range seconds

Default—600

<sample-type>— Method of sampling to use for the specified variable.

Note: Existence tests disregard the sample type when set to `delta-value`.

Value

- `absolute-value`— Use actual value of the trigger to compare to the threshold value.
- `delta-value`— Use the delta (difference between two samples) to compare to the value.

Default— No value

`<ignore-startup-alarm>`—(Optional) Whether the alarm can be sent when it is first activated. If this option is set, the monitor expression is not evaluated when the alarm activates the first time. If not set, the first evaluation is done after the alarm is activated.

Default—false

`<event>`—(Optional) The name of the event to be generated in response to the alarm condition. If you do not specify an event, the software uses one of the following DISMAN notification events: `mteTriggerFired` in existence or boolean tests, and `mteTriggerRising` or `mteTriggerFalling` in threshold tests.

Value— *event name*

Default— None

`<variable>`— Object identifier (OID) of the MIB variable to be monitored. The OID can be an identifier in dotted decimal notation or the name of a MIB object.

Value— *OID or name*

Default— No value

`<strict-oid>`—(Optional) Monitor the SNMP object instance specified by the variable attribute. If you do not set this option, the software monitors all objects in the MIB branch specified by the variable option.

Default—false

Required Privilege Level

snmp

<boolean-test> (configuration/snmp/monitor/alarm)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <alarm>
        <boolean-test>
          <comparison>comparison-choice</comparison>
          <value>value</value>
        </boolean-test>
      </alarm>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a monitor test to compare a sample value to a specified value or range of values. If the condition specified for the test is met, the software generates the event. The software generates the event again after the status of the condition changes to false then to true again.

Note: Configure only one monitor test at a time.

Contents

<comparison>— Type of boolean comparison to perform.

Value

- equal— True if the sample value equals object value.
- unequal— True if the sample value does not equal the object value.
- less— True if the sample is less than the object value.
- less-or-equal— True if the sample value is less than or equal to the object value.
- greater— True if the sample value is greater than the object value.
- greater-or-equal— True if the sample value is greater than or equal to the object value.

Default— No value

<value>— Value against which to compare the sample value.

Value—Integer in the range -2147483648–2147483647

Default— No Value

Required Privilege Level

snmp

<delta-discontinuity-check> (configuration/snmp/monitor/alarm)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <alarm>
        <delta-discontinuity-check>
          <variable>variable</variable>
          <strict-oid/>
        </delta-discontinuity-check>
      </alarm>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SNMP to detect a discontinuity in values to prevent false alarms caused by the value of a MIB object being reset. Use this statement when the sample type is delta-value (a change in the value of a monitored MIB object is compared to a threshold value). You define a variable, called a discontinuity marker, which is a MIB object to use to validate the delta, or difference, between values. The marker object should be of type TimeTicks, DateAndTime, or Timestamp.

Before the SNMP agent calculates a delta, it checks the discontinuity marker for the trigger condition at the end of a polling interval. A change in the value of the discontinuity marker indicates that a discontinuity occurs. As a result, the agent does not perform the test for the associated trigger condition until the next polling interval.

Contents

<variable>— Object identifier (OID) or name of a discontinuity marker.

Value— Marker object of type TimeTicks, DateAndTime or Timestamp

Default— No value

<strict-oid>—(Optional) Monitor the discontinuity marker instance specified by the variable attribute. If you do not set this option, the software monitors all discontinuity objects subordinate to the value set by the variable option.

Default—false

Required Privilege Level

snmp

<existence-test> (configuration/snmp/monitor/alarm)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <alarm>
        <existence-test>
          <type>type-choice</type>
        </existence-test>
      </alarm>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a monitor test to identify when an object appears, disappears, or changes value. If the test criteria are met, the test is successful.

Note: Configure only one monitor test at a time.

Contents

<type>— Type of monitor test to perform.

Value

- present— Test for appearance of object.
- absent— Test for disappearance of object.
- changed— Test for change in value of object.

Default— No value

Required Privilege Level

snmp

<threshold-test> (configuration/snmp/monitor/alarm)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <alarm>
        <threshold-test>
          <rising-threshold>rising-threshold</rising-threshold>
          <falling-threshold>falling-threshold</falling-threshold>
        </threshold-test>
      </alarm>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a threshold monitor test. A threshold test compares the sample value to a configured upper and lower threshold. The monitor generates a corresponding event when the value of the monitored object falls below the lower threshold or rises above the upper threshold.

After a rising threshold event is generated, it is generated again only after the sample value falls below the lower threshold. Similarly, a subsequent falling threshold event is generated when the sample value rises above the upper threshold.

Note: Configure only one monitor test at a time.

Contents

<rising-threshold>— Upper threshold for the sample value. The software generates an event when the sample value is greater than or equal to the rising threshold, and the value at the last sampling interval is less than this threshold.

Value— Integer in the range -2147483648–2147483647

Default— No value

<falling-threshold>— Lower threshold for the sample value. The software generates an event when the sample value is less than or equal to the falling threshold, and the value at the last sampling interval is greater than this threshold.

Value—Integer in the range -2147483648–2147483647
Default— No value

Required Privilege Level

snmp

<event> (configuration/snmp/monitor)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <event>
        <name>name</name> <!-- identifier -->
      </event>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<name>— The name of the event to be invoked in response to a trigger or an alarm. When the event is invoked, SNMP sends a notification or an snmp-set.

Value—Text

Required Privilege Level

snmp

<notification> (configuration/snmp/monitor/event)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <event>
        <notification>
          <oid>oid</oid>
          <strict-object>strict-object</strict-object>
          <wildcarded-object>wildcarded-object</wildcarded-object>
        </notification>
      </event>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define an event for which SNMP sends a notification.

Note: Do not define an event notification and an snmp-set for the same event.

Contents

<oid>— Notification Object identifier (OID).

Value— *OID*

Default— No value

<strict-object>—(Optional) (Multivalue) OIDs of VARBIND objects to be used as specified

Value— *OID*

Default— No value

<wildcarded-object>—(Optional) (Multivalue) OIDs of VARBIND objects include subidentifiers from the corresponding monitored object appended to the object.

Value— *OID*

Default— No value

Required Privilege Level

snmp

<snmp-set> (configuration/snmp/monitor/event)

Usage

```
<configuration>
  <snmp>
    <monitor>
      <event>
        <snmp-set>
          <variable>variable</variable>
          <value>value</value>
          <strict-oid/>
        </snmp-set>
      </event>
    </monitor>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define an event that sets a MIB variable. Do not define an event notification and an snmp-set for the same event.

Contents

<variable>— Object identifier (OID) of MIB variable to be set

Value— *OID*

Default— No value

<value>— Object value to set

Value— Integer in the range -2147483648–2147483647

Default— No value

<strict-oid>—(Optional) Monitor the OID exactly as specified by the variable option. If not set, the software adds any suffixes to any OID matches.

Default—false

Required Privilege Level

snmp

<category> (configuration/snmp/notify/alarm)

Usage

```
<configuration>
  <snmp>
    <notify>
      <alarm>
        <category>
          <category-name>category-name</category-name> <!-- identifier -->
        </category>
      </alarm>
    </notify>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure alarm category.

Contents

<category-name>— Category name for alarm.

Value— Category name from list of possible completions, including:

- acp
- jps
- nic-host
- policy-decision-point
- policy-engine
- radius-accounting-peer
- radius-authentication-peer
- sae
- sae-router-driver
- sdx-redirector
- system-management

Required Privilege Level

snmp

<alarm> (configuration/snmp/notify)

Usage

```
<configuration>
  <snmp>
    <notify>
      <alarm>
        <category>
          <alarm>
            <alarm-name>alarm-name</alarm-name> <!-- identifier -->
            <interval>interval</interval>
            <critical>critical</critical>
            <major>major</major>
            <minor>minor</minor>
          </alarm>
        </category>
      </alarm>
    </notify>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure alarm.

Contents

<alarm-name>— Alarm name.

Value— Alarm name from list of possible completions, depending on the specified alarm category

<interval>—(Optional) Interval at which the variable associated with the trap is polled.

Value—Integer in the range 1–2147483647
Default—60

<critical>— Threshold above which a critical alarm is generated.

Value—Integer in the range 0–2147483647

<major>— Threshold above which a major alarm is generated.

Value—Integer in the range 0–2147483647

<minor>— Threshold above which a minor alarm is generated.

Value—Integer in the range 0–2147483647

Required Privilege Level

snmp

<category> (configuration/snmp/notify/event)

Usage

```
<configuration>
  <snmp>
    <notify>
      <event>
        <category>
          <category-name>category-name</category-name> <!-- identifier -->
        </category>
      </event>
    </notify>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure event category.

Contents

<category-name>— Category name for event trap.

Value— Category name from list of possible completions, including:

- acp
- directory-eventing-system
- jps
- nic-host
- sae
- sae-router-driver
- system-management

Required Privilege Level

snmp

<event> (configuration/snmp/notify)

Usage

```
<configuration>
  <snmp>
    <notify>
      <event>
        <category>
          <event>
            <event-name>event-name</event-name> <!-- identifier -->
          </event>
        </category>
      </event>
    </notify>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable event notification.

Contents

<event-name>— Event trap name.

Value— Event name from list of possible completions, depending on the specified event category

Required Privilege Level

snmp

<target> (configuration/snmp/notify)

Usage

```
<configuration>
  <snmp>
    <notify>
      <target>
        <target-name>target-name</target-name> <!-- identifier -->
        <address>address</address>
        <port>port</port>
        <community>community</community>
        <type>type-choice</type>
      </target>
    </notify>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure notification target.

Contents

<target-name>— Notification target name.

Value—Text

<address>— IPv4 or IPv6 address of the system to receive notifications.

Value—IP address

<port>—(Optional) SNMP trap port number.

Value—Integer in the range 0–65535

Default—162

<community>— Community string used when sending traps.

Value—Text

<type>— Type of notifications to receive.

Value

- trapv1—SNMPv1 trap
- trapv2—SNMPv2c trap
- inform—SNMPv2 inform

Required Privilege Level

snmp

<snmp-community> (configuration/snmp/v3)

Usage

```
<configuration>
  <snmp>
    <v3>
      <snmp-community>
        <community-index>community-index</community-index> <!-- identifier -->
        <community-name>community-name</community-name>
        <security-name>security-name</security-name>
        <address>address</address>
      </snmp-community>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Map an SNMPv1 or SNMPv2c community string to a security name. Optionally, you can specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community. By default, all SNMP clients using this community string are authorized to access the agent.

Contents

<community-index>— Unique index that identifies an SNMP community.

Value—Text

<community-name>—(Optional) A community string for an SNMPv1 or SNMPv2c community. If unspecified, the community index is used.

Value—Text

<security-name>— The view-based access control model (VACM) security name to associate with the community string.

Value—Text

`<address>`— IP address or subnet of the SNMP client hosts that are authorized to use this community.

Value—Text

Default— 0.0.0.0/0

Required Privilege Level

snmp

<user> (configuration/snmp/v3/usm/local-engine)

Usage

```
<configuration>
  <snmp>
    <v3>
      <usm>
        <local-engine>
          <user>
            <username>username</username> <!-- identifier -->
          </user>
        </local-engine>
      </usm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a user associated with an SNMPv3 group. By default, no authentication or encryption is specified for the SNMPv3 user.

Contents

<username>— SNMPv3 user-based security model (USM) username

Value—Text

Required Privilege Level

snmp

<authentication-md5> (configuration/snmp/v3/usm/local-engine/user)

Usage

```
<configuration>
  <snmp>
    <v3>
      <usm>
        <local-engine>
          <user>
            <authentication-md5>
              <authentication-password>authentication-password</
authentication-password>
            </authentication-md5>
          </user>
        </local-engine>
      </usm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Message Digest 5 (MD5) as the authentication type for the SNMPv3 user.

Contents

<authentication-password>— Password used for authentication.

Value— Password; must be at least eight characters

Required Privilege Level

snmp

<authentication-sha> (configuration/snmp/v3/usm/local-engine/user)

Usage

```
<configuration>
  <snmp>
    <v3>
      <usm>
        <local-engine>
          <user>
            <authentication-sha>
              <authentication-password>authentication-password</
authentication-password>
            </authentication-sha>
          </user>
        </local-engine>
      </usm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Secure Hash Algorithm (SHA) as the authentication type for the SNMPv3 user.

Contents

<authentication-password>— Password used for authentication.

Value— Password; must be at least eight characters

Required Privilege Level

snmp

<privacy-aes> (configuration/snmp/v3/usm/local-engine/user)

Usage

```
<configuration>
  <snmp>
    <v3>
      <usm>
        <local-engine>
          <user>
            <privacy-aes>
              <privacy-password>privacy-password</privacy-password>
            </privacy-aes>
          </user>
        </local-engine>
      </usm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Advanced Encryption Standard (AES) for the SNMPv3 user.

Note: Before you configure encryption, you must configure MD5 or SHA authentication.

Contents

<privacy-password>— Privacy password for the SNMPv3 user.

Value— Password; must be at least eight characters

Required Privilege Level

snmp

<privacy-des> (configuration/snmp/v3/usm/local-engine/user)

Usage

```
<configuration>
  <snmp>
    <v3>
      <usm>
        <local-engine>
          <user>
            <privacy-des>
              <privacy-password>privacy-password</privacy-password>
            </privacy-des>
          </user>
        </local-engine>
      </usm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Data Encryption Standard (DES) for the SNMPv3 user.

Note: Before you configure encryption, you must configure MD5 or SHA authentication.

Contents

<privacy-password>— Privacy password for the SNMPv3 user.

Value— Password; must be at least eight characters

Required Privilege Level

snmp

<group> (configuration/snmp/v3/vacm/access)

Usage

```
<configuration>
  <snmp>
    <v3>
      <vacm>
        <access>
          <group>
            <group-name>group-name</group-name> <!-- identifier -->
          </group>
        </access>
      </vacm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define access privileges granted to a group.

Contents

<group-name>— Name for a collection of SNMP security names that belong to the same SNMP access policy.

Value—Text

Required Privilege Level

snmp

<security-model> (configuration/snmp/v3/vacm/access/group/default-context-prefix)

Usage

```

<configuration>
  <snmp>
    <v3>
      <vacm>
        <access>
          <group>
            <default-context-prefix>
              <security-model>
                <security-model>security-model-choice</security-model> <!--
identifier -->
              </security-model>
            </default-context-prefix>
          </group>
        </access>
      </vacm>
    </v3>
  </snmp>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure security model for access privileges.

Contents

Type of security model used for access privileges.

Value

- any—Any security model
- v1—SNMPv1 model
- v2c—SNMPv2c model
- usm—SNMPv3 user-based security model

Required Privilege Level

snmp

<security-level> (configuration/snmp/v3/vacm/access/group/default-context-prefix/security-model)

Usage

```

<configuration>
  <snmp>
    <v3>
      <vacm>
        <access>
          <group>
            <default-context-prefix>
              <security-model>
                <security-level>
                  <security-level>security-level-choice</security-level> <!--
identifier -->
                  <read-view>read-view</read-view>
                  <write-view>write-view</write-view>
                </security-level>
              </security-model>
            </default-context-prefix>
          </group>
        </access>
      </vacm>
    </v3>
  </snmp>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access privileges granted to a particular security model.

Contents

Security level granted to a security model. If you are configuring the SNMPv1 or SNMPv2c security model, use none as the security level.

Value

- authentication— Provides authentication but no encryption
- none— Provides no authentication and no encryption
- privacy— Provides authentication and encryption

`<read-view>`—(Optional) View used for SNMP Get requests.

Value—Text

Default—none

`<write-view>`—(Optional) View used for SNMP Set requests.

Value—Text

Default—none

Required Privilege Level

snmp

<security-model> (configuration/snmp/v3/vacm/security-to-group)

Usage

```
<configuration>
  <snmp>
    <v3>
      <vacm>
        <security-to-group>
          <security-model>
            <security-model>security-model-choice</security-model> <!--
identifier -->
          </security-model>
        </security-to-group>
      </vacm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure security model context for a group.

Contents

Type of security model.

Value

- v1—SNMPv1 model
- v2c—SNMPv2c model
- usm—SNMPv3 user-based security model

Required Privilege Level

snmp

<security-name> (configuration/snmp/v3/vacm/security-to-group/security-model)

Usage

```
<configuration>
  <snmp>
    <v3>
      <vacm>
        <security-to-group>
          <security-model>
            <security-name>
              <security-name>security-name</security-name> <!-- identifier -->
              <group-name>group-name</group-name>
            </security-name>
          </security-model>
        </security-to-group>
      </vacm>
    </v3>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Map a security name in the specified security model to a named group.

Contents

<security-name>— Security name to assign to group. If the security model is usm, the security name is the username configured at the [edit snmp v3 usm local-engine user] hierarchy level.

Value—Text

<group-name>— Group to which the security name is assigned.

Value—Text

Required Privilege Level

snmp

<view> (configuration/snmp)

Usage

```
<configuration>
  <snmp>
    <view>
      <view-name>view-name</view-name> <!-- identifier -->
    </view>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a MIB view.

Contents

<view-name>— MIB view name that identifies a group of MIB objects for which to define access. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy.

Value—Text

Required Privilege Level

snmp

<oid> (configuration/snmp/view)

Usage

```
<configuration>
  <snmp>
    <view>
      <oid>
        <oid>oid</oid> <!-- identifier -->
        <include/>
        <exclude/>
      </oid>
    </view>
  </snmp>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify an object identifier (OID) that represents a subtree of MIB objects for the view.

Contents

<oid>— Object identifier (OID) that represents a subtree of MIB objects.

Value—Text

Specifies whether the OID is included in or excluded from the view.

Value

- include—Include this OID in the view
- exclude—Exclude this OID from the view

Required Privilege Level

snmp

Juniper Policy Server (JPS) Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the JPS. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
slot number jps	<u>< jps ></u>
slot number jps am-interface	<u>< am-interface ></u>
slot number jps cmts-interface	<u>< cmts-interface ></u>
slot number jps cmts-registry cmts	<u>< cmts ></u>
slot number jps cmts-registry cmts cmts-ip range-pool	<u>< range-pool ></u>
slot number jps cmts-registry cmts cmts-ip subnet-pool	<u>< subnet-pool ></u>
slot number jps logger	<u>< logger ></u>
slot number jps logger name file	<u>< file ></u>
slot number jps logger name syslog	<u>< syslog ></u>
slot number jps rks-interface	<u>< rks-interface ></u>
slot number jps rks-interface am	<u>< am ></u>
slot number jps rks-interface rks-pair	<u>< rks-pair ></u>

<jps> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <jps>
      <java-heap-size>java-heap-size</java-heap-size>
      <snmp-agent/>
      <policy-server-id>policy-server-id</policy-server-id>
      <use-psid-in-gate-commands/>
      <cmts-message-buffer-size>cmts-message-buffer-size</cmts-message-buffer-
size>
      <am-message-buffer-size>am-message-buffer-size</am-message-buffer-size>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the Juniper Policy Server (JPS).

Contents

<java-heap-size>— Maximum amount of Java heap (memory) available to the JRE.

Value— Number of megabytes in the format *integerm*

Default—400m

<snmp-agent>—(Optional) Enables the JPS to communicate with the SNMP agent.

<policy-server-id>—(Optional) Network-wide unique identifier for the JPS that is sent to CMTS devices in Pdp-Config messages and gate commands generated by the JPS.

Value—Integer in the range 0–65535

Default—0

<use-psid-in-gate-commands>—(Optional) Specifies whether gate control messages (such as gate-info messages) generated by this JPS should contain its policy server

identifier. These gate control messages are not generated by an application manager for forwarding by the JPS.

When the JPS is communicating only with PCMM I03 CMTS devices, the value must be true. When the JPS is communicating with any pre-PCMM I03 CMTS devices, the value must be false.

Default—false

`<cmts-message-buffer-size>`—(Optional) Maximum number of messages buffered for each CMTS destination.

Value—Integer in the range 1–2147483647

`<am-message-buffer-size>`—(Optional) Maximum number of messages buffered for each application manager destination.

Value—Integer in the range 1–2147483647

Required Privilege Level

No specific privilege required.

<am-interface> (configuration/slot/jps)

Usage

```

<configuration>
  <slot>
    <jps>
      <am-interface>
        <pep-id>pep-id</pep-id>
        <listening-address>listening-address</listening-address>
        <validate-pcmm-objects/>
        <message-max-length>message-max-length</message-max-length>
        <message-read-buffer-size>message-read-buffer-size</message-read-
buffer-size>
        <message-write-buffer-size>message-write-buffer-size</message-write-
buffer-size>
        <open-connection-timeout>open-connection-timeout</open-connection-
timeout>
      </am-interface>
    </jps>
  </slot>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the application manager-to-policy server interface (PKT-MM3) so that the policy server can communicate with application managers.

Contents

<pep-id>—(Optional) Network-wide unique identifier for this JPS instance. Changes apply only to COPS connections that are established after you make the change.

Value—Text

Default—SDX-JPS

<listening-address>—(Optional) Local IP address on which the JPS listens for incoming connections from application managers. If no value is specified, the JPS listens on all IP addresses. Changes take effect only after you restart the JPS.

Value—IP address

`<validate-pcmm-objects>`—(Optional) Specifies whether to validate PCMM objects received from PDPs.

Default—true

`<message-max-length>`—(Optional) Maximum length of incoming messages.

Value—Integer in the range 1–2147483647

`<message-read-buffer-size>`—(Optional) Size of message read buffer.

Value—Integer in the range 1–2147483647

`<message-write-buffer-size>`—(Optional) Size of message write buffer.

Value—Integer in the range 1–2147483647

`<open-connection-timeout>`—(Optional) Maximum time to wait for the initial PCMM messages to be exchanged after a TCP connection is established. The connection is dropped when initial PCMM messages are not exchanged within this time period.

Value— Number of seconds in the range 1–65535

Default—5

Required Privilege Level

No specific privilege required.

<cmts-interface> (configuration/slot/jps)

Usage

```

<configuration>
  <slot>
    <jps>
      <cmts-interface>
        <cmts-addresses>cmts-addresses</cmts-addresses>
        <keepalive-interval>keepalive-interval</keepalive-interval>
        <synch-despite-unreachable-pep/>
        <synch-despite-pre-i03-pep/>
        <use-ssq-ssc-with-pre-i03-pep/>
        <local-address>local-address</local-address>
        <message-max-length>message-max-length</message-max-length>
        <message-read-buffer-size>message-read-buffer-size</message-read-
buffer-size>
        <message-write-buffer-size>message-write-buffer-size</message-write-
buffer-size>
        <open-connection-timeout>open-connection-timeout</open-connection-
timeout>
        <connection-open-retry-interval>connection-open-retry-interval</
connection-open-retry-interval>
        <sent-message-timeout>sent-message-timeout</sent-message-timeout>
        <validate-pcmm-objects/>
      </cmts-interface>
    </jps>
  </slot>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the policy server-to-CMTS interface (PKT-MM2) so that the policy server can communicate with CMTS devices.

Contents

<cmts-addresses>—(Multivalue) IP addresses of all the CMTS devices to which the JPS will try to connect.

Value— List of IP addresses

`<keepalive-interval>`—(Optional) Interval between keepalive messages sent from the COPS client (CMTS device) to the COPS server (JPS). Changes apply only to COPS connections that are established after you make the change.

Value— Number of seconds in the range 0-65535. A value of 0 means that no keepalive messages will be exchanged between the CMTS device and the JPS.

Default—45

`<synch-despite-unreachable-pep>`—(Optional) Controls whether synchronization proceeds when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is not connected to a CMTS device to which it should be connected.

If a CMTS device is not connected and `synch-despite-unreachable-pep` is false, synchronization does not proceed and ends with a transport-error in a synch-complete message. If a CMTS device is not connected and `synch-despite-unreachable-pep` is true, synchronization proceeds only with the connected CMTS devices and ends with a state-data-incomplete error in a synch-complete message.

Default—true

`<synch-despite-pre-i03-pep>`—(Optional) Controls whether synchronization proceeds when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is connected to a pre-PCMM I03 CMTS device.

If any connected CMTS device is pre-PCMM I03 and `synch-despite-pre-i03-pep` is false, synchronization does not proceed and ends with a state-data-incomplete error in a synch-complete message. If any connected CMTS device is pre-PCMM I03 and `synch-despite-pre-i03-pep` is true, synchronization proceeds; whether the pre-PCMM I03 CMTS devices are included in the synchronization depends on the `use-ssq-ssc-with-pre-i03-pep` value.

Default—false

`<use-ssq-ssc-with-pre-i03-pep>`—(Optional) Controls whether synchronization includes both pre-PCMM I03 and PCMM I03 CMTS devices when the JPS receives a synchronization request from an application manager (such as the SAE) and the JPS is connected to a pre-PCMM I03 CMTS device. Relevant only when at least one pre-PCMM I03 CMTS device is connected and `synch-despite-pre-i03-pep` is specified as true.

If `use-ssq-ssc-with-pre-i03-pep` is false, synchronization proceeds only with PCMM I03 CMTS devices and ends with a state-data-incomplete error in a synch-complete message. If `use-ssq-ssc-with-pre-i03-pep` is true, synchronization proceeds with both PCMM I03 and pre-PCMM I03 CMTS devices. With the pre-PCMM I03 CMTS devices, an SSQ solicits Gate-Info-Acks which are filtered based on the original Synch-Request's application manager ID and subscriber ID (if any). The Gate-Info-Acks are transformed into Synch-Reports. Note that if two synchronization attempts must send SSQs to pre-PCMM I03 CMTS devices

concurrently, the second attempt is rejected with an insufficient-resources error in a synch-complete message.

Default—false

`<local-address>`—(Optional) Source IP address that the JPS uses to communicate with CMTS devices. If a JPS has only one IP address, this value can be left blank.

Value— IP address. If no value is specified and there is more than one local address, a random local address is used as the source address.

`<message-max-length>`—(Optional) Maximum length of incoming messages.

Value—Integer in the range 1–2147483647

`<message-read-buffer-size>`—(Optional) Size of message read buffer.

Value—Integer in the range 1–2147483647

`<message-write-buffer-size>`—(Optional) Size of message write buffer.

Value—Integer in the range 1–2147483647

`<open-connection-timeout>`—(Optional) Maximum time to wait for the initial PCMM messages to be exchanged after a TCP connection is established. The connection is dropped when initial PCMM messages are not exchanged within this time period.

Value— Number of seconds in the range 1–65535

Default—5

`<connection-open-retry-interval>`—(Optional) Time to wait before the JPS tries to reconnect to CMTS devices.

Value— Number of seconds in the range 1–2147483647

`<sent-message-timeout>`—(Optional) Maximum time to wait for the sent messages to be exchanged after a TCP connection is established. This value must be less than held-decs-max-age and pending-rks-event-max-age of the corresponding RKS interface.

Value—Integer in the range 1–2147483647 s

`<validate-pcmm-objects>`—(Optional) Specifies whether to validate PCMM objects received from PEPs.

Default—true

Required Privilege Level

No specific privilege required.

<cmts> (configuration/slot/jps)

Usage

```
<configuration>
  <slot>
    <jps>
      <cmts-registry>
        <cmts>
          <cmts-ip>cmts-ip</cmts-ip> <!-- identifier -->
        </cmts>
      </cmts-registry>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a CMTS device to which the JPS can connect and the pools of subscriber IP addresses that are managed by the CMTS device.

Contents

<cmts-ip>— IP address of the CMTS device.

Value—IP address

Required Privilege Level

No specific privilege required.

<range-pool> (configuration/slot/jps/cmts-registry/cmts)

Usage

```
<configuration>
  <slot>
    <jps>
      <cmts-registry>
        <cmts>
          <range-pool>
            <pool-index>pool-index</pool-index> <!-- identifier -->
            <low>low</low>
            <high>high</high>
          </range-pool>
        </cmts>
      </cmts-registry>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscriber IP pools in IP address ranges.

Contents

<pool-index>—Address range pool index

Value—Integer in the range -2147483648–2147483647

<low>— First IP address in the IP range for the pool of subscriber IP addresses that are managed by the CMTS device.

Value—IP address

<high>— Last IP address in the IP range for the pool of subscriber IP addresses that are managed by the CMTS device.

Value—IP address

Required Privilege Level

No specific privilege required.

<subnet-pool> (configuration/slot/jps/cmts-registry/cmts)

Usage

```
<configuration>
  <slot>
    <jps>
      <cmts-registry>
        <cmts>
          <subnet-pool>
            <subnet>subnet</subnet> <!-- identifier -->
            <exclude>exclude</exclude>
          </subnet-pool>
        </cmts>
      </cmts-registry>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscriber IP pools in IP subnets.

Contents

<subnet>— IP address and mask of the subnet for the pool of subscriber IP addresses that are managed by the CMTS device.

Value— IP address/IP mask

<exclude>—(Optional) (Multivalue) IP addresses of the subnet that are excluded from the subscriber IP pool managed by the CMTS device.

Value—IP address

Required Privilege Level

No specific privilege required.

<logger> (configuration/slot/jps)

Usage

```
<configuration>
  <slot>
    <jps>
      <logger>
        <name>name</name> <!-- identifier -->
      </logger>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination.

Contents

<name>— Name used to group parameters for the logging destination.

Value—Text

Required Privilege Level

No specific privilege required.

<file> (configuration/slot/jps/logger)

Usage

```
<configuration>
  <slot>
    <jps>
      <logger>
        <file>
          <filter>filter</filter>
          <filename>filename</filename>
          <rollover-filename>rollover-filename</rollover-filename>
          <maximum-file-size>maximum-file-size</maximum-file-size>
        </file>
      </logger>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

No specific privilege required.

<syslog> (configuration/slot/jps/logger)

Usage

```
<configuration>
  <slot>
    <jps>
      <logger>
        <syslog>
          <filter>filter</filter>
          <host>host</host>
          <facility>facility</facility>
          <format>format</format>
        </syslog>
      </logger>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

<facility>—(Optional) Type of system log in accordance with the system logging

protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Required Privilege Level

No specific privilege required.

<rks-interface> (configuration/slot/jps)

Usage

```
<configuration>
  <slot>
    <jps>
      <rks-interface>
        <element-id>element-id</element-id>
        <local-address>local-address</local-address>
        <local-port>local-port</local-port>
        <retry-interval>retry-interval</retry-interval>
        <local-timeout>local-timeout</local-timeout>
        <mso-data>mso-data</mso-data>
        <mso-domain-name>mso-domain-name</mso-domain-name>
        <default-rks-pair>default-rks-pair</default-rks-pair>
        <pending-rks-event-max-size>pending-rks-event-max-size</pending-rks-
event-max-size>
        <pending-rks-event-max-age>pending-rks-event-max-age</pending-rks-
event-max-age>
        <held-decs-max-size>held-decs-max-size</held-decs-max-size>
        <held-decs-max-age>held-decs-max-age</held-decs-max-age>
        <bcid-cache-size>bcid-cache-size</bcid-cache-size>
        <bcid-cache-age>bcid-cache-age</bcid-cache-age>
        <use-default-when-am-requests-unconfigured-rks/>
      </rks-interface>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the the policy server-to-RKS interface (PKT-MM4) so that policy events can be sent to the RKS. As part of the configuration, you can configure RKS pairs and their associated application managers.

Contents

<element-id>— Network-wide unique identifier for RKS event origin.

Value—Integer in the range 0–99999

`<local-address>`—(Optional) Source IP address used to communicate with the RKS. If no value is specified and there is more than one local address, the JPS randomly selects a local address to be used as the source address.

Value—IP address

`<local-port>`—(Optional) (Multivalue) Source UDP port or a pool of ports used to communicate with the RKS.

Value—Text

`<retry-interval>`—(Optional) Time the JPS waits for a response from an RKS before it resends the packet. The JPS keeps sending packets until either the RKS acknowledges the packet or the maximum timeout is reached.

Value—Integer in the range 0–2147483647

`<local-timeout>`—(Optional) Maximum time (ms) the JPS waits for a response from an RKS.

Value—Integer in the range 0–2147483647 ms

`<mso-data>`—(Optional) MSO-defined data in the financial entity ID (FEID) attribute, which is included in event messages.

Value— ASCII character string of 8 bytes; first eight bytes of the FEID attribute.

`<mso-domain-name>`—(Optional) MSO domain name in the financial entity ID (FEID) attribute that uniquely identifies the MSO for billing and settlement purposes.

Value— ASCII character string of up to 239 bytes; begins at the ninth byte of the FEID attribute.

`<default-rks-pair>`—(Optional) Default RKS pair that the JPS uses unless an RKS pair is configured for a given application manager.

Value—Text

`<pending-rks-event-max-size>`—(Optional) Maximum number of RKS events waiting for Gate-Set/Del-Ack/Err messages.

Value—Integer in the range 0–2147483647

`<pending-rks-event-max-age>`—(Optional) The oldest age of RKS events waiting for Gate-Set/Del-Ack/Err messages. The maximum age must be greater than sent-message-timeout of the corresponding CMTS interface.

Value— Number of seconds in the range 0–2147483647

`<held-decs-max-size>`—(Optional) Maximum number of outstanding Gate-Info requests.

Value—Integer in the range 0–2147483647

`<held-decs-max-age>`—(Optional) The oldest age of outstanding Gate-Info requests. The maximum age must be greater than sent-message-timeout of the corresponding CMTS interface.

Value— Number of seconds in the range 0–2147483647

`<bcid-cache-size>`—(Optional) Size of billing correlation ID (BCID) cache.

Value—Integer in the range 0–2147483647

`<bcid-cache-age>`—(Optional) The oldest age of billing correlation ID (BCID) in cache.

Value—Integer in the range 0–2147483647 s

`<use-default-when-am-requests-unconfigured-rks>`—(Optional) Specifies whether the default RKS pair is used when an application manager requests the use of an unconfigured RKS pair.

If true, use the default RKS pair (normally used in cases where no RKS pair specific to an application manager is configured for a given application manager). If false, only use the default RKS pair when no RKS pair specific to an application manager is found.

Default—false

Required Privilege Level

No specific privilege required.

<am> (configuration/slot/jps/rks-interface)

Usage

```
<configuration>
  <slot>
    <jps>
      <rks-interface>
        <am>
          <am-name>am-name</am-name> <!-- identifier -->
          <am-id>am-id</am-id>
          <rks-pair-name>rks-pair-name</rks-pair-name>
          <trusted/>
        </am>
      </rks-interface>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure RKS pairs for associated application managers.

Contents

<am-name>— Name used to group parameters for the associated application manager. All parameters that share the same application manager name configure the RKS pair to which events associated with a specific application manager are sent.

Value—Text

<am-id>— Identifier of the application manager. The application manager includes this identifier in all messages that it sends to the JPS. The JPS passes this ID to the CMTS device in gate control messages. The CMTS device returns the ID associated with the gate to the JPS. The JPS sends events associated with this application manager to the RKS pair specified by rks-pair-name with the same application manager name (am-name).

If no value is specified, the RKS pair configuration is not defined for this application manager. If you must set trusted to true without defining the RKS pair configuration, you must specify a value for am-id and not specify a value for rks-pair-name.

Value—Integer in the range 0–2147483647

`<rks-pair-name>`—(Optional) RKS pair that the JPS will send events to when those events are triggered by gate transitions associated with the application manager specified by `am-id` with the same application manager name (`am-name`).

If no value is specified, the RKS pair configuration is not defined for this application manager. Use when you must set `trusted` to `true` without defining the RKS pair configuration.

Value—Text

`<trusted>`—(Optional) Specifies whether this application manager is a trusted network element to the JPS.

If an application manager is trusted by the JPS and it provides a billing correlation ID (BCID) as part of a gate-set message, the JPS reuses the BCID provided by the application manager instead of generating a new one. If an application manager is trusted by the JPS and it specifies an RKS pair as part of a gate-set message, the JPS uses the RKS pair supplied by the application manager instead of using the one specified by `rks-pair-name` (which might not be defined in the JPS configuration). However, the RKS pair specified by the application manager is used only if the RKS pair exists in the JPS configuration. If the application manager specifies an RKS pair that does not exist in the JPS configuration, the default RKS pair is used.

Required Privilege Level

No specific privilege required.

<rks-pair> (configuration/slot/jps/rks-interface)

Usage

```
<configuration>
  <slot>
    <jps>
      <rks-interface>
        <rks-pair>
          <rks-pair-name>rks-pair-name</rks-pair-name> <!-- identifier -->
          <primary-address>primary-address</primary-address>
          <primary-port>primary-port</primary-port>
          <secondary-address>secondary-address</secondary-address>
          <secondary-port>secondary-port</secondary-port>
        </rks-pair>
      </rks-interface>
    </jps>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure RKS pairs. When running more than one JPS in a group to provide redundancy, all the JPSs in that group must have same RKS pair configuration (including the default RKS pair and any configured RKS pairs associated with a specific application manager).

Contents

<rks-pair-name>—RKS pair name

Value—Text

<primary-address>— IP address of the primary RKS for this RKS pair.

Value—IP address

<primary-port>—(Optional) UDP port on the primary RKS to which the JPS sends events.

Value—Integer in the range 1–65535

Default—1813

<secondary-address>—(Optional) IP address of the secondary RKS for this RKS pair.

Value—IP address

<secondary-port>—(Optional) UDP port on the secondary RKS to which the JPS sends events.

Value—Integer in the range 1–65535

Default—1813

Required Privilege Level

No specific privilege required.

Service Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for configuring services. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
services global mutex-group	<u>< mutex-group ></u>
services global schedule	<u>< schedule ></u>
services global schedule name event	<u>< event ></u>
services global schedule name event name action	<u>< action ></u>
services global schedule name event name action name attribute	<u>< attribute ></u>
services global schedule name event name except	<u>< except ></u>
services global schedule name event name except name from	<u>< from ></u>
services global schedule name event name except name to	<u>< to ></u>
services global schedule name event name from	<u>< from ></u>
services global schedule name event name to	<u>< to ></u>
services global service	<u>< service ></u>
services global service name admission-control	<u>< admission-control ></u>
services global service name admission-control congestion-point-classification	<u>< congestion-point-classification ></u>
services global service name aggregate fragment	<u>< fragment ></u>
services global service name parameter	<u>< parameter ></u>
services global service name script	<u>< script ></u>
services scope	<u>< scope ></u>
services scope name mutex-group	<u>< mutex-group ></u>
services scope name schedule	<u>< schedule ></u>
services scope name schedule name event	<u>< event ></u>

services scope name schedule name event name action	<u>< action ></u>
services scope name schedule name event name action name attribute	<u>< attribute ></u>
services scope name schedule name event name except	<u>< except ></u>
services scope name schedule name event name except name from	<u>< from ></u>
services scope name schedule name event name except name to	<u>< to ></u>
services scope name schedule name event name from	<u>< from ></u>
services scope name schedule name event name to	<u>< to ></u>
services scope name service	<u>< service ></u>
services scope name service name admission-control	<u>< admission-control ></u>
services scope service name admission-control congestion-point-classification	<u>< congestion-point-classification ></u>
services scope name service name aggregate fragment	<u>< fragment ></u>
services scope name service name parameter	<u>< parameter ></u>
services scope name service name script	<u>< script ></u>

<mutex-group> (configuration/services/global)

Usage

```
<configuration>
  <services>
    <global>
      <mutex-group>
        <name>name</name> <!-- identifier -->
        <auto-deactivate>auto-deactivate-choice</auto-deactivate>
        <description>description</description>
        <services>services</services>
      </mutex-group>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a mutex group. A mutex group is a collection of services that are mutually exclusive—services that the SAE cannot simultaneously activate for a particular subscriber.

Contents

<name>— Name of the mutex group.

Value— Text

<auto-deactivate>— Specify whether to allow activation of a service if another service is already active.

Value

- yes— For any one subscriber, the SAE deactivates a service in the group before activating another service in the group.
- no— The SAE refuses access to a requested service if the subscriber is already using another service in this group.

Default— Yes

<description>—(Optional) Description of the mutex group.

Value— Text

Default— No value

<services>—(Optional) (Multivalue) List of services in the mutex group.

Value— List of services

Default— No value

Required Privilege Level

service

<schedule> (configuration/services/global)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <name>name</name> <!-- identifier -->
        <description>description</description>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

service

<event> (configuration/services/global/schedule)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <name>name</name> <!-- identifier -->
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

service

<action> (configuration/services/global/schedule/event)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <action>
            <name>name</name> <!-- identifier -->
            <type>type-choice</type>
            <service>service</service>
            <substitution>substitution</substitution>
          </action>
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry schedule.
- deactivate— Deactivate service at the time specified in the entry schedule.
- deny— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This

value applies only to services that have an authorization plug-in configured.

- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value—Text

Default— No value

<substitution>—(Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

service

<attribute> (configuration/services/global/schedule/event/action)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <action>
            <attribute>
              <name>name-choice</name> <!-- identifier -->
              <value>value</value>
            </attribute>
          </action>
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

service

<except> (configuration/services/global/schedule/event)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <except>
            <name>name</name> <!-- identifier -->
          </except>
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

service

<from> (configuration/services/global/schedule/event/except)

Usage

```

<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <except>
            <from>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </from>
          </except>
        </event>
      </schedule>
    </global>
  </services>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<to> (configuration/services/global/schedule/event/except)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <except>
            <to>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </to>
          </except>
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<from> (configuration/services/global/schedule/event)

Usage

```

<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <from>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </from>
        </event>
      </schedule>
    </global>
  </services>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated `from` or `to` time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<to> (configuration/services/global/schedule/event)

Usage

```
<configuration>
  <services>
    <global>
      <schedule>
        <event>
          <to>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </to>
        </event>
      </schedule>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

`<hour>`—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

service

<service> (configuration/services/global)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <type>type-choice</type>
        <category>category</category>
        <url>url</url>
        <policy-group>policy-group</policy-group>
        <authentication-required/>
        <authorization-plug-in>authorization-plug-in</authorization-plug-in>
        <tracking-plug-in>tracking-plug-in</tracking-plug-in>
        <session-timeout>session-timeout</session-timeout>
        <idle-timeout>idle-timeout</idle-timeout>
        <accounting-interim-interval>accounting-interim-interval</accounting-
interim-interval>
        <radius-class>radius-class</radius-class>
        <status>status-choice</status>
        <activate-only/>
        <permanent/>
        <available/>
        <secret/>
        <shared-service-name>shared-service-name</shared-service-name>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service.

Contents

<name>— Name of the service.

Value— Text

<description>—(Optional) Description of the service.

Value— Text

Default— No value

<type>— Type of service.

Value

- **normal**— Individual service that a subscriber activates and deactivates. A normal service provisions a set of policies when activated.
- **aggregate**— Group of services that a subscriber activates and deactivates as a unit. An aggregate service contains other services (called fragments) that are managed by the aggregate service. The aggregate service is responsible for activating, deactivating, and monitoring the fragments.
- **script**— Service into which you insert or reference a script. You can use the script to manage third-party devices, provision layer 2 devices, such as DSLAMs, or set up network connections such as MPLS tunnels.
- **infrastructure**— Service that can be provisioned only once and then activated a number of times across network devices.

Default— Normal

<category>—(Optional) The service category is not used by SRC directly. You can use it, for example, to group related services in an SRC application such as a portal. For example, in the residential portal, it is the text that appears in the set of tabs that categorize services.

Value— Text

Default— No value

<url>—(Optional) The service URL is not used by SRC directly. You can use it in applications such as a portal to provide a link to a service provider or to the Web page that a subscriber sees after activating a service.

Value— URL

Default— No value

<policy-group>—(Optional) Policy group that is applied when the service is activated. The policy engine does not allow the activation of a normal service without an associated

policy group.

Value— Policy group

Default— No value

`<authentication-required>`—(Optional) Determines whether activation of the service requires authentication with a username and password that are specific to this service. The service authentication-required flag is not used by the SRC software directly. You can use it, for example, to request a name and password when the service is activated by an SRC application such as a portal.

Default— Disabled

`<authorization-plug-in>`—(Optional) (Multivalue) Name of the plug-ins that authorize this service. The authorization plug-ins are called when the service is activated.

Value— Single authorization plug-in or a list of authorization plug-ins.

Default— No value

`<tracking-plug-in>`—(Optional) (Multivalue) Name of the plug-ins that track this service. The tracking plug-ins are called when a service is activated and deactivated, as well as for interim updates.

Value— Single tracking plug-in or a list of tracking plug-ins.

Default— No value

`<session-timeout>`—(Optional) Time after which the service session is deactivated.

Changes to the session timeout take effect immediately if the new value is lower than the remaining time for a session or if you specify that no session timeout applies. Other changes apply only to services that are activated after you make the change.

The session timeout can also be controlled dynamically for each service session by a plug-in.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<idle-timeout>`—(Optional) Idle time after which the SAE deactivates service. To decide whether a service is idle, the SAE collects accounting information for the service, which means that the service activation policy must specify an accounting rule. The idle timeout is the minimum time the service must be idle before it is deactivated. A service is considered idle if the volume accounting data does not change between interim updates. The actual deactivation time depends on the length of the accounting interval.

The idle timeout can also be dynamically updated per service session by an authorization plug-in.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<accounting-interim-interval>`—(Optional) Time between interim accounting messages for this service. The accounting interim interval can also be controlled dynamically for each service session by a plug-in.

Value— Number of seconds in the range 0–2147483647. Setting the value to 0 turns off interim accounting.

Default— No value

`<radius-class>`—(Optional) Default value used in the RADIUS class attribute in RADIUS accounting messages. If RADIUS authenticates the service session, the class attribute received in the RADIUS Access-Accept response from the server overrides this value. You can use this option to set the RADIUS attribute to 25.

The RADIUS class can also be dynamically for each service session by a plug-in.

Value— Text

Default— Name of the service

`<status>`—(Optional) Status of the service.

Value

- `inactive`— Service does not accept new subscriptions.
- `active`— Service accepts new subscriptions.

Default— `active`

`<activate-only>`—(Optional) A service that is marked activate only cannot be directly deactivated. It can be deactivated indirectly through a mutex group or a session timeout.

Default— Disabled

`<permanent>`—(Optional) Specifies whether the SAE maintains permanent activation of this service for a subscriber. A service that is marked as permanent is automatically activated as soon as a subscriber subscribes to it.

Default— Disabled

`<available>`—(Optional) Specifies whether a subscriber can activate a service. To be activated, the service must be available in the currently selected scope.

Default— Enabled

`<secret>`—(Optional) Secret services are visible only to administrators who have permission to see secret information. You can use this flag to hide services from subscribers and unprivileged administrators.

`<shared-service-name>`—(Optional) For infrastructure services, the name of the service to be shared.

Value— Text

Default— No value

Required Privilege Level

service

<admission-control> (configuration/services/global/service)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <admission-control>
          <required-downstream-bandwidth>required-downstream-bandwidth</
required-downstream-bandwidth>
          <required-upstream-bandwidth>required-upstream-bandwidth</required-
upstream-bandwidth>
          <congestion-points>congestion-points</congestion-points>
        </admission-control>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure upstream and downstream bandwidths for services that ACP manages.

Contents

<required-downstream-bandwidth>—(Optional) Downstream bandwidth to the subscriber required for the service.

Value— Number of bps

Default— No value

<required-upstream-bandwidth>—(Optional) Upstream bandwidth from the subscriber required for the service.

Value— Number of bps

Default— No value

<congestion-points>—(Optional) (Multivalue) Congestion points for this service.

Value—
Default— No value

Required Privilege Level

service

<congestion-point-classification> (configuration/services/global/service/admission-control)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <admission-control>
          <congestion-point-classification>
            <script>script</script>
            <expression>expression</expression>
          </congestion-point-classification>
        </admission-control>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Congestion point classification for this service. It overrides expressions defined with congestion-point attribute.

Contents

<script>—(Optional) Congestion point classification script in python. Functions or variables defined in the script can be referred in congestion point classification expressions.

Value—Multi-line text

<expression>—(Multivalue) Congestion point classification expressions for this service.

Value—

Default— No value

Required Privilege Level

service

<fragment> (configuration/services/global/service/aggregate)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <aggregate>
          <fragment>
            <name>name</name> <!-- identifier -->
            <expression>expression</expression>
            <service>service</service>
            <mandatory/>
            <redundancy-group>redundancy-group</redundancy-group>
            <subscription-required/>
            <substitution>substitution</substitution>
          </fragment>
        </aggregate>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure service fragments for an aggregate service.

Contents

<name>— Name for service fragment. The fragment name is not stored and is re-created every time the object is read.

Value— Text

<expression>— Subscriber reference expression that identifies the remote subscriber session that will host the fragment. The remote subscriber session is an assigned IP subscriber. If the remote SAE manages the specified interface, the SAE creates an assigned IP subscriber session if necessary.

Value— Valid expressions are:

- current
- address = "A.B.C.D"
- vr = "vrName", interfaceName = "ifName"
- vr = "vrName", interfaceName = "ifName", address = "A.B.C.D"
- vr = "vrName", ifIndex = "1234"
- vr = "vrName", login_name = "user@domain"
- vr = "vrName", primary_user_name = "user@domain"
- dn = "uniqueId = ..."
- login_name = "user@domain"
- primary_user_name = "user@domain"
- ref = "rdn/rdn"

The rdn/rdn identifies the hierarchy of directory objects below the LDAP object *o= aggregateService*. The final object contains the attribute *subscriberRefExpr* to identify the subscriber session. A forward slash (/) separates the objects in the path.

You can also use a substitution or a Python expression that represents any of the literal values listed above. For a substitution or Python expression, type `< -` before the expression and type `- >` after it; for example, `< -ifAlias- >`. For a list and description of the fields that you can use to compose Python expressions, see *Managing Services for the SRC CLI* in the *SRC-PE Services and Policies Guide*.

Examples of valid expressions are:

- current
- address = "10.10.10.1"
- vr = "`< -substitution.serviceVr- >`", interfaceName = "`< -substitution.serviceInterface- >`"
- dn = "uniqueId = `< -ifAlias- >`, `< -userDn- >`"
- vr = "`< -[\"vr1\", \"vr2\"]- >`", loginName = "`< -[\"joe@abc\", \"jane@abc\"]- >`".

When you include lists, fragment services are created for all combinations of values in the list. For example, `vr = < -[\"vr1\", \"vr2\"]- >`, `loginName = < -[\"joe@abc\", \"jane@abc\"]- >` would cause four fragments to be created with the following expressions:

- vr = "vr1", loginName = "joe@abc"
- vr = "vr1", loginName = "jane@abc"
- vr = "vr2", loginName = "joe@abc"
- vr = "vr2", loginName = "jane@abc"

Default— No value

`<service>`— Name of the service to be included in the aggregate service as a fragment service.

Value— Name of a service

Default— No value

`<mandatory>`—(Optional) Specifies whether the fragment service must be active for the aggregate service to become active.

Default— Mandatory

`<redundancy-group>`—(Optional) Group name to be applied to each fragment service that is to be part of a redundancy group. The fragment services that have the same group name provide redundancy for each other.

Value— Text

Default— No value

`<subscription-required>`—(Optional) Specifies whether a remote subscriber session must be subscribed to the fragment service for it to become active.

Enabling subscription-required can be used to limit the services that can be activated as fragments. Enabling this option lets you control which services can be used as fragments. For example, for an aggregate service that supports VoIP to push a policy to the caller and the callee, you can require that both subscribers sign up for VoIP services. If you disable the option, only one party needs to subscribe to the aggregate service; the policy service sessions are created automatically.

Default— Disabled

`<substitution>`—(Optional) (Multivalue) List of substitutions that are used as arguments for the fragment to become active. If a parameter does not acquire a value, the associated fragment service does not become active.

Value— One or more of the following:

- `< parameter-name >` —The parameter name is defined to have the same value in the fragment service session as in the aggregate service session.
- `< parameter-name > = < substitution-expression >` —The parameter name on the left side of the equals sign is defined for the fragment service session. This parameter name is the result of the evaluation of the expression (in the aggregate service session) on the right side of the equals sign.

Default— No value

Required Privilege Level

service

<parameter> (configuration/services/global/service)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <parameter>
          <gateway-ip-address>gateway-ip-address</gateway-ip-address>
          <service-ip-address>service-ip-address</service-ip-address>
          <service-ip-mask>service-ip-mask</service-ip-mask>
          <service-port>service-port</service-port>
          <substitution>substitution</substitution>
          <session-volume-quota>session-volume-quota</session-volume-quota>
        </parameter>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure parameter values for services. The policy engine substitutes parameters in policies associated with this service with the values that you specify in this parameter configuration.

Contents

<gateway-ip-address>—(Optional) Actual IP address of the gateway router. This value is substituted for the policy global parameter called gateway_ipAddress.

Value— IP address

Default— No value

<service-ip-address>—(Optional) Actual IP address of the host(s) that provides the service. This value is substituted for the policy global parameter called service_ipAddress.

Value— IP address

Default— No value

`<service-ip-mask>`—(Optional) Actual IP mask for the service. This value is substituted for the policy global parameter called `service_ipMask`.

Value— IP address

Default— No value

`<service-port>`—(Optional) Actual port for the service. This value is substituted for the policy global parameter called `service_port`.

Value— TCP or UDP port number in the range 0–65535

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for other parameters. These values are substituted for the parameters that you specify.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

`<session-volume-quota>`—(Optional) Upstream and downstream volume quota for the service session.

The SAE does not directly use this value. It is used by applications that implement tracking plug-ins. The value of a service session can be defined at runtime either through an authorization plug-in or a call to the SAE API. If the Session Volume Quota attribute is defined in more than one place, which value is used depends on where the value is defined. The SRC software searches for the value in the following order:

1. Value set in a call to the SAE
2. Value set in an authorization plug-in
3. Value set in a service definition

Value— Volume quota in the format "downstream-quota:upstream-quota"

where

- Downstream quota is the number of bytes available for transmitting data from the network to the subscriber.
- Upstream quota is the number of bytes available for transmitting data from the subscriber to the network.

Default— No value

Required Privilege Level

service

<script> (configuration/services/global/service)

Usage

```
<configuration>
  <services>
    <global>
      <service>
        <script>
          <script-type>script-type-choice</script-type>
          <class-name>class-name</class-name>
          <file>file</file>
          <filename>filename</filename>
        </script>
      </service>
    </global>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the script service.

Contents

<script-type>— Type of script service. Determines how the contents of the "file" attribute will be interpreted.

Value

- `url`— The value of attribute "file" is a URL that specifies where to find a Java archive (.jar file) containing the script service implementation.
- `python`— The value of attribute "file" is Python code.
- `java-class`— The value of attribute "file" is the binary contents of a compiled Java class file (.class file).
- `java-archive`— The value of attribute "file" is the binary contents of a Java archive file (.jar file).

Default— No value

<class-name>— Name of the Java or Python class that implements the script service.
The SAE instantiates the named class when it starts the script service.

Value— Name of the class

Default— No value

<file>— If the script type is "URL", this attribute contains the URL of a Java archive (.jar) file containing the script service implementation. Otherwise, this attribute contains the script service implementation itself (i.e. python code, the binary contents of a compiled .class file, or the binary contents of a .jar file).

Value— The script itself, or a URL pointing to a .jar file containing the script

Default— No value

<filename>—(Optional) The file needs to exist locally. Its content will be read and loaded into the "file" attribute.

Value—Text

Required Privilege Level

service

<scope> (configuration/services)

Usage

```
<configuration>
  <services>
    <scope>
      <name>name</name> <!-- identifier -->
      <precedence>precedence</precedence>
      <substitution>substitution</substitution>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service scope. Service scopes let you customize which services are delivered to specific organizations or locales.

Contents

<name>— Name of a service scope.

Value— Text

<precedence>—(Optional) If multiple scopes are selected for the same subscriber session, they are sorted by their precedence level.

Value— Positive integer; the lower the precedence value, the higher the ranking of the service scope.

Default— No value

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

Required Privilege Level

service

<mutex-group> (configuration/services/scope)

Usage

```
<configuration>
  <services>
    <scope>
      <mutex-group>
        <name>name</name> <!-- identifier -->
        <auto-deactivate>auto-deactivate-choice</auto-deactivate>
        <description>description</description>
        <services>services</services>
      </mutex-group>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a mutex group. A mutex group is a collection of services that are mutually exclusive—services that the SAE cannot simultaneously activate for a particular subscriber.

Contents

<name>— Name of the mutex group.

Value— Text

<auto-deactivate>— Specify whether to allow activation of a service if another service is already active.

Value

- yes— For any one subscriber, the SAE deactivates a service in the group before activating another service in the group.
- no— The SAE refuses access to a requested service if the subscriber is already using another service in this group.

Default— Yes

<description>—(Optional) Description of the mutex group.

Value— Text

Default— No value

<services>—(Optional) (Multivalue) List of services in the mutex group.

Value— List of services

Default— No value

Required Privilege Level

service

<schedule> (configuration/services/scope)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <name>name</name> <!-- identifier -->
        <description>description</description>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

service

<event> (configuration/services/scope/schedule)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <name>name</name> <!-- identifier -->
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

service

<action> (configuration/services/scope/schedule/event)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <action>
            <name>name</name> <!-- identifier -->
            <type>type-choice</type>
            <service>service</service>
            <substitution>substitution</substitution>
          </action>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry schedule.
- deactivate— Deactivate service at the time specified in the entry schedule.
- deny— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This

value applies only to services that have an authorization plug-in configured.

- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value—Text

Default— No value

<substitution>—(Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

service

<attribute> (configuration/services/scope/schedule/event/action)

Usage

```

<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <action>
            <attribute>
              <name>name-choice</name> <!-- identifier -->
              <value>value</value>
            </attribute>
          </action>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

service

<except> (configuration/services/scope/schedule/event)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <except>
            <name>name</name> <!-- identifier -->
          </except>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

service

<from> (configuration/services/scope/schedule/event/except)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <except>
            <from>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </from>
          </except>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31**Default**— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<to> (configuration/services/scope/schedule/event/except)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <except>
            <to>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </to>
          </except>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<from> (configuration/services/scope/schedule/event)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <from>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </from>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated `from` or `to` time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

service

<to> (configuration/services/scope/schedule/event)

Usage

```
<configuration>
  <services>
    <scope>
      <schedule>
        <event>
          <to>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </to>
        </event>
      </schedule>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

service

<service> (configuration/services/scope)

Usage

```

<configuration>
  <services>
    <scope>
      <service>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <type>type-choice</type>
        <category>category</category>
        <url>url</url>
        <policy-group>policy-group</policy-group>
        <authentication-required/>
        <authorization-plug-in>authorization-plug-in</authorization-plug-in>
        <tracking-plug-in>tracking-plug-in</tracking-plug-in>
        <session-timeout>session-timeout</session-timeout>
        <idle-timeout>idle-timeout</idle-timeout>
        <accounting-interim-interval>accounting-interim-interval</accounting-
interim-interval>
        <radius-class>radius-class</radius-class>
        <status>status-choice</status>
        <activate-only/>
        <permanent/>
        <available/>
        <secret/>
        <shared-service-name>shared-service-name</shared-service-name>
      </service>
    </scope>
  </services>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service.

Contents

<name>— Name of the service.

Value— Text

`<description>`—(Optional) Description of the service.

Value— Text

Default— No value

`<type>`— Type of service.

Value

- **normal**— Individual service that a subscriber activates and deactivates. A normal service provisions a set of policies when activated.
- **aggregate**— Group of services that a subscriber activates and deactivates as a unit. An aggregate service contains other services (called fragments) that are managed by the aggregate service. The aggregate service is responsible for activating, deactivating, and monitoring the fragments.
- **script**— Service into which you insert or reference a script. You can use the script to manage third-party devices, provision layer 2 devices, such as DSLAMs, or set up network connections such as MPLS tunnels.
- **infrastructure**— Service that can be provisioned only once and then activated a number of times across network devices.

Default— Normal

`<category>`—(Optional) The service category is not used by SRC directly. You can use it, for example, to group related services in an SRC application such as a portal. For example, in the residential portal, it is the text that appears in the set of tabs that categorize services.

Value— Text

Default— No value

`<url>`—(Optional) The service URL is not used by SRC directly. You can use it in applications such as a portal to provide a link to a service provider or to the Web page that a subscriber sees after activating a service.

Value— URL

Default— No value

`<policy-group>`—(Optional) Policy group that is applied when the service is activated. The policy engine does not allow the activation of a normal service without an associated

policy group.

Value— Policy group

Default— No value

`<authentication-required>`—(Optional) Determines whether activation of the service requires authentication with a username and password that are specific to this service. The service authentication-required flag is not used by the SRC software directly. You can use it, for example, to request a name and password when the service is activated by an SRC application such as a portal.

Default— Disabled

`<authorization-plug-in>`—(Optional) (Multivalue) Name of the plug-ins that authorize this service. The authorization plug-ins are called when the service is activated.

Value— Single authorization plug-in or a list of authorization plug-ins.

Default— No value

`<tracking-plug-in>`—(Optional) (Multivalue) Name of the plug-ins that track this service. The tracking plug-ins are called when a service is activated and deactivated, as well as for interim updates.

Value— Single tracking plug-in or a list of tracking plug-ins.

Default— No value

`<session-timeout>`—(Optional) Time after which the service session is deactivated.

Changes to the session timeout take effect immediately if the new value is lower than the remaining time for a session or if you specify that no session timeout applies. Other changes apply only to services that are activated after you make the change.

The session timeout can also be controlled dynamically for each service session by a plug-in.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<idle-timeout>`—(Optional) Idle time after which the SAE deactivates service. To decide whether a service is idle, the SAE collects accounting information for the service, which means that the service activation policy must specify an accounting rule. The idle timeout is the minimum time the service must be idle before it is deactivated. A service is considered idle if the volume accounting data does not change between interim updates. The actual deactivation time depends on the length of the accounting interval.

The idle timeout can also be dynamically updated per service session by an authorization plug-in.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<accounting-interim-interval>`—(Optional) Time between interim accounting messages for this service. The accounting interim interval can also be controlled dynamically for each service session by a plug-in.

Value— Number of seconds in the range 0–2147483647. Setting the value to 0 turns off interim accounting.

Default— No value

`<radius-class>`—(Optional) Default value used in the RADIUS class attribute in RADIUS accounting messages. If RADIUS authenticates the service session, the class attribute received in the RADIUS Access-Accept response from the server overrides this value. You can use this option to set the RADIUS attribute to 25.

The RADIUS class can also be dynamically for each service session by a plug-in.

Value— Text

Default— Name of the service

`<status>`—(Optional) Status of the service.

Value

- `inactive`— Service does not accept new subscriptions.
- `active`— Service accepts new subscriptions.

Default— `active`

`<activate-only>`—(Optional) A service that is marked activate only cannot be directly deactivated. It can be deactivated indirectly through a mutex group or a session timeout.

Default— Disabled

`<permanent>`—(Optional) Specifies whether the SAE maintains permanent activation of this service for a subscriber. A service that is marked as permanent is automatically activated as soon as a subscriber subscribes to it.

Default— Disabled

`<available>`—(Optional) Specifies whether a subscriber can activate a service. To be activated, the service must be available in the currently selected scope.

Default— Enabled

`<secret>`—(Optional) Secret services are visible only to administrators who have permission to see secret information. You can use this flag to hide services from subscribers and unprivileged administrators.

`<shared-service-name>`—(Optional) For infrastructure services, the name of the service to be shared.

Value— Text

Default— No value

Required Privilege Level

service

<admission-control> (configuration/services/scope/service)

Usage

```

<configuration>
  <services>
    <scope>
      <service>
        <admission-control>
          <required-downstream-bandwidth>required-downstream-bandwidth</
required-downstream-bandwidth>
          <required-upstream-bandwidth>required-upstream-bandwidth</required-
upstream-bandwidth>
          <congestion-points>congestion-points</congestion-points>
        </admission-control>
      </service>
    </scope>
  </services>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure upstream and downstream bandwidths for services that ACP manages.

Contents

<required-downstream-bandwidth>—(Optional) Downstream bandwidth to the subscriber required for the service.

Value— Number of bps

Default— No value

<required-upstream-bandwidth>—(Optional) Upstream bandwidth from the subscriber required for the service.

Value— Number of bps

Default— No value

<congestion-points>—(Optional) (Multivalue) Congestion points for this service.

Value—
Default— No value

Required Privilege Level

service

<congestion-point-classification> (configuration/services/scope/service/admission-control)

Usage

```
<configuration>
  <services>
    <scope>
      <service>
        <admission-control>
          <congestion-point-classification>
            <script>script</script>
            <expression>expression</expression>
          </congestion-point-classification>
        </admission-control>
      </service>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Congestion point classification for this service. It overrides expressions defined with congestion-point attribute.

Contents

<script>—(Optional) Congestion point classification script in python. Functions or variables defined in the script can be referred in congestion point classification expressions.

Value—Multi-line text

<expression>—(Multivalue) Congestion point classification expressions for this service.

Value—

Default— No value

Required Privilege Level

service

<fragment> (configuration/services/scope/service/aggregate)

Usage

```
<configuration>
  <services>
    <scope>
      <service>
        <aggregate>
          <fragment>
            <name>name</name> <!-- identifier -->
            <expression>expression</expression>
            <service>service</service>
            <mandatory/>
            <redundancy-group>redundancy-group</redundancy-group>
            <subscription-required/>
            <substitution>substitution</substitution>
          </fragment>
        </aggregate>
      </service>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure service fragments for an aggregate service.

Contents

<name>— Name for service fragment. The fragment name is not stored and is re-created every time the object is read.

Value— Text

<expression>— Subscriber reference expression that identifies the remote subscriber session that will host the fragment. The remote subscriber session is an assigned IP subscriber. If the remote SAE manages the specified interface, the SAE creates an assigned IP subscriber session if necessary.

Value— Valid expressions are:

- current
- address = "A.B.C.D"
- vr = "vrName", interfaceName = "ifName"
- vr = "vrName", interfaceName = "ifName", address = "A.B.C.D"
- vr = "vrName", ifIndex = "1234"
- vr = "vrName", login_name = "user@domain"
- vr = "vrName", primary_user_name = "user@domain"
- dn = "uniqueId = ..."
- login_name = "user@domain"
- primary_user_name = "user@domain"
- ref = "rdn/rdn"

The rdn/rdn identifies the hierarchy of directory objects below the LDAP object *o= aggregateService*. The final object contains the attribute *subscriberRefExpr* to identify the subscriber session. A forward slash (/) separates the objects in the path.

You can also use a substitution or a Python expression that represents any of the literal values listed above. For a substitution or Python expression, type `< -` before the expression and type `- >` after it; for example, `< -ifAlias- >`. For a list and description of the fields that you can use to compose Python expressions, see *Managing Services for the SRC CLI* in the *SRC-PE Services and Policies Guide*.

Examples of valid expressions are:

- current
- address = "10.10.10.1"
- vr = "`< -substitution.serviceVr- >`", interfaceName = "`< -substitution.serviceInterface- >`"
- dn = "uniqueId = `< -ifAlias- >`, `< -userDn- >`"
- vr = "`< -[\"vr1\", \"vr2\"]- >`", loginName = "`< -[\"joe@abc\", \"jane@abc\"]- >`".

When you include lists, fragment services are created for all combinations of values in the list. For example, `vr = < -[\"vr1\", \"vr2\"]- >`, `loginName = < -[\"joe@abc\", \"jane@abc\"]- >` would cause four fragments to be created with the following expressions:

- vr = "vr1", loginName = "joe@abc"
- vr = "vr1", loginName = "jane@abc"
- vr = "vr2", loginName = "joe@abc"
- vr = "vr2", loginName = "jane@abc"

Default— No value

`<service>`— Name of the service to be included in the aggregate service as a fragment service.

Value— Name of a service

Default— No value

`<mandatory>`—(Optional) Specifies whether the fragment service must be active for the aggregate service to become active.

Default— Mandatory

`<redundancy-group>`—(Optional) Group name to be applied to each fragment service that is to be part of a redundancy group. The fragment services that have the same group name provide redundancy for each other.

Value— Text

Default— No value

`<subscription-required>`—(Optional) Specifies whether a remote subscriber session must be subscribed to the fragment service for it to become active.

Enabling subscription-required can be used to limit the services that can be activated as fragments. Enabling this option lets you control which services can be used as fragments. For example, for an aggregate service that supports VoIP to push a policy to the caller and the callee, you can require that both subscribers sign up for VoIP services. If you disable the option, only one party needs to subscribe to the aggregate service; the policy service sessions are created automatically.

Default— Disabled

`<substitution>`—(Optional) (Multivalue) List of substitutions that are used as arguments for the fragment to become active. If a parameter does not acquire a value, the associated fragment service does not become active.

Value— One or more of the following:

- `< parameter-name >` —The parameter name is defined to have the same value in the fragment service session as in the aggregate service session.
- `< parameter-name > = < substitution-expression >` —The parameter name on the left side of the equals sign is defined for the fragment service session. This parameter name is the result of the evaluation of the expression (in the aggregate service session) on the right side of the equals sign.

Default— No value

Required Privilege Level

service

<parameter> (configuration/services/scope/service)

Usage

```
<configuration>
  <services>
    <scope>
      <service>
        <parameter>
          <gateway-ip-address>gateway-ip-address</gateway-ip-address>
          <service-ip-address>service-ip-address</service-ip-address>
          <service-ip-mask>service-ip-mask</service-ip-mask>
          <service-port>service-port</service-port>
          <substitution>substitution</substitution>
          <session-volume-quota>session-volume-quota</session-volume-quota>
        </parameter>
      </service>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure parameter values for services. The policy engine substitutes parameters in policies associated with this service with the values that you specify in this parameter configuration.

Contents

<gateway-ip-address>—(Optional) Actual IP address of the gateway router. This value is substituted for the policy global parameter called gateway_ipAddress.

Value— IP address

Default— No value

<service-ip-address>—(Optional) Actual IP address of the host(s) that provides the service. This value is substituted for the policy global parameter called service_ipAddress.

Value— IP address

Default— No value

<service-ip-mask>—(Optional) Actual IP mask for the service. This value is substituted for the policy global parameter called service_ipMask.

Value— IP address

Default— No value

<service-port>—(Optional) Actual port for the service. This value is substituted for the policy global parameter called service_port.

Value— TCP or UDP port number in the range 0–65535

Default— No value

<substitution>—(Optional) (Multivalue) Actual values for other parameters. These values are substituted for the parameters that you specify.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

<session-volume-quota>—(Optional) Upstream and downstream volume quota for the service session.

The SAE does not directly use this value. It is used by applications that implement tracking plug-ins. The value of a service session can be defined at runtime either through an authorization plug-in or a call to the SAE API. If the Session Volume Quota attribute is defined in more than one place, which value is used depends on where the value is defined. The SRC software searches for the value in the following order:

1. Value set in a call to the SAE
2. Value set in an authorization plug-in
3. Value set in a service definition

Value— Volume quota in the format "downstream-quota:upstream-quota"

where

- Downstream quota is the number of bytes available for transmitting data from the network to the subscriber.
- Upstream quota is the number of bytes available for transmitting data from the subscriber to the network.

Default— No value

Required Privilege Level

service

<script> (configuration/services/scope/service)

Usage

```
<configuration>
  <services>
    <scope>
      <service>
        <script>
          <script-type>script-type-choice</script-type>
          <class-name>class-name</class-name>
          <file>file</file>
          <filename>filename</filename>
        </script>
      </service>
    </scope>
  </services>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the script service.

Contents

<script-type>— Type of script service. Determines how the contents of the "file" attribute will be interpreted.

Value

- `url`— The value of attribute "file" is a URL that specifies where to find a Java archive (.jar file) containing the script service implementation.
- `python`— The value of attribute "file" is Python code.
- `java-class`— The value of attribute "file" is the binary contents of a compiled Java class file (.class file).
- `java-archive`— The value of attribute "file" is the binary contents of a Java archive file (.jar file).

Default— No value

`<class-name>`— Name of the Java or Python class that implements the script service. The SAE instantiates the named class when it starts the script service.

Value— Name of the class

Default— No value

`<file>`— If the script type is "URL", this attribute contains the URL of a Java archive (.jar) file containing the script service implementation. Otherwise, this attribute contains the script service implementation itself (i.e. python code, the binary contents of a compiled .class file, or the binary contents of a .jar file).

Value— The script itself, or a URL pointing to a .jar file containing the script

Default— No value

`<filename>`—(Optional) The file needs to exist locally. Its content will be read and loaded into the "file" attribute.

Value—Text

Required Privilege Level

service

Policy Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for configuring policies. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
policies folder	<u>< folder ></u>
policies global-parameters	<u>< parameter ></u>
policies group	<u>< group ></u>
policies group name list	<u>< list ></u>
policies group name list name rule	<u>< rule ></u>
policies group name list name rule name color	<u>< color ></u>
policies group name list name rule name docsis-best-effort	<u>< docsis-best-effort ></u>
policies group name list name rule name docsis-down-stream	<u>< docsis-down-stream ></u>
policies group name list name rule name docsis-non-real-time	<u>< docsis-non-real-time ></u>
policies group name list name rule name docsis-parameter	<u>< docsis-parameter ></u>
policies group name list name rule name docsis-real-time	<u>< docsis-real-time ></u>
policies group name list name rule name docsis-unsolicited-grant	<u>< docsis-unsolicited-grant ></u>
policies group name list name rule name docsis-unsolicited-grant-ad	<u>< docsis-unsolicited-grant-ad ></u>
policies group name list name rule name exception-application	<u>< exception-application ></u>
policies group name list name rule name filter	<u>< filter ></u>
policies group name list name rule name flow-spec	<u>< flow-spec ></u>
policies group name list name rule name forward	<u>< forward ></u>
policies group name list name rule name forwarding-class	<u>< forwarding-class ></u>
policies group name list name rule name gate-spec	<u>< gate-spec ></u>
policies group name list name rule name http-redirect	<u>< http-redirect ></u>

policies group name list name rule name loss-priority	<u>< loss-priority ></u>
policies group name list name rule name mark	<u>< mark ></u>
policies group name list name rule name mark name info	<u>< info ></u>
policies group name list name rule name nat	<u>< nat ></u>
policies group name list name rule name nat name ip-network group-network	<u>< group-network ></u>
policies group name list name rule name nat name port	<u>< port ></u>
policies group name list name rule name next-hop	<u>< next-hop ></u>
policies group name list name rule name next-interface	<u>< next-interface ></u>
policies group name list name rule name next-rule	<u>< next-rule ></u>
policies group name list name rule name policer	<u>< policer ></u>
policies group name list name rule name policer name packet- action	<u>< packet-action ></u>
policies group name list name rule name policer name packet- action name filter	<u>< filter ></u>
policies group name list name rule name policer name packet- action name forwarding-class	<u>< forwarding-class ></u>
policies group name list name rule name policer name packet- action name loss-priority	<u>< loss-priority ></u>
policies group name list name rule name policer name packet- action name parameter	<u>< parameter ></u>
policies group name list name rule name qos-attach	<u>< qos-attach ></u>
policies group name list name rule name qos-condition	<u>< qos-condition ></u>
policies group name list name rule name rate-limit	<u>< rate-limit ></u>
policies group name list name rule name rate-limit name committed-action filter	<u>< filter ></u>
policies group name list name rule name rate-limit name committed-action forward	<u>< forward ></u>
policies group name list name rule name rate-limit name committed-action mark mark-info	<u>< mark-info ></u>
policies group name list name rule name rate-limit name committed-action parameter	<u>< parameter ></u>

policies group name list name rule name rate-limit name conformed-action filter	<u>< filter ></u>
policies group name list name rule name rate-limit name conformed-action forward	<u>< forward ></u>
policies group name list name rule name rate-limit name conformed-action mark mark-info	<u>< mark-info ></u>
policies group name list name rule name rate-limit name conformed-action parameter	<u>< parameter ></u>
policies group name list name rule name rate-limit name exceed- action filter	<u>< filter ></u>
policies group name list name rule name rate-limit name exceed- action forward	<u>< forward ></u>
policies group name list name rule name rate-limit name exceed- action mark mark-info	<u>< mark-info ></u>
policies group name list name rule name rate-limit name exceed- action parameter	<u>< parameter ></u>
policies group name list name rule name reject	<u>< reject ></u>
policies group name list name rule name routing-instance	<u>< routing-instance ></u>
policies group name list name rule name scheduler-action	<u>< scheduler-action ></u>
policies group name list name rule name scheduler-action name drop-profile	<u>< drop-profile ></u>
policies group name list name rule name service-class-name	<u>< service-class-name ></u>
policies group name list name rule name stateful-firewall	<u>< stateful-firewall ></u>
policies group name list name rule name stateful-firewall name packet-action filter	<u>< filter ></u>
policies group name list name rule name stateful-firewall name packet-action forward	<u>< forward ></u>
policies group name list name rule name stateful-firewall name packet-action parameter	<u>< parameter ></u>
policies group name list name rule name stateful-firewall name packet-action reject	<u>< reject ></u>
policies group name list name rule name template-activation	<u>< template-activation ></u>
policies group name list name rule name template-activation name variables	<u>< variables ></u>

policies group name list name rule name traffic-class	<u>< traffic-class ></u>
policies group name list name rule name traffic-condition	<u>< traffic-condition ></u>
policies group name list name rule name traffic-condition name application-protocol-condition	<u>< application-protocol-condition ></u>
policies group name list name rule name traffic-condition name application-protocol-condition name proto-attr	<u>< proto-attr ></u>
policies group name list name rule name traffic-condition name application-protocol-condition name proto-attr destination-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name application-protocol-condition name proto-attr source-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name destination-network group-network	<u>< group-network ></u>
policies group name list name rule name traffic-condition name destination-network network	<u>< network ></u>
policies group name list name rule name traffic-condition name icmp-condition	<u>< icmp-condition ></u>
policies group name list name rule name traffic-condition name igmp-condition	<u>< igmp-condition ></u>
policies group name list name rule name traffic-condition name ipsec-condition	<u>< ipsec-condition ></u>
policies group name list name rule name traffic-condition name parameter-protocol-condition	<u>< parameter-protocol-condition ></u>
policies group name list name rule name traffic-condition name parameter-protocol-condition proto-attr	<u>< proto-attr ></u>
policies group name list name rule name traffic-condition name parameter-protocol-condition proto-attr destination-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name parameter-protocol-condition proto-attr source-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name protocol-condition	<u>< protocol-condition ></u>
policies group name list name rule name traffic-condition name protocol-port-condition	<u>< protocol-port-condition ></u>
policies group name list name rule name traffic-condition name protocol-port-condition destination-port port	<u>< port ></u>

policies group name list name rule name traffic-condition name protocol-port-condition source-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name source-network group-network	<u>< group-network ></u>
policies group name list name rule name traffic-condition name source-network network	<u>< network ></u>
policies group name list name rule name traffic-condition name tcp-condition	<u>< tcp-condition ></u>
policies group name list name rule name traffic-condition name tcp-condition destination-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name tcp-condition source-port port	<u>< port ></u>
policies group name list name rule name traffic-condition name tos	<u>< tos ></u>
policies group name list name rule name traffic-condition name traffic-match-condition	<u>< traffic-match-condition ></u>
policies group name list name rule name traffic-mirror	<u>< traffic-mirror ></u>
policies group name list name rule name traffic-shape	<u>< traffic-shape ></u>
policies group name list name rule name user-packet-class	<u>< user-packet-class ></u>
policies group name local-parameters	<u>< parameter ></u>

<folder> (configuration/policies)

Usage

```
<configuration>
  <policies>
    <folder>
      <name>name</name> <!-- identifier -->
      <description>description</description>
    </folder>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a policy folder, which is a collection of policies.

Contents

<name>— Name for a policy folder, which is a collection of policy folders or groups.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

service

<parameter> (configuration/policies/global-parameters)

Usage

```
<configuration>
  <policies>
    <global-parameters>
      <parameter>
        <name>name</name> <!-- identifier -->
        <description>description</description>
        <default-value>default-value</default-value>
        <type>type</type>
      </parameter>
    </global-parameters>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Defines a global parameter. A global parameter is available for use in any policy. With global parameters, you can define parameters once and then reuse them in many policies. Typically, you would use global parameters if the parameter does not need to change often. If parameters require changes, use local parameters.

Contents

<name>— Name of the parameter

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

<default-value>—(Optional) Value that the policy engine uses if no other values are provided during the parameter value acquisition process. If other values are provided to the policy engine but problems are encountered, the default value for the parameter is not used. The policy engine generates an error message.

Value— Valid value for the parameter type. See the policy documentation in the *SRC-PE Services and Policies Guide* for valid values for each parameter type.

Default— No value

`<type>`—(Optional) Type of attribute for which you can use the parameter. The parameter type determines where you can use the parameter.

Value— See the policy documentation in the *SRC-PE Services and Policies Guide* for a list of parameter types, where each type of parameter is used, and what each parameter is used to specify.

Default— No value

Required Privilege Level

service

<group> (configuration/policies)

Usage

```
<configuration>
  <policies>
    <group>
      <name>name</name> <!-- identifier -->
      <description>description</description>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a policy group, which is a collection of policy lists.

Contents

<name>— Name for a collection of policy lists.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

service

<list> (configuration/policies/group)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <name>name</name> <!-- identifier -->
        <role>role-choice</role>
        <applicability>applicability-choice</applicability>
        <description>description</description>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a policy list that holds a collection of policy rules.

Contents

<name>— Name for a collection of policy rules.

Value— Text

<role>— Platform for which the policy list is created. The selection that you make controls the type of policy rules that you can add to the policy list. You must configure the role before you can configure the policy rule.

Value

- junos— JUNOS routing platform
- junose-ipv4— JUNOSe router that is running IPv4
- junose-ipv6— JUNOSe router that is running IPv6
- pcmm— PCMM platform
- aaa— AAA supporting platforms

Default— No value

`<applicability>`— Indicates where the policy is applied on the router or, for PCMM policies, indicates whether the policy applies to the upstream or downstream channel.

For JUNOS routing platforms, applicability determines the types of policy rules that you can create:

- JUNOS ASP—Applicability must be both.
- JUNOS FILTER—Applicability must be input or output.
- JUNOS POLICER—Applicability must be input or output.
- JUNOS SCHEDULER—Applicability must be both.
- JUNOS SHAPING—Applicability must be both.

Value

- `input`— Policy is applied to the input (ingress) side of the router interface. For PCMM policies, the policy is provisioned on upstream service flows (from the cable modem to the CMTS device).
- `output`— Policy is applied to the output (egress) side of the router interface. For PCMM policies, the policy is provisioned on the downstream channel (from the CMTS device to the cable modem).
- `both`— Policy is applied to both the input (ingress) and output (egress) side of the interface, or it is attached implicitly to the interface without indicating direction. The both value is not valid for PCMM or JUNOSe policies.

In the case of JUNOS ASP policy rules, the policy is attached to both sides of the interface; for JUNOS scheduler policy rules, the policy is attached implicitly to the interface without indicating direction.

- `secondary-input`— Policy is applied to the secondary input attachment point of the router interface. Valid for JUNOSe devices.

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

service

<rule> (configuration/policies/group/list)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <name>name</name> <!-- identifier -->
          <type>type</type>
          <precedence>precedence</precedence>
          <accounting/>
          <description>description</description>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a policy rule, which is a collection of conditions and actions.

Contents

<name>— Name for a policy rule, which is a collection of conditions and actions.

Value— Text

<type>— Policy rule type, which is based on the applicability and the role of the policy.

Value— The type of policy rule that you can create depends on the role and applicability of the policy list in which you create the policy rule.

- For JUNOS policy lists, there is only one type—junose.
- For PCMM policy lists, there is only one type—pcmm.
- For AAA policy lists, there is only one type—aaa
- For JUNOS policy lists, you can create the following policy rule types:
 - JUNOS ASP—Applicability of policy list must be both

- input and output.
- JUNOS FILTER—Applicability of policy list must be input or output.
- JUNOS POLICER—Applicability of policy list must be input or output.
- JUNOS SCHEDULER—Applicability of policy list must be both.
- JUNOS SHAPING—Applicability of policy list must be both.

Default— No value

<precedence>—(Optional) Order in which the policy manager applies policy rules. Rules are evaluated from lowest to highest precedence value. Precedence has meaning only if two rules have different classifiers and if those classifiers overlap. If this is the case and a packet is received that satisfies both classifiers, then only the action of the rule with the lower precedence value is performed.

- For JUNOSe policies, rules with equal precedence are evaluated in the order of creation.
- For JUNOS policies, rules with equal precedence are evaluated in random order. Precedence is not a factor for JUNOS SCHEDULER and JUNOS POLICER policy rules.

Value— One of the following:

- For JUNOS and JUNOSe policies, integer in the range 0–32767
- For PCMM policies, integer in the range 64–191
- Parameter of type prPrecedence

Default— 100

<accounting>—(Optional) Specifies whether accounting data is collected for the actions specified in the rule.

If you specify that accounting data is collected, the SAE begins collecting accounting information when a service that uses the policy rule is activated. When the service is deactivated, the SAE sends the accounting records to the RADIUS accounting server or to a plug-in.

When you specify multiple actions for accounting, the SAE adds the accounting data for individual actions together to obtain a summary accounting record for that interface direction.

Accounting is not available for all actions. For example, the NAT action does not provide accounting.

Value— One of the following:

- true—Accounting data is collected.
- false—Accountding data is not collected.

Default— false

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

service

<color> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <color>
            <name>name</name> <!-- identifier -->
            <color>color</color>
            <description>description</description>
          </color>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a color action. Use this action to specify the color that is applied to a packet when it passes through the router. You can configure color actions for JUNOS policy rules.

Contents

<name>— Name for the color action.

Value— Text

<color>—(Optional) Color that is applied to a packet when it passes through the router.

Value— One of the following:

- Integer in the range 1–3
 - 1—green
 - 2—yellow
 - 3—red
- Parameter of type color

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-best-effort> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-best-effort>
            <name>name</name> <!-- identifier -->
            <traffic-priority>traffic-priority</traffic-priority>
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <maximum-sustained-rate>maximum-sustained-rate</maximum-sustained-
rate>
            <maximum-traffic-burst>maximum-traffic-burst</maximum-traffic-
burst>
            <minimum-reserved-rate>minimum-reserved-rate</minimum-reserved-
rate>
            <assumed-minimum-res-packet-size>assumed-minimum-res-packet-size</
assumed-minimum-res-packet-size>
            <description>description</description>
          </docsis-best-effort>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to best-effort service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to best-effort service flow scheduling type.

Value— Text

<traffic-priority>—(Optional) Priority for the service flow. If two traffic flows are

identical in all QoS parameters except priority, the higher-priority service flow is given preference.

Value— One of the following:

- Number in the range 0–7, where 0 is the lowest priority and 7 is the highest priority
- Parameter of type `trafficPriority`

Default— No value

`<request-transmission-policy>`—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type `requestTransmissionPolicy`

Default— No value

`<maximum-sustained-rate>`—(Optional) Maximum sustained rate at which traffic can operate over the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<maximum-traffic-burst>`—(Optional) Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum sustained rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 1522–4294967295
- Numeric expression
- Parameter of type burst

Default— No value

`<minimum-reserved-rate>`—(Optional) Guaranteed minimum rate that is reserved for the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
- Numeric expression
- Parameter of type rate

Default— No value

`<assumed-minimum-res-packet-size>`—(Optional) Assumed minimum packet size for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this option.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `packetLength`

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-down-stream> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-down-stream>
            <name>name</name> <!-- identifier -->
            <traffic-priority>traffic-priority</traffic-priority>
            <maximum-latency>maximum-latency</maximum-latency>
            <maximum-sustained-rate>maximum-sustained-rate</maximum-sustained-
rate>
            <maximum-traffic-burst>maximum-traffic-burst</maximum-traffic-
burst>
            <minimum-reserved-rate>minimum-reserved-rate</minimum-reserved-
rate>
            <assumed-minimum-res-packet-size>assumed-minimum-res-packet-size</
assumed-minimum-res-packet-size>
            <description>description</description>
          </docsis-down-stream>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to downstream service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to downstream service flow scheduling type.

Value— Text

<traffic-priority>—(Optional) Priority for the service flow. If two traffic flows are

identical in all QoS parameters except priority, the higher-priority service flow is given preference.

Value— One of the following:

- Number in the range 0–7, where 0 is the lowest priority and 7 is the highest priority
- Parameter of type `trafficPriority`

Default— No value

`<maximum-latency>`—(Optional) Maximum latency for downstream service flows. It is the maximum latency for a packet that passes through the CMTS device, from the time that the CMTS device's network side interface receives the packet until the CMTS device forwards the packet on its radio frequency (RF) interface.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type `maxLatency`

Default— No value

`<maximum-sustained-rate>`—(Optional) Maximum sustained rate at which traffic can operate over the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<maximum-traffic-burst>`—(Optional) Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum sustained rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 1522–4294967295
- Numeric expression
- Parameter of type burst

Default— No value

`<minimum-reserved-rate>`—(Optional) Guaranteed minimum rate that is reserved for the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
- Numeric expression
- Parameter of type rate

Default— No value

`<assumed-minimum-res-packet-size>`—(Optional) Assumed minimum packet size for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this option.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `packetLength`

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-non-real-time> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-non-real-time>
            <name>name</name> <!-- identifier -->
            <traffic-priority>traffic-priority</traffic-priority>
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <maximum-sustained-rate>maximum-sustained-rate</maximum-sustained-
rate>
            <maximum-traffic-burst>maximum-traffic-burst</maximum-traffic-
burst>
            <minimum-reserved-rate>minimum-reserved-rate</minimum-reserved-
rate>
            <assumed-minimum-res-packet-size>assumed-minimum-res-packet-size</
assumed-minimum-res-packet-size>
            <nominal-polling-interval>nominal-polling-interval</nominal-
polling-interval>
            <description>description</description>
          </docsis-non-real-time>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to non-real-time service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to non-real-time service flow scheduling type.

Value— Text

`<traffic-priority>`—(Optional) Priority for the service flow. If two traffic flows are identical in all QoS parameters except priority, the higher-priority service flow is given preference.

Value— One of the following:

- Number in the range 0–7, where 0 is the lowest priority and 7 is the highest priority
- Parameter of type `trafficPriority`

Default— No value

`<request-transmission-policy>`—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type `requestTransmissionPolicy`

Default— No value

`<maximum-sustained-rate>`—(Optional) Maximum sustained rate at which traffic can operate over the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<maximum-traffic-burst>`—(Optional) Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum sustained

rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 1522–4294967295
- Numeric expression
- Parameter of type burst

Default— No value

`<minimum-reserved-rate>`—(Optional) Guaranteed minimum rate that is reserved for the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
- Numeric expression
- Parameter of type rate

Default— No value

`<assumed-minimum-res-packet-size>`—(Optional) Assumed minimum packet size for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this option.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `packetLength`

Default— No value

`<nominal-polling-interval>`—(Optional) Nominal interval between successive unicast request opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type interval

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-parameter> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-parameter>
            <name>name</name> <!-- identifier -->
            <service-flow-type>service-flow-type</service-flow-type>
            <traffic-priority>traffic-priority</traffic-priority>
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <maximum-sustained-rate>maximum-sustained-rate</maximum-sustained-
rate>
            <maximum-traffic-burst>maximum-traffic-burst</maximum-traffic-
burst>
            <minimum-reserved-rate>minimum-reserved-rate</minimum-reserved-
rate>
            <assumed-minimum-res-packet-size>assumed-minimum-res-packet-size</
assumed-minimum-res-packet-size>
            <maximum-latency>maximum-latency</maximum-latency>
            <nominal-polling-interval>nominal-polling-interval</nominal-
polling-interval>
            <tolerated-poll-jitter>tolerated-poll-jitter</tolerated-poll-
jitter>
            <grant-size>grant-size</grant-size>
            <grants-per-interval>grants-per-interval</grants-per-interval>
            <tolerated-grant-jitter>tolerated-grant-jitter</tolerated-grant-
jitter>
            <nominal-grant-interval>nominal-grant-interval</nominal-grant-
interval>
            <description>description</description>
          </docsis-parameter>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action with the service flow scheduling type set to a parameter. The parameter is a trafficProfileType parameter.

Contents

<name>— Name of a DOCSIS action that is set to the trafficProfileType parameter as the service flow scheduling type.

Value— Text

<service-flow-type>— Parameter that is used to determine the service flow scheduling type.

Value— Parameter of type trafficProfileType. You must enter a parameter that has been created and has been committed.

Default— No value

<traffic-priority>—(Optional) Priority for the service flow. If two traffic flows are identical in all QoS parameters except priority, the higher-priority service flow is given preference.

Value— One of the following:

- Number in the range 0–7, where 0 is the lowest priority and 7 is the highest priority
- Parameter of type trafficPriority

Default— No value

<request-transmission-policy>—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type requestTransmissionPolicy

Default— No value

`<maximum-sustained-rate>`—(Optional) Maximum sustained rate at which traffic can operate over the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<maximum-traffic-burst>`—(Optional) Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum sustained rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 1522–4294967295
- Numeric expression
- Parameter of type `burst`

Default— No value

`<minimum-reserved-rate>`—(Optional) Guaranteed minimum rate that is reserved for the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
- Numeric expression
- Parameter of type `rate`

Default— No value

`<assumed-minimum-res-packet-size>`—(Optional) Assumed minimum packet size

for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this option.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type packetLength

Default— No value

`<maximum-latency>`—(Optional) Maximum latency for downstream service flows. It is the maximum latency for a packet that passes through the CMTS device, from the time that the CMTS device's network side interface receives the packet until the CMTS device forwards the packet on its radio frequency (RF) interface.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type maxLatency

Default— No value

`<nominal-polling-interval>`—(Optional) Nominal interval between successive unicast request opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type interval

Default— No value

`<tolerated-poll-jitter>`—(Optional) Maximum amount of time that unicast request intervals can be delayed beyond the nominal polling interval. Delaying requests allows the service flow scheduler to fit as much data as possible in an upstream packet, thereby reducing fragmentation.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type jitter

Default— No value

`<grant-size>`—(Optional) Size of the individual data grants provided to the service flow.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type grantSize

Default— No value

`<grants-per-interval>`—(Optional) Actual number of data grants given to the service flow during each nominal grant interval.

Value— One of the following:

- Integer in the range 0–127
- Numeric expression
- Parameter of type interval

Default— No value

`<tolerated-grant-jitter>`—(Optional) Maximum amount of time that the transmission opportunities can be delayed beyond the nominal grant interval. A jitter buffer can stop latency, but an improperly sized buffer can cause additional latency.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type jitter

Default— No value

`<nominal-grant-interval>`—(Optional) Nominal interval between successive

unsolicited data grant opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type interval

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-real-time> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-real-time>
            <name>name</name> <!-- identifier -->
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <maximum-sustained-rate>maximum-sustained-rate</maximum-sustained-
rate>
            <maximum-traffic-burst>maximum-traffic-burst</maximum-traffic-
burst>
            <minimum-reserved-rate>minimum-reserved-rate</minimum-reserved-
rate>
            <assumed-minimum-res-packet-size>assumed-minimum-res-packet-size</
assumed-minimum-res-packet-size>
            <nominal-polling-interval>nominal-polling-interval</nominal-
polling-interval>
            <tolerated-poll-jitter>tolerated-poll-jitter</tolerated-poll-
jitter>
            <description>description</description>
          </docsis-real-time>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to real-time service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to real-time service flow scheduling type.

Value— Text

`<request-transmission-policy>`—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type `requestTransmissionPolicy`

Default— No value

`<maximum-sustained-rate>`—(Optional) Maximum sustained rate at which traffic can operate over the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<maximum-traffic-burst>`—(Optional) Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum sustained rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bytes in the range 1522–4294967295
- Numeric expression
- Parameter of type `burst`

Default— No value

`<minimum-reserved-rate>`—(Optional) Guaranteed minimum rate that is reserved for the service flow.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
- Numeric expression
- Parameter of type `rate`

Default— No value

`<assumed-minimum-res-packet-size>`—(Optional) Assumed minimum packet size for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this option.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `packetLength`

Default— No value

`<nominal-polling-interval>`—(Optional) Nominal interval between successive unicast request opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type `interval`

Default— No value

`<tolerated-poll-jitter>`—(Optional) Maximum amount of time that unicast request intervals can be delayed beyond the nominal polling interval. Delaying requests allows the service flow scheduler to fit as much data as possible in an upstream packet, thereby reducing fragmentation.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type jitter

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-unsolicited-grant> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-unsolicited-grant>
            <name>name</name> <!-- identifier -->
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <grant-size>grant-size</grant-size>
            <grants-per-interval>grants-per-interval</grants-per-interval>
            <tolerated-grant-jitter>tolerated-grant-jitter</tolerated-grant-
jitter>
            <nominal-grant-interval>nominal-grant-interval</nominal-grant-
interval>
            <description>description</description>
          </docsis-unsolicited-grant>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to unsolicited grant (UGS) service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to UGS service flow scheduling type.

Value— Text

<request-transmission-policy>—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service

flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type requestTransmissionPolicy

Default— No value

`<grant-size>`—(Optional) Size of the individual data grants provided to the service flow.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type grantSize

Default— No value

`<grants-per-interval>`—(Optional) Actual number of data grants given to the service flow during each nominal grant interval.

Value— One of the following:

- Integer in the range 0–127
- Numeric expression
- Parameter of type interval

Default— No value

`<tolerated-grant-jitter>`—(Optional) Maximum amount of time that the transmission opportunities can be delayed beyond the nominal grant interval. A jitter buffer can stop latency, but an improperly sized buffer can cause additional latency.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type jitter

Default— No value

`<nominal-grant-interval>`—(Optional) Nominal interval between successive unsolicited data grant opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type interval

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<docsis-unsolicited-grant-ad> (configuration/policies/group/list/rule)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <docsis-unsolicited-grant-ad>
            <name>name</name> <!-- identifier -->
            <request-transmission-policy>request-transmission-policy</request-
transmission-policy>
            <nominal-polling-interval>nominal-polling-interval</nominal-
polling-interval>
            <grant-size>grant-size</grant-size>
            <grants-per-interval>grants-per-interval</grants-per-interval>
            <tolerated-grant-jitter>tolerated-grant-jitter</tolerated-grant-
jitter>
            <nominal-grant-interval>nominal-grant-interval</nominal-grant-
interval>
            <description>description</description>
          </docsis-unsolicited-grant-ad>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a DOCSIS action that is set to unsolicited grant service with activity detection (UGS-AD) service flow scheduling type. DOCSIS actions are for PCMM policy rules.

Contents

<name>— Name of a DOCSIS action that is set to unsolicited grant service with activity detection (UGS-AD) service flow scheduling type.

Value— Text

`<request-transmission-policy>`—(Optional) Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. Specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS flows, this option also specifies how to treat packets that do not fit into the UGS grant.

Value— One of the following:

- 4-byte bit field; the valid range is 0–511
- Parameter of type `requestTransmissionPolicy`

Default— No value

`<nominal-polling-interval>`—(Optional) Nominal interval between successive unicast request opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type `interval`

Default— No value

`<grant-size>`—(Optional) Size of the individual data grants provided to the service flow.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `grantSize`

Default— No value

`<grants-per-interval>`—(Optional) Actual number of data grants given to the service flow during each nominal grant interval.

Value— One of the following:

- Integer in the range 0–127

- Numeric expression
- Parameter of type interval

Default— No value

`<tolerated-grant-jitter>`—(Optional) Maximum amount of time that the transmission opportunities can be delayed beyond the nominal grant interval. A jitter buffer can stop latency, but an improperly sized buffer can cause additional latency.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type jitter

Default— No value

`<nominal-grant-interval>`—(Optional) Nominal interval between successive unsolicited data grant opportunities for this service flow.

Value— One of the following:

- Number of microseconds in the range 0–4294967295
- Numeric expression
- Parameter of type interval

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<exception-application> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <exception-application>
            <name>name</name> <!-- identifier -->
            <application-type>application-type</application-type>
            <description>description</description>
          </exception-application>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify exceptions to a policy rule to identify the client application that is a destination for packets Use this action in policy rules for JUNOSe routers.

Contents

<name>— Name for the exception application action.

Value— Text

<application-type>— Specify the type of application to receive packets to which the exception action applies.

Value—

Default— http

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <filter>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </filter>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a filter action. Use this action to discard packets. You can configure filter actions for JUNOS filters and JUNOS policy rules.

Contents

<name>— Name for the filter action.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<flow-spec> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <flow-spec>
            <name>name</name> <!-- identifier -->
            <service-type>service-type</service-type>
            <token-bucket-rate>token-bucket-rate</token-bucket-rate>
            <token-bucket-size>token-bucket-size</token-bucket-size>
            <peak-data-rate>peak-data-rate</peak-data-rate>
            <minimum-policed-unit>minimum-policed-unit</minimum-policed-unit>
            <maximum-packet-size>maximum-packet-size</maximum-packet-size>
            <rate>rate</rate>
            <slack-term>slack-term</slack-term>
            <description>description</description>
          </flow-spec>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a FlowSpec action, which uses an RSVP-style FlowSpec to specify a traffic profile. A FlowSpec is made up of two parts, a traffic specification (TSpec) and a service request specification (RSpec). The TSpec describes the traffic requirements for the flow, and the RSpec specifies resource requirements for the desired service. You can configure FlowSpec actions for PCMM policy rules.

Contents

<name>— Name of the FlowSpec action.

Value— Text

<service-type>—(Optional) Type of FlowSpec service.

Value— One of the following:

- 2—guaranteed_service, which provides both bandwidth and latency and delay guarantees. A guaranteed service can contain both TSpec and RSpec parameters.
- 5—controlled_load_service, which provides minimum bandwidth guarantees, but not latency and delay guarantees. A controlled-load service can contain only TSpec token-bucket parameters, and not RSpec parameters.
- Parameter of type serviceNumber

Default— No value

<token-bucket-rate>—(Optional) Guaranteed minimum rate that is reserved for the service flow. Token bucket rate is a TSpec parameter.

Value— One of the following:

- Predefined global parameter interface_speed, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295
- Numeric expression
- Parameter of type rate

Default— No value

<token-bucket-size>—(Optional) Maximum burst size for the service flow. Token bucket size is a TSpec parameter.

Value— One of the following:

- Number of bits per second in the range 1522–4294967295
- Numeric expression
- Parameter of type tokenBucketSize

Default— No value

<peak-data-rate>—(Optional) Amount of bandwidth over the committed rate that is allocated to accommodate excess traffic flow over the committed rate. Peak data rate is a TSpec parameter.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<minimum-policed-unit>`—(Optional) Assumed minimum-reserved-rate packet size. If a packet is smaller than the minimum policed unit, the software treats the packet as if its size is equal to the value specified in this option. Minimum policed unit is a TSpec parameter.

Value— One of the following:

- Number of bytes in the range 0–65535
- Numeric expression
- Parameter of type `policedUnit`

Default— No value

`<maximum-packet-size>`—(Optional) Maximum packet size for the FlowSpec. Maximum packet size is a TSpec parameter.

Value— One of the following:

- Number of bytes in the range 0–4294967295
- Numeric expression
- Parameter of type `packetLength`

Default— No value

`<rate>`—(Optional) Average rate. Rate is an RSpec parameter.

Value— One of the following:

- Predefined global parameter `interface_speed`—Speed of the subscriber's DOCSIS interface
- Number of bits per second in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

Default— No value

`<slack-term>`—(Optional) Amount of slack in the bandwidth reservation that can be used without redefining the reservation. Slack is the difference between the desired delay and the actual delay obtained with the current bandwidth reservation. It allows some flexibility in bandwidth reservations. Slack term is an RSpec parameter.

Value— One of the following:

- Integer in the range 0–4294967295
- Numeric expression
- Parameter of type slackTerm

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<forward> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <forward>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </forward>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a forward action. Use this action to forward packets, such as packets that are sent by means of a routing table. You can configure forward actions for JUNOS filters and JUNOS policy rules.

Contents

<name>— Name for the forward action.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<forwarding-class> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <forwarding-class>
            <name>name</name> <!-- identifier -->
            <forwarding-class>forwarding-class</forwarding-class>
            <description>description</description>
          </forwarding-class>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a forwarding class action. The forwarding class action causes the router to assign a forwarding class to packets that match the associated classify-traffic condition. You can configure forwarding class actions for JUNOS filter policy rules.

Contents

<name>— Name of the forwarding class action.

Value— Text

<forwarding-class>—(Optional) Name of the forwarding class assigned to packets.

Value— One of the following:

- String expression that matches a forwarding class that is configured on the router. Be sure to include quotation marks. For example:
 - "assured-forwarding"
 - "best-effort"

- "expedited-forwarding"
- "network-control"
- Parameter of type forwardingClass

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<gate-spec> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <gate-spec>
            <name>name</name> <!-- identifier -->
            <session-class-id-priority>session-class-id-priority</session-
class-id-priority>
            <session-class-id-preemption>session-class-id-preemption</session-
class-id-preemption>
            <session-class-id-configurable>session-class-id-configurable</
session-class-id-configurable>
            <description>description</description>
          </gate-spec>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a GateSpec action. Use the GateSpec action to specify the session class ID for a gate. You can configure GateSpec actions for PCMM policy rules.

The session class ID provides a way for the application manager and the policy server to group gates into classes with different authorization characteristics. A CMTS device can perform authorization based not only on the requested QoS and the gate's authorized flow specification (FlowSpec), but also on the session class ID specified in the GateSpec. For example, you could use the session class ID to represent a prioritization scheme that allows either the policy server or the CMTS device to preempt a preauthorized gate in favor of allowing a new gate with a higher priority to be authorized.

Contents

<name>— Name of the GateSpec action.

Value— Text

`<session-class-id-priority>`—(Optional) Priority bits in the session class ID. The priority field describes the relative importance of the session as compared with other sessions generated by the same policy decision point.

Value— One of the following:

- Number in the range 0–7, where 0 is low priority and 7 is high priority
- String expression
- Parameter of type `sessionClassIdPriority`

Default— No value

`<session-class-id-preemption>`—(Optional) Preemption bit in the session class ID. Use the preemption bit to allocate bandwidth to lower-priority sessions.

Value— One of the following:

- 0—Enables preemption
- 1—Disables preemption
- String expression
- Parameter of type `sessionClassIdPreemption`

Default— No value

`<session-class-id-configurable>`—(Optional) Configurable bit in the session class ID. Application managers that provide novel services may use this value to specify new session classes. Use this option if your policy server supports configurable policies based on this value or if your CMTS device implements a novel session class based on this value.

Value— One of the following:

- Number in the range 0–15
- String expression
- Parameter of type `sessionClassIdConfigurable`

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<http-redirect> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <http-redirect>
            <name>name</name> <!-- identifier -->
            <subscriber-url>subscriber-url</subscriber-url>
            <description>description</description>
          </http-redirect>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a destination URL to which subscriber traffic is redirected. Use this action in policy rules for JUNOSe routers.

Contents

<name>— Name for the HTTP redirect action.

Value— Text

<subscriber-url>—(Optional) Destination URL for redirected Web traffic.

You can use the exception-application action to specify exceptions to a rule to identify the client, in this case HTTP, application that is a destination for packets.

Value— Literal string or parameter of type url

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<loss-priority> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <loss-priority>
            <name>name</name> <!-- identifier -->
            <loss-priority>loss-priority</loss-priority>
            <description>description</description>
          </loss-priority>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a loss priority action. The loss priority action causes the router to assign a packet loss priority to packets that match the associated classify-traffic condition. You can configure loss priority actions for JUNOS filter policy rules.

Contents

<name>— Name of the loss priority action.

Value— Text

<loss-priority>—(Optional) Packet loss priority.

Value— One of the following:

- Predefined global parameter:
 - any_priority—Sets the packet loss priority to "any." Do not select this value for loss priority actions. In this context, a value of any_priority is not valid.
 - high_priority—Sets the packet loss priority to high

- `low_priority`—Sets the packet loss priority to low
- String expression that matches valid values on the router; for example, "high" or "low"
- Parameter of type `packetLossPriority`

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<mark> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <mark>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </mark>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a mark action. Use this action to mark packets. You can configure mark actions for JUNOS and PCMM policy rules.

Contents

<name>— Name for the mark action.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<info> (configuration/policies/group/list/rule/mark)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <mark>
            <info>
              <value>value</value>
              <mask>mask</mask>
            </info>
          </mark>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the mark value and mark mask for mark actions.

Contents

<value>—(Optional) For IPv4 packets, sets the ToS field in the IP header. For IPv6 packets, sets the traffic-class field in the IP header.

Value— One of the following:

- Integer in the range 0–255
- Parameter of type tosByteMask

Default— 0

<mask>—(Optional) Mask associated with the mark value.

Value— One of the following:

- Integer values of 224, 252, 255

For IPv4:

- 255 (tos)—Specifies the use of the whole 8 bits of the ToS byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the ToS byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the ToS byte; tos-byte range is 0–7.

For IPv6:

- 255 (tcfield)—Specifies the use of the whole 8 bits of the traffic-class byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the traffic-class byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the traffic-class byte; tos-byte range is 0–7.
- Parameter of type tosByteMask

Default— 255

Required Privilege Level

service

<nat> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <nat>
            <name>name</name> <!-- identifier -->
            <translation-type>translation-type</translation-type>
            <description>description</description>
          </nat>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NAT action. You can configure NAT actions for JUNOS ASP policy rules.

Contents

<name>— Name for the NAT action.

Value— Text

<translation-type>—(Optional) Type of network address translation that is used.

Value— One of the following:

- String expression that matches a NAT type on the router; for example:
 - "destination static"—Implements address translation for destination traffic without port translation; makes selected private servers accessible
 - "source dynamic"—Implements address translation for source traffic with port translation

- "source static"—Implements address translation for source traffic without port mapping
- Parameter of type natTranslationType

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<group-network> (configuration/policies/group/list/rule/nat/ip-network)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <nat>
            <ip-network>
              <group-network>
                <network-specifier>network-specifier</network-specifier>
              </group-network>
            </ip-network>
          </nat>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configuration of the network specifier for the NAT action.

Contents

<network-specifier>—(Optional) Specifies an IP address and mask.

Value— Specify the subnet in one of the following formats:

- [not] < address > / < mask > or < address > / < prefix length >
 - Include *not* to indicate that the condition matches every address that is not in the specified subnet.
 - < prefix length > is a number in the range 0–32, and specifies how many of the first bits in the address specify the network
- For JUNOS ASP policies, you must enter network in the format: < address > / < prefix length >

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/nat)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <nat>
            <port>
              <from-port>from-port</from-port>
            </port>
          </nat>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the port range for the NAT action.

Contents

<from-port>—(Optional) Port range to restrict port translation when NAT is configured in dynamic-source mode.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–64000
- Numeric expression that indicates a range of ports; for example, 2010..2020
- 0..65535—Provides the same effect as the automatic option. JUNOS routing platforms support a port option called automatic, which means that it is a router-assigned port.
- Parameter of type port

Default— No value

Required Privilege Level

service

<next-hop> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <next-hop>
            <name>name</name> <!-- identifier -->
            <next-hop-address>next-hop-address</next-hop-address>
            <description>description</description>
          </next-hop>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a next-hop action. Use this action for the ingress side of the interface to specify the next IP address where the classified packets should go. You can configure next-hop actions for JUNOS filters and JUNOS policy rules.

Contents

<name>— Name for the next-hop action.

Value— Text

<next-hop-address>—(Optional) Address of next hop through which to send traffic.

Value— One of the following:

- IP address
- Predefined global parameter:
 - gateway_ipAddress—IP address of the gateway as specified by the service object
 - interface_ipAddress—IP address of the router

- interface
 - service_ipAddress—IP address of the service as specified by the service object
 - user_ipAddress—IP address of the subscriber
 - virtual_ipAddress—Virtual portal address of the SAE that is used in redundant redirect server installations
- Parameter of type address

Default— 0

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<next-interface> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <next-interface>
            <name>name</name> <!-- identifier -->
            <interface-specifier>interface-specifier</interface-specifier>
            <next-hop-address>next-hop-address</next-hop-address>
            <description>description</description>
          </next-interface>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a next-interface action. Use this action to forward packets to a particular interface and/or a next-hop address. You can configure next-interface actions for JUNOS filters and JUNOS policy rules. On JUNOS routers, you can use this action for both ingress and egress sides of the interface.

Contents

<name>— Name for the next-interface action.

Value— Text

<interface-specifier>— IP interface to be used as the next interface for packets.

Value— One of the following:

- For JUNOS interfaces, enter interface specifiers in the format:

' < type of specifier > = < value > '

where < type of specifier > is the interface name, alias, description, or UID.

For example: name = 'fastEthernet3/0'

For lists of valid interface specifiers for JUNOS routers, see "Interface Types and Specifiers" in the JUNOS Command Reference Guides.

- For JUNOS interfaces, enter interface specifiers in the format:

'name = < mediatype > - < slot > / < pic > / < port > . < unit > '

For example: 'name = AT-0/1/0.0'

- Predefined global parameter:
 - bfwlf (interface that leads to the bronze firewall server)
 - gfwlf (interface that leads to gold firewall server).
- Parameter of type interfaceSpec

Default— No value

<next-hop-address>—(Optional) Address of next hop through which to send traffic.

Value— One of the following:

- IP address
- Predefined global parameter:
 - gateway_ipAddress—IP address of the gateway as specified by the service object
 - interface_ipAddress—IP address of the router interface
 - service_ipAddress—IP address of the service as specified by the service object
 - user_ipAddress—IP address of the subscriber
 - virtual_ipAddress—Virtual portal address of the SAE that is used in redundant redirect server installations
- Parameter of type address

Default— 0

<description>—(Optional) Description of the object that you are configuring.

Value—Text
Default— No value

Required Privilege Level

service

<next-rule> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <next-rule>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </next-rule>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a next-rule action. If a packet matches the classify-traffic condition, the next-rule action causes the router to continue to the next rule in the policy list for evaluation. You can configure next-rule actions for JUNOS filter policy rules.

Contents

<name>— Name of the next-rule action.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<policer> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <name>name</name> <!-- identifier -->
            <bandwidth-limit>bandwidth-limit</bandwidth-limit>
            <bandwidth-limit-unit>bandwidth-limit-unit</bandwidth-limit-unit>
            <burst>burst</burst>
            <description>description</description>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a policer action. The policer action specifies rate and burst size limits and the action taken if a packet exceeds those limits. You can create policer actions in JUNOS policer and JUNOS filter policy rules.

Contents

<name>— Name of the policer action.

Value—Text

<bandwidth-limit>—(Optional) Traffic rate, that if exceeded, causes the router to take the indicated packet action.

Value— One of the following:

- Predefined global parameter interface_speed, which is the speed of the subscriber's router interface.
- Bits per second in the range 32000–320000000000

- Percentage of bandwidth (1–100)
- Numeric expression
- Parameter of type rate

Default— No value

`<bandwidth-limit-unit>`—(Optional) Indicates the type of value that you entered for bandwidth limit.

Value— One of the following:

- Predefined global parameter:
 - bps—Value entered for bandwidth limit is bps
 - percent—Value entered for bandwidth limit is a percentage of the port speed
- String expression
- Parameter of type bandwidthSizeUnit

Default— No value

`<burst>`—(Optional) Maximum burst size. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed.

Value— One of the following:

- Number of bytes
- Numeric expression; for example 8*64000
- Parameter of type burst

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<packet-action> (configuration/policies/group/list/rule/policer)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <packet-action>
              <name>name</name> <!-- identifier -->
            </packet-action>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the action taken on a packet.

Contents

<name>— Name for the action that is taken on packets that exceed the rate and burst size limits specified in the policer action.

Value— Text

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule/policer/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <packet-action>
              <filter>
              </filter>
            </packet-action>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the bandwidth and burst rate limits, the packet is dropped.

Contents

Required Privilege Level

service

<forwarding-class> (configuration/policies/group/list/rule/policer/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <packet-action>
              <forwarding-class>
                <forwarding-class>forwarding-class</forwarding-class>
              </forwarding-class>
            </packet-action>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the bandwidth and burst rate limits, it is assigned to a forwarding class.

Contents

<forwarding-class>—(Optional) Name of the forwarding class assigned to packets.

Value— One of the following:

- String expression that matches a forwarding class that is configured on the router. Be sure to include quotation marks. For example:
 - "assured-forwarding"
 - "best-effort"
 - "expedited-forwarding"
 - "network-control"
- Parameter of type forwardingClass

Default— No value

Required Privilege Level

service

<loss-priority> (configuration/policies/group/list/rule/policer/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <packet-action>
              <loss-priority>
                <loss-priority>loss-priority</loss-priority>
              </loss-priority>
            </packet-action>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

For a policer action, set the loss priority level as the action taken on a packet that exceeds its rate limit.

Contents

<loss-priority>—(Optional) Packet loss priority.

Value— One of the following:

- Predefined global parameter:
 - any_priority—Sets the packet loss priority to "any." Do not select this value for loss priority actions. In this context, a value of any_priority is not valid.
 - high_priority—Sets the packet loss priority to high
 - low_priority—Sets the packet loss priority to low
- String expression that matches valid values on the router; for example, "high" or "low"
- Parameter of type packetLossPriority

Default— No value

Required Privilege Level

service

<parameter> (configuration/policies/group/list/rule/policer/ packet-action)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <policer>
            <packet-action>
              <parameter>
                <action>action</action>
              </parameter>
            </packet-action>
          </policer>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the bandwidth and burst rate limits, the action specified by the parameter is applied.

Contents

<action>—(Optional) Parameter that specifies the action to take on traffic.

Value— Parameter of type packetOperation.

Default— No value

Required Privilege Level

service

<qos-attach> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <qos-attach>
            <name>name</name> <!-- identifier -->
            <qos-profile>qos-profile</qos-profile>
            <qos-parameters>qos-parameters</qos-parameters>
            <description>description</description>
          </qos-attach>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a QoS attachment action. Use this action to specify the name of the QoS profile and the QoS parameters list to attach to the router interface when this action is taken. You can configure QoS profile attachment actions for JUNOS policy rules.

Contents

<name>— Name for the QoS profile attachment action.

Value— Text

<qos-profile>— Name of the QoS profile to attach to the JUNOS interface when this action is taken.

Value— One of the following:

- Name of a QoS profile that is configured on the router. Enclose the name in quotation marks. For example: "qp-vod-1024".
- Parameter of type qosProfileSpec.

Default— No value

`<qos-parameters>`—(Optional) Name-value pairs of the QoS parameters to attach to the interface when this action is taken. The parameters are configured on the JUNOS router and referenced in the scheduler profiles referred to by the QoS profile.

Value— One of the following:

- Name-value pair that defines QoS parameter; map expressions define multiple QoS parameters.

Maps are a list of `parameterName = parameterValue` pairs separated by commas and enclosed in curly brackets. For example, the map `{max-bw = 512000, shape-rate = 1000000}` supplies two QoS parameters.

- Parameter of type map.

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<qos-condition> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <qos-condition>
            <name>name</name> <!-- identifier -->
            <forwarding-class>forwarding-class</forwarding-class>
            <description>description</description>
          </qos-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a QoS condition. You can create QoS conditions within JUNOS scheduler policy rules.

Contents

<name>— Name for the QoS condition.

Value— Text

<forwarding-class>—(Optional) Matches packets based on forwarding class

Value— One of the following:

- String expression that matches forwarding classes that are configured on the router. Be sure to include quotation marks. For example:
 - "assured-forwarding"
 - "best-effort"
 - "expedited-forwarding"
 - "network-control"

- Parameter of type forwardingClass

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<rate-limit> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <name>name</name> <!-- identifier -->
            <type>type</type>
            <committed-rate>committed-rate</committed-rate>
            <committed-burst>committed-burst</committed-burst>
            <peak-rate>peak-rate</peak-rate>
            <peak-burst>peak-burst</peak-burst>
            <excess-burst>excess-burst</excess-burst>
            <description>description</description>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a rate-limit action. Use this action to define the quality of service. You can configure rate-limit actions for JUNOS policy rules.

Contents

<name>— Name for the rate-limit action.

Value— Text

<type>— Specify that the rate-limit profile is either one rate or two rate. The one-rate rate-limit profile provides a hard-limit rate limiter or a TCP-friendly rate limiter. The two-rate rate-limit profile provides a two-rate, three-color marking mechanism.

Value— One of the following:

- `one_rate`—Uses a single-rate committed rate with two burst parameters: committed burst and excess burst; supports a TCP-friendly rate limiter
- `two_rate`—Uses committed rate and peak rate, each with a burst parameter
- Parameter of type `rateLimitType`

Default— No value

`<committed-rate>`—(Optional) Target rate for the traffic that the policy covers.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's router interface
- Number of bits per second in the range 0–4294967295
- Parameter of type `rate`

Default— 0

`<committed-burst>`—(Optional) Amount of bandwidth allocated to burst traffic in bytes.

Value— One of the following:

- Number of bytes in the range 8192–4294967295
- Numeric expression.
- Parameter of type `burst`

For example, `max(qos*0.1/8, 16384)` sets the burst size to the maximum of 100-ms burst at committed rate (`qos*0.1`) in bytes (/8) or 16384

where `qos` is a local parameter that represents the committed rate

Default— 16384

`<peak-rate>`—(Optional) For two-rate rate-limit profiles, specifies the amount of bandwidth allocated to excess traffic flow over the committed rate.

Value— One of the following:

- Predefined global parameter `interface_speed`, which is the speed of the subscriber's router interface
- Number of bits per second in the range 0–4294967295
- Numeric expression
- Parameter of type `rate`

For example, `qos*1.5` sets the peak rate to 1.5 times the committed rate

where `qos` is a local parameter that represents the committed rate

Default— 0

`<peak-burst>`—(Optional) For two-rate rate-limit profiles, specifies the amount of bandwidth allocated to burst traffic in excess of the peak rate.

Value— One of the following:

- Number of bytes in the range 8192–4294967295
- Numeric expression
- Parameter of type `burst`

For example, `max(qos*1.5*0.1/8, 16384)`

where `qos` is a local parameter that represents the committed rate

Default— 16384

`<excess-burst>`—(Optional) For one-rate rate-limit profiles, specifies the amount of bandwidth allocated to accommodate burst traffic.

Value— One of the following:

- Number of bytes in the range $< 0 \mid [\text{committed-burst} + 1, 4294967295] >$
- Numeric expression
- Parameter of type `burst`

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule/rate-limit/committed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <committed-action>
              <filter>
              </filter>
            </committed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow does not exceed the committed rate, the packet is dropped.

Contents

Required Privilege Level

service

<forward> (configuration/policies/group/list/rule/rate-limit/committed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <committed-action>
              <forward>
            </forward>
          </committed-action>
        </rate-limit>
      </rule>
    </list>
  </group>
</policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow does not exceed the committed rate, the packet is forwarded.

Contents

Required Privilege Level

service

<mark-info> (configuration/policies/group/list/rule/rate-limit/committed-action/mark)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <committed-action>
              <mark>
                <mark-info>
                  <value>value</value>
                  <mask>mask</mask>
                </mark-info>
              </mark>
            </committed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the mark value and the mark mask.

Contents

<value>—(Optional) For IPv4 packets, sets the ToS field in the IP header. For IPv6 packets, sets the traffic-class field in the IP header.

Value— Integer in the range 0–255

Default— 0

<mask>—(Optional) Mask associated with the mark value.

Value— Integer values of 224, 252, 255 for JUNOS; values of 224, 252

for JUNOS

For IPv4:

- 255 (tos)—Specifies the use of the whole 8 bits of the ToS byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the ToS byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the ToS byte; tos-byte range is 0–7.

For IPv6:

- 255 (tcfield)—Specifies the use of the whole 8 bits of the traffic-class byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the traffic-class byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the traffic-class byte; tos-byte range is 0–7.

Default— 255

Required Privilege Level

service

<parameter> (configuration/policies/group/list/rule/rate-limit/committed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <committed-action>
              <parameter>
                <action>action</action>
              </parameter>
            </committed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow does not exceed the committed rate, the action specified by the parameter is applied.

Contents

<action>—(Optional) Parameter that specifies the action to take on traffic.

Value— Parameter of type packetOperation.

Default— No value

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule/rate-limit/conformed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <conformed-action>
              <filter>
                </filter>
            </conformed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the committed rate but remains below the peak rate, the packet is dropped.

Contents

Required Privilege Level

service

<forward> (configuration/policies/group/list/rule/rate-limit/conformed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <conformed-action>
              <forward>
            </forward>
          </conformed-action>
        </rate-limit>
      </rule>
    </list>
  </group>
</policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the committed rate but remains below the peak rate, the packet is forwarded.

Contents

Required Privilege Level

service

<mark-info> (configuration/policies/group/list/rule/rate-limit/conformed-action/mark)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <conformed-action>
              <mark>
                <mark-info>
                  <value>value</value>
                  <mask>mask</mask>
                </mark-info>
              </mark>
            </conformed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the mark value and the mark mask.

Contents

<value>—(Optional) For IPv4 packets, sets the ToS field in the IP header. For IPv6 packets, sets the traffic-class field in the IP header.

Value— Integer in the range 0–255

Default— 0

<mask>—(Optional) Mask associated with the mark value.

Value— Integer values of 224, 252, 255 for JUNOS; values of 224, 252

for JUNOS

For IPv4:

- 255 (tos)—Specifies the use of the whole 8 bits of the ToS byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the ToS byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the ToS byte; tos-byte range is 0–7.

For IPv6:

- 255 (tcfield)—Specifies the use of the whole 8 bits of the traffic-class byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the traffic-class byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the traffic-class byte; tos-byte range is 0–7.

Default— 255

Required Privilege Level

service

<parameter> (configuration/policies/group/list/rule/rate-limit/conformed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <conformed-action>
              <parameter>
                <action>action</action>
              </parameter>
            </conformed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the committed rate but remains below the peak rate, the action specified by the parameter is applied.

Contents

<action>—(Optional) Parameter that specifies the action to take on traffic.

Value— Parameter of type packetOperation.

Default— No value

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule/rate-limit/exceed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <exceed-action>
              <filter>
                </filter>
            </exceed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the peak rate, the packet is dropped.

Contents

Required Privilege Level

service

<forward> (configuration/policies/group/list/rule/rate-limit/exceed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <exceed-action>
              <forward>
            </forward>
          </exceed-action>
        </rate-limit>
      </rule>
    </list>
  </group>
</policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the peak rate, the packet is forwarded.

Contents

Required Privilege Level

service

<mark-info> (configuration/policies/group/list/rule/rate-limit/exceed-action/mark)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <exceed-action>
              <mark>
                <mark-info>
                  <value>value</value>
                  <mask>mask</mask>
                </mark-info>
              </mark>
            </exceed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the mark value and the mark mask.

Contents

<value>—(Optional) For IPv4 packets, sets the ToS field in the IP header. For IPv6 packets, sets the traffic-class field in the IP header.

Value— Integer in the range 0–255

Default— 0

<mask>—(Optional) Mask associated with the mark value.

Value— Integer values of 224, 252, 255 for JUNOS; values of 224, 252

for JUNOS

For IPv4:

- 255 (tos)—Specifies the use of the whole 8 bits of the ToS byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the ToS byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the ToS byte; tos-byte range is 0–7.

For IPv6:

- 255 (tcfield)—Specifies the use of the whole 8 bits of the traffic-class byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the traffic-class byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the traffic-class byte; tos-byte range is 0–7.

Default— 255

Required Privilege Level

service

<parameter> (configuration/policies/group/list/rule/rate-limit/exceed-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <rate-limit>
            <exceed-action>
              <parameter>
                <action>action</action>
              </parameter>
            </exceed-action>
          </rate-limit>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify that if traffic flow exceeds the peak rate, the action specified by the parameter is applied.

Contents

<action>—(Optional) Parameter that specifies the action to take on traffic.

Value— Parameter of type packetOperation.

Default— No value

Required Privilege Level

service

<reject> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <reject>
            <name>name</name> <!-- identifier -->
            <message-type>message-type</message-type>
            <description>description</description>
          </reject>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a reject action. The reject action causes the router to discard a packet and send an ICMP destination unreachable message. You can configure reject actions for JUNOS filter policy rules.

Contents

<name>— Name of the reject action.

Value— Text

<message-type>—(Optional) Type of ICMP destination unreachable message sent to the client.

Value— One of the following:

- String expression that matches a type of ICMP destination unreachable message supported on the router; for example:
 - "administratively-prohibited"
 - "bad-host-tos"
 - "bad-network-tos"

- "host-prohibited"
- "host-unknown"
- "host-unreachable"
- "network-prohibited"
- "network-unknown"
- "network-unreachable"
- "port-unreachable"
- "precedence-cutoff"
- "precedence-violation"
- "protocol-unreachable"
- "source-host-isolated"
- "source-route-failed"
- "tcp-reset"—If you specify tcp-reset, a TCP reset message is sent if the packet is a TCP packet. Otherwise, nothing is sent.
- Parameter of type messageType

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<routing-instance> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <routing-instance>
            <name>name</name> <!-- identifier -->
            <routing-instance>routing-instance</routing-instance>
            <description>description</description>
          </routing-instance>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a routing instance action. Use routing instance actions for filter-based forwarding to direct traffic to a specific routing instance configured on the router. You can configure routing instance actions for JUNOS filter policy rules.

Contents

<name>— Name of the routing instance action.

Value— Text

<routing-instance>—(Optional) Routing instance on the router to which packets are forwarded.

Value— One of the following:

- String expression that matches the name of a routing instance configured on the router; for example "isp2-route-table"
- Parameter of type routingInstance

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<scheduler-action> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <scheduler-action>
            <name>name</name> <!-- identifier -->
            <buffer-size>buffer-size</buffer-size>
            <buffer-size-unit>buffer-size-unit</buffer-size-unit>
            <priority>priority</priority>
            <transmit-rate>transmit-rate</transmit-rate>
            <transmit-rate-unit>transmit-rate-unit</transmit-rate-unit>
            <exact>exact</exact>
            <description>description</description>
          </scheduler-action>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduler action. You use scheduler actions along with QoS conditions and traffic-shape actions to configure transmission scheduling and rate control. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and random early detection (RED) drop profiles to be applied to a particular class of traffic. You can create scheduler actions in JUNOS scheduler policy rules.

Contents

<name>— Name for the scheduler action.

Value— Text

<buffer-size>—(Optional) Queue transmission buffer size.

Value— One of the following:

- Integer that represents the number of microseconds or a percentage of total buffer size.
- "remainder"—Uses available buffer that is not assigned to other queues.
- Expression
- Parameter of type schedulerBufferSize

Default— No value

<buffer-size-unit>—(Optional) Type of value that you entered for buffer size.

Value— One of the following:

- Predefined global parameter:
 - buffer_size_percentage—The value is a percentage of the total buffer.
 - buffer_size_remainder—The value is the remaining buffer available.
 - temporal—The value is temporal, in microseconds.
- String expression; for example, "percent"
- Parameter of type schedulerBufferSizeUnit

Default— No value

<priority>—(Optional) Packet-scheduling priority. The priority determines the order in which an output interface transmits traffic from the queues.

Value— One of the following:

- Predefined global parameter:
 - low
 - medium_low
 - medium_high
 - high—Assigning high priority to a queue prevents the queue from being starved by traffic in a strict high-priority queue
 - strict_high—Configures a high-priority queue with unlimited transmission bandwidth available to it. As long as it has traffic to send, the strict high-priority queue receives precedence over low, medium-low, and medium-high priority queues, but not high-priority queues. You can configure strict high-priority on only one queue per interface.
- String expression—For example, "strict-high"
- Parameter of type schedulerPriority

Default— No value

`<transmit-rate>`—(Optional) Transmit rate.

Value— One of the following:

- Integer that represents the rate in bps or a percentage of bandwidth
- "remainder"—Uses remaining rate available
- Numeric expression
- Parameter of type `schedulerTransmitRate`

Default— No value

`<transmit-rate-unit>`—(Optional) Type of value that you entered for transmit rate.

Value—Text

Default— No value

`<exact>`—(Optional) Specifies whether or not to enforce the exact transmission rate. Under sustained congestion, a rate-controlled queue that goes into negative credit fills up and eventually drops packets.

Value— True or false

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<drop-profile> (configuration/policies/group/list/rule/scheduler-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <scheduler-action>
            <drop-profile>
              <name>name</name> <!-- identifier -->
              <loss-priority>loss-priority</loss-priority>
              <protocol>protocol</protocol>
              <drop-probability>drop-probability</drop-probability>
              <drop-profile-type>drop-profile-type</drop-profile-type>
              <queue-threshold>queue-threshold</queue-threshold>
            </drop-profile>
          </scheduler-action>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a drop profile. The scheduler drop profile defines the drop probabilities across the range of delay-buffer occupancy, thereby supporting the RED process. For a packet to be dropped, it must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet. Depending on the drop probabilities, RED might drop packets aggressively long before the buffer becomes full, or it might drop only a few packets even if the buffer is almost full.

In drop profiles you configure queue threshold (fill level) and drop probability as paired values. The values can be either percentage values (segmented) or data points (interpolated). These two alternatives enable you to configure each drop probability at up to 64 queue threshold/drop-probability paired values, or to configure a profile represented as a series of line segments. For more information about configuring fill level and drop probabilities, see the JUNOS routing platform documentation.

Contents

`<name>`— Name for the drop profile.

Value— Text

`<loss-priority>`— Packet loss priority.

Value—Text

Default— No value

`<protocol>`— Protocol type for the drop profile map. The protocol type is ignored for priority levels greater than 2.

Value—Text

Default— No value

`<drop-probability>`— Probability that a packet will be dropped.

Value— One of the following:

- If the drop profile type is segmented, specify the drop probability as a percentage. A value of 0 means that a packet will never be dropped, and a value of 100 means that all packets will be dropped. The range is 0–100.
- If the drop profile type is interpolated, specify a data point for packet drop probability in the range 0–100.
- Predefined parameter:
 - fwEnterpriseMaxPriority
 - fwEnterpriseMinPriority
 - fwMaxPriority
 - fwMinPriority
- Parameter of type percent

Default— No value

`<drop-profile-type>`— Relationship between the queue threshold (fill level) and drop probability.

Value— One of the following:

- Predefined global parameter:
 - interpolated—Specifies values for interpolating relationship between queue fill level and drop probability
 - segmented—Specifies fill level and drop probability

as percentages

- Parameter of type dropProfileType

Default— No value

<queue-threshold>— Fill level of the queue.

Value— One of the following:

- If the drop profile type is segmented, specify how full the queue is as a percentage.
- If the drop profile type is interpolated, specify a data point for mapping the queue fill percentage in the range 0–100.
- Parameter of type percent

Default— No value

Required Privilege Level

service

<service-class-name> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <service-class-name>
            <name>name</name> <!-- identifier -->
            <service-class-name>service-class-name</service-class-name>
            <description>description</description>
          </service-class-name>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service class name action. You can configure service class name actions for PCMM policy rules.

Contents

<name>— Name of the service class name action.

Value— Text

<service-class-name>—(Optional) Name of a service class on the CMTS device that specifies QoS parameters for a service flow.

Value— One of the following:

- Name of a service class
- String expression
- Parameter of type serviceClassName

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<stateful-firewall> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <stateful-firewall>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </stateful-firewall>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a stateful firewall action. Stateful firewall actions specify the action to take on packets that match the classify-traffic condition. You can configure stateful firewall actions for JUNOS ASP policy rules.

Contents

<name>— Name for the stateful firewall action.

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<filter> (configuration/policies/group/list/rule/stateful-firewall/ packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <stateful-firewall>
            <packet-action>
              <filter>
              </filter>
            </packet-action>
          </stateful-firewall>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Set the packet action for a stateful firewall to filter. The packet is not accepted and is not processed further.

Contents

Required Privilege Level

service

<forward> (configuration/policies/group/list/rule/stateful-firewall/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <stateful-firewall>
            <packet-action>
              <forward>
            </forward>
          </packet-action>
        </stateful-firewall>
      </rule>
    </list>
  </group>
</policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Set the packet action for a stateful firewall to forward.

Contents

Required Privilege Level

service

<parameter> (configuration/policies/group/list/rule/stateful-firewall/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <stateful-firewall>
            <packet-action>
              <parameter>
                <action>action</action>
              </parameter>
            </packet-action>
          </stateful-firewall>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Set the packet action for a stateful firewall to parameter. The action specified in the parameter is applied.

Contents

<action>—(Optional) Parameter that specifies the action to take on traffic.

Value— Parameter of type packetOperation.

Default— No value

Required Privilege Level

service

<reject> (configuration/policies/group/list/rule/stateful-firewall/packet-action)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <stateful-firewall>
            <packet-action>
              <reject>
                <message-type>message-type</message-type>
              </reject>
            </packet-action>
          </stateful-firewall>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Set the action for a stateful firewall to reject. The packet is not accepted, and a rejection message is returned; UDP sends an ICMP unreachable code, and TCP sends RST Reject action in stateful firewall.

Contents

<message-type>—(Optional) Type of ICMP destination unreachable message sent to the client.

Value— One of the following:

- String expression that matches a type of ICMP destination unreachable message supported on the router; for example:
 - "administratively-prohibited"
 - "bad-host-tos"
 - "bad-network-tos"
 - "host-prohibited"
 - "host-unknown"
 - "host-unreachable"

- "network-prohibited"
- "network-unknown"
- "network-unreachable"
- "port-unreachable"
- "precedence-cutoff"
- "precedence-violation"
- "protocol-unreachable"
- "source-host-isolated"
- "source-route-failed"
- "tcp-reset"—If you specify tcp-reset, a TCP reset message is sent if the packet is a TCP packet. Otherwise, nothing is sent.
- Parameter of type messageType

Default— No value

Required Privilege Level

service

<template-activation> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <template-activation>
            <name>name</name> <!-- identifier -->
            <template-name>template-name</template-name>
            <description>description</description>
          </template-activation>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a template activation action. Use this action for CoA supporting devices.

Contents

<name>— Name for the template activation action.

Value— Text

<template-name>—

Value—

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<variable> (configuration/policies/group/list/rule/template-activation)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <template-activation>
            <variables>
              <variable>
                <name>name</name> <!-- identifier -->
                <value>value</value>
                <type>type</type>
              </variable>
            </variables>
          </template-activation>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Contents

<name>—

Value— Text

<value>—(Optional) Provide a value for a variable.

Value—

Default— No value

<type>—(Optional) The variable type determines where you can use the variable.

Value— See the policy documentation in the *SRC-PE Services and Policies Guide* for a list of parameter types, where each type of parameter

is used, and what each parameter is used to specify. Variable types are mapped to parameters types.

Default— No value

Required Privilege Level

service

<traffic-class> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-class>
            <name>name</name> <!-- identifier -->
            <traffic-class>traffic-class</traffic-class>
            <description>description</description>
          </traffic-class>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a traffic-class action. Use this action to put packets in a particular traffic class. You can configure traffic-class actions for JUNOS policy rules.

Contents

<name>— Name for the traffic-class action.

Value— Text

<traffic-class>— Name of the traffic-class profile that is applied to a packet when it passes through the router.

Value— One of the following:

- Name of a traffic-class profile that is configured on the router
- Parameter of type trafficClassSpec

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<traffic-condition> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <name>name</name> <!-- identifier -->
            <match-direction>match-direction</match-direction>
            <description>description</description>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a classify-traffic condition. A classify-traffic condition contains values or fields that a packet must contain. If a policy rule does not contain a match condition, all packets are considered to match.

You can create classify-traffic conditions in JUNOS policy rules, in JUNOS ASP and JUNOS filter policy rules, and in PCMM policy rules.

Contents

<name>— Name for the classify-traffic condition.

Value— Text

<match-direction>—(Optional) Applies only to JUNOS ASP policy rules. Matches packets based on the direction of the packet flow. For stateful firewall actions, this value is used in place of the **policies group list name applicability** statement.

Value— One of the following:

- input

- output
- both (Both is invalid for NAT actions.)
- String expression
- Parameter of type matchDirection

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<application-protocol-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <application-protocol-condition>
              <name>name</name> <!-- identifier -->
              <protocol>protocol</protocol>
              <application-protocol>application-protocol</application-
protocol>
              <idle-timeout>idle-timeout</idle-timeout>
              <dce-rpc-uuid>dce-rpc-uuid</dce-rpc-uuid>
              <rpc-program-number>rpc-program-number</rpc-program-number>
              <snmp-command>snmp-command</snmp-command>
              <ttl-threshold>ttl-threshold</ttl-threshold>
            </application-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure application protocols for stateful firewall and NAT services to use in match condition rules. An application protocol defines application parameters by using information from network layer 3 and above. Examples of such applications are FTP and H.323.

Contents

<name>— Name for the application protocol condition.

Value— Text

<protocol>—(Optional) Protocol matched by this classifier list.

Value— One of the following:

- Predefined parameter of type protocol
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression

Default— No value

<application-protocol>—(Optional) Application protocol to match.

Value— One of the following:

- Predefined global parameter:
 - bootp—BOOTP protocol
 - dce_rpc—DCE RPC protocol
 - dce_rpc_portmap—DCE RPC portmap
 - dns—DNS protocol
 - exec—Exec protocol
 - ftp—FTP protocol
 - h323—H.323 protocol
 - icmp_app—ICMP protocol
 - iiop—Internet Inter-ORB Protocol, a TCP protocol
 - netbios—NetBIOS protocol
 - netshow—NetShow protocol
 - realaudio—RealAudio protocol
 - rpc—RPC UDP or TCP protocols
 - rpc_portmap—RPC portmap protocol
 - rtsp—Real-Time Streaming Protocol
 - shell—Shell protocol
 - snmp—SNMP protocol
 - sqlnet—SQLNet protocol
 - tftp—Trivial File Transfer Protocol
 - traceroute—Traceroute protocol
 - winframe—WinFrame protocol
- String expression that matches an application protocol name supported on the router
- Map expression—You can use a map expression to define multiple attributes with one command. Maps are a list of attributeName = value pairs separated by commas and enclosed in curly brackets.

For example, the map { applicationProtocol = "ftp", sourcePort = 123, inactivityTimeout = 60 } supplies the application protocol, source port, and inactivity timeout in one

command. Another map {applicationProtocol = "tcp", inactivityTimeout = 60, destinationPort = 80} supplies the protocol, inactivity timeout, and destination port.

- Parameter of type applicationProtocol—You can add a map expression as the default value of the parameter.

Default— No value

`<idle-timeout>`—(Optional) Length of time the application is inactive before it times out.

Value— One of the following:

- Number of seconds in the range 4–65535
- Numeric expression
- Parameter of type timeout

Default— Unspecified; the router's default value is used

`<dce-rpc-uuid>`—(Optional) For the DCE RPC application protocol, specifies the universal unique identifier (UUID). For information about UUIDs, see <http://www.opengroup.org/onlinepubs/9629399/apdx.htm>.

Value— One of the following:

- Hex digits in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Numeric expression
- Parameter of type dceRpcUuid

Default— dceRpcUuid

`<rpc-program-number>`—(Optional) For the remote procedure call (RPC) application protocol, specifies an RPC program number.

Value— One of the following:

- Integer—RPC or DCE program number in the range 100000–400000
- Numeric expression
- Parameter of type rpcProgramNumber

Default— No value

`<snmp-command>`—(Optional) SNMP command for packet matching.

Value— One of the following:

- Predefined parameter:
 - `get`
 - `get_next`
 - `set`
 - `trap`
- String expression that matches an SNMP command supported on the router
- Parameter of type `snmpCommand`

Default— No value

`<t1-threshold>`—(Optional) For the traceroute application protocol, specifies the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.

Value— One of the following:

- Integer in the range 0–255
- Numeric expression
- Parameter of type `traceRouteTtlThreshold`

Default— No value

Required Privilege Level

service

<proto-attr> (configuration/policies/group/list/rule/traffic-condition/application-protocol-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <application-protocol-condition>
              <proto-attr>
                <icmp-type>icmp-type</icmp-type>
                <icmp-code>icmp-code</icmp-code>
              </proto-attr>
            </application-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure ICMP packet type and code.

Contents

<icmp-type>—(Optional) ICMP packet type.

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP packet type supported on the router
- Numeric expression
- Parameter of type icmpType

Default— No value

`<icmp-code>`—(Optional) ICMP code

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP code supported on the router
- Numeric expression
- Parameter of type icmpCode

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/application-protocol-condition/proto-attr/destination-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <application-protocol-condition>
              <proto-attr>
                <destination-port>
                  <port>
                    <from-port>from-port</from-port>
                  </port>
                </destination-port>
              </proto-attr>
            </application-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching destination ports.

Contents

<from-port>—(Optional) Destination port

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/application-protocol-condition/proto-attr/source-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <application-protocol-condition>
              <proto-attr>
                <source-port>
                  <port>
                    <from-port>from-port</from-port>
                  </port>
                </source-port>
              </proto-attr>
            </application-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching source ports.

Contents

<from-port>—(Optional) Source port

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Default— No value

Required Privilege Level

service

<group-network> (configuration/policies/group/list/rule/traffic-condition/destination-network)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <destination-network>
              <group-network>
                <network-specifier>network-specifier</network-specifier>
              </group-network>
            </destination-network>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify the destination network to match using a network specifier. For JUNOS ASP and JUNOSe IPv6 policy rules, you must specify destination networks in the network specifier format.

Contents

<network-specifier>—(Optional) Specifies an IP address and mask.

Value— Specify the subnet in one of the following formats:

- [not] < address > / < mask > or < address > / < prefix length >
 - Include *not* to indicate that the condition matches every address that is not in the specified subnet.
 - < prefix length > is a number in the range 0–32, and specifies how many of the first bits in the address specify the network
- For JUNOS ASP policies, you must enter network in the format:
 - < address > / < prefix length >

Default— No value

Required Privilege Level

service

<network> (configuration/policies/group/list/rule/traffic-condition/destination-network)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <destination-network>
              <network>
                <ip-address>ip-address</ip-address>
                <ip-mask>ip-mask</ip-mask>
                <ip-operation>ip-operation</ip-operation>
              </network>
            </destination-network>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify the destination network in IP address and mask format. You also use this statement to specify whether the software matches or does not match the IP address and mask.

Contents

<ip-address>—(Optional) IP address of the source or destination network or host.

Value— One of the following:

- IP address
- Predefined global parameter:
 - gateway_ipAddress—IP address of the gateway as specified by the service object
 - interface_ipAddress—IP address of the router interface
 - service_ipAddress—IP address of the service as

- specified by the service object
 - user_ipAddress—IP address of the subscriber
 - virtual_ipAddress—Virtual portal address of the SAE that is used in redundant redirect server installations
- Expression—For NAT actions, you can enter a range of addresses; for example, 10.10.13.1..10.10.13.100
- Parameter of type address

Default— 0.0.0.0

<ip-mask>—(Optional) IP address mask applied to the IP address.

Value— One of the following:

- IP address mask
- Predefined global parameter:
 - interface_ipMask—IP mask of the interface
 - service_ipMask—IP mask of the service as specified by the service object
 - user_ipMask—IP mask of the subscriber
- Parameter of type addressMask

Default— 255.255.255.255

<ip-operation>—(Optional) Matches packets with an IP address and mask that either is equal or is not equal to the specified address and mask.

Value— One of the following:

- is—Matches the specified IP address and mask
- is_not—Matches any IP address and mask except the specified address and mask
- Parameter of type networkOperation

Default— is

Required Privilege Level

service

<icmp-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <icmp-condition>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
              <icmp-type>icmp-type</icmp-type>
              <icmp-code>icmp-code</icmp-code>
            </icmp-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for the ICMP protocol.

<protocol>— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression

- Parameter of type protocol

Default— No value

<protocol-operation>—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - is—Matches packets that are equal to the specified protocol
 - is_not—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, is_not is not a valid option.
- Boolean expression:
 - 1—is
 - 0—is_not
- Parameter of type protocolOperation

Default— 1

<ip-flags>—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type ipFlags

Default— 0

<ip-flags-mask>—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type ipFlagsMask

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOS routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type fragOffset

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

`<icmp-type>`—(Optional) Matches ICMP packet type.

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP packet type supported on the router or CMTS device
- Numeric expression
- Parameter of type icmpType

Default— 255

`<icmp-code>`—(Optional) Matches ICMP code

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP code supported on the router or CMTS device
- Numeric expression
- Parameter of type icmpCode

Default— 255

Required Privilege Level

service

<igmp-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <igmp-condition>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
              <igmp-type>igmp-type</igmp-type>
            </igmp-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for the IGMP protocol.

<protocol>— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression
- Parameter of type protocol

Default— No value

`<protocol-operation>`—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - `is`—Matches packets that are equal to the specified protocol
 - `is_not`—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, `is_not` is not a valid option.
- Boolean expression:
 - `1`—`is`
 - `0`—`is_not`
- Parameter of type `protocolOperation`

Default— 1

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type `ipFlags`

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type `ipFlagsMask`

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOS routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type fragOffset

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

`<igmp-type>`—(Optional) IGMP packets that can be filtered by IGMP packet type or message name.

Value— One of the following:

- Integer in the range 1–255
- Numeric expression
- Parameter of type igmpType

Default— 255

Required Privilege Level

service

<ipsec-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <ipsec-condition>
              <spi>spi</spi>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
            </ipsec-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for the IPSec protocol.

Contents

<spi>—(Optional) For IPSec classifiers, specifies the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI). This option appears only in JUNOS policy rules.

Value— One of the following:

- Integer in the range 0–255
- Parameter of type ipSecSpi

Default— No value

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type `ipFlags`

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type `ipFlagsMask`

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOSe routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type `fragOffset`

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

<protocol>— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression
- Parameter of type protocol

Default— No value

<protocol-operation>—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - is—Matches packets that are equal to the specified protocol
 - is_not—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, is_not is not a valid option.
- Boolean expression:
 - 1—is
 - 0—is_not
- Parameter of type protocolOperation

Default— 1

Required Privilege Level

service

<parameter-protocol-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <parameter-protocol-condition>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <tcp-flags>tcp-flags</tcp-flags>
              <tcp-flags-mask>tcp-flags-mask</tcp-flags-mask>
              <spi>spi</spi>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
            </parameter-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure protocol conditions that contain a parameter value for the protocol.

Contents

<protocol>— Parameter that is used to determine the protocol that this classifier matches.

Value— Parameter of type protocol. You must enter a parameter that has been created and has been committed.

Default— No value

`<protocol-operation>`—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - `is`—Matches packets that are equal to the specified protocol
 - `is_not`—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, `is_not` is not a valid option.
- Boolean expression:
 - `1`—`is`
 - `0`—`is_not`
- Parameter of type `protocolOperation`

Default— 1

`<tcp-flags>`—(Optional) Value of the TCP flags field in the IP header.

Value— One of the following:

- Integer in the range 0–63
- Numeric expression
- Parameter of type `tcpFlags`

Default— 0

`<tcp-flags-mask>`—(Optional) Mask associated with TCP flags.

Value— One of the following:

- Integer in the range 0–63
- Numeric expression
- Parameter of type `tcpFlagsMask`

Default— 0

`<spi>`—(Optional) For IPSec classifiers, specifies the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI). This option appears only in JUNOS policy rules.

Value— One of the following:

- Integer in the range 0–255
- Parameter of type ipSecSpi

Default— No value

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type ipFlags

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type ipFlagsMask

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOS routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type fragOffset

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type `packetLength`

Default— No value

Required Privilege Level

service

<proto-attr> (configuration/policies/group/list/rule/traffic-condition/parameter-protocol-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <parameter-protocol-condition>
              <proto-attr>
                <icmp-type>icmp-type</icmp-type>
                <icmp-code>icmp-code</icmp-code>
                <igmp-type>igmp-type</igmp-type>
              </proto-attr>
            </parameter-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure ICMP packet type and code and IGMP type.

Contents

<icmp-type>—(Optional) ICMP packet type

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP packet type supported on the router
- Numeric expression
- Parameter of type icmpType

Default— No value

`<icmp-code>`—(Optional) ICMP code

Value— One of the following:

- Integer in the range 0–255 that represents an ICMP code supported on the router
- Numeric expression
- Parameter of type icmpCode

Default— No value

`<igmp-type>`—(Optional) IGMP packets that can be filtered by IGMP packet type or message name.

Value— One of the following:

- Integer in the range 1–255
- Numeric expression
- Parameter of type igmpType

Default— 255

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/parameter-protocol-condition/proto-attr/destination-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <parameter-protocol-condition>
              <proto-attr>
                <destination-port>
                  <port>
                    <port-operation>port-operation</port-operation>
                    <from-port>from-port</from-port>
                  </port>
                </destination-port>
              </proto-attr>
            </parameter-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain

the specified port number

- String
- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/parameter-protocol-condition/proto-attr/source-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <parameter-protocol-condition>
              <proto-attr>
                <source-port>
                  <port>
                    <port-operation>port-operation</port-operation>
                    <from-port>from-port</from-port>
                  </port>
                </source-port>
              </proto-attr>
            </parameter-protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain

the specified port number

- String
- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<protocol-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <protocol-condition>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
            </protocol-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure protocol conditions that do not include port conditions.

<protocol>— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression
- Parameter of type protocol

Default— No value

`<protocol-operation>`—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - `is`—Matches packets that are equal to the specified protocol
 - `is_not`—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, `is_not` is not a valid option.
- Boolean expression:
 - `1`—`is`
 - `0`—`is_not`
- Parameter of type `protocolOperation`

Default— 1

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type `ipFlags`

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type `ipFlagsMask`

Default— 0

<fragment-offset>—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOSe routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type fragOffset

Default— No value

<packet-length>—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

Required Privilege Level

service

<protocol-port-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <protocol-port-condition>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
            </protocol-port-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for protocols and ports.

<protocol>— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression
- Parameter of type protocol

Default— No value

`<protocol-operation>`—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - `is`—Matches packets that are equal to the specified protocol
 - `is_not`—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, `is_not` is not a valid option.
- Boolean expression:
 - `1`—`is`
 - `0`—`is_not`
- Parameter of type `protocolOperation`

Default— 1

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type `ipFlags`

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type `ipFlagsMask`

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOSe routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type fragOffset

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/protocol-port-condition/destination-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <protocol-port-condition>
              <destination-port>
                <port>
                  <port-operation>port-operation</port-operation>
                  <from-port>from-port</from-port>
                </port>
              </destination-port>
            </protocol-port-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain the specified port number
- String

- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/protocol-port-condition/source-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <protocol-port-condition>
              <source-port>
                <port>
                  <port-operation>port-operation</port-operation>
                  <from-port>from-port</from-port>
                </port>
              </source-port>
            </protocol-port-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain the specified port number
- String

- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<group-network> (configuration/policies/group/list/rule/traffic-condition/source-network)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <source-network>
              <group-network>
                <network-specifier>network-specifier</network-specifier>
              </group-network>
            </source-network>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify the source network to match using a network specifier. For JUNOS ASP and JUNOSe IPv6 policy rules, you must specify source networks in the network specifier format.

Contents

<network-specifier>—(Optional) Specifies an IP address and mask.

Value— Specify the subnet in one of the following formats:

- [not] < address > / < mask > or < address > / < prefix length >
 - Include *not* to indicate that the condition matches every address that is not in the specified subnet.
 - < prefix length > is a number in the range 0–32, and specifies how many of the first bits in the address specify the network
- For JUNOS ASP policies, you must enter network in the format:
 - < address > / < prefix length >

Default— No value

Required Privilege Level

service

<network> (configuration/policies/group/list/rule/traffic-condition/source-network)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <source-network>
              <network>
                <ip-address>ip-address</ip-address>
                <ip-mask>ip-mask</ip-mask>
                <ip-operation>ip-operation</ip-operation>
              </network>
            </source-network>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify the source network in IP address and mask format. You also use this statement to specify whether the software matches or does not match the IP address and mask.

Contents

<ip-address>—(Optional) IP address of the source or destination network or host.

Value— One of the following:

- IP address
- Predefined global parameter:
 - gateway_ipAddress—IP address of the gateway as specified by the service object
 - interface_ipAddress—IP address of the router interface
 - service_ipAddress—IP address of the service as

- specified by the service object
 - user_ipAddress—IP address of the subscriber
 - virtual_ipAddress—Virtual portal address of the SAE that is used in redundant redirect server installations
- Expression—For NAT actions, you can enter a range of addresses; for example, 10.10.13.1..10.10.13.100
- Parameter of type address

Default— 0.0.0.0

<ip-mask>—(Optional) IP address mask applied to the IP address.

Value— One of the following:

- IP address mask
- Predefined global parameter:
 - interface_ipMask—IP mask of the interface
 - service_ipMask—IP mask of the service as specified by the service object
 - user_ipMask—IP mask of the subscriber
- Parameter of type addressMask

Default— 255.255.255.255

<ip-operation>—(Optional) Matches packets with an IP address and mask that either is equal or is not equal to the specified address and mask.

Value— One of the following:

- is—Matches the specified IP address and mask
- is_not—Matches any IP address and mask except the specified address and mask
- Parameter of type networkOperation

Default— is

Required Privilege Level

service

<tcp-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <tcp-condition>
              <tcp-flags>tcp-flags</tcp-flags>
              <tcp-flags-mask>tcp-flags-mask</tcp-flags-mask>
              <protocol>protocol</protocol>
              <protocol-operation>protocol-operation</protocol-operation>
              <ip-flags>ip-flags</ip-flags>
              <ip-flags-mask>ip-flags-mask</ip-flags-mask>
              <fragment-offset>fragment-offset</fragment-offset>
              <packet-length>packet-length</packet-length>
            </tcp-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for the TCP protocol.

Contents

<tcp-flags>—(Optional) Value of the TCP flags field in the IP header.

Value— One of the following:

- Integer in the range 0–63
- Numeric expression
- Parameter of type tcpFlags

Default— 0

`<tcp-flags-mask>`—(Optional) Mask associated with TCP flags.

Value— One of the following:

- Integer in the range 0–63
- Numeric expression
- Parameter of type `tcpFlagsMask`

Default— 0

`<protocol>`— Protocol matched by this classifier list.

Value— One of the following:

- Predefined global parameter—Use a ? at the command line to see a list of valid protocols.
- Protocol number in the range 0–257
- For PCMM classifiers, there are two special protocol values:
 - 256 matches traffic that has any IP protocol value
 - 257 matches both TCP and UDP traffic
- String expression
- Parameter of type `protocol`

Default— No value

`<protocol-operation>`—(Optional) Matches packets with the protocol that is either equal or not equal to the specified protocol.

Value— One of the following:

- Predefined global parameter:
 - `is`—Matches packets that are equal to the specified protocol
 - `is_not`—Matches any packets except those that are equal to the specified protocol. If you are configuring an ICMP, IGMP, IPSec, or TCP classifier, `is_not` is not a valid option.
- Boolean expression:
 - 1—`is`
 - 0—`is_not`
- Parameter of type `protocolOperation`

Default— 1

`<ip-flags>`—(Optional) Value of the IP flags field in the IP header.

Value— One of the following:

- 0—Reserved
- 1—Do not fragment
- 2—More fragments
- Numeric expression
- Parameter of type `ipFlags`

Default— 0

`<ip-flags-mask>`—(Optional) Mask that is associated with the IP flag.

Value— One of the following:

- Integer in the range 0–7
- Numeric expression
- Parameter of type `ipFlagsMask`

Default— 0

`<fragment-offset>`—(Optional) Value of the fragment offset field.

Value— One of the following:

- For JUNOSe routers:
 - 0—Equal to 0
 - 1—Equal to 1
 - 2..8191
- For JUNOS routing platforms, integer in the range 0–8191
- Numeric expression
- Parameter of type `fragOffset`

Default— No value

`<packet-length>`—(Optional) Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation

overhead. This option is available only in JUNOS policy rules.

Value— One of the following:

- Number of bytes; all positive numbers and 0 are valid
- Parameter of type packetLength

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/tcp-condition/destination-port)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <tcp-condition>
              <destination-port>
                <port>
                  <port-operation>port-operation</port-operation>
                  <from-port>from-port</from-port>
                </port>
              </destination-port>
            </tcp-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain the specified port number
- String

- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<port> (configuration/policies/group/list/rule/traffic-condition/tcp-condition/source-port)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <tcp-condition>
              <source-port>
                <port>
                  <port-operation>port-operation</port-operation>
                  <from-port>from-port</from-port>
                </port>
              </source-port>
            </tcp-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure matching conditions for ports.

Contents

<port-operation>—(Optional) Matches packets with a port that is either equal or not equal to the specified port.

Value— One of the following:

- Predefined global parameter:
 - eq—Matches packets that contain the specified port number
 - neq—Matches any packet except those that contain the specified port number
- String

- Parameter of type portOperation

Default— No value

<from-port>—(Optional) Source or destination port.

Value— One of the following:

- service_port—A predefined global parameter that is the port of the service as specified by the service object
- Integer in the range 0–65535
- Expression—A range of port numbers; for example, 10..20
- Parameter of type port

Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

One of the following:

- To set a range of ports that is greater than 10, use 11..65535.
- To set a range of ports that is less than 200, use 0..199.

Note that PCMM IO2 classifiers do not support port ranges. If you are using PCMM IO2 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.

PCMM IO3 classifiers do support port ranges.

Default— No value

Required Privilege Level

service

<tos> (configuration/policies/group/list/rule/traffic-condition)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <tos>
              <tos-byte>tos-byte</tos-byte>
              <tos-byte-mask>tos-byte-mask</tos-byte-mask>
            </tos>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a particular traffic flow to the service's network for the DA IP field in the IP packet. The CoS feature on JUNOS routing platforms supports DiffServ as well as six-bit IP header ToS byte settings. The DiffServ protocol uses the ToS byte in the IP header. The most significant six bits of this byte form the Differentiated Services code point (DSCP). The CoS feature uses DSCPs to determine the forwarding class associated with each packet. It also uses the ToS byte and ToS byte mask to determine IP precedence.

<tos-byte>—(Optional) For IPv4 packets, matches the value of the ToS field in the IP packet header. For IPv6 packets, matches the traffic-class field in the IP packet header.

Value— One of the following:

- Integer in the range 0–255; uses whole 8 bits of the ToS byte
- Numeric expression
- Parameter of type tosByte

Default— 0

<tos-byte-mask>—(Optional) Mask associated with the ToS byte.

Value— One of the following:

- Integer values of 224, 252, 255 for JUNOS; values of 224, 252 for JUNOS

For IPv4:

- 255 (tos)—Specifies the use of the whole 8 bits of the ToS byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the ToS byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the ToS byte; tos-byte range is 0–7.

For IPv6:

- 255 (tcfield)—Specifies the use of the whole 8 bits of the traffic-class byte; tos-byte range is 0–255.
- 252 (dsfield)—Specifies the use of the upper 6 bits of the traffic-class byte; tos-byte range is 0–63.
- 224 (precedence)—Specifies the use of the upper 3 bits of the traffic-class byte; tos-byte range is 0–7.
- Numeric expression
- Parameter of type tosByteMask

Default— 0

Required Privilege Level

service

<traffic-match-condition> (configuration/policies/group/list/rule/traffic-condition)

Usage

```

<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-condition>
            <traffic-match-condition>
              <forwarding-class>forwarding-class</forwarding-class>
              <interface-group>interface-group</interface-group>
              <source-class>source-class</source-class>
              <destination-class>destination-class</destination-class>
              <allow-ip-options>allow-ip-options</allow-ip-options>
              <traffic-class>traffic-class</traffic-class>
              <color>color</color>
              <user-packet-class>user-packet-class</user-packet-class>
              <destination-local-interface>destination-local-interface</
destination-local-interface>
            </traffic-match-condition>
          </traffic-condition>
        </rule>
      </list>
    </group>
  </policies>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions for a classify-traffic condition.

Contents

<forwarding-class>—(Optional) Matches packets based on the name of a forwarding class

Value— One of the following:

- String expression that matches a forwarding class on the

router; for example, "assured-forwarding," "best-effort,"
"expedited-forwarding," or "network-control"

- Parameter of type forwardingClass
- Predefined runtime parameter: fc_assured, fc_besteffort, fc_expedited

Default— No value

<interface-group>—(Optional) Matches packets based on the interface group on which the packet was received.

Value— One of the following:

- Integer in the range 0–4294967295
- Numeric expression
- Parameter of type interfaceGroup

Default— No value

<source-class>—(Optional) Matches packets based on source class. For JUNOS filter policies, a source class is a set of source prefixes grouped together and given a class name. You would usually match source and destination classes for output firewall filters. Note that you cannot match on both source class and destination class at the same time. You must choose one or the other. For JUNOSe policies, a source class classifies on packets associated with a route class based on the packet's source address.

Value— One of the following:

- For JUNOS policies, string expression that matches a source class that is configured on the router; for example, "gold-class"
- For JUNOSe policies, route-class in the range 0-255.
- Parameter of type trafficClassSpec

Default— No value

<destination-class>—(Optional) Matches packets based on destination class. For JUNOS filter policies, a destination class is a set of destination prefixes grouped together and given a class name. You would usually match source and destination classes for output firewall filters. Note that you cannot match on both source class and destination class at the same time. You must choose one or the other. For JUNOSe policies, a destination class classifies on packets associated with a route class based on the packet's destination address.

Value— One of the following:

- For JUNOS policies, string expression that matches a destination class that is configured on the router; for example, "gold-class"
- For JUNOSe policies, route-class in the range 0-255.
- Parameter of type trafficClassSpec

Default— No value

<allow-ip-options>—(Optional) Matches on IP options.

Value— One of the following:

- Numeric value of the IP option
- String expression that matches a text synonym of an IP option on the router; for example, "loose-source-route," "record-route," "router-alert," "strict-source-route," or "timestamp"
- Parameter of type allowIpOptions

Default— No value

<traffic-class>—(Optional) Matches packets based on traffic class.

Value—Text

Default— No value

<color>—(Optional) Matches packets based on packet color. Matches packets based on packet color for JUNOSe policy rules.

Value— One of the following:

- Integer in the range 1–3
 - 1—green
 - 2—yellow
 - 3—red
- Parameter of type color

One of the following:

- Integer in the range 1–3
 - 1—green
 - 2—yellow
 - 3—red
- Parameter of type color

Default— No value No value

`<user-packet-class>`—(Optional) Matches packets based on the user packet class action number.

Value— One of the following:

- Integer in the range 0–15
- Parameter of type `userPacketClass`

Default— No value

`<destination-local-interface>`—(Optional) Matches packets based on whether the destination interface is local.

Value—Text

Default— No value

Required Privilege Level

service

<traffic-mirror> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-mirror>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </traffic-mirror>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a traffic-mirror action. Use this action to mirror traffic from a destination to a source or from a source to a destination. You can configure traffic-mirror actions for JUNOS input policy rules.

Before you use traffic-mirror actions, you must configure forwarding options on JUNOS routing platforms for port mirroring and next-hop group. For information about these features, see the *JUNOS Policy Framework Configuration Guide*.

The policy rule that contains a traffic-mirror action must comply with these conditions:

- It must be combined with forward actions in the same rule. One of the forward actions must accept the traffic if the source and/or destination IP addresses do not match the conditions.
- It contains either no classify-traffic condition or only one classify-traffic condition.
- It can be marked for accounting.

Contents

<name>— Name of the traffic-mirror action.

Value— Text

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<traffic-shape> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <traffic-shape>
            <name>name</name> <!-- identifier -->
            <rate>rate</rate>
            <description>description</description>
          </traffic-shape>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a traffic-shape action. Traffic-shape actions specify the maximum rate of traffic transmitted on an interface. You can create traffic-shape actions in JUNOS shaping policy rules.

Contents

<name>— Name of the traffic-shape action.

Value— Text

<rate>—(Optional) Maximum transmission rate.

Value— One of the following:

- Predefined global parameter interface_speed—Speed of the subscriber's router interface
- Bits per second in the range 1000–32000000000
- Numeric expression
- Parameter of type rate

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<user-packet-class> (configuration/policies/group/list/rule)

Usage

```
<configuration>
  <policies>
    <group>
      <list>
        <rule>
          <user-packet-class>
            <name>name</name> <!-- identifier -->
            <user-packet-class>user-packet-class</user-packet-class>
            <description>description</description>
          </user-packet-class>
        </rule>
      </list>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a user packet class action. Use this action to put packets in a particular user packet class. You can configure user packet class actions for JUNOS policy rules.

Contents

<name>— Name for the user packet class action.

Value— Text

<user-packet-class>—(Optional) User packet class that is applied to a packet when it passes through the router.

Value— One of the following:

- Integer in the range 0–15
- Parameter of type userPacketClass

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value—Text

Default— No value

Required Privilege Level

service

<parameter> (configuration/policies/group/local-parameters)

Usage

```
<configuration>
  <policies>
    <group>
      <local-parameters>
        <parameter>
          <name>name</name> <!-- identifier -->
          <description>description</description>
          <default-value>default-value</default-value>
          <type>type</type>
        </parameter>
      </local-parameters>
    </group>
  </policies>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a local parameter. Local parameters are available only for the policy group in which the parameter is defined.

Contents

<name>— Name of the parameter

Value— Text

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

<default-value>—(Optional) Value that the policy engine uses if no other values are provided during the parameter value acquisition process. If other values are provided to the policy engine but problems are encountered, the default value for the parameter is not used. The policy engine generates an error message.

Value— Valid value for the parameter type. See the policy documentation in the *SRC-PE Services and Policies Guide* for valid values for each parameter type.

Default— No value

`<type>`—(Optional) Type of attribute for which you can use the parameter. The parameter type determines where you can use the parameter.

Value— See the policy documentation in the *SRC-PE Services and Policies Guide* for a list of parameter types, where each type of parameter is used, and what each parameter is used to specify.

Default— No value

Required Privilege Level

service

Subscriber Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for configuring subscribers. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
subscribers retailer	<u>< retailer ></u>
subscribers retailer name info	<u>< info ></u>
subscribers retailer name manager	<u>< manager ></u>
subscribers retailer name schedule	<u>< schedule ></u>
subscribers retailer name schedule name event	<u>< event ></u>
subscribers retailer name schedule name event name action	<u>< action ></u>
subscribers retailer name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name schedule name event name except	<u>< except ></u>
subscribers retailer name schedule name event name except name from	<u>< from ></u>
subscribers retailer name schedule name event name except name to	<u>< to ></u>
subscribers retailer name schedule name event name from	<u>< from ></u>
subscribers retailer name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder	<u>< subscriber-folder ></u>
subscribers retailer name subscriber-folder folder-name device	<u>< device ></u>
subscribers retailer name subscriber-folder folder-name device device-name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name action	<u>< action ></u>

subscribers retailer name subscriber-folder folder-name device device-name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name device device-name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name device device-name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise	<u>< enterprise ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access	<u>< access ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name admission-control	<u>< admission-control ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name except name to	<u>< to ></u>

subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name access name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device	<u>< device ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name device device-name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name info	<u>< info ></u>
subscribers retailer name subscriber-folder folder-name enterprise name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule	<u>< schedule ></u>

subscribers retailer name subscriber-folder folder-name enterprise name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site	<u>< site ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access	<u>< access ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name admission-control	<u>< admission-control ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name except name from	<u>< from ></u>

subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name access name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device	<u>< device ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name device device-name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name manager	<u>< manager ></u>

subscribers retailer name subscriber-folder folder-name enterprise name site name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name enterprise name site name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name enterprise name vpn	<u>< vpn ></u>
subscribers retailer name subscriber-folder folder-name manager	<u>< manager ></u>
subscribers retailer name subscriber-folder folder-name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name except name from	<u>< from ></u>

subscribers retailer name subscriber-folder folder-name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name subscriber	<u>< subscriber ></u>
subscribers retailer name subscriber-folder folder-name subscriber name admission-control	<u>< admission-control ></u>
subscribers retailer name subscriber-folder folder-name subscriber name info	<u>< info ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule	<u>< schedule ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event	<u>< event ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name action	<u>< action ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name action name attribute	<u>< attribute ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name except	<u>< except ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name except name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name except name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name from	<u>< from ></u>
subscribers retailer name subscriber-folder folder-name subscriber name schedule name event name to	<u>< to ></u>
subscribers retailer name subscriber-folder folder-name subscriber name subscription	<u>< subscription ></u>
subscribers retailer name subscriber-folder folder-name subscription	<u>< subscription ></u>
subscribers retailer name subscription	<u>< subscription ></u>
subscribers retailer name vpn	<u>< vpn ></u>

<retailer> (configuration/subscribers)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <name>name</name> <!-- identifier -->
      <domain-name>domain-name</domain-name>
      <authentication-plugin-in>authentication-plugin-in</authentication-plugin-in>
      <dhcp-authentication-plugin-in>dhcp-authentication-plugin-in</dhcp-
authentication-plugin-in>
      <tracking-plugin-in>tracking-plugin-in</tracking-plugin-in>
      <maximum-login>maximum-login</maximum-login>
      <session-timeout>session-timeout</session-timeout>
      <scope>scope</scope>
      <imported-extranet>imported-extranet</imported-extranet>
      <substitution>substitution</substitution>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a retailer subscriber.

Contents

<name>— Name of the retailer.

Value— Text

<domain-name>—(Multivalue) Domain names associated with the retailer.

Value— Domain name in the format domainName.domainExtension.
For example: virneo.com.

Default— No value

<authentication-plugin-in>—(Optional) (Multivalue) Single authentication plug-in or

a list of plug-ins used to authenticate subscribers who log in to the domains specified for this retailer. If you do not specify a plug-in for the retailer, the SAE uses the default retailer authentication plug-in.

Value— Single authentication plug-in or a list of plug-ins

Default— No value

`<dhcp-authentication-plug-in>`—(Optional) (Multivalue) Single authentication plug-in or a list of plug-ins used to authenticate DHCP address requests for subscribers who log in to the domains specified for this retailer. If you do not specify a plug-in for the retailer, the SAE uses the default retailer DHCP authentication plug-in.

Value— Single authentication plug-in or a list of plug-ins

Default— No value

`<tracking-plug-in>`—(Optional) (Multivalue) Single tracking plug-in or a list of tracking plug-ins used to track subscriber sessions associated with this retailer. If you do not specify a plug-in for the retailer, the SAE uses the global subscriber tracking plug-in.

Value— Single tracking plug-in or a list of tracking plug-ins

Default— No value

`<maximum-login>`—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

`<session-timeout>`—(Optional) Timeout for subscriber sessions. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<scope>`—(Optional) (Multivalue) Service scope(s) assigned to subscribers. By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Value— Single service or a list of scopes

Default— No value

`<imported-extranet>`—(Optional) (Multivalue) Extranet exported by another retailer or enterprise.

Value— DN of the extranet

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value > .` For example, `bandwidth = 1000000.`

Default— No value

Required Privilege Level

subscriber

<info> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <info>
        <contact>contact</contact>
        <e-mail>e-mail</e-mail>
        <url>url</url>
      </info>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure contact information for the retailer.

Contents

<contact>—(Optional) Name of the contact person at the retailer.

Value— Text
Default— No value

<e-mail>—(Optional) E-mail address of the contact person at the retailer.

Value— E-mail address
Default— No value

<url>—(Optional) URL of the retailer.

Value— URL
Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <manager>
        <name>name</name> <!-- identifier -->
        <role>role-choice</role>
        <encrypted-password>encrypted-password</encrypted-password>
        <description>description</description>
      </manager>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify other enterprise manager objects.
- subscription— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- substitution— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.

- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is /etc/passwd
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <name>name</name> <!-- identifier -->
        <description>description</description>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <name>name</name> <!-- identifier -->
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <action>
            <name>name</name> <!-- identifier -->
            <type>type-choice</type>
            <service>service</service>
            <substitution>substitution</substitution>
          </action>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry schedule.
- deactivate— Deactivate service at the time specified in the entry schedule.
- deny— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This

value applies only to services that have an authorization plug-in configured.

- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value—Text

Default— No value

<substitution>—(Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <action>
            <attribute>
              <name>name-choice</name> <!-- identifier -->
              <value>value</value>
            </attribute>
          </action>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <except>
            <name>name</name> <!-- identifier -->
          </except>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <except>
            <from>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </from>
          </except>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or

exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/schedule/event/except)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <except>
            <to>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </to>
          </except>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <from>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </from>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated `from` or `to` time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <schedule>
        <event>
          <to>
            <effective>effective</effective>
            <hour>hour</hour>
            <minute>minute</minute>
            <day-of-month>day-of-month</day-of-month>
            <day-of-week>day-of-week</day-of-week>
            <month>month</month>
            <year>year</year>
            <time-zone>time-zone</time-zone>
          </to>
        </event>
      </schedule>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

`<hour>`—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscriber-folder> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <folder-name>folder-name</folder-name> <!-- identifier -->
        <maximum-login>maximum-login</maximum-login>
        <session-timeout>session-timeout</session-timeout>
        <scope>scope</scope>
        <substitution>substitution</substitution>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a subscriber folder. You can create subscriber folders for retailers, existing subscriber folders, enterprises, and sites. You must create a subscriber folder in a retailer object before you can add other types of subscribers.

Contents

<folder-name>— Name of the subscriber folder.

Value— Text

<maximum-login>—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

<session-timeout>—(Optional) Timeout for subscriber sessions. By default, all subordinate objects use this value. However, if you specify this value for a subordinate

object, that object and its subordinate objects will use the subordinate's value.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<scope>`—(Optional) (Multivalue) Service scope(s) assigned to subscribers. By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Value— Single service or a list of scopes

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<device> (configuration/subscribers/retailer/subscriber-folder)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <device-name>device-name</device-name> <!-- identifier -->
          <display-name>display-name</display-name>
          <maximum-login>maximum-login</maximum-login>
          <accounting-user-id>accounting-user-id</accounting-user-id>
          <substitution>substitution</substitution>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a device subscriber for subscriber sessions that manage the forwarding interface on JUNOS routing platforms and the router pseudo-subscriber on JUNOSe routers.

Contents

<device-name>— Name of the device subscriber.

Value— Text

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

<maximum-login>—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will

use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/device)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <manager>
            <name>name</name> <!-- identifier -->
            <role>role-choice</role>
            <encrypted-password>encrypted-password</encrypted-password>
            <description>description</description>
          </manager>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify

- other enterprise manager objects.
- **subscription**— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is /etc/passwd
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/device)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/device/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <name>name</name> <!-- identifier -->
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <action>
                <name>name</name> <!-- identifier -->
                <type>type-choice</type>
                <service>service</service>
                <substitution>substitution</substitution>
              </action>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry

- schedule.
- `deactivate`— Deactivate service at the time specified in the entry schedule.
- `deny`— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- `deny-deactivate`— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

`<service>`— Name of service affected by this action.

Value— Text

Default— No value

`<substitution>`— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <action>
                <attribute>
                  <name>name-choice</name> <!-- identifier -->
                  <value>value</value>
                </attribute>
              </action>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify

the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <except>
                <name>name</name> <!-- identifier -->
              </except>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <except>
                <from>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </except>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <except>
                <to>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </except>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23

- *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <from>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </from>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <schedule>
            <event>
              <to>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </to>
            </event>
          </schedule>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/device)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <device>
          <subscription>
            <subscription-name>subscription-name</subscription-name> <!--
identifier -->
            <status>status-choice</status>
            <activation>activation-choice</activation>
            <activation-order>activation-order</activation-order>
            <substitution>substitution</substitution>
          </subscription>
        </device>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- active— The subscriber can activate the subscription.

- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

`<activation>`— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

`<activation-order>`—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–21474863647

Default— 10000

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<enterprise> (configuration/subscribers/retailer/subscriber-folder)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <name>name</name> <!-- identifier -->
          <display-name>display-name</display-name>
          <accounting-user-id>accounting-user-id</accounting-user-id>
          <description>description</description>
          <scope>scope</scope>
          <imported-extranet>imported-extranet</imported-extranet>
          <substitution>substitution</substitution>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an enterprise subscriber.

Contents

<name>— Name of the enterprise subscriber

Value— Text

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

`<scope>`—(Optional) (Multivalue) Service scope(s) assigned to subscribers. By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Value— Single service or a list of scopes

Default— No value

`<imported-extranet>`—(Optional) (Multivalue) Extranet exported by another retailer or enterprise.

Value— DN of the extranet

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<access> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <name>name</name> <!-- identifier -->
            <routing-protocol>routing-protocol</routing-protocol>
            <interface-alias>interface-alias</interface-alias>
            <interface-description>interface-description</interface-
description>
            <interface-name>interface-name</interface-name>
            <unique-id>unique-id</unique-id>
            <port-id>port-id</port-id>
            <device-name>device-name</device-name>
            <display-name>display-name</display-name>
            <accounting-user-id>accounting-user-id</accounting-user-id>
            <substitution>substitution</substitution>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an access. You can configure an access for an enterprise or for a site. An access determines the way that the enterprise or site accesses Internet services, and specifies a set of services that are available to the enterprise or site.

Contents

<name>— Name of the access.

Value— Text

`<routing-protocol>`—(Optional) Routing protocol used at the enterprise or site. If you build a custom enterprise manager application, you can access this information through the enterprise portal APIs.

Value— Routing protocol

Default— No value

`<interface-alias>`—(Optional) Description of the router interface. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Interface description that is configured on the router.

Default— No value

`<interface-description>`—(Optional) Name of the interface that SNMP uses. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— One of the following:

- For JUNOSe routers, the format of the description is ip < slot > / < port > . < subinterface >
- On the JUNOS routing platform, interface description is the same as interfaceName

Default— No value

`<interface-name>`—(Optional) Name of the interface. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— One of the following:

- Name of the interface in your router CLI syntax.
- FORWARDING_INTERFACE for routing instance (used by traffic mirroring).

Default— No value

`<unique-id>`—(Optional) Unique identifier of the router. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Index of the router in the SNMP table for all interfaces.

Default— No value

`<port-id>`—(Optional) NAS port ID reported by the JUNOS router through COPS. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Includes the interface name and additional layer 2 information.

Default— No value

`<device-name>`—(Optional) Name of the router or other device.

Value— Name of the device

Default— No value

`<display-name>`—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<admission-control> (configuration/subscribers/retailer/subscriber-folder/enterprise/access)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <admission-control>
              <downstream-provisioned-rate>downstream-provisioned-rate</
downstream-provisioned-rate>
              <upstream-provisioned-rate>upstream-provisioned-rate</upstream-
provisioned-rate>
              <downstream-sync-rate>downstream-sync-rate</downstream-sync-
rate>
              <upstream-sync-rate>upstream-sync-rate</upstream-sync-rate>
              <congestion-points>congestion-points</congestion-points>
            </admission-control>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure bandwidths for subscribers that the SRC-ACP manages.

Contents

<downstream-provisioned-rate>—(Optional) Provisioned downstream bandwidth. This rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the downstream-sync-rate option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<upstream-provisioned-rate>—(Optional) Provisioned upstream bandwidth. This

rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the upstream-sync-rate option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<downstream-sync-rate>—(Optional) Actual downstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the downstream-provisioned-rate option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<upstream-sync-rate>—(Optional) Actual upstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the upstream-provisioned-rate option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<congestion-points>—(Optional) (Multivalue) Congestion points for the subscriber.

Value— DN of interface associated with congestion point

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise/access)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <manager>
              <name>name</name> <!-- identifier -->
              <role>role-choice</role>
              <encrypted-password>encrypted-password</encrypted-password>
              <description>description</description>
            </manager>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles.

Additionally, administrators can create, delete, and modify other enterprise manager objects.

- `subscription`— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- `substitution`— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- `activation`— Activation managers can activate and deactivate subscriptions.
- `vpn`— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

`<encrypted-password>`—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- `crypt`—Style is `/etc/passwd`
- `sha`—Secure hash algorithm
- `md5`—Message digest #5

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise/access)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <name>name</name> <!-- identifier -->
              <description>description</description>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <name>name</name> <!-- identifier -->
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <action>
                  <name>name</name> <!-- identifier -->
                  <type>type-choice</type>
                  <service>service</service>
                  <substitution>substitution</substitution>
                </action>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- **activate**— Activate service at the time specified in the entry schedule.
- **deactivate**— Deactivate service at the time specified in the entry schedule.
- **deny**— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value— Text

Default— No value

<substitution>— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <action>
                  <attribute>
                    <name>name-choice</name> <!-- identifier -->
                    <value>value</value>
                  </attribute>
                </action>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between

- the network and the subscriber.
- upStreamBandwidth— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <except>
                  <name>name</name> <!-- identifier -->
                </except>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <except>
                  <from>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </from>
                </except>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <except>
                  <to>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </to>
                </except>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <from>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <schedule>
              <event>
                <to>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </event>
            </schedule>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the

scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise/access)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <access>
            <subscription>
              <subscription-name>subscription-name</subscription-name> <!--
identifier -->
              <status>status-choice</status>
              <activation>activation-choice</activation>
              <activation-order>activation-order</activation-order>
              <substitution>substitution</substitution>
            </subscription>
          </access>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- **active**— The subscriber can activate the subscription.
- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367

Default— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form **< parameter name > = < value >** . For example, **bandwidth = 1000000**.

Default— No value

Required Privilege Level

subscriber

<device> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <device-name>device-name</device-name> <!-- identifier -->
            <display-name>display-name</display-name>
            <maximum-login>maximum-login</maximum-login>
            <accounting-user-id>accounting-user-id</accounting-user-id>
            <substitution>substitution</substitution>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a device subscriber for subscriber sessions that manage the forwarding interface on JUNOS routing platforms and the router pseudo-subscriber on JUNOSe routers.

Contents

<device-name>— Name of the device subscriber.

Value— Text

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<maximum-login>`—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise/device)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <manager>
              <name>name</name> <!-- identifier -->
              <role>role-choice</role>
              <encrypted-password>encrypted-password</encrypted-password>
              <description>description</description>
            </manager>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles.

Additionally, administrators can create, delete, and modify other enterprise manager objects.

- **subscription**— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is `/etc/passwd`
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise/device)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <name>name</name> <!-- identifier -->
              <description>description</description>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <name>name</name> <!-- identifier -->
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <action>
                  <name>name</name> <!-- identifier -->
                  <type>type-choice</type>
                  <service>service</service>
                  <substitution>substitution</substitution>
                </action>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- **activate**— Activate service at the time specified in the entry schedule.
- **deactivate**— Deactivate service at the time specified in the entry schedule.
- **deny**— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value— Text

Default— No value

<substitution>— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event/action)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <action>
                  <attribute>
                    <name>name-choice</name> <!-- identifier -->
                    <value>value</value>
                  </attribute>
                </action>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between

- the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

`<value>`— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <except>
                  <name>name</name> <!-- identifier -->
                </except>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <except>
                  <from>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </from>
                </except>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <except>
                  <to>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </to>
                </except>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <from>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <schedule>
              <event>
                <to>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </event>
            </schedule>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the

scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both **day-of-month** and **day-of-week**, **day-of-month** is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both **day-of-month** and **day-of-week**, **day-of-month** is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise/device)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <device>
            <subscription>
              <subscription-name>subscription-name</subscription-name> <!--
identifier -->
              <status>status-choice</status>
              <activation>activation-choice</activation>
              <activation-order>activation-order</activation-order>
              <substitution>substitution</substitution>
            </subscription>
          </device>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- **active**— The subscriber can activate the subscription.
- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367

Default— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

Required Privilege Level

subscriber

<info> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <info>
            <phone>phone</phone>
            <fax>fax</fax>
            <po-box>po-box</po-box>
            <city>city</city>
            <street>street</street>
            <state>state</state>
            <postal-code>postal-code</postal-code>
          </info>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure additional information about the enterprise subscriber.

Contents

<phone>—(Optional) Telephone number for the subscriber.

Value— Telephone number

Default— No value

<fax>—(Optional) Fax number for the subscriber.

Value— Fax number

Default— No value

<po-box>—(Optional) Post office box for the subscriber.

Value— Post office box

Default— No value

<city>—(Optional) City name for the subscriber.

Value— City name

Default— No value

<street>—(Optional) Street address for the subscriber.

Value— Street address

Default— No value

<state>—(Optional) State or province for the subscriber.

Value— State or province

Default— No value

<postal-code>—(Optional) Postal code for the subscriber.

Value— Postal code

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <manager>
            <name>name</name> <!-- identifier -->
            <role>role-choice</role>
            <encrypted-password>encrypted-password</encrypted-password>
            <description>description</description>
          </manager>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- **administrator**— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify

other enterprise manager objects.

- **subscription**— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is /etc/passwd
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <name>name</name> <!-- identifier -->
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <action>
                <name>name</name> <!-- identifier -->
                <type>type-choice</type>
                <service>service</service>
                <substitution>substitution</substitution>
              </action>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry

schedule.

- `deactivate`— Deactivate service at the time specified in the entry schedule.
- `deny`— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- `deny-deactivate`— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

`<service>`— Name of service affected by this action.

Value— Text

Default— No value

`<substitution>`— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event/action)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <action>
                <attribute>
                  <name>name-choice</name> <!-- identifier -->
                  <value>value</value>
                </attribute>
              </action>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- **sessionName**— Name of the service session.
- **sessionTag**— Tag that can be used for accounting purposes.
- **sessionTimeout**— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- **downStreamBandwidth**— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- **upStreamBandwidth**— Attribute used by SRC-ACP to specify

the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <except>
                <name>name</name> <!-- identifier -->
              </except>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <except>
                <from>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </except>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <except>
                <to>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </except>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23

- *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <from>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </from>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <schedule>
            <event>
              <to>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </to>
            </event>
          </schedule>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<site> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <name>name</name> <!-- identifier -->
            <network>network</network>
            <display-name>display-name</display-name>
            <accounting-user-id>accounting-user-id</accounting-user-id>
            <description>description</description>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an enterprise site.

Contents

<name>— Name of the site.

Value— Text

<network>—(Optional) (Multivalue) Network used at the enterprise or site. If you build a custom enterprise manager application, you can access this information through the enterprise portal APIs.

Value— Network

Default— No value

`<display-name>`—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<access> (configuration/subscribers/retailer/subscriber-folder/enterprise/site)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <name>name</name> <!-- identifier -->
              <routing-protocol>routing-protocol</routing-protocol>
              <interface-alias>interface-alias</interface-alias>
              <interface-description>interface-description</interface-
description>
              <interface-name>interface-name</interface-name>
              <unique-id>unique-id</unique-id>
              <port-id>port-id</port-id>
              <device-name>device-name</device-name>
              <display-name>display-name</display-name>
              <accounting-user-id>accounting-user-id</accounting-user-id>
              <substitution>substitution</substitution>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an access. You can configure an access for an enterprise or for a site. An access determines the way that the enterprise or site accesses Internet services, and specifies a set of services that are available to the enterprise or site.

Contents

<name>— Name of the access.

Value— Text

`<routing-protocol>`—(Optional) Routing protocol used at the enterprise or site. If you build a custom enterprise manager application, you can access this information through the enterprise portal APIs.

Value— Routing protocol

Default— No value

`<interface-alias>`—(Optional) Description of the router interface. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Interface description that is configured on the router.

Default— No value

`<interface-description>`—(Optional) Name of the interface that SNMP uses. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— One of the following:

- For JUNOS routers, the format of the description is `ip < slot > / < port > . < subinterface >`
- On the JUNOS routing platform, interface description is the same as `interfaceName`

Default— No value

`<interface-name>`—(Optional) Name of the interface. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— One of the following:

- Name of the interface in your router CLI syntax.
- `FORWARDING_INTERFACE` for routing instance (used by traffic mirroring).

Default— No value

`<unique-id>`—(Optional) Unique identifier of the router. You can use this option to allow

subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Index of the router in the SNMP table for all interfaces.

Default— No value

`<port-id>`—(Optional) NAS port ID reported by the JUNOSe router through COPS. You can use this option to allow subscriber classification scripts to match interfaces reported from the network to be matched with the corresponding access.

Value— Includes the interface name and additional layer 2 information.

Default— No value

`<device-name>`—(Optional) Name of the router or other device.

Value— Name of the device

Default— No value

`<display-name>`—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<admission-control> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <admission-control>
                <downstream-provisioned-rate>downstream-provisioned-rate</
downstream-provisioned-rate>
                <upstream-provisioned-rate>upstream-provisioned-rate</
upstream-provisioned-rate>
                <downstream-sync-rate>downstream-sync-rate</downstream-sync-
rate>
                <upstream-sync-rate>upstream-sync-rate</upstream-sync-rate>
                <congestion-points>congestion-points</congestion-points>
              </admission-control>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure bandwidths for subscribers that the SRC-ACP manages.

Contents

<downstream-provisioned-rate>—(Optional) Provisioned downstream bandwidth. This rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the downstream-sync-rate option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

`<upstream-provisioned-rate>`—(Optional) Provisioned upstream bandwidth. This rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the `upstream-sync-rate` option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

`<downstream-sync-rate>`—(Optional) Actual downstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the `downstream-provisioned-rate` option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

`<upstream-sync-rate>`—(Optional) Actual upstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the `upstream-provisioned-rate` option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

`<congestion-points>`—(Optional) (Multivalue) Congestion points for the subscriber.

Value— DN of interface associated with congestion point

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <manager>
                <name>name</name> <!-- identifier -->
                <role>role-choice</role>
                <encrypted-password>encrypted-password</encrypted-password>
                <description>description</description>
              </manager>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- **administrator**— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify other enterprise manager objects.
- **subscription**— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

`<encrypted-password>`—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is `/etc/passwd`
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <name>name</name> <!-- identifier -->
                <description>description</description>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <name>name</name> <!-- identifier -->
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <action>
                    <name>name</name> <!-- identifier -->
                    <type>type-choice</type>
                    <service>service</service>
                    <substitution>substitution</substitution>
                  </action>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- `activate`— Activate service at the time specified in the entry schedule.
- `deactivate`— Deactivate service at the time specified in the entry schedule.
- `deny`— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- `deny-deactivate`— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value—Text**Default**— No value

<substitution>—(Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.**Default**— No value**Required Privilege Level**

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <action>
                    <attribute>
                      <name>name-choice</name> <!-- identifier -->
                      <value>value</value>
                    </attribute>
                  </action>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- **sessionName**— Name of the service session.
- **sessionTag**— Tag that can be used for accounting purposes.
- **sessionTimeout**— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.

- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

`<value>`— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <except>
                    <name>name</name> <!-- identifier -->
                  </except>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <except>
                    <from>
                      <hour>hour</hour>
                      <minute>minute</minute>
                      <day-of-month>day-of-month</day-of-month>
                      <day-of-week>day-of-week</day-of-week>
                      <month>month</month>
                      <year>year</year>
                      <time-zone>time-zone</time-zone>
                    </from>
                  </except>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event

or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE

- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <except>
                    <to>
                      <hour>hour</hour>
                      <minute>minute</minute>
                      <day-of-month>day-of-month</day-of-month>
                      <day-of-week>day-of-week</day-of-week>
                      <month>month</month>
                      <year>year</year>
                      <time-zone>time-zone</time-zone>
                    </to>
                  </except>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+|-) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <from>
                    <effective>effective</effective>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </from>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <schedule>
                <event>
                  <to>
                    <effective>effective</effective>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </to>
                </event>
              </schedule>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

`<effective>`—(Optional) Interval after the associated `from` or `to` time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

`<hour>`—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/access)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <access>
              <subscription>
                <subscription-name>subscription-name</subscription-name> <!--
identifier -->
                <status>status-choice</status>
                <activation>activation-choice</activation>
                <activation-order>activation-order</activation-order>
                <substitution>substitution</substitution>
              </subscription>
            </access>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- **active**— The subscriber can activate the subscription.
- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367**Default**— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

Required Privilege Level

subscriber

<device> (configuration/subscribers/retailer/subscriber-folder/enterprise/site)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <device-name>device-name</device-name> <!-- identifier -->
              <display-name>display-name</display-name>
              <maximum-login>maximum-login</maximum-login>
              <accounting-user-id>accounting-user-id</accounting-user-id>
              <substitution>substitution</substitution>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a device subscriber for subscriber sessions that manage the forwarding interface on JUNOS routing platforms and the router pseudo-subscriber on JUNOSe routers.

Contents

<device-name>— Name of the device subscriber.

Value— Text

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<maximum-login>`—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <manager>
                <name>name</name> <!-- identifier -->
                <role>role-choice</role>
                <encrypted-password>encrypted-password</encrypted-password>
                <description>description</description>
              </manager>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- **administrator**— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify other enterprise manager objects.
- **subscription**— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is `/etc/passwd`
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <name>name</name> <!-- identifier -->
                <description>description</description>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <name>name</name> <!-- identifier -->
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <action>
                    <name>name</name> <!-- identifier -->
                    <type>type-choice</type>
                    <service>service</service>
                    <substitution>substitution</substitution>
                  </action>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- **activate**— Activate service at the time specified in the entry schedule.
- **deactivate**— Deactivate service at the time specified in the entry schedule.
- **deny**— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value—Text**Default**— No value

<substitution>—(Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.**Default**— No value**Required Privilege Level**

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <action>
                    <attribute>
                      <name>name-choice</name> <!-- identifier -->
                      <value>value</value>
                    </attribute>
                  </action>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- **sessionName**— Name of the service session.
- **sessionTag**— Tag that can be used for accounting purposes.
- **sessionTimeout**— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.

- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

`<value>`— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <except>
                    <name>name</name> <!-- identifier -->
                  </except>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <except>
                    <from>
                      <hour>hour</hour>
                      <minute>minute</minute>
                      <day-of-month>day-of-month</day-of-month>
                      <day-of-week>day-of-week</day-of-week>
                      <month>month</month>
                      <year>year</year>
                      <time-zone>time-zone</time-zone>
                    </from>
                  </except>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event

or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE

- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <except>
                    <to>
                      <hour>hour</hour>
                      <minute>minute</minute>
                      <day-of-month>day-of-month</day-of-month>
                      <day-of-week>day-of-week</day-of-week>
                      <month>month</month>
                      <year>year</year>
                      <time-zone>time-zone</time-zone>
                    </to>
                  </except>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <from>
                    <effective>effective</effective>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </from>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912
Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23
Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59
Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31
Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week
Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12
Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year
Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <schedule>
                <event>
                  <to>
                    <effective>effective</effective>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </to>
                </event>
              </schedule>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

`<effective>`—(Optional) Interval after the associated `from` or `to` time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

`<hour>`—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

`<minute>`—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

`<day-of-month>`—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 1-31

Default— *

`<day-of-week>`—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both `day-of-month` and `day-of-week`, `day-of-month` is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

`<month>`—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

`<year>`—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/device)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <device>
              <subscription>
                <subscription-name>subscription-name</subscription-name> <!--
identifier -->
                <status>status-choice</status>
                <activation>activation-choice</activation>
                <activation-order>activation-order</activation-order>
                <substitution>substitution</substitution>
              </subscription>
            </device>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- **active**— The subscriber can activate the subscription.
- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367**Default**— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder/enterprise/site)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <manager>
              <name>name</name> <!-- identifier -->
              <role>role-choice</role>
              <encrypted-password>encrypted-password</encrypted-password>
              <description>description</description>
            </manager>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles.

Additionally, administrators can create, delete, and modify other enterprise manager objects.

- `subscription`— Subscription managers can create, delete, modify, activate, and deactivate subscriptions.
- `substitution`— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- `activation`— Activation managers can activate and deactivate subscriptions.
- `vpn`— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

`<encrypted-password>`—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- `crypt`—Style is `/etc/passwd`
- `sha`—Secure hash algorithm
- `md5`—Message digest #5

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/enterprise/site)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <name>name</name> <!-- identifier -->
              <description>description</description>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <name>name</name> <!-- identifier -->
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <action>
                  <name>name</name> <!-- identifier -->
                  <type>type-choice</type>
                  <service>service</service>
                  <substitution>substitution</substitution>
                </action>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- **activate**— Activate service at the time specified in the entry schedule.
- **deactivate**— Deactivate service at the time specified in the entry schedule.
- **deny**— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- **deny-deactivate**— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

<service>— Name of service affected by this action.

Value— Text

Default— No value

<substitution>— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <action>
                  <attribute>
                    <name>name-choice</name> <!-- identifier -->
                    <value>value</value>
                  </attribute>
                </action>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- `sessionName`— Name of the service session.
- `sessionTag`— Tag that can be used for accounting purposes.
- `sessionTimeout`— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- `downStreamBandwidth`— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between

the network and the subscriber.

- `upStreamBandwidth`— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

`<value>`— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <except>
                  <name>name</name> <!-- identifier -->
                </except>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <except>
                  <from>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </from>
                </except>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <except>
                  <to>
                    <hour>hour</hour>
                    <minute>minute</minute>
                    <day-of-month>day-of-month</day-of-month>
                    <day-of-week>day-of-week</day-of-week>
                    <month>month</month>
                    <year>year</year>
                    <time-zone>time-zone</time-zone>
                  </to>
                </except>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <from>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/enterprise/site/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <schedule>
              <event>
                <to>
                  <effective>effective</effective>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </event>
            </schedule>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the

scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

`<time-zone>`—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise/site)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <site>
            <subscription>
              <subscription-name>subscription-name</subscription-name> <!--
identifier -->
              <status>status-choice</status>
              <activation>activation-choice</activation>
              <activation-order>activation-order</activation-order>
              <substitution>substitution</substitution>
            </subscription>
          </site>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- **active**— The subscriber can activate the subscription.
- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

`<activation>`— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

`<activation-order>`—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367

Default— 10000

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <subscription>
            <subscription-name>subscription-name</subscription-name> <!--
identifier -->
            <status>status-choice</status>
            <activation>activation-choice</activation>
            <activation-order>activation-order</activation-order>
            <substitution>substitution</substitution>
          </subscription>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "% *subscription-id*". Use "% *subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- active— The subscriber can activate the subscription.

- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147483647

Default— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form **< parameter name > = < value >** . For example, **bandwidth = 1000000**.

Default— No value

Required Privilege Level

subscriber

<vpn> (configuration/subscribers/retailer/subscriber-folder/enterprise)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <enterprise>
          <vpn>
            <vpn-id>vpn-id</vpn-id> <!-- identifier -->
            <extranet-client>extranet-client</extranet-client>
            <display-name>display-name</display-name>
            <description>description</description>
          </vpn>
        </enterprise>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Add a VPN to the subscriber configuration.

Contents

<vpn-id>— Name of the routing instance on a JUNOS routing platform that implements the VPN.

Value— Text

<extranet-client>—(Optional) (Multivalue) DN of a retailer or an enterprise that is an extranet client of this VPN.

Value— DN

Default— No value

`<display-name>`—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<manager> (configuration/subscribers/retailer/subscriber-folder)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <manager>
          <name>name</name> <!-- identifier -->
          <role>role-choice</role>
          <encrypted-password>encrypted-password</encrypted-password>
          <description>description</description>
        </manager>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a manager account.

Contents

<name>— Name of the manager account.

Value— Text

<role>—(Multivalue) Privilege level of the enterprise manager account. If you do not specify a privilege level, the manager has read-only access to associated objects.

Value

- administrator— Administrators have all privileges of the subscription, substitution, activation, and vpn roles. Additionally, administrators can create, delete, and modify other enterprise manager objects.
- subscription— Subscription managers can create, delete,

modify, activate, and deactivate subscriptions.

- **substitution**— Substitution managers can modify policy parameters provided by subscriptions, enterprises, sites, and accesses.
- **activation**— Activation managers can activate and deactivate subscriptions.
- **vpn**— VPN managers can modify, export, and cancel the export of VPNs.

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- **crypt**—Style is `/etc/passwd`
- **sha**—Secure hash algorithm
- **md5**—Message digest #5

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <name>name</name> <!-- identifier -->
          <description>description</description>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <name>name</name> <!-- identifier -->
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/schedule/event)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <action>
              <name>name</name> <!-- identifier -->
              <type>type-choice</type>
              <service>service</service>
              <substitution>substitution</substitution>
            </action>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- **activate**— Activate service at the time specified in the entry schedule.

- `deactivate`— Deactivate service at the time specified in the entry schedule.
- `deny`— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- `deny-deactivate`— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

`<service>`— Name of service affected by this action.

Value— Text

Default— No value

`<substitution>`— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/schedule/event/action)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <action>
              <attribute>
                <name>name-choice</name> <!-- identifier -->
                <value>value</value>
              </attribute>
            </action>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- **sessionName**— Name of the service session.
- **sessionTag**— Tag that can be used for accounting purposes.
- **sessionTimeout**— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- **downStreamBandwidth**— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- **upStreamBandwidth**— Attribute used by SRC-ACP to specify the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <except>
              <name>name</name> <!-- identifier -->
            </except>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/schedule/event/except)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <except>
              <from>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </from>
            </except>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/schedule/event/except)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <except>
              <to>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </to>
            </except>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <from>
              <effective>effective</effective>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </from>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <schedule>
          <event>
            <to>
              <effective>effective</effective>
              <hour>hour</hour>
              <minute>minute</minute>
              <day-of-month>day-of-month</day-of-month>
              <day-of-week>day-of-week</day-of-week>
              <month>month</month>
              <year>year</year>
              <time-zone>time-zone</time-zone>
            </to>
          </event>
        </schedule>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated **from** or **to** time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscriber> (configuration/subscribers/retailer)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <name>name</name> <!-- identifier -->
          <common-name>common-name</common-name>
          <surname>surname</surname>
          <given-name>given-name</given-name>
          <initials>initials</initials>
          <anonymous/>
          <ip-address>ip-address</ip-address>
          <interface-name>interface-name</interface-name>
          <maximum-login-group>maximum-login-group</maximum-login-group>
          <display-name>display-name</display-name>
          <encrypted-password>encrypted-password</encrypted-password>
          <maximum-login>maximum-login</maximum-login>
          <session-timeout>session-timeout</session-timeout>
          <accounting-user-id>accounting-user-id</accounting-user-id>
          <substitution>substitution</substitution>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a residential subscriber. The SRC software uses the information in the subscriber definition to create a subscriber profile.

Contents

<name>— Name of the residential subscriber

Value— Text

<common-name>— Name that defines the subscriber in the directory. The value is not used directly by the SRC software, but it is not optional because it is required by the LDAP schema. The common name is available through SRC APIs.

Value— Text. Typically in the format firstName lastName or lastname
firstName

Default— No value

<surname>— Subscriber's last name. The surname is not directly used by the SRC software, but it is not optional because it is required by the LDAP schema. The surname is available through SRC APIs.

Value— Text

Default— No value

<given-name>—(Optional) Subscriber's given name. The given name is not used directly by the SRC software, but it is available through SRC APIs.

Value— Text

Default— No value

<initials>—(Optional) Subscriber's initials. The initials are not used directly by the SRC software but are available through SRC APIs.

Value— Text

Default— No value

<anonymous>—(Optional) A flag that marks the subscriber profile as a shared profile. Shared profiles can be used by multiple subscriber sessions. The SAE API prevents subscribers from making changes to their profile if the profile is marked as anonymous.

Default— Disabled

<ip-address>—(Optional) IP address for subscribers who have fixed addresses, and for whom the SRC does not learn addresses through its management of routers or through calls to its notification API.

Value— IP address

Default— No value

<interface-name>—(Optional) Type and specifier of the router interface and virtual router that manage this subscriber. Use this option when you want the subscriber classification script to identify the subscriber entry in the directory based on the interface

name received from the router.

Value— Interface as configured on the router. For example:

- For JUNOS routers:
"fastethernet6/0.1@vrName@routerName"
- For JUNOS routing platforms: "fe-0/10.0@vrName@routerName"

Default— No value

<maximum-login-group>—(Optional) Maximum number of concurrent logins for this subscriber and all subordinate objects; typically the maximum number of concurrent logins for a household.

Value— Integer in the range 0–2147483647

Default— No value

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

<encrypted-password>—(Optional) Login password and type of encryption.

Value— Enter a password, and select an encryption method that your directory supports.

- crypt—Style is /etc/passwd
- sha—Secure hash algorithm
- md5—Message digest #5

Default— No value

<maximum-login>—(Optional) Maximum number of concurrent logins for subscribers associated with this object. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Integer in the range 0–2147483647

Default— No value

`<session-timeout>`—(Optional) Timeout for subscriber sessions. By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.

Value— Number of seconds in the range 0–2147483647

Default— No value

`<accounting-user-id>`—(Optional) Value that identifies the subscriber in accounting records. For a household subscriber, all subordinate subscribers generally use the same ID. For an enterprise, all parts of the enterprise generally use the same ID.

Value— Text

Default— No value

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value >` . For example, `bandwidth = 1000000`.

Default— No value

Required Privilege Level

subscriber

<admission-control> (configuration/subscribers/retailer/subscriber-folder/subscriber)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <admission-control>
            <downstream-provisioned-rate>downstream-provisioned-rate</
downstream-provisioned-rate>
            <upstream-provisioned-rate>upstream-provisioned-rate</upstream-
provisioned-rate>
            <downstream-sync-rate>downstream-sync-rate</downstream-sync-rate>
            <upstream-sync-rate>upstream-sync-rate</upstream-sync-rate>
            <congestion-points>congestion-points</congestion-points>
          </admission-control>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure bandwidths for subscribers that the SRC-ACP manages.

Contents

<downstream-provisioned-rate>—(Optional) Provisioned downstream bandwidth. This rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the downstream-sync-rate option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<upstream-provisioned-rate>—(Optional) Provisioned upstream bandwidth. This rate is used if the subscriber bandwidth settings are not provided by the API for ACP or by the upstream-sync-rate option.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<downstream-sync-rate>—(Optional) Actual downstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the downstream-provisioned-rate option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<upstream-sync-rate>—(Optional) Actual upstream bandwidth for the current subscriber session. If you do not set this value and it is not provided by the API for ACP, the value of the upstream-provisioned-rate option is used.

Value— Number of bps in the range 0–9223372036854775807

Default— No value

<congestion-points>—(Optional) (Multivalue) Congestion points for the subscriber.

Value— DN of interface associated with congestion point

Default— No value

Required Privilege Level

subscriber

<info> (configuration/subscribers/retailer/subscriber-folder/subscriber)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <info>
            <home-phone>home-phone</home-phone>
            <additional-phone>additional-phone</additional-phone>
            <fax>fax</fax>
            <e-mail>e-mail</e-mail>
            <city>city</city>
            <street>street</street>
            <postal-code>postal-code</postal-code>
            <language>language</language>
            <job>job</job>
            <description>description</description>
          </info>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure administrative information about the subscriber. The additional subscriber information is not used directly by the SRC software.

Contents

<home-phone>—(Optional) Home telephone number of the subscriber.

Value— Telephone number

Default— No value

<additional-phone>—(Optional) Additional telephone number for the subscriber.

Value— Telephone number

Default— No value

<fax>—(Optional) Fax number for the subscriber.

Value— Fax number

Default— No value

<e-mail>—(Optional) E-mail address for the subscriber.

Value— E-mail address

Default— No value

<city>—(Optional) City name for the subscriber.

Value— City name

Default— No value

<street>—(Optional) Street address for the subscriber.

Value— Street address

Default— No value

<postal-code>—(Optional) Postal code for the subscriber.

Value— Postal code

Default— No value

<language>—(Optional) Preferred language for the subscriber.

Value— Language name

Default— No value

<job>—(Optional) Job or business category for the subscriber.

Value— Job or business category

Default— No value

<description>—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

<schedule> (configuration/subscribers/retailer/subscriber-folder/subscriber)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <name>name</name> <!-- identifier -->
            <description>description</description>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service schedule.

Contents

<name>— Name of service schedule.

Value—Text

<description>—(Optional) Description of the service schedule.

Value—Text

Default— No value

Required Privilege Level

subscriber

<event> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <name>name</name> <!-- identifier -->
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a scheduling event.

Contents

<name>— Name of the scheduling event.

Value—Text

Required Privilege Level

subscriber

<action> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <action>
                <name>name</name> <!-- identifier -->
                <type>type-choice</type>
                <service>service</service>
                <substitution>substitution</substitution>
              </action>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure actions to perform for the scheduled event.

Contents

<name>— Arbitrary identifier for action.

Value—Text

<type>— Type of action.

Value

- activate— Activate service at the time specified in the entry

schedule.

- `deactivate`— Deactivate service at the time specified in the entry schedule.
- `deny`— Deny new activation requests during the time specified in the entry schedule; current sessions are not affected. This value applies only to services that have an authorization plug-in configured.
- `deny-deactivate`— Deny new activation requests during the time specified in the entry schedule; current sessions are deactivated at the specified time. This value applies only to services that have an authorization plug-in configured.

Default— No value

`<service>`— Name of service affected by this action.

Value— Text

Default— No value

`<substitution>`— (Optional) (Multivalue) Substitutions to be used when activating the service. Substitutions apply only to service activations.

Value— An entry in valid substitution format. See the *SRC-PE Services and Policies Guide*.

Default— No value

Required Privilege Level

subscriber

<attribute> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event/action)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <action>
                <attribute>
                  <name>name-choice</name> <!-- identifier -->
                  <value>value</value>
                </attribute>
              </action>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure subscription attributes. Subscription attributes apply only to service activations.

Contents

Value

- **sessionName**— Name of the service session.
- **sessionTag**— Tag that can be used for accounting purposes.
- **sessionTimeout**— Session timeout to be used when the service is activated. The service session is deactivated when this timeout expires.
- **downStreamBandwidth**— Attribute used by SRC Admission Control Plug-In (SRC-ACP) to specify the rate of traffic between the network and the subscriber.
- **upStreamBandwidth**— Attribute used by SRC-ACP to specify

the rate of traffic between the subscriber and the network.

<value>— Value of the specified subscription attribute.

Value— Depends on the specified subscription attribute

Default— No value

Required Privilege Level

subscriber

<except> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <except>
                <name>name</name> <!-- identifier -->
              </except>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an exclusion for the event.

Contents

<name>— Arbitrary identifier for exclusion rule.

Value—Text

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event/except)

Usage

```

<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <except>
                <from>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </from>
              </except>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23
 - *mm*—Minutes past the hour in the range of 0-59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event/except)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <except>
                <to>
                  <hour>hour</hour>
                  <minute>minute</minute>
                  <day-of-month>day-of-month</day-of-month>
                  <day-of-week>day-of-week</day-of-week>
                  <month>month</month>
                  <year>year</year>
                  <time-zone>time-zone</time-zone>
                </to>
              </except>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time of the exclusion. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23**Default**— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59**Default**— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31**Default**— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12**Default**— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year**Default**— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0-23

- *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<from> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <from>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </from>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the start time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<to> (configuration/subscribers/retailer/subscriber-folder/subscriber/schedule/event)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <schedule>
            <event>
              <to>
                <effective>effective</effective>
                <hour>hour</hour>
                <minute>minute</minute>
                <day-of-month>day-of-month</day-of-month>
                <day-of-week>day-of-week</day-of-week>
                <month>month</month>
                <year>year</year>
                <time-zone>time-zone</time-zone>
              </to>
            </event>
          </schedule>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the end time for the event. For guidelines about entering time values, see the *SRC-PE Services and Policies Guide*.

These values apply only to services that have an authorization plug-in configured. If an authorization plug-in is not configured for the service associated with the schedule, these values are ignored.

Contents

<effective>—(Optional) Interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

Value— Number of minutes in the range 0–153722867280912

Default— *

<hour>—(Optional) Hour of the day in the indicated month in which to schedule the event or exclusion.

Value— 0-23

Default— *

<minute>—(Optional) Minutes past the indicated hour in which to schedule the event or exclusion.

Value— 0-59

Default— *

<day-of-month>—(Optional) Day of the month in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 1-31

Default— *

<day-of-week>—(Optional) Day of the week in which to schedule the event or exclusion. If you specify both day-of-month and day-of-week, day-of-month is used.

Value— 0-6, with 0 representing Sunday and each subsequent number representing the next day of the week

Default— *

<month>—(Optional) Month of the year in which to schedule the event or exclusion.

Value— 1-12

Default— *

<year>—(Optional) Year in which to schedule the event or exclusion.

Value— Four integers that indicate the year

Default— *

<time-zone>—(Optional) Name of the time zone to use in the schedule.

Value— One of the following values:

- *—Local time zone of the SAE
- An offset to GMT in the format: GMT (+ | -) (*hh:mm* | *hh mm* | *hh*)
 - *hh*—Hour of the day in the range of 0–23
 - *mm*—Minutes past the hour in the range of 0–59

Default— *

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder/subscriber)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscriber>
          <subscription>
            <subscription-name>subscription-name</subscription-name> <!--
identifier -->
            <status>status-choice</status>
            <activation>activation-choice</activation>
            <activation-order>activation-order</activation-order>
            <substitution>substitution</substitution>
          </subscription>
        </subscriber>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "*%subscription-id*". Use "*%subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- active— The subscriber can activate the subscription.

- **suspended**— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–21474863647

Default— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form **< parameter name > = < value >** . For example, **bandwidth = 1000000**.

Default— No value

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer/subscriber-folder)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscriber-folder>
        <subscription>
          <subscription-name>subscription-name</subscription-name> <!--
identifier -->
          <status>status-choice</status>
          <activation>activation-choice</activation>
          <activation-order>activation-order</activation-order>
          <substitution>substitution</substitution>
        </subscription>
      </subscriber-folder>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "%*subscription-id*". Use "%*subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- active— The subscriber can activate the subscription.
- suspended— The subscriber cannot activate the subscription,

although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.

- **hidden**— Service is not available through a portal and cannot be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

`<activation>`— Specify how the service is activated.

Value

- **manual**— Subscriber must manually activate the service.
- **automatically-on-login**— Service is activated automatically when the subscriber logs in.

Default— Manual activation

`<activation-order>`—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147486367

Default— 10000

`<substitution>`—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form `< parameter name > = < value > .` For example, `bandwidth = 1000000.`

Default— No value

Required Privilege Level

subscriber

<subscription> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <subscription>
        <subscription-name>subscription-name</subscription-name> <!--
identifier -->
        <status>status-choice</status>
        <activation>activation-choice</activation>
        <activation-order>activation-order</activation-order>
        <substitution>substitution</substitution>
      </subscription>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a service subscription.

Contents

<subscription-name>— Name of the service optionally followed by "%*subscription-id*". Use "%*subscription-id*" to subscribe subscribers to the same service multiple times with different subscription attributes.

Value— Text

<status>— Status of the service subscription.

Value

- *active*— The subscriber can activate the subscription.
- *suspended*— The subscriber cannot activate the subscription, although it may be visible through the portal. If you change the status of the subscription to suspended while the subscription is active, the service is deactivated.
- *hidden*— Service is not available through a portal and cannot

be activated automatically when the subscribers log in. If you change the status of the subscription to hidden while the subscription is active, the service is not deactivated.

Default— Active

<activation>— Specify how the service is activated.

Value

- manual— Subscriber must manually activate the service.
- automatically-on-login— Service is activated automatically when the subscriber logs in.

Default— Manual activation

<activation-order>—(Optional) Order in which subscriptions are automatically activated on login relative to the subscriber's other subscriptions that are configured to activate on login. Review all subscriptions that are configured to activate on login for the subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order that you want the SAE to activate them. If you assign the same number to multiple subscriptions, the SAE activates them in an unspecified order.

Value— Integer in the range 0–2147483647

Default— 10000

<substitution>—(Optional) (Multivalue) Actual values for parameters associated with this object. The policy engine substitutes parameters in policies associated with this object with the values that you specify in the substitution configuration.

Value— Substitution in the form < parameter name > = < value > . For example, bandwidth = 1000000.

Default— No value

Required Privilege Level

subscriber

<vpn> (configuration/subscribers/retailer)

Usage

```
<configuration>
  <subscribers>
    <retailer>
      <vpn>
        <vpn-id>vpn-id</vpn-id> <!-- identifier -->
        <extranet-client>extranet-client</extranet-client>
        <display-name>display-name</display-name>
        <description>description</description>
      </vpn>
    </retailer>
  </subscribers>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Add a VPN to the subscriber configuration.

Contents

<vpn-id>— Name of the routing instance on a JUNOS routing platform that implements the VPN.

Value— Text

<extranet-client>—(Optional) (Multivalue) DN of a retailer or an enterprise that is an extranet client of this VPN.

Value— DN

Default— No value

<display-name>—(Optional) Subscriber's name as it appears in portal applications. If you do not specify a display name, the value of the name option is used.

Value— Text

Default— No value

`<description>`—(Optional) Description of the object that you are configuring.

Value— Text

Default— No value

Required Privilege Level

subscriber

Redirect Server Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the Redirect Server. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
redirect-server	<u>< redirect-server ></u>
redirect-server dns	<u>< dns ></u>
redirect-server ip-redirect	<u>< ip-redirect ></u>
redirect-server ldap	<u>< ldap ></u>
redirect-server monitor	<u>< monitor ></u>

<redirect-server> (configuration)

Usage

```
<configuration>
  <redirect-server>
    <tcp-port>tcp-port</tcp-port>
    <destination-url>destination-url</destination-url>
    <proxy-support/>
    <proxy-destination-url>proxy-destination-url</proxy-destination-url>
    <refresh/>
    <refresh-document>refresh-document</refresh-document>
    <request-rate>request-rate</request-rate>
    <request-burst-size>request-burst-size</request-burst-size>
    <client-rate>client-rate</client-rate>
    <client-burst-size>client-burst-size</client-burst-size>
    <check-file-extensions/>
    <file-extensions>file-extensions</file-extensions>
    <redundancy/>
  </redirect-server>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure redirect server properties. The redirect server redirects HTTP requests to a captive portal page.

Contents

<tcp-port>—(Optional) TCP port number on which the redirect server listens for requests. Use any valid TCP port number.

Value—Integer in the range 1–65535

Default—8800

<destination-url>—URL sent as a response to redirect requests. Typically, this URL is the URL of the captive portal.

The URL can contain the special strings "%(url)s" and "%(proxy)s." If the HTTP request is sent to a proxy, the "%(url)s" string is replaced with the originally requested URL, and the "%(proxy)s" string is replaced with the proxy's "<ipAddress> : <port>". If the request is sent directly, the string is replaced with "None."

If the `proxy-destination-url` option is not configured, this URL is used for both proxy and nonproxy requests.

Value— `http://<serverHost>/accessDenied.do?url=%(url)s` where `<serverHost>` is a valid URL; a string of ASCII characters.

`<proxy-support>`—(Optional) Enable proxy support. If you do not enable proxy support, the redirect server handles proxy requests in the same manner as direct requests.

`<proxy-destination-url>`—(Optional) URL sent as a response to proxy requests. If you do not configure a value, then the URL defaults to the value for the `destination-url` option. You can use this option to send proxy requests to a page different from the page specified by the `destination-url` option.

Value— Valid URL; string of ASCII characters in URL string format

`<refresh>`—(Optional) Specify that the redirect server send an HTTP 200 OK response with an HTML document that includes the `<HTTP-Equiv = "Refresh">` header to a subscriber's browser in response to a captured request. If not set, the redirect server sends a 302 Found response to the client. If the client is not a Web browser, typically it does not follow the URL included in the `refresh` option.

`<refresh-document>`—(Optional)

Directory path to a local HTML file that the redirect server returns to a subscriber's browser in response to a captured HTTP request.

If you enter an invalid path, the redirect server uses a default file. This file can contain the string `"%(url)s"` which is replaced with the URL of the local HTML file to be returned to the subscriber's browser.

Value— Path to HTML file

`<request-rate>`—(Optional) Number of requests that the redirect server can accept per minute from all clients (global sustained rate).

Value— Integer in the range 0–2147483647

Default— 12000

`<request-burst-size>`—(Optional) Maximum number of requests that the redirect server can accept from all clients (burst size). This value should exceed value set by the

`request-rate` option. If the number of requests exceeds this value, the redirect server drops the excess requests.

Value— Integer in the range 0–2147483647

Default— 18000

`<client-rate>`—(Optional) Number of requests that the redirect server can accept per minute for a single client (per client sustained rate).

Value— Integer in the range 0–2147483647

Default— 25

`<client-burst-size>`—(Optional) Maximum number of requests that the redirect server can accept for a single client (per client burst size). This value should exceed the value set by the `client-rate` option. If at any time the number of requests from one client exceeds this value, the redirect server drops the excess requests.

Value— Integer in the range 0–2147483647

Default— 50

`<check-file-extensions>`—(Optional) Check file extension of requested URLs and accept only URLs that point to files that have standard file extensions— `<empty>`, `.asp`, `.htm`, `.html`, `.jsp`, `.php`, `.shtml`, `.shtm` and `.xml`, and extensions specified by the `file-extensions` option. If a URL does not have a standard extension, the redirect server returns an HTTP 403 Forbidden message.

If not set, the redirect server accepts all file extensions.

Default— false

`<file-extensions>`—(Optional) (Multivalue) List of file extensions that augments the standard list of extensions. Entries for extensions are case-sensitive and are preceded by a period.

Value— Text string of file extensions.

`<redundancy>`—(Optional) Enable redundancy for the redirect server on this system, which then monitors a redundant redirect server and configures static routes in the managed JUNOS routers to facilitate failover.

Required Privilege Level

system

<dns> (configuration/redirect-server)

Usage

```
<configuration>
  <redirect-server>
    <dns>
      <enable/>
      <tcp-port>tcp-port</tcp-port>
      <udp-port>udp-port</udp-port>
      <forwarder>forwarder</forwarder>
      <error-ip-address>error-ip-address</error-ip-address>
    </dns>
  </redirect-server>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for the DNS server included with the redirect server.

Contents

<enable>—(Optional) Enable the DNS server included with the redirect server.

A DNS server is required to support HTTP proxies to resolve the name of any HTTP proxy, even if the name is valid only in the private domain of the client. You can use an external DNS server or the DNS server that is included with the redirect for this purpose.

<tcp-port>— TCP port on which the DNS server listens. You can disable the TCP port by entering 0.

Value—Integer in the range 0–65535

Default—8853

<udp-port>— UDP port on which the DNS server listens. You can disable the UDP port by entering 0.

Value—Integer in the range 0–65535

Default—8853

`<forwarder>`—(Optional) (Multivalue) DNS servers to which requests are forwarded.

If you specify DNS servers for this option, incoming requests are forwarded to one of these servers. If you do not specify servers, the DNS server will resolve incoming requests using the normal DNS method.

Value— List of fully qualified IP address of DNS servers.

`<error-ip-address>`—(Optional) IP address that is returned when a DNS request results in an unknown name (NXDOMAIN) error.

Value— Fully qualified IP address

Default— 192.168.254.2

Required Privilege Level

system

<ip-redirect> (configuration/redirect-server)

Usage

```
<configuration>
  <redirect-server>
    <ip-redirect>
      <interface>interface</interface>
      <port>port</port>
    </ip-redirect>
  </redirect-server>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure IP redirection.

Contents

<interface>—(Optional) (Multivalue) Interface on a C-series platform that forwards traffic to be redirected. If you do not specify one or more interface names, the redirect server accepts specified traffic from all interfaces.

Value— Interface name

<port>—(Optional) (Multivalue) Port number that identifies traffic destined for this port to be redirected to another URL.

Value—Integer in the range 1–65535

Default— 80

Required Privilege Level

system

<ldap> (configuration/redirect-server)

Usage

```
<configuration>
  <redirect-server>
    <ldap>
      <url>url</url>
      <bind-dn>bind-dn</bind-dn>
      <bind-password>bind-password</bind-password>
      <base-dn>base-dn</base-dn>
    </ldap>
  </redirect-server>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure directories employed by the redirect server.

Contents

<url>—(Multivalue) List of the URLs for directories employed by the redirect server.

Value— URL in the format `ldap:// <host> : <portNumber>` , where
 < host > is the IP address or name of the host that supports the
 directory, and < portNumber > is the number of the TCP port. Example
 — `ldap://localhost ldap://1.2.3.4:389`

<bind-dn>— DN that the redirect server uses to authorize connections to the directory.
 The DN must have read and write access to *o= Network*, < baseDN> , where < baseDN> is
 the root of the SDX directory tree.

Value— DN

<bind-password>— Password used to authorize connections to the directory.

Value— Text string in LDAP format

`<base-dn>`—(Optional) Base DN that is the root of the SDX directory tree. The redirect server can store information at any DN subordinate to the base DN that you specify.

Value— DN

Default—o = umc

Required Privilege Level

system

<monitor> (configuration/redirect-server)

Usage

```
<configuration>
  <redirect-server>
    <monitor>
      <redundant-host-ip-address>redundant-host-ip-address</redundant-host-ip-
address>
      <virtual-ip-address>virtual-ip-address</virtual-ip-address>
      <real-ip-address>real-ip-address</real-ip-address>
      <primary-server/>
      <check-interval>check-interval</check-interval>
      <virtual-routers>virtual-routers</virtual-routers>
    </monitor>
  </redirect-server>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure redundancy for the redirect server. With redundancy configured, a pair of redirect servers monitor each other. If one server detects that the other server is not responding, it reconfigures all managed JUNOS virtual routers with a static route that points to a virtual IP address to the active redirect server.

Contents

<redundant-host-ip-address>— IP address of the redundant redirect server.

Value— Fully qualified IP address

<virtual-ip-address>— Virtual IP address of the redirect server. Do not specify a hostname.

You can configure the primary and redundant redirect servers to share this address under a common name in the DNS. Each redirect server dynamically sets up and maintains a static route on managed JUNOS routers. The static route directs client traffic destined for the virtual IP address to the real IP address of the active redirect server.

Value— Fully qualified IP address

Default— 192.168.254.1

`<real-ip-address>`— Real IP address of the redirect server. Do not specify a hostname.

Each redirect server dynamically sets up and maintains a static route on managed JUNOS routers. The static route directs client traffic that is destined for the virtual IP address to the real IP address of the active redirect server.

Value— Fully qualified IP address

`<primary-server>`—(Optional) Set this redirect server as the primary server. When the primary redirect server is started, it configures a static route for the virtual IP address.

If not enabled for this redirect server, this server becomes the redundant one.

Default—false

`<check-interval>`—(Optional) Interval at which the primary redirect server polls the redundant redirect server.

A shorter interval leads to faster detection of problems and results in higher consumption of CPU resources.

Value— Number of seconds in the range 60/clientRate–2147483647, where clientRate is the number of requests per minute that the redirect server accepts from one client.

Default—30

`<virtual-routers>`—(Multivalue) List of virtual routers to which the redirect server connects.

Value— Identifier for the virtual router in the format `< vrName > @ < routerName >`, where `< vrName >` is the name of the virtual router, and `< routerName >` is the name of the router on which the virtual router is configured.

Required Privilege Level

system

SRC Admission Control Plug-In (SRC-ACP) Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for providing admission control. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
shared acp configuration acp-options	<u>< acp-options ></u>
shared acp configuration corba	<u>< corba ></u>
shared acp configuration ldap service-data	<u>< service-data ></u>
shared acp configuration ldap subscriber-data	<u>< subscriber-data ></u>
shared acp configuration logger	<u>< logger ></u>
shared acp configuration logger name file	<u>< file ></u>
shared acp configuration logger name syslog	<u>< syslog ></u>
shared acp configuration nic-proxy-configuration nic-proxy	<u>< nic-proxy ></u>
shared acp configuration nic-proxy-configuration nic-proxy name cache	<u>< cache ></u>
shared acp configuration nic-proxy-configuration nic-proxy name nic-host-selection	<u>< nic-host-selection ></u>
shared acp configuration nic-proxy-configuration nic-proxy name nic-host-selection blacklisting	<u>< blacklisting ></u>
shared acp configuration nic-proxy-configuration nic-proxy name resolution	<u>< resolution ></u>
shared acp configuration nic-proxy-configuration nic-proxy name test-nic-bindings	<u>< test-nic-bindings ></u>
shared acp configuration nic-proxy-configuration nic-proxy name test-nic-bindings key-values	<u>< key-values ></u>
shared acp configuration redundancy	<u>< redundancy ></u>
shared acp configuration scripts-and-classification	<u>< scripts-and-classification ></u>
shared acp congestion-point-classifier rule	<u>< rule ></u>
shared acp congestion-point-classifier rule name condition	<u>< condition ></u>

shared acp group	<u>< group ></u>
shared admission-control device	<u>< device ></u>
shared admission-control device name interface	<u>< interface ></u>
shared congestion-points congestion-point-profile	<u>< congestion-point-profile ></u>
shared congestion-points profile	<u>< profile ></u>
slot number acp	<u>< acp ></u>
slot number acp initial	<u>< initial ></u>
slot number acp initial directory-connection	<u>< directory-connection ></u>
slot number acp initial directory-eventing	<u>< directory-eventing ></u>

<acp-options> (configuration/shared/acp/configuration)

Usage

```

<configuration>
  <shared>
    <acp>
      <configuration>
        <acp-options>
          <backup-directory>backup-directory</backup-directory>
          <mode>mode-choice</mode>
          <event-cache-size>event-cache-size</event-cache-size>
          <overload-method>overload-method</overload-method>
          <reservation-timeout>reservation-timeout</reservation-timeout>
          <congestion-point-auto-completion/>
          <tuning-factor>tuning-factor</tuning-factor>
          <subscriber-bandwidth-exceed-message>subscriber-bandwidth-exceed-
message</subscriber-bandwidth-exceed-message>
          <network-bandwidth-exceed-message>network-bandwidth-exceed-message</
network-bandwidth-exceed-message>
          <backup-database-maximum-size>backup-database-maximum-size</backup-
database-maximum-size>
          <remote-update-database-index-keys>remote-update-database-index-
keys</remote-update-database-index-keys>
          <interface-tracking-filter>interface-tracking-filter</interface-
tracking-filter>
          <state-sync-bulk-size>state-sync-bulk-size</state-sync-bulk-size>
        </acp-options>
      </configuration>
    </acp>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP operation.

Contents

<backup-directory>— Folder that stores backup information about subscribers, services, and congestion points.

Value—Text

Default— var/backup

`<mode>`— Regions of the network that SRC-ACP manages.

Value— One of the following regions:

- edge—SRC-ACP operates in the edge region of network only
- backbone—SRC-ACP operates in the backbone region of the network only
- dual—SRC-ACP operates in both the edge and backbone regions of network

Default— dual

`<event-cache-size>`— Number of plug-in events from the SAE that SRC-ACP can store in its cache. Specifying a large number increases the efficiency of SRC-ACP, and minimizes the use of CPU resources; however, the amount of memory available for the cache will depend on the host's resources.

Value— Integer in the range 0–2147483647

Default— 1000

`<overload-method>`— Specifies how SRC-ACP deals with situations where the components exceed the allocated bandwidth because the service was activated after the authorization was granted.

Value— Integer in the range -1–2147483647

- -1—SRC-ACP ignores overload
- Integer greater than or equal to 0—Bandwidth (in bps) by which the maximum may be exceeded

Default— 0

`<reservation-timeout>`—(Optional) Time to wait until a bandwidth reservation expires. The reserved bandwidth is reclaimed by SRC-ACP when the reservation expires.

Value— Integer in the range 0–2147483647 ms

Default— 10000

`<congestion-point-auto-completion>`—(Optional) Specifies whether SRC-ACP uses the information acquired from the router to determine the congestion points.

<tuning-factor>—(Optional) Specifies factors that compensate for actual use of bandwidth, as opposed to allocated bandwidth.

Value— List of tuning factors, separated by commas; each tuning factor is a floating number in the range 0–1

<subscriber-bandwidth-exceed-message>— Error message that SRC-ACP sends when the subscriber exceeds the allocated bandwidth.

Value—Text

Default— Subscriber bandwidth exceeded

<network-bandwidth-exceed-message>— Error message that SRC-ACP sends when traffic flow exceeds the allocated bandwidth on an interface between the subscriber and the router.

Value—Text

Default— Network bandwidth exceeded

<backup-database-maximum-size>— Value by which the sum of the sizes of the files that contain SRC-ACP data can increment before SRC-ACP reorganizes the files. Reorganizing the files reduces their size. Choose a value that is significantly lower than the capacity of the machine's hard disk.

Value— Text string in the format *numberm* or *numberg*

- *numberm*—Size of database in megabytes
- *numberg*—Size of database in gigabytes

Default— 100m

<remote-update-database-index-keys>— Values to look for in the configuration data. Specifying index keys can improve performance by filtering the data. For information about the values you can specify, see the documentation that describes how to configure SRC-ACP operation.

Value— List of attributes, separated by commas

Default— interfaceName, routerName, portId

<interface-tracking-filter>— A filter specifying the interfaces to be tracked by

SRC-ACP. Filtering the interface tracking events can improve performance and can reduce the amount of memory required for keeping the congestion points updated. For information about the values you can specify, see the documentation that describes how to configure SRC-ACP operation.

Value— Filter strings in the format of a list of < attribute > = < value > pairs; that can be contained within query operations. For example: (&(interfaceName = *) (interfaceSpeed = 1000000))

<state-sync-bulk-size>—(Optional) Number of events the SAE sends to SRC-ACP in a single method call during state synchronization.

Value—Integer in the range 1–1000

Default— 100

Required Privilege Level

system

<corba> (configuration/shared/acp/configuration)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <corba>
          <acp-ior>acp-ior</acp-ior>
          <remote-update-ior>remote-update-ior</remote-update-ior>
        </corba>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure CORBA interfaces.

Contents

<acp-ior>— Object reference for SRC-ACP that is exported through either a local file or a Common Object Services (COS) naming service.

Value— One of the following references:

- *file://path*—Exports object reference through a local file where *path* is the absolute path to local file
- *corbaname::cosNameServer#KEY*—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- *corbaname:rir#KEY*—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— *file:///var/acp/acp.ior*

`<remote-update-ior>`—(Optional) Object reference for the SRC-ACP external interface.

Value— One of the following references:

- `file://path`—Exports object reference through a local file where *path* is the absolute path to local file
- `corbaname::cosNameServer#KEY`—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- `corbaname:rir#KEY`—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— `file:///var/acp/sra.ior`

Required Privilege Level

system

<service-data> (configuration/shared/acp/configuration/ldap)

Usage

```

<configuration>
  <shared>
    <acp>
      <configuration>
        <ldap>
          <service-data>
            <edge-congestion-point-dn>edge-congestion-point-dn</edge-
congestion-point-dn>
            <backbone-congestion-point-dn>backbone-congestion-point-dn</
backbone-congestion-point-dn>
            <reload-congestion-points/>
            <congestion-points-eventing/>
            <server-address>server-address</server-address>
            <server-port>server-port</server-port>
            <dn>dn</dn>
            <principal>principal</principal>
            <password>password</password>
            <event-dn>event-dn</event-dn>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
            <secured-ldap-protocol>secured-ldap-protocol-choice</secured-ldap-
protocol>
          </service-data>
        </ldap>
      </configuration>
    </acp>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP connection to the directory that stores information about services.

Contents

<edge-congestion-point-dn>— DN of the directory that contains information about network interfaces for edge congestion points.

Value— DN

Default— o = AdmissionControl, o = umc

<backbone-congestion-point-dn>— DN of the directory that contains information about network interfaces for backbone congestion point objects.

Value— DN

Default— o = CongestionPoints, o = umc

<reload-congestion-points>—(Optional) Specifies whether SRC-ACP detects changes in the backbone congestion point for a service while SRC-ACP is operative.

Enable only when you want to modify a congestion point. Disable when you have modified the congestion point.

<congestion-points-eventing>—(Optional) Enables directory eventing for congestion points.

<server-address>— List of primary and redundant servers that manage data.

Value— List of IP addresses or hostnames separated by spaces

Default— 127.0.0.1

<server-port>— TCP port for the directory.

Value— Integer in the range 0–65535

Default— 389

<dn>— DN of the root of the directory.

Value— List of attribute = value pairs separated by commas

<principal>— DN used to authorize connections to the directory.

Value— List of attribute = value pairs separated by commas

Default— cn = umcadmin, o = umc

<password>— Password used to authorize connections to the directory.

Value— Secret text

Default— admin123

<event-dn>— DN of the directory that contains event information.

Value— DN

<directory-eventing>—(Optional) Enable directory eventing.

<polling-interval>— Time interval at which the SRC component polls the directory.

Value— Number of seconds in the range 15–86400

Default— 30

<secured-ldap-protocol>—(Optional) Secured LDAP protocol

Value

- ldaps—

Required Privilege Level

system

<subscriber-data> (configuration/shared/acp/configuration/ldap)

Usage

```

<configuration>
  <shared>
    <acp>
      <configuration>
        <ldap>
          <subscriber-data>
            <congestion-points-eventing/>
            <server-address>server-address</server-address>
            <server-port>server-port</server-port>
            <dn>dn</dn>
            <principal>principal</principal>
            <password>password</password>
            <event-dn>event-dn</event-dn>
            <directory-eventing/>
            <polling-interval>polling-interval</polling-interval>
            <secured-ldap-protocol>secured-ldap-protocol-choice</secured-ldap-
protocol>
          </subscriber-data>
        </ldap>
      </configuration>
    </acp>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP connection to the directory that stores subscriber information.

Contents

<congestion-points-eventing>—(Optional) Enables directory eventing for congestion points.

<server-address>— List of primary and redundant servers that manage data.

Value— List of IP addresses or hostnames separated by spaces

Default— 127.0.0.1

<server-port>— TCP port for the directory.

Value— Integer in the range 0–65535

Default— 389

<dn>— DN of the root of the directory.

Value— List of attribute = value pairs separated by commas

<principal>— DN used to authorize connections to the directory.

Value— List of attribute = value pairs separated by commas

Default— cn = umcadmin, o = umc

<password>— Password used to authorize connections to the directory.

Value— Secret text

Default— admin123

<event-dn>— DN of the directory that contains event information.

Value— DN

<directory-eventing>—(Optional) Enable directory eventing.

<polling-interval>— Time interval at which the SRC component polls the directory.

Value— Number of seconds in the range 15–86400

Default— 30

<secured-ldap-protocol>—(Optional) Secured LDAP protocol

Value

- ldaps—

Required Privilege Level

system

<logger> (configuration/shared/acp/configuration)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <logger>
          <name>name</name> <!-- identifier -->
        </logger>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination.

Contents

<name>— Name of logging destination.

Value—Text

Required Privilege Level

system

<file> (configuration/shared/acp/configuration/logger)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <logger>
          <file>
            <filter>filter</filter>
            <filename>filename</filename>
            <rollover-filename>rollover-filename</rollover-filename>
            <maximum-file-size>maximum-file-size</maximum-file-size>
          </file>
        </logger>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename**Default**— No value

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filenameExample—`/opt/UMC/sae/var/log/sae.alt`**Default**— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes**Default**— 1000000**Required Privilege Level**

system

<syslog> (configuration/shared/acp/configuration/logger)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <logger>
          <syslog>
            <filter>filter</filter>
            <host>host</host>
            <facility>facility</facility>
            <format>format</format>
          </syslog>
        </logger>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Default— None

Required Privilege Level

system

<nic-proxy> (configuration/shared/acp/configuration)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <name>name</name> <!-- identifier -->
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Contents

<name>—

Value—Text

Required Privilege Level

system

<cache> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <cache>
              <cache-size>cache-size</cache-size>
              <cache-cleanup-interval>cache-cleanup-interval</cache-cleanup-
interval>
              <cache-entry-age>cache-entry-age</cache-entry-age>
            </cache>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Description

Configure the NIC Proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

Contents

<cache-size>—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default— 10000

<cache-cleanup-interval>— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default— 15

`<cache-entry-age>`—(Optional) Maximum time that the NIC proxy can cache an entry. The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Required Privilege Level

system

<nic-host-selection> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <nic-host-selection>
              <groups>groups</groups>
              <selection-criteria>selection-criteria-choice</selection-
criteria>
            </nic-host-selection>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

Contents

<groups>—(Optional) (Multivalue) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

<selection-criteria>— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.

- **priorityList**—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default—round-

Required Privilege Level

system

<blacklisting> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy/nic-host-selection)

Usage

```

<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <nic-host-selection>
              <blacklisting>
                <try-next-system-on-error/>
                <number-of-retries-before-blacklisting>number-of-retries-
before-blacklisting</number-of-retries-before-blacklisting>
                <blacklist-retry-interval>blacklist-retry-interval</blacklist-
retry-interval>
              </blacklisting>
            </nic-host-selection>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Contents

<try-next-system-on-error>—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

<number-of-retries-before-blacklisting>— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the

NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

`<blacklist-retry-interval>`— Interval at which the NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s

Default—15

Required Privilege Level

system

<resolution> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <resolution>
              <resolver-name>resolver-name</resolver-name>
              <key-type>key-type</key-type>
              <value-type>value-type</value-type>
              <expect-multiple-values/>
              <constraints>constraints</constraints>
            </resolution>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

<key-type>— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

`<value-type>`— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaeId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

`<expect-multiple-values>`—(Optional) Specifies whether or not the key can have multiple corresponding values.

`<constraints>`—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.
Default— No value

Required Privilege Level

system

<test-nic-bindings> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <test-nic-bindings>
              <use-test-bindings/>
            </test-nic-bindings>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure key-value mappings to be used to test a NIC resolution.

Contents

<use-test-bindings>—(Optional) Test the NIC resolutions without having to configure or run a NIC host. The values returned are those configured in the key-values property.

Default—false

Required Privilege Level

system

<key-values> (configuration/shared/acp/configuration/nic-proxy-configuration/nic-proxy/test-nic-bindings)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxy>
            <test-nic-bindings>
              <key-values>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </key-values>
            </test-nic-bindings>
          </nic-proxy>
        </nic-proxy-configuration>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure keys and associated values to use for testing. Define all of values to be returned for specified keys.

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<redundancy> (configuration/shared/acp/configuration)

Usage

```
<configuration>
  <shared>
    <acp>
      <configuration>
        <redundancy>
          <enable-redundancy/>
          <local-ior>local-ior</local-ior>
          <remote-ior>remote-ior</remote-ior>
          <ignore-user-tracking-out-of-sync/>
          <community-heartbeat>community-heartbeat</community-heartbeat>
          <community-acquire-timeout>community-acquire-timeout</community-
acquire-timeout>
          <community-blackout-timeout>community-blackout-timeout</community-
blackout-timeout>
          <redundant-naming-service>redundant-naming-service</redundant-
naming-service>
        </redundancy>
      </configuration>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure redundancy and state synchronization for SRC-ACP.

Contents

<enable-redundancy>—(Optional) Enables SRC-ACP redundancy.

<local-ior>— In a redundant SRC-ACP configuration, exports the object reference for this SRC-ACP (local interface) through a Common Object Services (COS) naming service.

Value— One of the following references:

- corbaname::cosNameServer#KEY—Exports object reference through COS naming services
 - cosNameServer—IP address or Domain Name System

- (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- *corbaname:rir#KEY*—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

For example: *corbaname::coshost#acp.redundancy.primary*

<remote-ior>— In a redundant SRC-ACP configuration, resolves the object reference for the other SRC-ACP (remote interface) through a Common Object Services (COS) naming service. For redundancy, the remote IOR value of one SRC-ACP must match the local IOR value of the other SRC-ACP.

Value— One of the following references:

- *corbaname::cosNameServer#KEY*—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- *corbaname:rir#KEY*—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

For example: *corbaname::coshost#acp.redundancy.backup*

<ignore-user-tracking-out-of-sync>—(Optional) Specifies whether user tracking events should be ignored when they raise an OutOfSync exception to the SAE when state synchronization is enabled. SRC-ACP raises an OutOfSync exception when SRC-ACP handles service tracking or authentication events without receiving a user start event first.

Default— false

<community-heartbeat>—(Optional) Time interval for community members to check each other's availability when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 30

<community-acquire-timeout>—(Optional) Time to wait before trying to reacquire the distributed lock when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 15

`<community-blackout-timeout>`—(Optional) Time to wait before regaining control when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 30

`<redundant-naming-service>`—(Optional) In a redundant SRC-ACP configuration, exports the object reference for the backup naming service through a local file or COS naming service. The primary SRC-ACP registers the IOR and redundancy IOR to both naming services, while the secondary SRC-ACP registers the redundancy IOR to both naming services.

Value— One of the following references:

- `file://path`—Exports object reference through a local file where *path* is the absolute path to local file
- `corbaname::cosNameServer#KEY`—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- `corbaname:rir#KEY`—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— None

Required Privilege Level

system

<scripts-and-classification> (configuration/shared/acp/configuration)

Usage

```

<configuration>
  <shared>
    <acp>
      <configuration>
        <scripts-and-classification>
          <script-factory-class>script-factory-class</script-factory-class>
          <classification-factory-class>classification-factory-class</
classification-factory-class>
          <classification-script>classification-script</classification-script>
          <congestion-point-profile-script>congestion-point-profile-script</
congestion-point-profile-script>
          <extension-path>extension-path</extension-path>
        </scripts-and-classification>
      </configuration>
    </acp>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP scripts and classification.

Contents

<script-factory-class>— Script factory class name.

Value—Text

Default— net.juniper.smgt.acp.classify.ScriptFactory

<classification-factory-class>— Congestion point classifier factory class name.

Value—Text

Default— net.juniper.smgt.acp.classify.ClassifyCPFactory

`<classification-script>`— Class name for congestion point classification.

Value—Text

Default— cpClassify

`<congestion-point-profile-script>`— Class name for generating the congestion point DN by using the congestion point profile.

Value—Text

Default— cpProfile

`<extension-path>`— Extension class path for classes not located in the `/opt/UMC/acp/lib` directory.

Value—Text

Required Privilege Level

system

<rule> (configuration/shared/acp/congestion-point-classifier)

Usage

```
<configuration>
  <shared>
    <acp>
      <congestion-point-classifier>
        <rule>
          <name>name</name> <!-- identifier -->
          <target>target</target>
          <script>script</script>
        </rule>
      </congestion-point-classifier>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a congestion point classification script.

Contents

<name>— Name of a congestion point classification script.

Value—Text

<target>—(Optional) Result of the classification script. The result is the DN of a congestion point in the directory or an LDAP query that uniquely identifies a congestion point entry in the directory.

Value—Text

<script>—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Required Privilege Level

No specific privilege required.

<condition> (configuration/shared/acp/congestion-point-classifier/rule)

Usage

```
<configuration>
  <shared>
    <acp>
      <congestion-point-classifier>
        <rule>
          <condition>
            <criteria>criteria</criteria> <!-- identifier -->
          </condition>
        </rule>
      </congestion-point-classifier>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure classification criteria that is used to find a target.

Contents

<criteria>— Classification criteria. For information about configuring classification criteria, see *Classifying Congestion Points* in the *SRC-PE Network Guide*.

Value— Classification criteria are organized by putting one criterion per line. A criterion is joined with the previous criterion by:

- OR if the line does not contain a prefix or if it is prefixed with a | (pipe) character. A criterion joined by OR is examined only if the previous conditions have not produced a positive match. If any of the criteria joined by OR matches, the target is selected.
- AND if the line is prefixed with an & (ampersand) character. A criterion joined by AND is examined only if the previous condition matches.

You can use glob or regular expression matching to configure each target's criteria.

Required Privilege Level

No specific privilege required.

<group> (configuration/shared/acp)

Usage

```
<configuration>
  <shared>
    <acp>
      <group>
        <name>name</name> <!-- identifier -->
      </group>
    </acp>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure group of SRC-ACP configuration properties.

Contents

<name>— Name of an SRC-ACP configuration.

Value—Text

Required Privilege Level

system

<device> (configuration/shared/admission-control)

Usage

```
<configuration>
  <shared>
    <admission-control>
      <device>
        <name>name</name> <!-- identifier -->
        <description>description</description>
      </device>
    </admission-control>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the locations of congestion points in the directory.

Contents

<name>— Network device name.

Value—Text

<description>—(Optional) Network device description.

Value—Text

Required Privilege Level

system

<interface> (configuration/shared/admission-control/device)

Usage

```

<configuration>
  <shared>
    <admission-control>
      <device>
        <interface>
          <name>name</name> <!-- identifier -->
          <description>description</description>
          <upstream-provisioned-rate>upstream-provisioned-rate</upstream-
provisioned-rate>
          <downstream-provisioned-rate>downstream-provisioned-rate</
downstream-provisioned-rate>
          <upstream-background-bandwidth>upstream-background-bandwidth</
upstream-background-bandwidth>
          <downstream-background-bandwidth>downstream-background-bandwidth</
downstream-background-bandwidth>
          <action-type>action-type-choice</action-type>
          <action-class-name>action-class-name</action-class-name>
          <action-file-url>action-file-url</action-file-url>
          <action-parameters>action-parameters</action-parameters>
          <action-file-name>action-file-name</action-file-name>
          <detect-link-rate/>
        </interface>
      </device>
    </admission-control>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the network interfaces that represent locations of congestion points in the directory.

Contents

<name>— Interface name.

Value—Text

<description>—(Optional) Network interface description.

Value—Text

<upstream-provisioned-rate>—(Optional) Upstream provisioned rate.

Value—Integer in the range 0–9223372036854775807 bps

<downstream-provisioned-rate>—(Optional) Downstream provisioned rate.

Value—Integer in the range 0–9223372036854775807 bps

<upstream-background-bandwidth>—(Optional) (Multivalue) Upstream background bandwidth.

Value—Integer in the range 0–9223372036854775807 bps

<downstream-background-bandwidth>—(Optional) (Multivalue) Downstream background bandwidth.

Value—Integer in the range 0–9223372036854775807 bps

<action-type>—(Optional) Type of action congestion point. Determines how the contents of the "action-file-url" attribute will be interpreted.

Value

- url— The value of attribute "action-file-url" is a URL that specifies where to find a Java archive (.jar file) containing the script service implementation.
- python— The value of attribute "action-file-url" is Python code.
- java-class— The value of attribute "action-file-url" is the binary contents of a compiled Java class file (.class file).
- java-archive— The value of attribute "action-file-url" is the binary contents of a Java archive file (.jar file).

<action-class-name>—(Optional) Name of Java or Python class implementing the action congestion point. The ACP instantiates the named class.

Value—Text

`<action-file-url>`—(Optional) If the action type is "URL", this attribute contains the URL of a Java archive (.jar) file containing the action congestion point implementation. Otherwise, this attribute contains the action congestion point implementation itself (i.e. python code, the binary contents of a compiled .class file, or the binary contents of a .jar file).

`<action-parameters>`—(Optional) (Multivalue) Parameters used by the action congestion point.

Value— Text string in the format of a list of `< attribute > = < value >` pairs

`<action-file-name>`—(Optional) The file needs to exist locally. Its content will be read and loaded into the "action-file-url" attribute.

Value—Text

`<detect-link-rate>`—(Optional) To identify the possibility of getting the actual link rate information for a congestion point via L2C or other solutions developed later. By default , it is false for the sake of backward compatibility.

Default—false

Required Privilege Level

system

<congestion-point-profile> (configuration/shared/congestion-points)

Usage

```
<configuration>
  <shared>
    <congestion-points>
      <congestion-point-profile>
        <name>name</name> <!-- identifier -->
        <expression>expression</expression>
      </congestion-point-profile>
    </congestion-points>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure congestion point profile.

Contents

<name>— Congestion point profile name.

Value—Text

<expression>—(Optional) (Multivalue) Congestion point expression.

Value—Text

Required Privilege Level

system

<profile> (configuration/shared/congestion-points)

Usage

```
<configuration>
  <shared>
    <congestion-points>
      <profile>
        <name>name</name> <!-- identifier -->
        <interface>interface</interface>
      </profile>
    </congestion-points>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure congestion point.

Contents

<name>— Congestion point name.

Value—Text

<interface>—(Optional) (Multivalue) Congestion point reference.

Value—Text

Required Privilege Level

system

<acp> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <acp>
      <java-runtime-environment>java-runtime-environment</java-runtime-
environment>
      <java-heap-size>java-heap-size</java-heap-size>
      <java-garbage-collection-options>java-garbage-collection-options</java-
garbage-collection-options>
      <base-dn>base-dn</base-dn>
      <snmp-agent/>
      <shared>shared</shared>
    </acp>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local properties for SRC-ACP.

Contents

<java-runtime-environment>— Path to the Java Runtime Environment (JRE). The SRC software requires a JRE that conforms to the Java 2 specification.

Value—Text

Default— `../jre/bin/java`

<java-heap-size>— Maximum amount of Java heap (memory) available to the JRE.

Value— Number of megabytes in the format *integerm*

Default— 64m

<java-garbage-collection-options>— Garbage collection functionality of the Java Virtual Machine.

Value—**Default—** -Xbatch -XX: + UseConcMarkSweepGC -XX:

CMSInitiatingOccupancyFraction = 80 -XX:NewRatio = 5 -XX:

+ UseParNewGC -XX:SurvivorRatio = 1 -XX:

InitialTenuringThreshold = 8 -XX:MaxTenuringThreshold = 10 -XX:

TargetSurvivorRatio = 90 -XX: + UseCMSCompactAtFullCollection -XX:

CMSFullGCsBeforeCompaction = 0 -XX: + CMSClassUnloadingEnabled -

XX: + CMSParallelRemarkEnabled

<base-dn>— DN of the root of the SDX data in the directory.

If you are storing non-SDX data in the directory, and that data changes frequently whereas the SDX data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SDX data and the changing non-SDX data.

Value— DN

<snmp-agent>—(Optional) Enables SRC-ACP to communicate with the SNMP agent.

<shared>— Shared configuration object that holds most of the SRC-ACP specific configuration.

Value— Name of the object in the format "/ < path > ". If the < path > contains multiple levels, the levels are separated by a slash (/). The effective configuration is combined by all configuration objects in the path, with more specific configuration in the lower levels of the path.

Default— /config**Required Privilege Level**

system

<initial> (configuration/slot/acp)

Usage

```
<configuration>
  <slot>
    <acp>
      <initial>
        <static-dn>static-dn</static-dn>
        <dynamic-dn>dynamic-dn</dynamic-dn>
      </initial>
    </acp>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for SRC components.

Contents

<static-dn>—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—ou = staticConfiguration,ou = Configuration,o = Management,
o = umc

<dynamic-dn>—(Optional) Location of programmatically-defined configuration data in the directory.

Value—Text

Default—ou = dynamicConfiguration,ou = Configuration,
o = Management,o = umc

Required Privilege Level

system

<directory-connection> (configuration/slot/acp/initial)

Usage

```
<configuration>
  <slot>
    <acp>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </acp>
  </slot>
</configuration>
```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

system

<directory-eventing> (configuration/slot/acp/initial)

Usage

```
<configuration>
  <slot>
    <acp>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </acp>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

<polling-interval>—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s
Default—30

<event-base-dn>—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN
Default—o = UMC

<dispatcher-pool-size>—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default— 1

Required Privilege Level

system

External Subscriber Monitor Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for External Subscriber Monitor. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

| CLI Configuration Statement | Configuration Tag Element |
|---|--|
| slot external-subscriber-monitor | <u>< external-subscriber-monitor ></u> |
| slot external-subscriber-monitor event-notification | <u>< event-notification ></u> |
| slot external-subscriber-monitor initial | <u>< initial ></u> |
| slot external-subscriber-monitor initial directory-connection | <u>< directory-connection ></u> |
| slot external-subscriber-monitor initial directory-eventing | <u>< directory-eventing ></u> |
| slot external-subscriber-monitor logger | <u>< logger ></u> |
| slot external-subscriber-monitor logger name file | <u>< file ></u> |
| slot external-subscriber-monitor logger name syslog | <u>< syslog ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-accounting-nic cache | <u>< cache ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-accounting-nic nic-host-selection | <u>< nic-host-selection ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-accounting-nic nic-host-selection blacklisting | <u>< blacklisting ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-accounting-nic resolution | <u>< resolution ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-authorization-nic cache | <u>< cache ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-authorization-nic nic-host-selection | <u>< nic-host-selection ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-authorization-nic nic-host-selection blacklisting | <u>< blacklisting ></u> |
| slot external-subscriber-monitor nic-proxy-configuration radius-authorization-nic resolution | <u>< resolution ></u> |
| slot external-subscriber-monitor radius-accounting | <u>< radius-accounting ></u> |

| | |
|---|---|
| slot external-subscriber-monitor radius-accounting client | <u>< client ></u> |
| slot external-subscriber-monitor radius-attribute-extraction default interface-name | <u>< interface-name ></u> |
| slot external-subscriber-monitor radius-attribute-extraction default virtual-router-name | <u>< virtual-router-name ></u> |
| slot external-subscriber-monitor radius-authorization | <u>< radius-authorization ></u> |
| slot external-subscriber-monitor radius-authorization client | <u>< client ></u> |
| slot external-subscriber-monitor radius-authorization ldap cached-dhcp-profile | <u>< cached-dhcp-profile ></u> |
| slot external-subscriber-monitor radius-authorization ldap cached-dhcp-profile directory-connection | <u>< directory-connection ></u> |
| slot external-subscriber-monitor radius-authorization ldap subscriber-data | <u>< subscriber-data ></u> |
| slot external-subscriber-monitor radius-authorization ldap subscriber-data directory-connection | <u>< directory-connection ></u> |

<external-subscriber-monitor> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <java-heap-size>java-heap-size</java-heap-size>
      <java-garbage-collection-options>java-garbage-collection-options</java-
garbage-collection-options>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the local properties for External Subscriber Monitor.

Contents

<java-heap-size>— Maximum Java heap (memory) size available to the JRE. Changes take effect only after you restart External Subscriber Monitor.

Value— Number of megabytes in the format *integerm*

Default— 160m

<java-garbage-collection-options>—(Optional) Garbage collection functionality of the Java Virtual Machine.

Value—

Default— -Xbatch -XX: + UseConcMarkSweepGC -XX:

CMSInitiatingOccupancyFraction = 80 -XX: + UseParNewGC -XX:

SurvivorRatio = 1 -XX:InitialTenuringThreshold = 8 -XX:

MaxTenuringThreshold = 10 -XX:TargetSurvivorRatio = 90 -XX:

+ UseCMSCompactAtFullCollection -XX:

CMSFullGCsBeforeCompaction = 0 -XX: + CMSClassUnloadingEnabled -

XX: + CMSParallelRemarkEnabled

Required Privilege Level

No specific privilege required.

<event-notification> (configuration/slot/external-subscriber-monitor)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <event-notification>
        <event-threads>event-threads</event-threads>
        <event-thread-idle-timeout>event-thread-idle-timeout</event-thread-
idle-timeout>
        <event-retry-timeout>event-retry-timeout</event-retry-timeout>
        <event-retry-interval>event-retry-interval</event-retry-interval>
        <session-timeout>session-timeout</session-timeout>
      </event-notification>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure event notification. This is mandatory if radius-accounting is on.

Contents

<event-threads>—(Optional) Maximum number of concurrent threads in a pool for event handler.

Value—Integer in the range 1-2147483648

Default— 8

<event-thread-idle-timeout>—(Optional) Time to keep an event handler alive for reuse.

Value—Integer in the range 1-2147483648 second

Default— 300

<event-retry-timeout>—(Optional) Maximum time to wait before discarding failed

events.

Value—Integer in the range 1–2147483648 second

Default— 300

`<event-retry-interval>`—(Optional) Time to wait before retrying failed events.

Value—Integer in the range 1–2147483648 second

Default— 30

`<session-timeout>`—(Optional) Keepalive time for a RADIUS subscriber or service.

This value should be larger than the interim update interval. We recommend twice the interim update interval. Setting the session timeout less than or equal to zero means the subscriber session never expires.

Value—Integer in the range -2147483648–2147483647 second

Default— 1800

Required Privilege Level

No specific privilege required.

<initial> (configuration/slot/external-subscriber-monitor)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <initial>
        <dynamic-dn>dynamic-dn</dynamic-dn>
      </initial>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure initial properties for SRC components.

Contents

<dynamic-dn>—(Optional) Location of programmatically-defined configuration data in the directory.

Value—Text

Default—ou = dynamicConfiguration, ou = Configuration,
o = Management, o = umc

Required Privilege Level

No specific privilege required.

<directory-connection> (configuration/slot/external-subscriber-monitor/initial)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use < base > to indicate the base DN.

<credentials>— Password with which the SRC component accesses the directory.

Value— Password

<protocol>—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- ldaps— LDAPS which uses SSL.

<timeout>—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

<check-interval>—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

<blacklist>—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

<snmp-agent>—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

No specific privilege required.

<directory-eventing> (configuration/slot/external-subscriber-monitor/initial)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

`<polling-interval>`—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30

`<event-base-dn>`—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default—o = UMC

`<dispatcher-pool-size>`—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

Default—1

Required Privilege Level

No specific privilege required.

<logger> (configuration/slot/external-subscriber-monitor)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <logger>
        <name>name</name> <!-- identifier -->
      </logger>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the logging destination.

Contents

<name>— Name used to group parameters for the logging destination.

Value— Text

Required Privilege Level

No specific privilege required.

<file> (configuration/slot/external-subscriber-monitor/logger)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <logger>
        <file>
          <filter>filter</filter>
          <filename>filename</filename>
          <rollover-filename>rollover-filename</rollover-filename>
          <maximum-file-size>maximum-file-size</maximum-file-size>
        </file>
      </logger>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the logging destination for file-based logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

No specific privilege required.

<syslog> (configuration/slot/external-subscriber-monitor/logger)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <logger>
        <syslog>
          <filter>filter</filter>
          <host>host</host>
          <facility>facility</facility>
          <format>format</format>
        </syslog>
      </logger>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the logging destination for syslog-based logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Required Privilege Level

No specific privilege required.

<cache> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-accounting-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-accounting-nic>
          <cache>
            <cache-size>cache-size</cache-size>
            <cache-cleanup-interval>cache-cleanup-interval</cache-cleanup-
interval>
            <cache-entry-age>cache-entry-age</cache-entry-age>
          </cache>
        </radius-accounting-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure the NIC Proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

Contents

<cache-size>—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default— 10000

<cache-cleanup-interval>— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default— 15

<cache-entry-age>—(Optional) Maximum time that the NIC proxy can cache an entry.

The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Required Privilege Level

No specific privilege required.

<nic-host-selection> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-accounting-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-accounting-nic>
          <nic-host-selection>
            <groups>groups</groups>
            <selection-criteria>selection-criteria-choice</selection-
criteria>
          </nic-host-selection>
        </radius-accounting-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

Contents

<groups>—(Optional) (Multivalue) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

<selection-criteria>— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest

priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default—roundRobin

Required Privilege Level

No specific privilege required.

<blacklisting> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-accounting-nic/nic-host-selection)

Usage

```

<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-accounting-nic>
          <nic-host-selection>
            <blacklisting>
              <try-next-system-on-error/>
              <number-of-retries-before-blacklisting>number-of-retries-before-
blacklisting</number-of-retries-before-blacklisting>
              <blacklist-retry-interval>blacklist-retry-interval</blacklist-
retry-interval>
            </blacklisting>
          </nic-host-selection>
        </radius-accounting-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Contents

<try-next-system-on-error>—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

<number-of-retries-before-blacklisting>— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the

NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

`<blacklist-retry-interval>`— Interval at which the NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s

Default—15

Required Privilege Level

No specific privilege required.

<resolution> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-accounting-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-accounting-nic>
          <resolution>
            <resolver-name>resolver-name</resolver-name>
            <constraints>constraints</constraints>
          </resolution>
        </radius-accounting-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1

Default— No value

<constraints>—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.
Default— No value

Required Privilege Level

No specific privilege required.

<cache> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-authorization-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-authorization-nic>
          <cache>
            <cache-size>cache-size</cache-size>
            <cache-cleanup-interval>cache-cleanup-interval</cache-cleanup-
interval>
            <cache-entry-age>cache-entry-age</cache-entry-age>
          </cache>
        </radius-authorization-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure the NIC Proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

Contents

<cache-size>—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default— 10000

<cache-cleanup-interval>— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default— 15

<cache-entry-age>—(Optional) Maximum time that the NIC proxy can cache an entry.

The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Required Privilege Level

No specific privilege required.

<nic-host-selection> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-authorization-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-authorization-nic>
          <nic-host-selection>
            <groups>groups</groups>
            <selection-criteria>selection-criteria-choice</selection-
criteria>
          </nic-host-selection>
        </radius-authorization-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

Contents

<groups>—(Optional) (Multivalue) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

<selection-criteria>— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest

priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default—roundRobin

Required Privilege Level

No specific privilege required.

<blacklisting> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-authorization-nic/nic-host-selection)

Usage

```

<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-authorization-nic>
          <nic-host-selection>
            <blacklisting>
              <try-next-system-on-error/>
              <number-of-retries-before-blacklisting>number-of-retries-before-
blacklisting</number-of-retries-before-blacklisting>
              <blacklist-retry-interval>blacklist-retry-interval</blacklist-
retry-interval>
            </blacklisting>
          </nic-host-selection>
        </radius-authorization-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>

```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Contents

<try-next-system-on-error>—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

<number-of-retries-before-blacklisting>— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the

NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

`<blacklist-retry-interval>`— Interval at which the NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s

Default—15

Required Privilege Level

No specific privilege required.

<resolution> (configuration/slot/external-subscriber-monitor/nic-proxy-configuration/radius-authorization-nic)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <nic-proxy-configuration>
        <radius-authorization-nic>
          <resolution>
            <resolver-name>resolver-name</resolver-name>
            <constraints>constraints</constraints>
          </resolution>
        </radius-authorization-nic>
      </nic-proxy-configuration>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1

Default— No value

<constraints>—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Required Privilege Level

No specific privilege required.

<radius-accounting> (configuration/slot/external-subscriber-monitor)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-accounting>
        <port>port</port>
        <include-mac-address/>
        <include-interface-name/>
        <service-type>service-type-choice</service-type>
        <allow>allow</allow>
        <deny>deny</deny>
        <maximum-queue-length>maximum-queue-length</maximum-queue-length>
      </radius-accounting>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the pseudo-RADIUS server. If not configured, no pseudo-RADIUS service is started.

Contents

<port>— Listening port for RADIUS accounting requests.

Value—Integer in the range 1–65535

Default— 1813

<include-mac-address>—(Optional) Specify whether the MAC address is included in the event notification.

NOTE: Do not configure if you are not extracting RADIUS attributes with the pseudo-RADIUS server.

Default— false

<include-interface-name>—(Optional) Specify whether the interface name is included in the event notification.

NOTE: Do not configure if you are not extracting RADIUS attributes with the pseudo-RADIUS server.

Default— false

<service-type>—(Optional) Service type of RADIUS packets that will be forwarded.

Value

- all— Forward all packets
- login— Forward packets with type of Login
- framed— Forward packets with type of Framed
- callback-login— Forward packets with type of Callback Login
- callback-framed— Forward packets with type of Callback Framed
- outbound— Forward packets with type of Outbound
- administrative— Forward packets with type of Administrative
- nas-prompt— Forward packets with type of NAS Prompt
- authenticate-only— Forward packets with type of Authenticate Only
- callback-nas-prompt— Forward packets with type of Callback NAS Prompt
- callback-check— Forward packets with type of Callback Check
- callback-administrative— Forward packets with type of Callback Administrative

Default— framed

<allow>—(Optional) (Multivalue) List of hosts that filters which packets are forwarded. If both the allow and deny lists are empty, forward all packets. If the allow list has entries and the deny list is empty, forward packets from the listed hosts and ignore all others. If the allow list is empty and the deny list has entries, forward all packets except those from the listed hosts in the deny list. If both the allow and deny lists have entries, forward packets from the listed hosts in the allow list, and ignore the deny list entries.

Value— Entries are delimited by spaces in the format ID = < regular expression > or IP = < regular expression >

Example—allow = ID = C2000.*

Default— Empty list

<deny>—(Optional) (Multivalue) List of hosts that filters which packets are forwarded. If both the allow and deny lists are empty, forward all packets. If the allow list has entries and the deny list is empty, forward packets from the listed hosts and ignore all others. If the allow list is empty and the deny list has entries, forward all packets except those from the listed hosts in the deny list. If both the allow and deny lists have entries, forward packets from the listed hosts in the allow list and ignore the deny list entries.

Value— Entries are delimited by spaces in the format ID = < regular expression > or IP = < regular expression >

Example—deny = ID = SAE.*

Default— Empty list

<maximum-queue-length>— Maximum number of unacknowledged RADIUS messages received from the RADIUS server before it discards new messages. 0 or negative number means infinite number of messages are allowed.

Value— Integer in the range 0–2147483647

Default— 10000

Required Privilege Level

No specific privilege required.

<client> (configuration/slot/external-subscriber-monitor/radius-accounting)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-accounting>
        <client>
          <client-address>client-address</client-address> <!-- identifier -->
          <secret>secret</secret>
        </client>
      </radius-accounting>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the shared secret between the RADIUS server and its clients.

Contents

<client-address>— Address of the specific RADIUS client.

Value— Address in dot format. Currently, only IPv4 addresses are supported.

<secret>— Shared secret of a specific RADIUS client.

Value—Secret text

Required Privilege Level

No specific privilege required.

<interface-name> (configuration/slot/external-subscriber-monitor/radius-attribute-extraction/default)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-attribute-extraction>
        <default>
          <interface-name>
            <regular-expression>regular-expression</regular-expression>
          </interface-name>
        </default>
      </radius-attribute-extraction>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the interface-name attribute value extraction. By default, the interface-name attribute value is extracted from standard RADIUS attribute id = 87(RADIUS, 87) with RADIUS attribute type of chars.

Contents

<regular-expression>—(Optional) (Multivalue) The regular expression of the radius attribute, A multi-value can be specified. If no regular expression is specified, the whole value would be considered the valid value; if any regular expression is present, Only the first group of regular expression is considered the valid value. Note that if type is raw-byte, the regular expression should be described hexadecimal format

Value—Text

Default— None

Required Privilege Level

No specific privilege required.

<virtual-router-name> (configuration/slot/external-subscriber-monitor/radius-attribute-extraction/default)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-attribute-extraction>
        <default>
          <virtual-router-name>
            <id>id</id>
            <vsa/>
            <vsa-id>vsa-id</vsa-id>
            <regular-expression>regular-expression</regular-expression>
            <type>type-choice</type>
            <prefix>prefix</prefix>
          </virtual-router-name>
        </default>
      </radius-attribute-extraction>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the virtual router name attribute value extraction.

Contents

<id>— Specifies RADIUS attribute ID

Value— Integer in the range 0–2147483647

<vsa>—(Optional) Indicates whether this attribute is vendor specific

Default— false

<vsa-id>—(Optional) Specifies RADIUS vendor-specific identifier

Value—Integer in the range 0–2147483647

`<regular-expression>`—(Optional) (Multivalue) The regular expression of the radius attribute. A multivalue can be specified. If no regular expression is specified, the whole value would be considered the valid value; if any regular expression is present, only the first group of regular expression is considered the valid value. Note that if type is raw-byte, the regular expression should be described hexadecimal format.

Value—Text

Default— None

`<type>`—(Optional) The value type of this radius attribute. Currently only supports two type: 'r' (raw bytes) and 's' (string). By default, the type is raw type, 'r'

Value

- raw-byte— Set type as raw byte
- chars— Set type as a sequence of characters

Default— r

`<prefix>`—(Optional) The prefix that is to be appended to radius attribute's value.

Value—Text

Default— None

Required Privilege Level

No specific privilege required.

<radius-authorization> (configuration/slot/external-subscriber-monitor)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <port>port</port>
        <local-address>local-address</local-address>
        <check-lease-limit-with-sae/>
        <query-cached-dhcp-profile/>
        <default-lease-limit>default-lease-limit</default-lease-limit>
        <invalid-pool-name>invalid-pool-name</invalid-pool-name>
        <lease-time-limit>lease-time-limit</lease-time-limit>
        <cleanup-interval>cleanup-interval</cleanup-interval>
        <maximum-age>maximum-age</maximum-age>
        <minimum-pool-size>minimum-pool-size</minimum-pool-size>
        <maximum-queue-length>maximum-queue-length</maximum-queue-length>
        <service-type>service-type-choice</service-type>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the pseudo-RADIUS authorization server.

Contents

<port>— Listening port for RADIUS access requests.

Value—Integer in the range 1–65535

Default— 1812

<local-address>—(Optional) Address to bind to pseudo-RADIUS authorization server. Absence of this attribute means binding the server to a wildcard (*) address. Currently, only IPV4 addresses are supported.

Value—Text

`<check-lease-limit-with-sae>`—(Optional) Specify whether to query the SAE for the number of active subscribers for a given interface. If set to true, the response to the RADIUS access request depends on the comparison between the number of active subscriber sessions and the lease limit for the interface. If the number of active subscriber sessions is less than the lease limit, the response is a RADIUS access accept message without the lease limit RADIUS attribute; otherwise, the response is a RADIUS access deny message. If set to false, the response is a RADIUS access accept message with the lease limit RADIUS attribute.

Default— false

`<query-cached-dhcp-profile>`—(Optional) Specify whether to search for a cached DHCP profile in the o = AuthCache directory based on the MAC address.

If set to true, you must configure a directory connection to the cached DHCP profiles and the following conditions apply:

- If a cached DHCP profile is found, the RADIUS response message includes the RADIUS attributes for framed IP address, pool name, service bundle, and RADIUS class attributes.
- If the check-lease-limit-with-sae option is set to true and the number of active subscriber sessions is less than the lease limit, the RADIUS access accept message includes the cached DHCP profile.
- If the check-lease-limit-with-sae option is set to false, the RADIUS response always includes the cached DHCP profile.

If set to false, the cached DHCP profile information is not included in the RADIUS response.

Default— false

`<default-lease-limit>`—(Optional) Default lease limit for all interfaces.

Value—Integer in the range -2147483648–2147483647

Default— 1

`<invalid-pool-name>`—(Optional) Invalid pool name returned when number of active subscriber sessions exceeds the lease limit.

Value— None empty pool name

`<lease-time-limit>`—(Optional) Timeout of a cached authenticated request.

Value—Integer in the range 1–9223372036854775807 ms

Default— 60000

<cleanup-interval>—(Optional) Time to wait before cleaning up cached RADIUS access requests that have been authenticated or accepted.

Value—Integer in the range 1–9223372036854775807 ms

Default— 3600000

<maximum-age>—(Optional) Maximum age of an unacknowledged request packet cached in memory. We recommend a value slightly greater than the RADIUS packet retry interval.

Value—Integer in the range 1–9223372036854775807 ms

Default— 60000

<minimum-pool-size>—(Optional) Number of concurrent threads processing RADIUS message subtasks.

Value—Integer in the range 1–2147483647

Default— 8

<maximum-queue-length>— Maximum number of unacknowledged RADIUS messages received from the RADIUS server before it discards new messages. 0 or negative number means that an infinite number of messages are allowed.

Value— Integer in the range 0–2147483647

Default— 10000

<service-type>—(Optional) Service type of RADIUS packets that will be forwarded.

Value

- all— Forward all packets
- login— Forward packets with type of Login
- framed— Forward packets with type of Framed
- callback-login— Forward packets with type of Callback Login
- callback-framed— Forward packets with type of Callback Framed
- outbound— Forward packets with type of Outbound
- administrative— Forward packets with type of Administrative

- `nas-prompt`— Forward packets with type of NAS Prompt
- `authenticate-only`— Forward packets with type of Authenticate Only
- `callback-nas-prompt`— Forward packets with type of Callback NAS Prompt
- `callback-check`— Forward packets with type of Callback Check
- `callback-administrative`— Forward packets with type of Callback Administrative

Default— framed

Required Privilege Level

No specific privilege required.

<client> (configuration/slot/external-subscriber-monitor/radius-authorization)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <client>
          <client-address>client-address</client-address> <!-- identifier -->
          <secret>secret</secret>
        </client>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the shared secret between the RADIUS server and its clients.

Contents

<client-address>— Address of the specific RADIUS client.

Value— Address in dot format. Currently, only IPv4 addresses are supported.

<secret>— Shared secret of a specific RADIUS client.

Value—Secret text

Required Privilege Level

No specific privilege required.

<cached-dhcp-profile> (configuration/slot/external-subscriber-monitor/radius-authorization/ldap)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <ldap>
          <cached-dhcp-profile>
            <base>base</base>
            <base-dn>base-dn</base-dn>
          </cached-dhcp-profile>
        </ldap>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the connection to the directory in which the cached DHCP profile data is stored.

Contents

<base>—(Optional) Top level or base or directory DN

Value— DN. You can use < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— < base >

<base-dn>—(Optional) Subtree in the directory in which authCache profile data is stored.

Value— DN. You can use < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— o = authCache, < base >

Required Privilege Level

No specific privilege required.

<directory-connection> (configuration/slot/external-subscriber-monitor/radius-authorization/ldap/cached-dhcp-profile)

Usage

```

<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <ldap>
          <cached-dhcp-profile>
            <directory-connection>
              <url>url</url>
              <principal>principal</principal>
              <credentials>credentials</credentials>
              <protocol>protocol-choice</protocol>
              <backup-urls>backup-urls</backup-urls>
              <timeout>timeout</timeout>
              <check-interval>check-interval</check-interval>
              <blacklist/>
              <snmp-agent/>
              <signature-dn>signature-dn</signature-dn>
            </directory-connection>
          </cached-dhcp-profile>
        </ldap>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>

```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<backup-urls>`—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

`<check-interval>`—(Optional) Time interval at which the directory-monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory

connection.

Default—false

`<signature-dn>`—(Optional) DN of the directory entry that specifies the `usedDirectory` attribute for the SRC CLI. The `usedDirectory` attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

Required Privilege Level

No specific privilege required.

<subscriber-data> (configuration/slot/external-subscriber-monitor/radius-authorization/ldap)

Usage

```
<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <ldap>
          <subscriber-data>
            <base>base</base>
            <base-dn>base-dn</base-dn>
          </subscriber-data>
        </ldap>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the connection to the directory in which subscriber data is stored.

Contents

<base>—(Optional) Top level or base or directory DN.

Value— DN. You can use < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— < base >

<base-dn>—(Optional) Subtree in the directory in which subscriber data is stored.

Value— DN. You can use < base > to refer to the globally configured base DN. The string < base > is replaced with the directory base DN.

Default— o = Users, < base >

Required Privilege Level

No specific privilege required.

<directory-connection> (configuration/slot/external-subscriber-monitor/radius-authorization/ldap/subscriber-data)

Usage

```

<configuration>
  <slot>
    <external-subscriber-monitor>
      <radius-authorization>
        <ldap>
          <subscriber-data>
            <directory-connection>
              <url>url</url>
              <principal>principal</principal>
              <credentials>credentials</credentials>
              <protocol>protocol-choice</protocol>
              <backup-urls>backup-urls</backup-urls>
              <timeout>timeout</timeout>
              <check-interval>check-interval</check-interval>
              <blacklist/>
              <snmp-agent/>
              <signature-dn>signature-dn</signature-dn>
            </directory-connection>
          </subscriber-data>
        </ldap>
      </radius-authorization>
    </external-subscriber-monitor>
  </slot>
</configuration>

```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `<base>` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<backup-urls>`—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory connection.

Default—false

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

Required Privilege Level

No specific privilege required.

Dynamic Service Activator Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for Dynamic Service Activator. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

| CLI Configuration Statement | Configuration Tag Element |
|---|--|
| shared dsa configuration | <u>< configuration ></u> |
| shared dsa configuration client | <u>< client ></u> |
| shared dsa configuration client name permissions | <u>< permissions ></u> |
| shared dsa configuration client name permissions method | <u>< method ></u> |
| shared dsa configuration client name permissions method name constraints | <u>< constraints ></u> |
| shared dsa configuration client name permissions script | <u>< script ></u> |
| shared dsa configuration client name permissions script name constraints | <u>< constraints ></u> |
| shared dsa configuration logger | <u>< logger ></u> |
| shared dsa configuration logger name file | <u>< file ></u> |
| shared dsa configuration logger name syslog | <u>< syslog ></u> |
| shared dsa configuration method commit-resources constraints | <u>< constraints ></u> |
| shared dsa configuration method invoke-gateway-extension constraints | <u>< constraints ></u> |
| shared dsa configuration method invoke-script constraints | <u>< constraints ></u> |
| shared dsa configuration method query-available-services constraints | <u>< constraints ></u> |
| shared dsa configuration method query-contexts constraints | <u>< constraints ></u> |
| shared dsa configuration method release-resources constraints | <u>< constraints ></u> |
| shared dsa configuration method subscriber-activate-service constraints | <u>< constraints ></u> |
| shared dsa configuration method subscriber-deactivate-service constraints | <u>< constraints ></u> |
| shared dsa configuration method subscriber-login constraints | <u>< constraints ></u> |

| | |
|---|---|
| shared dsa configuration method subscriber-logout constraints | <u>< constraints ></u> |
| shared dsa configuration method subscriber-modify-service constraints | <u>< constraints ></u> |
| shared dsa configuration method subscriber-read-subscription constraints | <u>< constraints ></u> |
| shared dsa configuration nic-proxy-configuration | <u>< nic-proxies ></u> |
| shared dsa configuration nic-proxy-configuration name cache | <u>< cache ></u> |
| shared dsa configuration nic-proxy-configuration name nic-host-selection | <u>< nic-host-selection ></u> |
| shared dsa configuration nic-proxy-configuration name nic-host-selection blacklisting | <u>< blacklisting ></u> |
| shared dsa configuration nic-proxy-configuration name resolution | <u>< resolution ></u> |
| shared dsa configuration nic-proxy-configuration name test-nic-bindings | <u>< test-nic-bindings ></u> |
| shared dsa configuration nic-proxy-configuration name test-nic-bindings key-values | <u>< key-values ></u> |
| shared dsa configuration script | <u>< script ></u> |
| shared dsa configuration script constraints | <u>< constraints ></u> |
| shared dsa configuration subscriber-types | <u>< subscriber-types ></u> |
| shared dsa group | <u>< group ></u> |
| slot dsa | <u>< dsa ></u> |
| slot dsa deploy | <u>< deploy ></u> |
| slot dsa initial | <u>< initial ></u> |
| slot dsa initial directory-connection | <u>< directory-connection ></u> |
| slot dsa initial directory-eventing | <u>< directory-eventing ></u> |

<configuration> (configuration/shared/dsa)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <disable-access-control-mechanism/>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the general properties that determine the behavior of the application.

Contents

`<disable-access-control-mechanism>`—(Optional) Specify whether the access control mechanism is disabled.

Required Privilege Level

system

<client> (configuration/shared/dsa/configuration)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <name>name</name> <!-- identifier -->
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the client.

Contents

<name>— Name of Dynamic Service Activator client. You must use a name that is configured on the Web application server for the user account.

Value—Text

Required Privilege Level

system

<permissions> (configuration/shared/dsa/configuration/client)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <permissions>
            <pcmm-service>pcmm-service</pcmm-service>
          </permissions>
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the services available to the client.

Contents

<pcmm-service>—(Optional) (Multivalue) PCMM services available to the client.

Value—Text

Required Privilege Level

system

<method> (configuration/shared/dsa/configuration/client/permissions)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <permissions>
            <method>
              <name>name</name> <!-- identifier -->
            </method>
          </permissions>
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure client access to methods.

Contents

<name>— Name of the method.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/client/permissions/method)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <permissions>
            <method>
              <constraints>
                <argument-index>argument-index</argument-index> <!--
identifier -->
                <value>value</value>
              </constraints>
            </method>
          </permissions>
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the access constraints for this gateway client.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<script> (configuration/shared/dsa/configuration/client/permissions)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <permissions>
            <script>
              <name>name</name> <!-- identifier -->
            </script>
          </permissions>
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure client access to scripts.

Contents

<name>— Name of the script.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/client/permissions/script)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <client>
          <permissions>
            <script>
              <constraints>
                <argument-index>argument-index</argument-index> <!--
identifier -->
                <value>value</value>
              </constraints>
            </script>
          </permissions>
        </client>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the access constraints for this gateway client.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1-2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<logger> (configuration/shared/dsa/configuration)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <logger>
          <name>name</name> <!-- identifier -->
        </logger>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Create a logging configuration for Dynamic Service Activator.

Contents

<name>— Name of the logging configuration.

Value—Text

Required Privilege Level

system

<file> (configuration/shared/dsa/configuration/logger)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <logger>
          <file>
            <filter>filter</filter>
            <filename>filename</filename>
            <rollover-filename>rollover-filename</rollover-filename>
            <maximum-file-size>maximum-file-size</maximum-file-size>
          </file>
        </logger>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— No value

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system

<syslog> (configuration/shared/dsa/configuration/logger)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <logger>
          <syslog>
            <filter>filter</filter>
            <host>host</host>
            <facility>facility</facility>
            <format>format</format>
          </syslog>
        </logger>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging of messages to system logging.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

<host>— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

`<facility>`—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

`<format>`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

Value— MessageFormat string as specified in <http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>.

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Default— None

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/commit-resources)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <commit-resources>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </commit-resources>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/invoke-gateway-extension)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <invoke-gateway-extension>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </invoke-gateway-extension>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/invoke-script)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <invoke-script>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </invoke-script>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/query-available-services)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <query-available-services>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </query-available-services>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/query-contexts)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <query-contexts>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </query-contexts>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/release-resources)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <release-resources>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </release-resources>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-activate-service)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-activate-service>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-activate-service>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-deactivate-service)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-deactivate-service>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-deactivate-service>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-login)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-login>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-login>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-logout)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-logout>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-logout>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-modify-service)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-modify-service>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-modify-service>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/method/subscriber-read-subscription)

Usage

```

<configuration>
  <shared>
    <dsa>
      <configuration>
        <method>
          <subscriber-read-subscription>
            <constraints>
              <argument-index>argument-index</argument-index> <!-- identifier
-->
              <value>value</value>
            </constraints>
          </subscriber-read-subscription>
        </method>
      </configuration>
    </dsa>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the method for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<nic-proxies> (configuration/shared/dsa/configuration/nic-proxy-configuration)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <name>name</name> <!-- identifier -->
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the NIC proxy.

Contents

<name>— Name of the NIC proxy configuration.

Value—Text

Required Privilege Level

system

<cache> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <cache>
              <cache-size>cache-size</cache-size>
              <cache-cleanup-interval>cache-cleanup-interval</cache-cleanup-
interval>
              <cache-entry-age>cache-entry-age</cache-entry-age>
            </cache>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Description

Configure the NIC proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

Contents

<cache-size>—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default— 10000

<cache-cleanup-interval>— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default— 15

`<cache-entry-age>`—(Optional) Maximum time that the NIC proxy can cache an entry. The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Required Privilege Level

system

<nic-host-selection> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <nic-host-selection>
              <groups>groups</groups>
              <selection-criteria>selection-criteria-choice</selection-
criteria>
            </nic-host-selection>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

Contents

<groups>—(Optional) (Multivalue) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

<selection-criteria>— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.

- **priorityList**—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default—round-

Required Privilege Level

system

<blacklisting> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies/nic-host-selection)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <nic-host-selection>
              <blacklisting>
                <try-next-system-on-error/>
                <number-of-retries-before-blacklisting>number-of-retries-
before-blacklisting</number-of-retries-before-blacklisting>
                <blacklist-retry-interval>blacklist-retry-interval</blacklist-
retry-interval>
              </blacklisting>
            </nic-host-selection>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Contents

<try-next-system-on-error>—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

<number-of-retries-before-blacklisting>— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the

NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

`<blacklist-retry-interval>`— Interval at which the NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s

Default—15

Required Privilege Level

system

<resolution> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <resolution>
              <resolver-name>resolver-name</resolver-name>
              <key-type>key-type</key-type>
              <value-type>value-type</value-type>
              <expect-multiple-values/>
              <constraints>constraints</constraints>
            </resolution>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

Contents

<resolver-name>— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

<key-type>— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<value-type>— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaeId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

<expect-multiple-values>—(Optional) Specifies whether or not the key can have multiple corresponding values.

<constraints>—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Required Privilege Level

system

<test-nic-bindings> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <test-nic-bindings>
              <use-test-bindings/>
            </test-nic-bindings>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure key-value mappings to be used to test a NIC resolution.

Contents

`<use-test-bindings>`—(Optional) Test the NIC resolutions without having to configure or run a NIC host. The values returned are those configured in the key-values property.

Default—false

Required Privilege Level

system

<key-values> (configuration/shared/dsa/configuration/nic-proxy-configuration/nic-proxies/test-nic-bindings)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <nic-proxy-configuration>
          <nic-proxies>
            <test-nic-bindings>
              <key-values>
                <name>name</name> <!-- identifier -->
                <value>value</value>
              </key-values>
            </test-nic-bindings>
          </nic-proxies>
        </nic-proxy-configuration>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure keys and associated values to use for testing. Define all of values to be returned for specified keys.

Contents

<name>—

Value—Text

<value>—

Value—Text

Required Privilege Level

system

<script> (configuration/shared/dsa/configuration)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <script>
          <name>name</name> <!-- identifier -->
          <sae-locator-index>sae-locator-index</sae-locator-index>
        </script>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure a script for Dynamic Service Activator.

Contents

<name>— Name of Dynamic Service Activator script.

Value—Text

<sae-locator-index>— The zero-based index of the script argument to be used to locate the SAE server on which to invoke the script.

Value—Integer in the range -2147483648–2147483647

Required Privilege Level

system

<constraints> (configuration/shared/dsa/configuration/script)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <script>
          <constraints>
            <argument-index>argument-index</argument-index> <!-- identifier --
>
            <value>value</value>
          </constraints>
        </script>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure access constraints for the script for all clients.

Contents

<argument-index>— Zero-based index of the argument.

Value—Integer in the range 1–2147483647

<value>— Regular expression that the argument must match.

Value—Text

Required Privilege Level

system

<subscriber-types> (configuration/shared/dsa/configuration)

Usage

```
<configuration>
  <shared>
    <dsa>
      <configuration>
        <subscriber-types>
          <name>name</name> <!-- identifier -->
          <subscriber-id-type>subscriber-id-type-choice</subscriber-id-type>
          <nic-proxy>nic-proxy</nic-proxy>
        </subscriber-types>
      </configuration>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the subscriber types.

Contents

<name>— Name of the subscriber type used to construct the subscriber URI.

Value—Text

<subscriber-id-type>— The subscriber ID type used to pass correct argument to the subscriber URI.

Value— One of the following types:

- address—Subscriber's IP address
- dn—Distinguished name of subscriber profile
- login-name—Subscriber's login name
- interface-name—Name of the interface and name of the virtual router to which the subscriber connects
- interface-index—SNMP index of the interface and name of the virtual router to which the subscriber connects
- address-interface-name—Subscriber's IP address, name of the

- managed interface, and name of the virtual router to which the subscriber connects
- primary-user-name—Primary username

<nic-proxy>— The configuration that contains the NIC proxy configuration properties for the subscriber type.

Value—Text

Required Privilege Level

system

<group> (configuration/shared/dsa)

Usage

```
<configuration>
  <shared>
    <dsa>
      <group>
        <name>name</name> <!-- identifier -->
      </group>
    </dsa>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure group of Dynamic Service Activator configuration properties.

Contents

<name>— Name of an SRC-DSA configuration.

Value—Text

Required Privilege Level

system

<dsa> (configuration/slot)

Usage

```
<configuration>
  <slot>
    <dsa>
      <shared>shared</shared>
    </dsa>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure local properties for Dynamic Service Activator.

Contents

<shared>— The configuration namespace that contains the Dynamic Service Activator's configuration data. You cannot specify root (/).

Value—Text

Default—/sample

Required Privilege Level

system

<deploy> (configuration/slot/dsa)

Usage

```
<configuration>
  <slot>
    <dsa>
      <deploy>
        <virtual-host>virtual-host</virtual-host>
      </deploy>
    </dsa>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the virtual host on which to deploy the application.

Contents

`<virtual-host>`—(Optional) The host to which the application is deployed.

Value—Text

Required Privilege Level

system

<initial> (configuration/slot/dsa)

Usage

```
<configuration>
  <slot>
    <dsa>
      <initial>
        <base-dn>base-dn</base-dn>
        <static-dn>static-dn</static-dn>
        <dynamic-dn>dynamic-dn</dynamic-dn>
      </initial>
    </dsa>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure initial properties for SRC components.

Contents

<base-dn>— DN of the root of the SDX data in the directory.

If you are storing non-SDX data in the directory, and that data changes frequently whereas the SDX data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SDX data and the changing non-SDX data.

Value— DN

Default—o = UMC

<static-dn>—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—l = DynamicServiceActivation, l = WebApplication,
ou = staticConfiguration, ou = Configuration, o = Management, < base >

<dynamic-dn>—(Optional) Location of programmatically defined configuration data in

the directory.

Value—Text

Default—ou = dynamicConfiguration,ou = Configuration,
o = Management, < base >

Required Privilege Level

system

<directory-connection> (configuration/slot/dsa/initial)

Usage

```
<configuration>
  <slot>
    <dsa>
      <initial>
        <directory-connection>
          <url>url</url>
          <backup-urls>backup-urls</backup-urls>
          <principal>principal</principal>
          <credentials>credentials</credentials>
          <protocol>protocol-choice</protocol>
          <timeout>timeout</timeout>
          <check-interval>check-interval</check-interval>
          <blacklist/>
          <snmp-agent/>
        </directory-connection>
      </initial>
    </dsa>
  </slot>
</configuration>
```

Description

Configure properties for the directory connection.

Contents

<url>—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

<backup-urls>—(Optional) (Multivalue) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

<principal>— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `< base >` to indicate the base DN.

`<credentials>`— Password with which the SRC component accesses the directory.

Value— Password

`<protocol>`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

`<timeout>`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default— 10

`<check-interval>`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

`<blacklist>`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

`<snmp-agent>`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false

Required Privilege Level

system

<directory-eventing> (configuration/slot/dsa/initial)

Usage

```
<configuration>
  <slot>
    <dsa>
      <initial>
        <directory-eventing>
          <eventing/>
          <signature-dn>signature-dn</signature-dn>
          <polling-interval>polling-interval</polling-interval>
          <event-base-dn>event-base-dn</event-base-dn>
          <dispatcher-pool-size>dispatcher-pool-size</dispatcher-pool-size>
        </directory-eventing>
      </initial>
    </dsa>
  </slot>
</configuration>
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Contents

<eventing>—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

<signature-dn>—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o = umc

<polling-interval>—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30

<event-base-dn>—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default—o = UMC

<dispatcher-pool-size>—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

Default— 1

Required Privilege Level

system

DIAMETER Configuration Tag Elements

The following table summarizes the tag elements in the SRC XML API for the DIAMETER application. The table lists the SRC CLI configuration statements that have corresponding SRC XML tag elements, and maps each statement to its tag element. CLI commands are listed in alphabetical order.

CLI Configuration Statement	Configuration Tag Element
shared network nas-group	<u>< nas-group ></u>
shared network nas-group interface-classifier rule	<u>< rule ></u>
shared network nas-group interface-classifier rule name condition	<u>< condition ></u>
shared network nas-group peer	<u>< peer ></u>
shared network nas-group routes	<u>< route ></u>
shared network nas-group routes name term	<u>< term ></u>
system diameter	<u>< diameter ></u>
system diameter client	<u>< client ></u>
system diameter logger	<u>< logger ></u>
system diameter logger name file	<u>< file ></u>
system diameter server	<u>< server ></u>

<nas-group> (configuration/shared/network)

Usage

```
<configuration>
  <shared>
    <network>
      <nas-group>
        <name>name</name> <!-- identifier -->
        <hosted-by>hosted-by</hosted-by>
        <function>function-choice</function>
        <scope>scope</scope>
        <default-peer>default-peer</default-peer>
        <update-grace-period>update-grace-period</update-grace-period>
        <initial-ppr-delay>initial-ppr-delay</initial-ppr-delay>
      </nas-group>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure group of equivalent peers.

Contents

<name>— Name of the NAS group.

Value—Text

<hosted-by>—(Multivalue) Hosts that instantiate this peer group.

The DIAMETER server is running on every SRC-PE host. If the peer group is of type aaa, then the SAEs on the listed hosts will create device drivers for this peer group.

Value—Text

<function>— Functional interface of the peer group.

Value

- aaa—AAA interface

Default—aaa

<scope>—(Optional) (Multivalue) Service scopes associated with the NAS group. The scopes are available for subscribers connected to this NAS group for selecting customized versions of services.

Value— Text

Default— No value

<default-peer>—(Optional) Default peer.

Value—Text

<update-grace-period>—(Optional) Grace period for interim updates.

Value—Integer in the range 0–2147483647 s

<initial-ppr-delay>—(Optional) Delay for sending initial policy-install PPRs.

Value—Integer in the range 0–9223372036854775807 ms

Default—0

Required Privilege Level

system

<rule> (configuration/shared/network/nas-group/interface-classifier)

Usage

```
<configuration>
  <shared>
    <network>
      <nas-group>
        <interface-classifier>
          <rule>
            <name>name</name> <!-- identifier -->
            <target>target</target>
            <script>script</script>
          </rule>
        </interface-classifier>
      </nas-group>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure an interface classification rule.

Contents

<name>— Name of the rule in the interface classification script.

Value— Text

<target>—(Optional) Result of the classification script that gets returned to the SAE.

Value— Path to a policy group. For example, /sample/junose/DHCP.

Default— No value

<script>—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Required Privilege Level

system

<condition> (configuration/shared/network/nas-group/interface-classifier/rule)

Usage

```
<configuration>
  <shared>
    <network>
      <nas-group>
        <interface-classifier>
          <rule>
            <condition>
              <name>name</name> <!-- identifier -->
            </condition>
          </rule>
        </interface-classifier>
      </nas-group>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Contents

<name>— Match conditions used to find a target. For more information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC-PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

<peer> (configuration/shared/network/nas-group)

Usage

```

<configuration>
  <shared>
    <network>
      <nas-group>
        <peer>
          <name>name</name> <!-- identifier -->
          <protocol>protocol-choice</protocol>
          <address>address</address>
          <local-address>local-address</local-address>
          <connect-timeout>connect-timeout</connect-timeout>
          <watchdog-timeout>watchdog-timeout</watchdog-timeout>
          <state-machine-timeout>state-machine-timeout</state-machine-timeout>
          <reconnect-timeout>reconnect-timeout</reconnect-timeout>
          <port>port</port>
          <origin-host>origin-host</origin-host>
          <incoming-queue-limit>incoming-queue-limit</incoming-queue-limit>
          <active-peer/>
        </peer>
      </nas-group>
    </network>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the peer in the NAS group.

Contents

<name>— Name of the peer. The peer name must be unique in the NAS group.

Value—Text

<protocol>—(Multivalue) Supported transport protocol.

Value

- tcp—TCP
- sctp—SCTP

<address>—(Multivalue) Addresses to which the peer can be connected.

Value—IP address

<local-address>—(Optional) Local IP address.

Value—IP address

<connect-timeout>—(Optional) Connect timeout.

Value—Integer in the range 0–2147483 s

Default—10

<watchdog-timeout>—(Optional) Watchdog timeout used for the connection to the remote peer.

Value—Integer in the range 0–2147483 s

Default—30

<state-machine-timeout>—(Optional) Diameter state machine timeout as specified in RFC 3588.

Value—Integer in the range 0–2147483 s

Default—30

<reconnect-timeout>—(Optional) Time interval between connection attempts when the peer is in the disconnected state.

Value—Integer in the range 0–2147483 s

Default—10

<port>—(Optional) Client port.

Value—Integer in the range 1–65565

Default—3868

`<origin-host>`—(Optional) The expected origin-host that the peer presents during connection establishment.

Value—Text

`<incoming-queue-limit>`—(Optional) Number of messages of the incoming message queue for a peer. Whenever the number of messages in the queue exceeds any multiple of this limit, the peer connection stops reading incoming requests. Similarly, when the limit is no longer exceeded, the peer connection resumes reading from the operating system transports.

Value—Integer in the range 1–2147483647

`<active-peer>`—(Optional) Specify whether the peer connection is in active mode.

Required Privilege Level

system

<route> (configuration/shared/network/nas-group)

Usage

```
<configuration>
  <shared>
    <network>
      <nas-group>
        <routes>
          <route>
            <name>name</name> <!-- identifier -->
            <precedence>precedence</precedence>
          </route>
        </routes>
      </nas-group>
    </network>
  </shared>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure Diameter routing configuration.

Contents

<name>— Name of the route configuration.

Value—Text

<precedence>—(Optional) The order by which the route is selected. The route that meets all the matching criteria and has the lowest precedence is selected first. Routes without the precedence defined are considered after those that have the precedence defined. Route with precedence of -1 is the default route. The default route is considered after all the other routes, and only one default route can be defined.

Value—Integer in the range -1-2147483647

Required Privilege Level

system

<term> (configuration/shared/network/nas-group/routes/route)

Usage

```

<configuration>
  <shared>
    <network>
      <nas-group>
        <routes>
          <route>
            <term>
              <name>name</name> <!-- identifier -->
              <transaction-variable>transaction-variable-choice</transaction-
variable>
              <dictionary-attribute>dictionary-attribute-choice</dictionary-
attribute>
              <operator>operator-choice</operator>
              <value>value</value>
              <low>low</low>
              <high>high</high>
            </term>
          </route>
        </routes>
      </nas-group>
    </network>
  </shared>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the criteria for route selection.

Contents

<name>— Name of the matching criteria configuration.

Value—Text

<transaction-variable>— Name of the transaction variable used as the matching criterion.

Value

- request-packet—RequestPacket transaction variable
- user-name—User-Name transaction variable
- realm—Realm transaction variable

<dictionary-attribute>—(Optional) Name of the dictionary attribute contained in the attribute store. Applicable only if the transaction variable is 'request-packet'.

Value

- user-name—The name of the user to be authenticated
- user-password—The password of the user to be authenticated
- chap-password—The response value provided by a PPP CHAP user
- nas-ip-address—The identifying IP address of the NAS
- nas-port—The physical port number of the NAS
- service-type—The type of service the user has requested
- framed-protocol—The framing to be used for framed access
- framed-ip-address—The address to be configured for the user
- framed-ip-netmask—The IP netmask to be configured for the user
- framed-mtu—The Maximum Transmission Unit to be configured for user
- framed-compression—A compression protocol to be used for the link
- login-ip-host—The system with which to connect the user
- callback-number—A dialing string to be used for callback
- state—A state attribute provided by the RADIUS server
- vendor-specific—A vendor-specific extended attribute
- called-station-id—The phone number that the user called
- calling-station-id—The phone number that the call came from
- nas-identifier—A string identifying the NAS originating the request
- login-lat-service—The system with which to connect the user by LAT
- login-lat-node—The node with which to automatically connect user by LAT
- login-lat-group—The LAT group codes which the user is authorized to use
- chap-challenge—The challenge sent by the NAS to a PPP CHAP user
- nas-port-type—The type of the physical port of the NAS
- port-limit—The maximum number of ports to be provided

- to the user
- `login-lat-port`—The port with which to connect the user by LAT

`<operator>`—Operator for criterion matching.

Value

- `equals`—Target value equals
- `not_equal`—Target value does not equal
- `present`—Target exists
- `not_present`—Target does not exist
- `prefix`—Target value starts with
- `suffix`—Target value ends with
- `range`—Target value in the range of

`<value>`—(Optional) Value to be matched by the target.

Value—Text

`<low>`—(Optional) Low end of the range criterion.

Value—Integer in the range -2147483648–2147483647

`<high>`—(Optional) High end of the range criterion.

Value—Integer in the range -2147483648–2147483647

Required Privilege Level

system

<diameter> (configuration/system)

Usage

```

<configuration>
  <system>
    <diameter>
      <java-heap-size>java-heap-size</java-heap-size>
      <java-new-size>java-new-size</java-new-size>
      <java-garbage-collection-options>java-garbage-collection-options</java-
garbage-collection-options>
      <protocol>protocol-choice</protocol>
      <local-address>local-address</local-address>
      <port>port</port>
      <origin-host>origin-host</origin-host>
      <origin-realm>origin-realm</origin-realm>
      <active-peers/>
      <debug-mode/>
      <load-balancing-mode>load-balancing-mode-choice</load-balancing-mode>
      <transaction-processing-log>transaction-processing-log-choice</
transaction-processing-log>
      <packet-trace-log>packet-trace-log-choice</packet-trace-log>
      <peer-state-machine-log>peer-state-machine-log-choice</peer-state-
machine-log>
      <configuration-log>configuration-log-choice</configuration-log>
    </diameter>
  </system>
</configuration>

```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure DIAMETER application.

Contents

<java-heap-size>— Maximum Java heap (memory) size available to the JRE.

Value— Number of megabytes followed by m. For example, 896m. Change this value if you experience problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping. See the documentation for the JRE for valid values.

Default— The value is calculated dynamically to 70 % of the available

real memory.

<java-new-size>— Maximum Java new generation heap (memory) size available to the JRE when the Diameter server starts.

Value— Integer in the range 0– <Java heap size> . Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 200m. See the documentation for the JRE for valid values.

Default— 200m

<java-garbage-collection-options>— Garbage collection functionality of the Java Virtual Machine.

Value—

<protocol>—(Multivalue) Supported transport protocol.

Value

- tcp—TCP
- sctp—SCTP

<local-address>—(Optional) (Multivalue) Local IP addresses that the remote peers can use to reach this server.

Value—IP address

<port>—(Optional) Server port.

Value—Integer in the range 1–65565

Default—3868

<origin-host>—(Optional) Fully qualified domain name used to identify this host to its DIAMETER peers.

Value—Text

Default— The host name as reported by java.net.InetAddress.
getLocalHost().getCanonicalHostName()

<origin-realm>—(Optional) The DNS name of the machine used to identify this host to

its DIAMETER peers.

Value—Text

Default— The DNS name part of the local hostname as reported by java.
net.InetAddress.getLocalHost().getCanonicalHostName()

`<active-peers>`—(Optional) Specifies whether the peer connection is in active mode.

Default—true

`<debug-mode>`—(Optional) Specifies whether the peer connection is in debug mode.

Default—false

`<load-balancing-mode>`—(Optional) Strategy used to select a peer to forward a request message.

Value

- failover
- round-robin

Default—failover

`<transaction-processing-log>`—(Optional) Log level for transaction processing log.

Value

- log-no-messages
- log-severe-messages
- log-normal-messages
- log-debug-messages

`<packet-trace-log>`—(Optional) Log level for packet trace log.

Value

- log-no-messages
- log-severe-messages

- log-normal-messages
- log-debug-messages

<peer-state-machine-log>—(Optional) Log level for peer state machine log.

Value

- log-no-messages
- log-severe-messages
- log-normal-messages
- log-debug-messages

<configuration-log>—(Optional) Log level for configuration log.

Value

- log-no-messages
- log-severe-messages
- log-normal-messages
- log-debug-messages

Required Privilege Level

system

<client> (configuration/system/diameter)

Usage

```
<configuration>
  <system>
    <diameter>
      <client>
        <threads>threads</threads>
        <keep-alive-time>keep-alive-time</keep-alive-time>
      </client>
    </diameter>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure properties for the client.

Contents

<threads>—(Optional) Minimum number of threads to use.

Value—Integer in the range -2147483648–2147483647

Default—50

<keep-alive-time>—(Optional) Interval to keep threads alive waiting for new commands.

Value—Integer in the range -9223372036854775808–9223372036854775807 ms

Default—60000

Required Privilege Level

system

<logger> (configuration/system/diameter)

Usage

```
<configuration>
  <system>
    <diameter>
      <logger>
        <name>name</name> <!-- identifier -->
      </logger>
    </diameter>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the logging destination.

Contents

<name>— Name used to group parameters for the logging destination.

Value—Text

Required Privilege Level

system

<file> (configuration/system/diameter/logger)

Usage

```
<configuration>
  <system>
    <diameter>
      <logger>
        <file>
          <filter>filter</filter>
          <filename>filename</filename>
          <rollover-filename>rollover-filename</rollover-filename>
          <maximum-file-size>maximum-file-size</maximum-file-size>
        </file>
      </logger>
    </diameter>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging of messages to a file.

Contents

<filter>—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

<filename>— Absolute path of the filename that contains the current logs.

Note: Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

`<rollover-filename>`—(Optional) Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

Value— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

`<maximum-file-size>`—(Optional) Maximum size of the log file and the rollover file.

Do not set the maximum file size to a value greater than the available disk space.

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Required Privilege Level

system

<server> (configuration/system/diameter)

Usage

```
<configuration>
  <system>
    <diameter>
      <server>
        <threads>threads</threads>
        <keep-alive-time>keep-alive-time</keep-alive-time>
      </server>
    </diameter>
  </system>
</configuration>
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure properties for the server.

Contents

<threads>—(Optional) Minimum number of threads to use.

Value—Integer in the range -2147483648–2147483647

Default—50

<keep-alive-time>—(Optional) Interval to keep threads alive waiting for new commands.

Value—Integer in the range -9223372036854775808–9223372036854775807 ms

Default—60000

Required Privilege Level

system