JUNIPER NETWORKS

Junos® OS

JSRC Feature Guide for Subscriber Services

Release
13.2

Published: 2013-07-31

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS JSRC Feature Guide for Subscriber Services
13.2

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

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 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

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 https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

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/us/en/local/pdf/resource-guides/7100059-en.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 Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: 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 Management 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).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

JSRC and Juniper Networks Session Resource Control in Subscriber Access Networks

Juniper Networks Session and Resource Control (SRC) and JSRC Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local SRC peer is known as JSRC and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment. JSRC and the SAE jointly provide the remote control enforcement functionality (RCEF).

JSRC has the following responsibilities:

- Request address authorization from the SAE.
- Request service activations from the SAE.
- Activate and deactivate services as specified by the SAE. JSRC can activate multiple policies with the same service (dynamic profile) name.
- Optionally report volume statistics for service accounting.
- Log out subscribers as specified by the SAE.
- Update the SAE with status of new service activations and deactivations.
- Synchronize subscriber state and service information with the SAE.
- Notify the SAE when subscribers log out.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies) and log out subscribers. The SAE can control only those resources that have been provisioned through SAE. Therefore, the SAE receives information about only those subscribers for whom JSRC has requested provisioning from the SAE. For example, when a subscriber logs in, but the configuration did not require the session activation path to include SAE provisioning, the SAE does not receive information about this subscriber and cannot control the subscriber session.

Similarly, the SAE can control only the subscriber services that it has activated. When a service is not activated from the SAE—a RADIUS-activated service, for example—the SAE receives no information about the service and has no control over it.

The SAE can also direct JSRC to collect accounting statistics per service session.

NOTE: **More than one Diameter-based application (function) can run on a router simultaneously.**

Hardware Requirements for JSRC for Subscriber Access

JSRC is supported on Juniper Networks MX Series 3D Universal Edge Routers. JSRC currently supports subscriber sessions on static and dynamic interfaces.

Related Documentation

- Understanding JSRC-SAE Interactions on page 19
- Messages Used by Diameter Applications on page 6
- Diameter AVPs and Diameter Applications on page 10
- Configuring JSRC on page 29

Service Accounting with JSRC

A service session represents a service for a specific subscriber. Service sessions exist in the context of a subscriber session. JSRC activates and deactivates services as specified by the SAE (remote SRC peer). JSRC can collect and report service accounting data by volume. JSRC accounting requires that either classic firewall filters or fast update firewall filters be configured to count service packets—the service packet information provides the volume statistics.

NOTE: **JSRC supports only volume statistics accounting for service sessions. Time statistics and subscriber accounting are not supported.**

JSRC service accounting supports both accounting based on service activation/deactivation and interim accounting.

- Service activation/deactivation accounting—When accounting is enabled, JSRC sends an accounting start message to the SAE when it activates a service and an accounting stop message when it deactivates the service. The start message initiates the

accounting session and provides initial information about the service session. The stop message terminates the accounting session and reports the final (cumulative) accounting data.

- Interim accounting—When interim accounting is enabled for a service session, JSRC sends interim accounting messages to the SAE at a specified interval to report the cumulative accounting information available at that time. Interim accounting is ignored when accounting is not enabled for the corresponding service session.

JSRC accounting for a service begins when the service is activated, and remains in effect while the service is active. The SAE specifies the service (policy) to be activated for the subscriber with the Juniper-Policy-Install AVP (AVP code 2020). When this AVP includes the Juniper-Acct-Collect AVP (AVP code 2054), JSRC initiates service activation/deactivation accounting for the service.

JSRC initiates interim accounting when the Juniper-Policy-Install AVP includes the Acct-Interim-Interval AVP (AVP code 85). In this case, JSRC updates the accounting values at the interval specified in the AVP— in the range 600 through 86,400 seconds. Aggregate counters are reported for the dual stack case.

JSRC and the SAE exchange Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages to communicate accounting data. Both messages include the Juniper-Acct-Record AVP (AVP code 2053) to identify the service for which accounting information is requested.

JSRC sends ACR messages to report accounting data to the SAE. The ACR message includes the Accounting-Record-Type AVP (AVP code 480) to specify the kind of accounting record that it is sending. When a service is activated, this AVP has a value of START_RECORD. When a service is deactivated, it has a value of STOP_RECORD. For interim accounting, ACR messages are sent at the specified accounting interval and the AVP has a value of INTERIM_RECORD.

In addition to specifying the accounting record type, the ACR messages include standard RADIUS attributes to specify the desired statistics: Acct-Input-Octets [42], Acct-Output-Octets [43], Acct-Input-Packets [47], Acct-Output-Packets [48], and Acct-Session-Time [46].

The SAE returns ACA messages to the JSRC to acknowledge receipt of the ACR messages.

An access profile specifies subscriber access authentication and accounting parameters. When a service is activated through JSRC, the accounting reports can be sent either to the SAE or to RADIUS. The default configuration sends the reports to the SAE; you can also configure this by including the **service accounting-order activation-protocol** statement in the access profile. To send the reports instead to the RADIUS server, include the **service accounting-order radius** statement in the access profile.

When a service is activated through RADIUS rather than through JSRC, the accounting reports of the service session are sent to the RADIUS server.

Related Documentation

- *Configuring Service Packet Counting*
- Messages Used by Diameter Applications on page 6

- Diameter AVPs and Diameter Applications on page 10

Messages Used by Diameter Applications

The following Diameter applications are supported by Junos OS:

- JSRC—A Juniper Networks Diameter application registered with the IANA (http://www.iana.org) as Juniper Policy-Control-JSRC, with an ID of 16777244. Communicates with the SAE (remote SRC peer).
- PTSP—A Juniper Networks Diameter application registered with the IANA (http://www.iana.org) as Juniper JGx, with an ID of 16777273. Communicates with the SAE (remote SRC peer).
- Gx-Plus—An application that extends the 3GPP Gx interface for wireline use cases. 3GPP Gx is registered with the IANA (http://www.iana.org). Communicates with a PCRF.

  If data for a particular AVP included in a message is not available to the router, Gx-Plus simply omits the AVP from the message it sends to the PCRF. If the PCRF determines it has insufficient information to make a decision, it may deny the request. The Diameter answer messages include the Result-Code AVP (AVP 268); the values of this AVP convey success, failure, or errors to the requestor.

Juniper Networks has also registered the Juniper-Session-Recovery application (16777296) and two new command codes (8388628 for Juniper-Session-Events and 8388629 for Juniper-Session-Discovery) with the IANA (http://www.iana.org).

Table 3 on page 6 describes Diameter messages the applications use.

Table 3: Diameter Messages and Diameter Applications

Diameter Message	Code	Application	Description
AA-Request (AAR)	265	JSRC, PTSP	Request from the application to the SAE at new subscriber login or during SAE-application synchronization. The request can be one of three types: address-authorization, provisioning-request, or synchronization.
AA-Answer (AAA)	265	JSRC, PTSP	Response from the SAE to the application's AA-Request message.
Abort-Session-Request (ASR)	274	JSRC, PTSP	Request from the SAE to the application to log out a provisioned subscriber.
Abort-Session-Answer (ASA)	274	JSRC, PTSP	Response from the application to the SAE's ASR message. If the application sends the logout request to AAA, the ASA message includes a success notification (ACK). If the logout failed, the ASA message includes a failure notification (NAK).

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Accounting-Request (ACR)	271	JSRC, PTSP	Request from the SAE to the application or from the application to the SAE for statistics.
Accounting-Answer (ACA)	271	JSRC, PTSP	Response to the ACR message to provide statistics for each installed policy (service).
Credit-Control-Request (CCR)	272	Gx-Plus	Request from Gx-Plus to the PCRF at subscriber login, logout, or update. An initial request (CCR-I) is sent when a subscriber logs in and AAA is requested to activate the subscriber's session. Gx-Plus retries the CCR-I message if a CCA-I message is not received from the PCRF within 10 seconds. The CCR-I message is retried up to 3 times. If no CCA-I is received after the 4 CCR-I messages have been sent—the first message plus 3 retries—then Gx-Plus starts sending CCR-N messages. CCR-N messages are retried forever until a success or failure response is received from the PCRF. CCR-N messages include the Juniper-Provisioning-Source AVP (AVP code 2101) set to local to notify the PCRF that the router has the authority to make a local decision regarding subscriber service activation. An update request (CCR-U) message is sent when a usage threshold is reached. The CCR-U reports the actual usage for all statistics. The PCRF may return a CCA-U message that includes new monitoring thresholds, service activations, service deactivations. A CCR-U is also sent to report the status of service activation or deactivation. A termination request (CCR-T) is sent at subscriber logout to inform the PCRF that a provisioned subscriber session is being terminated. CCR-T messages are retried forever until a success response is received from the PCRF.

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Credit-Control-Answer (CCA)	272	Gx-Plus	Reply from the PCRF to a CCR message. In response to a CCR-I, the PCRF returns a CCA-I message that indicates success (DIAMETER_SUCCESS) or failure (DIAMETER AUTHORIZATION REJECTED) depending on whether the subscriber has sufficient credit for the requested services. All other responses are ignored and the CCR-I is retried. In response to a CCR-T, the PCRF returns a CCA-T message that indicates a successful termination with a value of 2001 (DIAMETER SUCCESS) in the Result-Code AVP. All other responses are ignored and the CCR-T is retried. A CCA-N is a response to a CCR-N.
Juniper-Session-Discovery-Request (JSDR)	8388629	Gx-Plus	Discovery request from the PCRF to Gx-Plus to discover subscriber sessions on the router.
Juniper-Session-Discovery-Answer (JSDA)	8388629	Gx-Plus	Reply from router to a JSDR message; describes session information. The Result-Code AVP includes one of the following values, or an error value: • 2001—DIAMETER_SUCCESS; the end of the database was reached, meaning all information has been sent. • 2002—DIAMETER_LIMITED_SUCCESS; some of the session information was sent, but more remains to be sent.
Juniper-Session-Event-Request (JSER)	8388628	Gx-Plus	Request from router to PCRF regarding events that take place on the router. Notifies the PCRF of certain events on the router by including the Juniper-Event-Type AVP (AVP code 2103). Events reported include cold or warm boots, explicit discovery requests, substantial configuration changes, non-response or error response from PCRF, and exhaustion of fault-tolerant resources.
Juniper-Session-Event-Answer (JSEA)	8388628	Gx-Plus	Reply from PCRF to a JSER message.
Push-Profile-Request (PPR)	288	JSRC, PTSP	Request from the SAE to the router to activate or deactivate services for a subscriber.

Table 3: Diameter Messages and Diameter Applications *(continued)*

Diameter Message	Code	Application	Description
Push-Profile-Answer (PPA)	288	JSRC, PTSP	Response from the router to the SAE's PPR message. Includes success or failure notification for each of the service activation or deactivation commands in the request.
Re-Auth-Request (RAR)	258	Gx-Plus	Audit request from the PCRF to router to determine whether a specific subscriber is still present.
Re-Auth-Answer (RAA)	258	Gx-Plus	Reply from router to a RAR message; indicates whether the subscriber is active. The Result-Code AVP includes one of the following values: • 2001—DIAMETER_SUCCESS; subscriber entry was found. • 5002—DIAMETER_UNKNOWN_SESSION_ID; subscriber entry was not found. • 3002—DIAMETER_UNABLE_TO_DELIVER; Gx-Plus is not configured.
Session-Resource-Query (SRQ)	277	JSRC, PTSP	Request from the router to the SAE or from the SAE to the router to initiate synchronization between router and the SAE.
Session-Resource-Reply (SRR)	277	JSRC, PTSP	Response to the SRQ message to begin synchronization.
Session-Termination-Request (STR)	275	JSRC, PTSP	Notification from the router to the SAE that a provisioned subscriber has logged out.
Session-Termination-Answer (STA)	275	JSRC, PTSP	Response from the SAE to the router's STR message. Includes success or failure notification.

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- Understanding JSRC-SAE Interactions on page 19
- *Juniper Networks Session and Resource Control (SRC) and PTSP Overview*
- *Understanding PTSP-SAE Interactions*
- *Gx-Plus for Provisioning Subscribers Overview*
- *Understanding Gx-Plus Interactions Between the Router and the PCRF*

Diameter AVPs and Diameter Applications

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. Table 4 on page 10 lists the standard Diameter AVPs used in interactions with the supported Diameter applications. Diameter reserves AVP code numbers 0 through 255 for RADIUS AVPs that are implemented in Diameter.

Table 4: Standard Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
1	User-Name	Gx-Plus, JSRC	Specifies the username. For a subscriber managed by AAA, the value is the subscriber's login name. For a static interface, the value is the interface name, which is used as the subscriber's login name.	UTF8String
8	Framed-IP-Address	Gx-Plus, JSRC, PTSP	Identifies the IPv4 address configured for the subscriber. This is the same value as for RADIUS Framed-IP-Address attribute [8].	OctetString
55	Event-Timestamp	Gx-Plus, JSRC, PTSP	Specifies the time of the event that triggered the message in which this AVP is included. Time is indicated in seconds since January 1, 1900, 00:00 UTC.	Time
85	Acct-Interim-Interval	JSRC, PTSP	Number of seconds between each interim accounting update for this session. The router uses the following guidelines for interim accounting: • Attribute value is within the acceptable range (600 through 86,400 seconds)—Accounting is updated at the specified interval. • Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds). • Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds).	Unsigned32
87	NAS-Port-Id	Gx-Plus, JSRC, PTSP	Identifies the port of the NAS that authenticates the user. This is the same value as for RADIUS NAS-Port-Id attribute [87].	UTF8String
263	Session-ID	Gx-Plus, JSRC, PTSP	Specifies the subscriber session identifier. The router assigns the value to uniquely identify a subscriber session.	UTF8String

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
268	Result-Code	Gx-Plus, JSRC, PTSP	Indicates whether a request completed successfully. Provides an error code if the request failed. The following classes are recognized by Diameter: • 1xxx—Informational • 2xxx—Success • 3xxx—Protocol errors • 4xxx—Transient errors • 5xxx—Permanent failures Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures. JSRC and PTSP support the following values; all non-success values are treated as permanent failures: • 1001—DIAMETER MULTI ROUND AUTH • 2001—DIAMETER SUCCESS • 5002—DIAMETER UNKNOWN SESSION ID • 5012—DIAMETER UNABLE TO COMPLY JSRC also supports the following value, which is treated as a permanent failure: • 3004—DIAMETER TOO BUSY; this is a transient condition, typically when the router already has a request in process for a specified subscriber. Gx-Plus supports the following values for errors in a PCRF response; when these values are received or the response is malformed or unrecognizable, the request is retried. • 3001—DIAMETER COMMAND NOT SUPPORTED; the application is not running or the command is not recognized. • 3004—DIAMETER TOO BUSY; the received message is above either the quota of downstream transactions or the outstanding message memory limit for messages from the network. • 5012—DIAMETER UNABLE TO COMPLY; the received message is greater than the local limit.	Unsigned32

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
277	Auth-Session-State	JSRC, PTSP	Indicates whether AAA session state is maintained. • 0—STATE MAINTAINED • 1—NO STATE MAINTAINED	Enumerated
295	Termination-Cause	JSRC, PTSP	Indicates the reason why a session was terminated on the access device. • 1—DIAMETER LOGOUT • 2—DIAMETER SERVICE NOT PROVIDED • 3—DIAMETER BAD ANSWER • 4—DIAMETER ADMINISTRATIVE • 5—DIAMETER LINK BROKEN • 6—DIAMETER AUTH EXPIRED • 7— DIAMETER USER MOVED • 8—DIAMETER SESSION TIMEOUT	Enumerated
415	CC-Request-Number	Gx-Plus	Identifies a request within a session. The combination of Session-Id and CC-Request-Type is globally unique. The number is incremented for each request during the course of a session. The number is reset when a router high availability event takes place.	Unsigned32
416	CC-Request-Type	Gx-Plus	Specifies the type of credit control request: • INITIAL REQUEST (1) • UPDATE REQUEST (2) • TERMINATION_REQUEST (3) • EVENT REQUEST (4)	Enumerated
431	Granted-Service-Unit	Gx-Plus	Contains the amount that can be provided of one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCA-I messages, and may be included in CCA-U messages.	Grouped
446	Used-Service-Unit	Gx-Plus	Contains the amount of the requested units that have been actually used; measured from 4 when the service is activated. The units are one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCR-U messages.	Grouped

Table 4: Standard Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
480	Accounting-Record-Type	JSRC, PTSP	Specifies the type of account record for service accounting: • INTERIM_RECORD—Accounting record sent between the start and stop records, at intervals specified by the Acct-Interim-Interval AVP (AVP code 85). It contains cumulative accounting data for the existing accounting session. • START_RECORD—Accounting record sent when the service is activated to initiate the accounting session. It contains accounting data relevant to the initiation of that session. • STOP_RECORD—Accounting record sent when the service is deactivated to terminate the accounting session. It contains cumulative data relevant to that session.	Enumerated
1001	Charging-Rule-Install	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1002	Charging-Rule-Remove	Gx-Plus	Requests the removal of the rule (deactivation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1005	Charging-Rule-Name	Gx-Plus	Name of a specific rule that has been installed, modified, or removed.	OctetString
1066	Monitoring-Key	Gx-Plus	Specifies which of the monitoring structures to use. Included in Charging-Rule-Install AVP (1001). The MX router does not support aggregation of statistics across services, so the value of this AVP must be different for each service. This AVP has a vendor ID of 10415 (3GPP).	OctetString
1067	Usage-Monitoring-Information	Gx-Plus	Sets monitoring thresholds. When service statistics match at least one of the granted service values, the router sends a CCR-U report with the current statistics to the PCRF. Includes the Monitoring-Key AVP (1066) and the Granted-Service-Unit AVP (431). This AVP has a vendor ID of 10415 (3GPP).	Grouped

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. Table 5 on page 14 lists the Juniper Networks AVPs that the supported Diameter applications use.

Table 5: Juniper Networks Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
2004	Juniper-Service-Bundle	JSRC	Specifies the name of the service bundle.	OctetString
2010	Juniper-DHCP-Options	JSRC	Specifies the client's DHCP options.	OctetString
2011	Juniper-DHCP-GI-Address	JSRC	Specifies the DHCP relay agent's IP address.	OctetString
2020	Juniper-Policy-Install	JSRC, PTSP	Specifies policies to be activated for the subscriber. Includes Juniper-Policy-Name and Juniper-Policy-Definition	Grouped
2021	Juniper-Policy-Name	JSRC, PTSP	Defines the name of a policy decision.	OctetString
2022	Juniper-Policy-Definition	JSRC, PTSP	Defines a policy decision. Includes Juniper-Policy-Name, Juniper-Template-Name, and Juniper-Substitution.	Grouped
2023	Juniper-Template-Name	JSRC, PTSP	Profile name defined by the router. PTSP supports only the **__svc_rule__** policy template.	UTF8String
2024	Juniper-Substitution	JSRC, PTSP	Defines the substitution attributes. Includes Juniper-Substitution-Name and Juniper-Substitution-Value.	OctetString
2025	Juniper-Substitution-Name	JSRC, PTSP	Defines the name of the variable to be replaced.	OctetString
2026	Juniper-Substitution-Value	JSRC, PTSP	Defines the value of the variable to be replaced.	OctetString
2027	Juniper-Policy-Remove	JSRC, PTSP	Specifies policies to be deactivated for the subscriber. Includes Juniper-Policy-Name.	Grouped
2035	Juniper-Policy-Failed	JSRC, PTSP	Specifies the name of the policy activation or deactivation that failed.	OctetString
2038	Juniper-Policy-Success	JSRC, PTSP	Specifies the name of the policy activation or deactivation that succeeded.	OctetString
2046	Juniper-Logical-System	JSRC, PTSP	Specifies the logical system.	UTF8String
2047	Juniper-Routing-Instance	JSRC, PTSP	Specifies the routing instance.	UTF8String
2048	Juniper-Jsrc-Partition	JSRC, PTSP	Specifies the logical system and routing instance for the subscriber or request. Includes Juniper-Logical-System and Juniper-Routing-Instance	Grouped

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2050	Juniper-Request-Type	JSRC, PTSP	Describes the type of request: • 1—ADDRESS_AUTHORIZATION • 2—PROVISIONING_REQUEST • 3—SYNCHRONIZATION	Enumerated
2051	Juniper-Synchronization-Type	JSRC, PTSP	Describes the type of synchronization: • 1—FULL-SYNC • 2—FAST-SYNC • 3—NO-STATE-TO-SYNC	Enumerated
2052	Juniper-Synchronization	JSRC, PTSP	Describes the state of synchronization: • 1—NO-SYNC; this is the default state • 2—SYNC-IN-PROGRESS • 3—SYNC-COMPLETE	Enumerated
2053	Juniper-Acct-Record	JSRC, PTSP	Statistics data for each policy installed for this subscriber. Includes Juniper-Policy-Name.	Grouped
2054	Juniper-Acct-Collect	JSRC, PTSP	Specifies whether to collect accounting data for the installed policy (service) when included in the Juniper-Policy-Install AVP: • 1—COLLECT_ACCT • 2—NOT_COLLECT_ACCT	Enumerated
2058	Juniper-State-ID	JSRC, PTSP	Specifies the value assigned to each synchronization cycle for the purpose of identifying which messages to discard. All solicited requests containing the same **Juniper-State-ID** belong to the same Session-Resource-Query (SRQ) synchronization cycle. Messages from a previous synchronization cycle are discarded. When a new cycle begins, the value of the **Juniper-State-ID** AVP is increased by 1. NOTE: For solicited synchronization requests, the SRQ message contains the incremented **Juniper-State-ID** value. For unsolicited synchronization requests, the Session-Resource-Reply (SRR) message contains the incremented **Juniper-State-ID** value.	Unsigned32
2100	Juniper-Virtual-Router	Gx-Plus, JSRC	Specifies the name of the virtual router associated with the session.	UTF8String

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2101	Juniper-Provisioning-Source	Gx-Plus	Specifies the provisioning source for the session in CCR-N and JSDA messages: • 1—Local • 2—Remote	Enumerated
2102	Juniper-Provisioning-Descriptor	Gx-Plus	Defines the group used in JSDA messages that includes the session ID, and optionally Juniper-Provisioning-Source and subscriber data.	Grouped
2103	Juniper-Event-Type	Gx-Plus	Communicates the event type in JSER messages: • 1–Cold boot; all sessions are lost • 2—Warm boot; sessions are preserved • 3—Discovery requested by the operator • 4—*Are you there?* (AYT); application level ping sent when the notification is due to no response or an erroneous response from the PCRF, or due to a configuration change. • 5—AWD; application-level watchdog sent by the router when there has been no other activity for 15 seconds. The watchdog is sent every 5 seconds unless preempted by higher-priority synchronization event.	Enumerated
2104	Juniper-Discovery-Descriptor	Gx-Plus	Defines the group used in JSDR and JSDA messages that includes parameters of a discovery request: discovery type, request string, verbosity, max results.	Grouped
2105	Juniper-Discovery-Type	Gx-Plus	Specifies the discovery subcommand for JSDR and JSDA messages: • 1—Exact: look up the data for the specified session. • 2—Bulk: Provide get-bulk kinds of information after the specified string. • 3—Done: Stop retries for all sessions up to the specified session.	Enumerated

Table 5: Juniper Networks Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
2106	Juniper-Verbosity-Level	Gx-Plus	Specifies the verbosity level for JSDR and JSDA messages: • 1—Summary; include only the Session-Id AVP. • 2—Brief; include the Session-Id, Juniper-Virtual-Router, and Framed-IP-Address AVPs. • 3—Detail; include the Session-Id, Juniper-Provisioning-Source, Juniper-Virtual-Router, Framed-IP-Address, and Event-Timestamp AVPs. 4—Extensive; include all available session information.	Enumerated
2107	Juniper-String-A	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2108	Juniper-String-B	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2109	Juniper-String-C	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2110	Juniper-Unsigned32-A	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2111	Juniper-Unsigned32-B	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2112	Juniper-Unsigned32-C	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32

Tekelec AVPs are used only for Gx-Plus. These AVPs have an enterprise number of 21274. Table 6 on page 17 lists the Tekelec AVPs. These four variables are used to provide substitution values for user-defined CoS service variables.

Table 6: Tekelec Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
5555	Tekelec-Charging-Rule-Argument-Name	Gx-Plus	Defines the name of the service variable to be replaced.	OctetString
5556	Tekelec-Charging-Rule-Argument-Value	Gx-Plus	Defines the value of the service variable to be replaced.	OctetString

Table 6: Tekelec Diameter AVPs *(continued)*

Attribute Number	Diameter AVP	Application	Description	Type
5557	Tekelec-Charging-Rule-Argument	Gx-Plus	Defines the substitution attributes used to replace service variables. Includes Tekelec-Charging-Rule-Argument-Name AVP (5555) and Tekelec-Charging-Rule-Argument-Value AVP (5556).	Grouped
5558	Tekelec-Charging-Rule-With-Arguments	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). Requested service variable substitutions are provided by the optionally included Tekelec-Charging-Rule-Argument AVP (5557).	Grouped

Related Documentation

- Understanding JSRC-SAE Interactions on page 19
- *Understanding PTSP-SAE Interactions*
- *Understanding Gx-Plus Interactions Between the Router and the PCRF*
- *Diameter Base Protocol Overview*
- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- *Juniper Networks Session and Resource Control (SRC) and PTSP Overview*
- *Gx-Plus for Provisioning Subscribers Overview*

Understanding JSRC-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between JSRC (the local SRC peer) and the SAE (the remote SRC peer) as they interact to perform the following tasks for subscriber access:

- Subscriber login
- Service activation
- Service deactivation
- Resynchronization
- SAE-initiated subscriber logout
- Statistics collection and reporting
- Subscriber-initiated logout

Subscriber Login

JSRC authorization is enabled for DHCP subscribers when you include the **authorization-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level. This setting causes AAA to ignore the authentication order setting in the access profile. As a result, AAA does not authenticate the DHCP subscribers. For non-DHCP subscribers, AAA ignores the **authorization-order** statement.

When a DHCP subscriber attempts to log in, DHCP sends an authentication request to AAA. In turn, JSRC sends a Diameter AA-Request message to the SAE. SAE returns a Diameter AA-Answer message that can include the Framed-IP-Address attribute and the Juniper-DHCP-Options AVP (AVP code 2010). JSRC ignores any other optional AVPs included in this AA-Answer message.

JSRC provisioning is enabled for DHCP (and SSC) subscribers when you include the **provisioning-order** statement at the **[edit access profile *profile-name*]** hierarchy level. When the application requests AAA to activate the subscriber's session, JSRC sends an AA-Request message that includes the Juniper-Request-Type AVP (AVP code 2050) with a value that indicates service provisioning is requested from the SAE.

The SAE returns a AA-Answer message that contains an ACK if the request is accepted or a NAK if the request is denied. If the request is accepted, the AA-Answer message includes the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify the service to attach to the subscriber's interface. When this AVP is included, the SAE sets the Result-Code AVP to 1001 (DIAMETER_MULTI_ROUND_AUTH). This code means that the JSRC must send another AA-Request message to the SAE to report the success or failure of the policy instantiation (service activation) by AAA. JSRC ignores any other optional AVPs included in this AA-Answer message. The SAE returns an AA-Answer message to acknowledge this second AA-Request message.

Subscriber Service Activation and Deactivation

SAE policies provision subscriber services. After a subscriber is logged in, the SAE can send a PPR message to JSRC to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service, the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service, or both (for different services). A PPR can include no more than three of these AVPs (install, remove, or mixed).

JSRC sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.

NOTE: If you use RADIUS or the CLI to deactivate a service that the SAE, the SAE becomes unsynchronized with the state of subscribers on the routing engine.

Subscriber Resynchronization

During resynchronization, JSRC informs the SAE about the services that are active for the provisioned subscribers. Either JSRC or the SAE initiates the resynchronization.

- The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.
- JSRC initiates resynchronization at JSRC startup, such as when AAA starts or restarts.

  JSRC can also initiate resynchronization in another circumstance. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to JSRC as its first message. JSRC then locks the Origin-Host AVP of the active SAE. JSRC subsequently triggers resynchronization if it receives a message from any other SAE as indicated by the Origin-Host AVP. Such an incident can occur if communication between the active SAE and a standby SAE is interrupted.

Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message. After the SRR is sent, regardless of whether the SAE or JSRC initiates the synchronization, JSRC sends an AA-Request message to the SAE for each provisioned subscriber present in the session database. The AA-Request message includes a Juniper-Policy-Install AVP for the active services. The SAE returns an AA-Answer message with an ACK to acknowledge receipt.

Subscriber Session Terminated by the SAE

When the SAE terminates a subscriber session, it sends an ASR message to JSRC. JSRC causes AAA to send a logout request to the DHCP (or SSC) client application. When the DHCP client application accepts the logout request, JSRC includes an ACK in the ASR message it sends to the SAE to signify success. If the DHCP client application does not accept the request, then JSRC includes a NAK in the ASR to signify failure. The DHCP client application is responsible for initiating the actual logout sequence with AAA.

Statistics Collection and Reporting per Service Rule

Statistics information can be sent from the router to the SAE or from the SAE to the router. Both the Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages include the Juniper-Acct-Record AVP (AVP code 2053), which identifies the policy (service) for which accounting information is requested.

Subscriber Logout

When the DHCP (or SSC) client application sends a subscriber logout notice to AAA, JSRC sends an STR message to notify the SAE that the provisioned subscriber session is being terminated. The SAE returns an STA message to JSRC, and JSRC notifies DHCP that the logout is complete.

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- Messages Used by Diameter Applications on page 6
- Diameter AVPs and Diameter Applications on page 10
- Configuring JSRC on page 29

CHAPTER 2

Subscribers over Static Interfaces in Subscriber Access Networks

Subscribers on Static Interfaces Overview

You can associate subscribers with statically configured interfaces and provide dynamic service activation and activation for these subscribers. When the static interface comes up, the event is treated as a subscriber login. When the interface goes down, it is treated as a subscriber logout. After the subscribers are present in the session database (SDB), JSRC can report the subscribers to the SAE so that the SRC software can subsequently manage the subscribers.

Alternatively, you can configure the static subscribers to be authenticated and authorized by means of RADIUS. In this case, RADIUS can then activate and deactivate services with change of authorization (CoA) messages. However, this configuration does not prevent the interface from coming up and forwarding traffic. Further, authorization parameters are not imposed on the subscriber interface.

Currently, only Ethernet interfaces support static subscribers. Only one static subscriber can exist over a given interface. An interface cannot appear in more than one group. Static subscribers cannot be created over dynamic interfaces.

Static subscribers are intended to work with JSRC. Include the **provisioning-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level to enable JSRC to handle the subscribers at the direction of the SRC software.

If the authentication request fails for a static subscriber, a 60-minute, nonconfigurable timer begins counting down. The request is reissued when the timer expires. This action repeats for as long as the interface is operationally up.

You can force a logout of the static subscriber by issuing the **request services static-subscribers logout interface *interface-name*** command. A static subscriber can also be logged out by AAA or an external policy manager. In both cases, no subsequent logins can take place on the underlying interface until you reset the state by issuing the **request services static-subscribers login interface *interface-name*** command or the router or process reboots.

You can log out an interface group by issuing the **request services static-subscriber logout group *group-name*** command. You can subsequently log in a group of interfaces by issuing the **request services static-subscriber login group *group-name*** command.

No new CLI statements are required to configure the dynamic profile for static subscribers. The dynamic profile can be very simple; it is activated at login and deactivated at logout. If you do not configure a profile, then the *junos-default-profile* is automatically activated.

During a graceful Routing Engine switchover (GRES) event, active static subscribers are recovered, inactive subscribers are cleaned up, and logout continues for subscribers that were in the process of logging out.

Include the **static-subscribers** statement at the **[edit system services]** hierarchy level to configure static subscribers. Include the **traceoptions** statement at the **[edit system processes static-subscribers]** hierarchy level to configure tracing operations for static subscribers.

You can configure the access profile, dynamic profile, and authentication parameters for all static subscribers or for a particular group of static subscribers:

- To configure the access profile that triggers AAA services for the static subscriber for all static subscribers, include the **access-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration.
- To configure the dynamic profile that is instantiated when the static subscriber logs in for all static subscribers, include the **dynamic-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration. Do not specify a dynamic profile that creates a dynamic interface.
- To configure the authentication parameters that trigger an Access-Request message to AAA for all static subscribers, include the **authentication** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to configure authentication for a specific group and override a top-level configuration. If you do not configure authentication, then by default the interface name is modified and used as the default username for the subscriber session and the authentication request.

The configurable authentication parameters include the password and details of how the username is formed. Include the **password** statement at the **[edit system services static-subscribers authentication]** hierarchy level to configure the authentication password for all static subscribers. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name* authentication]** hierarchy level to configure authentication for a specific group and override a top-level configuration.

The username that is sent to AAA for authentication must include at least one of the following attributes:

- Domain name
- User prefix
- Interface name
- Logical system name
- Routing instance name

To configure how the username is formed for all static subscribers, include the desired statements at the **[edit system services static-subscribers authentication]** hierarchy level: **domain-name**, **user-prefix**, **logical-system-name**, or **routing-instance-name**. Alternatively, include the desired statements at the **[edit system services static-subscribers group *group-name* authentication]** hierarchy level to configure the username for a specific group and override a top-level configuration.

If you change the authentication configuration for an existing group or for static subscribers globally, the change has no effect on existing static subscribers. The changes are applied only to any new logins that are attempted after you commit the changes.

A group configuration must specify all the interfaces that you expect to support static subscribers. Include the **interface** statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to specify the interfaces. This statement enables you to specify a single interface or a range of interfaces.

You must also statically configure these interfaces before any static subscribers can be supported on them. You must configure the static interfaces in the same logical system and routing instance as the group that includes the interfaces.

If you change the interfaces that are included in an existing interface group, existing static subscribers are automatically logged out and then back in when you commit the changes. However, changes made to the configuration of the interface itself have no effect on the login or logout state of the static subscriber associated with that interface.

By default, multiple subscribers are not supported on top of the same VLAN logical interface. If you want to support this behavior, then you can manage multiple subscribers on a single logical interface in one of two ways. You can either merge attributes such as firewall filters and CoS attributes for the multiple subscribers, or you can replace the current attributes with those of a new subscriber whenever a new subscriber logs into the underlying VLAN logical interface.

- To enable attribute merging for all static interfaces, include the **aggregate-clients merge** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to enable attribute merging for a specific group of static interfaces and override a top-level configuration.
- To enable attribute replacement for all static interfaces, include the **aggregate-clients replace** statement at the **[edit system services static-subscribers]** hierarchy level.

Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to enable attribute replacement for a specific group of static interfaces and override a top-level configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- Understanding JSRC-SAE Interactions on page 19

PART 2

Configuration

CHAPTER 3

Configuration Overview for JSRC

Configuring JSRC

You can configure the JSRC client application to work with Session and Resource Control (SRC) to centrally manage subscribers and services. JSRC requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE.

To configure JSRC:

1. Configure the JSRC partition.

   See "Configuring the JSRC Partition" on page 31.

2. Assign the JSRC partition.

   See "Assigning a Partition to JSRC" on page 32.

3. Configure JSRC authorization for subscribers.

   See "Authorizing Subscribers with JSRC" on page 32.

4. Configure JSRC provisioning for subscribers.

   See "Provisioning Subscribers with JSRC" on page 33.

5. Configure service accounting by JSRC.

   See "Configuring Service Accounting with JSRC" on page 33.

6. Configure JSRC event tracing as part of general authentication service tracing operations.

   See "Tracing General Authentication Service Processes" on page 115.

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3

CHAPTER 4

Configuration Tasks for JSRC

Configuring the JSRC Partition

JSRC works within a specific logical system:routing instance context, called a partition.

NOTE: Currently, only a single partition is supported; you must configure it within the default logical system:routing instance context.

Before you configure the JSRC partition, perform the following task:

- Configure the Diameter instance at the **[edit diameter]** hierarchy level. See *Configuring Diameter*.

Configuration for the JSRC partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the JSRC partition:

1. Create the partition.

   ```
   [edit jsrc]
   user@host# set partition partition1
   ```

2. Specify the Diameter instance for the JSRC partition.

   

   NOTE: Currently, only the default Diameter instance, *master*, is supported.

   ```
   [edit jsrc partition partition1]
   user@host# set diameter-instance master
   ```

3. Configure the destination host for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-host sae1
```

4. Configure the destination realm for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-realm generic.example.com
```

Related Documentation

- Configuring JSRC on page 29

Assigning a Partition to JSRC

You must associate a configured JSRC partition with the JSRC instance that you are configuring.

Before you assign a partition to JSRC, perform the following task:

- Configure the JSRC partition. See "Configuring the JSRC Partition" on page 31

To assign the JSRC partition:

- Specify the partition name.

```
[edit jsrc]
user@host# set jsrc-partition partition1
```

Related Documentation

- Configuring JSRC on page 29

Authorizing Subscribers with JSRC

You can configure AAA to use JSRC in an SRC environment to request authorization from the SAE when AAA is verifying whether a DHCP subscriber can access the router. When JSRC authorization is configured, AAA ignores any configured authentication order settings.

Before you configure JSRC authorization, perform the following tasks:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.
- Define the subscriber username with the **username-include** statement in the authentication configuration for DHCP local server or DHCP relay.

To configure JSRC authorization:

- Specify **jsrc** as the authorization method in the profile.

```
[edit access profile dhcpsub1]
user@host# set authorization-order jsrc
```

Related Documentation

- Configuring JSRC on page 29
- *Creating Unique Usernames for DHCP Clients*
- profile on page 54

Provisioning Subscribers with JSRC

You can configure AAA to use JSRC in an SRC environment to request provisioning from the SAE to instantiate services for an authenticated subscriber.

Before you configure JSRC provisioning for subscribers, perform the following task:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.

To configure JSRC provisioning:

- Specify **jsrc** as the provisioning method in the profile.

```
[edit access profile dhcpsub1]
user@host# set provisioning-order jsrc
```

Related Documentation

- Configuring JSRC on page 29

Configuring Service Accounting with JSRC

You can configure JSRC to report accounting statistics for service sessions.

In addition to the configuration shown here, the network context for JSRC service accounting includes the configuration of firewall filters to count the statistics, Diameter, JSRC, the subscriber services, RADIUS, and the SRC.

To configure service accounting by JSRC:

1. Configure JSRC to provision subscriber services.

   ```
   [edit access profile profile-name]
   user@host# set provisioning-order jsrc
   ```

2. Configure service accounting to be provided by the application that provisions the service—JSRC.

   ```
   [edit access profile profile-name service]
   user@host# set accounting-order activation-protocol
   ```

Related Documentation

- Service Accounting with JSRC on page 4

CHAPTER 5

Configuration Overview for Subscribers over Static Interfaces

Configuring Subscribers over Static Interfaces

This topic describes the procedure for configuring subscribers over static interfaces (static subscribers).

Before you configure subscribers over static interfaces, perform the following tasks:

- Configure the static interfaces on which you want to create and manage subscribers.
- Create an access profile to trigger AAA services for static subscribers.
- Create a dynamic profile that is instantiated when static subscribers log in.

To configure static subscribers:

1. Specify the global access profile that triggers AAA services for static subscribers.

   See "Specifying the Static Subscriber Global Access Profile" on page 37.
2. Specify the global dynamic profile that is instantiated when static subscribers log in.

   See "Specifying the Static Subscriber Global Dynamic Profile" on page 38.
3. Configure global method to handle multiple subscribers on a VLAN Logical Interface.

   See "Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers" on page 38
4. Configure the global authentication password for static subscribers.

   See "Configuring the Static Subscriber Global Authentication Password" on page 39.
5. Configure the global username for static subscribers.

   See "Configuring the Static Subscriber Global Username" on page 39.
6. Configure a group of subscribers to share values different from the global configuration.

   See "Creating a Static Subscriber Group" on page 40.
7. Specify the access profile for the static subscriber group.

See "Specifying the Static Subscriber Group Access Profile" on page 41.

8. Specify the dynamic profile for the static subscriber group.

   See "Specifying the Static Subscriber Group Dynamic Profile" on page 41.

9. Configure method to handle multiple subscribers on a VLAN Logical Interface for a static subscriber group.

   See "Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group" on page 42.

10. Configure the authentication password for the static subscriber group.

    See "Configuring the Static Subscriber Group Authentication Password" on page 42.

11. Configure the username for the static subscriber group.

    See "Configuring the Static Subscriber Group Username" on page 43.

12. (Optional) Force a static subscriber to be logged out from an interface.

    See "Forcing a Static Subscriber to Be Logged Out" on page 83.

13. (Optional) Enable an interface to accept static subscriber logins.

    See "Resetting the State of an Interface for Static Subscriber Login" on page 83.

14. (Optional) Force static subscribers to be logged out from a group of interfaces.

    See "Forcing a Group of Static Subscribers to Be Logged Out" on page 84.

15. (Optional) Enable a group of interfaces to accept static subscriber logins.

    See "Resetting the State of an Interface Group for Static Subscriber Login" on page 84.

16. Configure trace options for troubleshooting the configuration.

    See "Tracing Static Subscriber Operations" on page 123.

Related Documentation

- Subscribers on Static Interfaces Overview on page 23
- [edit system services static-subscribers] Hierarchy Level on page 61

CHAPTER 6

Configuration Tasks for Subscribers over Static Interfaces

Specifying the Static Subscriber Global Access Profile

You specify a previously created access profile that triggers AAA services for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the access profile used for all static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers]
user@host# set access-profile access5
```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Group Access Profile on page 41
- profile on page 54

Specifying the Static Subscriber Global Dynamic Profile

You specify a previously created dynamic profile that is instantiated when a static subscriber logs in. This profile is used for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the dynamic profile used for all static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers]
user@host# set dynamic-profile dyn-profile-1
```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Group Dynamic Profile on page 41
- *dynamic-profiles*

Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers

For a given interface, only a single static subscriber (or group) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for all static subscribers to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration can be overridden for a group of static subscribers when a different configuration is applied for that group.

To enable multiple subscribers to share the same VLAN logical interface for all static subscribers, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-1]
user@host# set aggregate-clients merge
```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-3]
user@host# set aggregate-clients replace
```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Group Dynamic Profile on page 41

- dynamic-profile on page 66

Configuring the Static Subscriber Global Authentication Password

You configure a password that is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different password is configured for that group.

To specify the authentication password used for all static subscribers:

- Specify the password.

  ```
  [edit system services static-subscribers authentication]
  user@host# set password Gj85*3mS
  ```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Group Authentication Password on page 42
- authentication on page 64

Configuring the Static Subscriber Global Username

You configure how the username is formed. The username serves as the username for all static subscribers that are created and is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different username is configured for that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

user-prefix.interface.logical-system-name.routing-instance-name@domain-name

To configure the username for all static subscribers:

1. (Optional) Specify a prefix for the username.

   ```
   [edit system services static-subscribers authentication username-include]
   user@host# set user-prefix Building5
   ```

2. (Optional) Specify that the interface name is included in the username.

   ```
   [edit system services static-subscribers authentication username-include]
   user@host# set interface
   ```

3. (Optional) Specify that the logical system name is included in the username.

   ```
   [edit system services static-subscribers authentication username-include]
   user@host# set logical-system-name
   ```

4. Specify that the routing instance name is included in the username.

   ```
   [edit system services static-subscribers authentication username-include]
   ```

```
user@host# set routing-instance-name
```

5. Specify the domain name included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set domain-name campus.example.com
```

Configured in the default logical system and master routing instance for interface ge-0/1/1.100, this sample configuration generates the following username:

Building5.ge-0-1-1-100.default.master.campus.example.com

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Group Username on page 43
- username-include on page 77

Creating a Static Subscriber Group

You can override the configuration that is applied globally to static subscribers by creating a static subscriber group that consists of a set of statically configured interfaces. You can then apply a common configuration for the group with values different from the global values for access and dynamic profiles, password, and username.

To configure an interface group for static subscribers:

1. Access the **[edit system services static-subscribers]** hierarchy level.
2. Create the group and assign the name.

```
[edit system services static-subscribers]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which static subscribers can be created. You can repeat the *interface* ***interface-name*** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services static-subscribers group boston]
user@host# set interface ge-1/0/1.1
user@host# set interface ge-1/0/1.2
```

4. (Optional) You can use the **upto** ***upto-interface-name*** option to specify a range of interfaces for a group.

```
[edit system services static-subscribers group boston]
user@host# set interface ge-1/0/1.3 upto ge-1/0/1.9
```

5. (Optional) You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services static-subscribers group boston]
user@host# set interface ge-1/0/1.1 upto ge-1/0/1.102
user@host# set interface ge-1/0/1.6 exclude
user@host# set interface ge-1/0/1.70 upto ge-1/0/1.80 exclude
```

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Group Access Profile on page 41
- Specifying the Static Subscriber Group Dynamic Profile on page 41
- Configuring the Static Subscriber Group Authentication Password on page 42
- Configuring the Static Subscriber Group Username on page 43

Specifying the Static Subscriber Group Access Profile

You can override the configured global access profile by specifying a different profile for a group of static subscribers. The access profile triggers AAA services for that group of static subscribers.

To specify the access profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]
user@host# set access-profile boston-acs
```

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- profile on page 54

Specifying the Static Subscriber Group Dynamic Profile

You can override the configured global dynamic profile by specifying a different profile for a group of static subscribers. The dynamic profile is instantiated when any static subscriber in the group logs in.

To specify the dynamic profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]
user@host# set dynamic-profile dyn-profile-2
```

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Global Dynamic Profile on page 38
- *dynamic-profiles*

Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group

For a given interface, only a single static subscriber group (or static subscriber) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for a static subscriber group to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber group is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration overrides the configuration applied to all static subscribers that are not members of the group.

To enable multiple subscribers to share the same VLAN logical interface for a static subscriber group, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

  ```
  [edit system services static-subscribers group boston dynamic-profile dyn-profile-2]
  user@host# set aggregate-clients merge
  ```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

  ```
  [edit system services static-subscribers group boston dynamic-profile dyn-profile-4]
  user@host# set aggregate-clients replace
  ```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Group Dynamic Profile on page 41
- dynamic-profile on page 66

Configuring the Static Subscriber Group Authentication Password

You can override the configured global authentication password by specifying a different password for a group of static subscribers. This password is included in the Access-Request message sent to AAA to authenticate all static subscribers in the group.

To specify the authentication password used for a group of static subscribers:

- Specify the password.

  ```
  [edit system services static-subscribers group boston authentication]
  user@host# set password knTS$$k2
  ```

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35

- Configuring the Static Subscriber Global Authentication Password on page 39
- authentication on page 64

Configuring the Static Subscriber Group Username

You can override the configured global username by specifying a different username for a group of static subscribers. The username serves as the username for a group of static subscribers that is created and is included in the Access-Request message sent to AAA to authenticate that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

user-prefix.interface.logical-system-name.routing-instance-name@domain-name

To configure the username for a group of static subscribers:

1. (Optional) Specify a prefix for the username.

   [edit system services static-subscribers group boston authentication username-include]
   user@host# **set** user-prefix **2ndFloor**

2. (Optional) Specify that the interface name is included in the username.

   [edit system services static-subscribers group boston authentication username-include]
   user@host# **set** interface

3. (Optional) Specify that the logical system name is included in the username.

   [edit system services static-subscribers group boston authentication username-include]
   user@host# **set** logical-system-name

4. Specify that the routing instance name is included in the username.

   [edit system services static-subscribers group boston authentication username-include]
   user@host# **set** routing-instance-name

5. Specify the domain name included in the username.

   [edit system services static-subscribers group boston authentication username-include]
   user@host# **set** domain-name **building5.example.com**

Configured in the default logical system and master routing instance for interface ge-0/1/2.50, this sample configuration generates the following username:

2ndfloor.ge-0-1-2-50.default.master.building5.example.com

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- username-include on page 77

CHAPTER 7

Static Subscriber Example

Example: Configuring Static Subscribers for Subscriber Access

This example shows a static subscriber configuration.

1. Configure the access profile to be used for static subscribers.

```
access {
  profile access5 {
    provisioning-order jsrc;
    accounting {
      order radius;
    }
    authentication {
      order radius;
    }
  }
}
```

2. Configure the dynamic profile to be used for static subscribers.

   If you do not configure this profile, the default profile, junos-default-profile, is used.

3. Configure the static interfaces on which to layer the static subscribers.

4. Configure the parameters that apply globally to all static subscribers in the configuration context.

```
static-subscribers {
  access-profile access5;
  dynamic-profile dyn-profile-1;
  authentication {
    password Gj85*3mS;
    username-include {
      user-prefix Building5;
      interface;
      logical-system-name;
      routing-instance-name;
      domain-name example.com;
    }
  }
}
```

5. If you want to override the global parameters for certain static subscribers, create a group of static interfaces for those subscribers and configure parameters to apply to that group. Repeat this step for as many groups as you need.

```
static-subscribers {
  group boston {
    interface ge-1/0/1.1 upto ge-1/0/1.102
    interface ge-1/0/1.6 exclude
    interface ge-1/0/1.70 upto ge-1/0/1.80 exclude
    access-profile boston-acs;
    dynamic-profile dyn-profile-2;
    authentication {
      password knTS$$k2;
      username-include {
        user-prefix 2ndFloor;
        interface;
        logical-system-name;
        routing-instance-name;
        domain-name example.net;
      }
    }
  }
}
```

6. Configure tracing options for static subscriber events.

```
static-subscribers {
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

Related Documentation

- Subscribers on Static Interfaces Overview on page 23
- Configuring Subscribers over Static Interfaces on page 35

CHAPTER 8

Configuration Statements for JSRC

[edit access profile] Hierarchy Level

```
access {
  profile profile-name {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      coa-immediate-update;
      coa-no-override service-class-attribute;
      duplication;
      immediate-update;
      order [ accounting-method ];
      statistics (time | volume-time);
      update-interval minutes;
      wait-for-acct-on-ack;
    }
    authentication-order [ authentication-methods ];
    authorization-order jsrc;
    client client-name {
      ...
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system–routing-instance;
          output-filter;
        }
      }
```

```
    authentication-server [ ip-address ];
    options {
      accounting-session-id-format (decimal | description);
      calling-station-id-delimiter delimiter-character;
      calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
      }
      client-accounting-algorithm (detail | round-robin);
      client-authentication-algorithm(detail | round-robin);
      coa-dynamic-variable-validation;
      ethernet-port-type-virtual;
      interface-description-format {
        exclude-adapter;
        exclude-sub-interface;
      }
      nas-identifier identifier-value;
      nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
        atm {
          adapter-width width;
          port-width width:
          slot-width width;
          vci-width width:
          vpi-width width;
        }
      }
      nas-port-id-delimiter delimiter-character;
      nas-port-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
      }
      nas-port-type {
        ethernet {
          port-type;
        }
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
  }
  radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
```

```
        max-outstanding-requests value;
        source-address source-address;
        timeout seconds;
      }
      service {
        accounting-order (activation-protocol | radius);
      }
      session-options {
        client-idle-timeout minutes;
        client-session-timeout minutes;
      }
    }
  }
```

Related Documentation

- *AAA Service Framework Overview*

[edit jsrc] Hierarchy Level

```
jsrc {
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm-name;
  }
}
```

Related Documentation

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- Configuring JSRC on page 29

accounting-order (Service Accounting)

Syntax accounting-order (activation-protocol | radius);

Hierarchy Level [edit access profile *profile-name* service]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify which method is used for reporting subscriber service accounting.

Default activation-protocol

Options **activation-protocol**—Send service accounting reports by means of the application that activates services, such as JSRC.

radius—Send service accounting reports by means of the RADIUS protocol.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring Service Accounting with JSRC on page 33
- Service Accounting with JSRC on page 4

authorization-order

Syntax authorization-order jsrc;

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.

Options jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Authorizing Subscribers with JSRC on page 32

destination-host

Syntax destination-host *hostname*

Hierarchy Level [edit jsrc partition *partition-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure the host on which the SAE application resides.

Options ***hostname***—Host on which the SAE is installed.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Configuring the JSRC Partition on page 31

destination-realm (JSRC)

Syntax destination-realm *realm*

Hierarchy Level [edit jsrc partition *partition-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure the realm in which the SAE host resides.

Options ***realm***—Realm in which the SAE host resides.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Configuring the JSRC Partition on page 31

diameter-instance (JSRC)

Syntax diameter-instance *instance-name*

Hierarchy Level [edit jsrc partition *partition-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify the Diameter instance associated with the JSRC partition.

Options ***instance-name***—Name of the Diameter instance. Currently, only **master** is supported.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Configuring the JSRC Partition on page 31

jsrc (JSRC)

Syntax

```
jsrc {
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm-name;
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure JSRC to interact with an SAE in an SRC environment to authorize and provision subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29

jsrc-partition

Syntax jsrc-partition *partition-name*;

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify the JSRC partition to use.

Options ***partition-name***—Name of the JSRC partition that you want JSRC to use. The name is defined with the **partition** statement at the **[edit jsrc]** hierarchy level.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Configuring the JSRC Partition on page 31

partition

Syntax
```
partition partition-name {
  diameter-instance instance-name;
  destination-host hostname;
  destination-realm realm;
}
```

Hierarchy Level [edit jsrc]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure a JSRC partition.

Options ***partition-name***—Name of the JSRC partition.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Configuring the JSRC Partition on page 31

profile (Access)

Syntax

```
profile profile-name {
  accounting {
    address-change-immediate-update
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    duplication-vrf {
      access-profile-name profile-name;
      vrf-name vrf-name;
    }
    immediate-update;
    order [ accounting-method ];
    send-acct-status-on-config-change;
    statistics (time | volume-time);
    update-interval minutes;
    wait-for-acct-on-ack;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      aaa-access-profile profile-name;
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
```

```
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
      user-group-profile profile-name;
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      authentication-server [ ip-address ];
      options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
          exclude-adapter;
          exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
          adapter-width width;
          ae-width width;
          port-width width;
          slot-width width;
          stacked-vlan-width width;
          vlan-width width;
          atm {
            adapter-width width;
            port-width width:
            slot-width width;
            vci-width width:
            vpi-width width;
          }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
```

```
        }
        nas-port-type {
          ethernet {
            port-type;
          }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
      }
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system:routing-instance;
          output-filter;
        }
      }
    }
    radius-server server-address {
      accounting-port port-number;
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      max-outstanding-requests value;
      source-address source-address;
      timeout seconds;
    }
    service {
      accounting-order (activation-protocol | radius);
    }
    session-options {
      client-group [ group-names ];
      client-idle-timeout minutes;
      client-session-timeoutminutes;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options ***profile-name***—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- *Configuring the PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- Configuring Service Accounting with JSRC on page 33
- *AAA Service Framework Overview*
- *show network-access aaa statistics*
- *clear network-access aaa statistics*

provisioning-order

Syntax
provisioning-order (gx-plus | jsrc);

Hierarchy Level
[edit access profile *profile-name*]

Release Information
Statement introduced in Junos OS Release 9.6.
Support for Gx-Plus introduced in Junos OS Release 11.2.

Description
Configure AAA to use the specified application for subscriber service provisioning.

Options
gx-plus—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.

jsrc—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring JSRC on page 29
- Provisioning Subscribers with JSRC on page 33
- *Configuring Gx-Plus*
- *Provisioning Subscribers with Gx-Plus*

service (Service Accounting)

Syntax

```
service {
  accounting-order (activation-protocol | radius);
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Define the subscriber service accounting configuration.

The remaining statement is explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Service Accounting with JSRC on page 33
- Service Accounting with JSRC on page 4

traceoptions (General Authentication Service)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit system processes general-authentication-service]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure tracing options for the general authentication service.

Options

file *filename*—Name of the file to receive the output of the tracing operation. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address-assignment**—Trace address-assignment pool events
- **all**—Trace all tracing operations
- **configuration**—Trace configuration events
- **framework**—Trace authentication framework events
- **gx-plus**—Trace Gx-Plus events
- **jsrc**—Trace JSRC events
- **ldap**—Trace LDAP authentication events
- **local-authentication**—Trace local authentication events
- **radius**—Trace RADIUS authentication events
- **user-access**—Trace user access events, such as login, logout, and authenticate.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing General Authentication Service Processes on page 115

CHAPTER 9

Configuration Statements for Subscribers on Static Interfaces

[edit system services static-subscribers] Hierarchy Level

```
system {
  services {
    static-subscribers {
      access-profile profile-name;
      authentication {
        password password-string;
        username-include {
          domain-name domain-name;
          interface;
          logical-system-name;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
      dynamic-profile profile-name {
        aggregate-clients (merge | replace);
      }
      group group-name {
        access-profile profile-name;
        authentication {
          password password-string;
          username-include {
            domain-name domain-name;
            interface;
            logical-system-name;
            routing-instance-name;
            user-prefix user-prefix-string;
          }
        }
        dynamic-profile profile-name {
          aggregate-clients (merge | replace);
        }
        interface interface-name <exclude> <upto upto-interface-name>;
      }
      traceoptions {
```

```
                file filename <files number> <match regular-expression > <size maximum-file-size>
                  <world-readable | no-world-readable>;
                flag flag;
                level (all | error | info | notice | verbose | warning);
                no-remote-trace;
            }
        }
    }
}
```

Related Documentation

- Subscribers on Static Interfaces Overview on page 23
- Configuring Subscribers over Static Interfaces on page 35

access-profile (Static Subscribers)

Syntax access-profile *profile-name*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit logical-systems *logical-system-name* system services static-subscribers],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit system services static-subscribers],
[edit system services static-subscribers group *group-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify the access profile that triggers AAA services for all static subscribers on interfaces configured at the **[edit system services static-subscribers interface]** hierarchy level or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.

Options ***profile-name***—Name of the static subscriber access profile.

Required Privilege Level
access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Global Access Profile on page 37
- Specifying the Static Subscriber Group Access Profile on page 41

aggregate-clients (Static Subscribers)

Syntax aggregate-clients (merge | replace);

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* system services static-subscribers dynamic-profile *profile-name*],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* dynamic-profile *profile-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers dynamic-profile *profile-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* dynamic-profile *profile-name*],
[edit system services static-subscribers dynamic-profile *profile-name*],
[edit system services static-subscribers group *group-name* dynamic-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify for all static subscribers or for a group of static subscribers that the router merge (chain) subscriber (client) attributes such as firewall filters and CoS attributes or replace them when multiple subscriber sessions exist on the same underlying VLAN. The group version of this statement overrides the global version.

This statement is not supported for IP demux subscriber interfaces.

Default By default, multiple subscribers cannot be on the same logical interface.

Options
merge—Aggregate the attributes of multiple subscribers for the logical interface.

replace—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers on page 38

authentication (Static Subscribers)

Syntax

```
authentication {
  password password-string;
  username-include {
    domain-name domain-name;
    interface;
    logical-system-name;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit logical-systems *logical-system-name* system services static-subscribers],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit system services static-subscribers],
[edit system services static-subscribers group *group-name*]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Specify the authentication parameters that trigger the Access-Request message to AAA for all static subscribers on interfaces configured at the **[edit system services static-subscribers interface]** hierarchy level, or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Authentication Password on page 39
- Configuring the Static Subscriber Group Authentication Password on page 42

domain-name (Static Subscribers)

Syntax domain-name *domain-name*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit system services static-subscribers authentication username-include],
[edit system services static-subscribers group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify the domain name that is included at the end of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version.

Options *domain-name*—Domain name that ends the username created for all static subscribers. The username is also sent to RADIUS in the Access-Request message. The string can include the following characters: a through z, A through Z, 0 through 9, "-", or ".".

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

dynamic-profile (Static Subscribers)

Syntax

```
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit logical-systems *logical-system-name* system services static-subscribers],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit system services static-subscribers],
[edit system services static-subscribers group *group-name*]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Specify the dynamic client profile that is instantiated at login and de-instantiated at logout for all static subscribers on interfaces configured at the **[edit system services static-subscribers interface]** hierarchy level or for the static subscribers in a specific group. The group version of the statement takes precedence over the global version.

NOTE: Do not specify a dynamic profile that creates a dynamic interface.

Default

By default, the *junos-default-profile* is used when you do not specify a global dynamic profile with this statement.

Options

profile-name—Name of the dynamic client profile profile.

The remaining statement is explained separately.

Required Privilege Level

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Specifying the Static Subscriber Global Dynamic Profile on page 38
- Specifying the Static Subscriber Group Dynamic Profile on page 41

group (Static Subscribers)

Syntax

```
group group-name {
  access-profile profile-name;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
  }
  authentication {
    password password-string;
    username-include {
      domain-name domain-name;
      interface;
      logical-system-name;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  interface interface-name <exclude> <upto upto-interface-name>;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system services static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers],
[edit routing-instances *routing-instances-name* system services static-subscribers],
[edit system services static-subscribers]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Configure a static subscriber group with values that override the values configured at the **[edit system services static-subscribers]** hierarchy level for subscribers outside the group. Includes the subscriber access and dynamic profiles, the authentication parameters that trigger the Access-Request message to AAA for static subscribers in the group, and the statically configured interfaces that form the group.

NOTE: The logical system and routing instance in which the group is configured must match the logical system and routing instance where the static interfaces are configured.

Options

group-name—Name of a group that defines authentication parameters for static subscribers to override the global authentication configuration.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Creating a Static Subscriber Group on page 40

interface (Static Subscriber Group)

Syntax interface *interface-name* <exclude> <upto *upto-interface-name*>;

Hierarchy Level [edit logical-systems *logical-system-name* system services static-subscribers group *group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name*],
[edit system services static-subscribers group *group-name*]

Release Information Statement introduced in Junos OS Release 9.6.
Support for IPv6 and IPv4 demux static interfaces introduced in Junos OS Release 11.2.

Description Specify one or more interfaces, or a range of interfaces, that are within a specified group on which static subscribers are created. You can repeat the **interface *interface-name*** statement to specify multiple interfaces within a group. You must configure each interface in only one group.

NOTE: The logical system and routing instance in which the static interfaces are configured must match the logical system and routing instance where the group is configured.

Options **exclude**—(Optional) Exclude an interface or a range of interfaces from the group.

interface-name—Name of the interface on which static subscribers are created. If you do not specify a unit number for the interface, then .0 is assumed. For example, **ge-0/1/0** is interpreted as **ge-0/1/0.0**.

upto-interface-name—(Optional) The upper end of the range of interfaces; the lower end of the range is the *interface-name* entry. The interface device name of *upto-interface-name* must be the same as the device name of *interface-name*.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Creating a Static Subscriber Group on page 40

interface (Static Subscriber Username)

Syntax interface;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit system services static-subscribers authentication username-include],
[edit system services static-subscribers group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify that a modified version of the interface name is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message. The interface name is modified by replacing the "/" character with the "-" character. For example, ge-0/1/2.50 is converted to ge-0-1-2.50.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

logical-system-name (Static Subscribers)

Syntax logical-system-name;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit system services static-subscribers authentication username-include],
[edit system services static-subscribers group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify that the name of the logical system is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

password (Static Subscribers)

Syntax

```
password password-string;
  username-include {
    domain-name domain-name;
    username-include;
    logical-system-name;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication],
[edit logical-systems *logical-system-name* system services static-subscribers authentication],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include], authentication],
[edit system services static-subscribers authentication],
[edit system services static-subscribers group *group-name* authentication]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Specify the password that is sent to AAA for user login for all static subscribers on interfaces configured at the **[edit system services static-subscribers interface]** hierarchy level, or for the subscribers in a specified group. The group version of the statement takes precedence over the global version.

Options

password-string—String that defines the password.

The remaining statements are explained separately.

Required Privilege Level

system-level—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Authentication Password on page 39
- Configuring the Static Subscriber Group Authentication Password on page 42

routing-instance-name (Static Subscribers)

Syntax routing-instance-name;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit system services static-subscribers authentication username-include],
[edit system services static-subscribers group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify that the name of the routing instance is included as part of the username created for all static subscribers or for the static subscribers in the specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

static-subscribers

Syntax

```
static-subscribers {
  access-profile profile-name;
  authentication {
    password password-string;
    username-include {
      domain-name domain-name;
      interface;
      logical-system-name;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
  }
  group group-name {
    access-profile profile-name;
    authentication {
      password password-string;
      username-include {
        domain-name domain-name;
        interface;
        logical-system-name;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      aggregate-clients (merge | replace);
    }
    interface interface-name <exclude> <upto upto-interface-name>;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system services],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services],
[edit routing-instances *routing-instances-name* system services],
[edit system services]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Configure and associate subscribers with statically configured interfaces for dynamic service provisioning.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35

traceoptions (Static Subscribers)

Syntax

```
traceoptions {
  file filename<files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system processes static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system processes static-subscribers],
[edit routing-instances *routing-instances-name* system processes static-subscribers],
[edit system processes static-subscribers]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Define tracing operations for static subscriber processes.

Options

file *filename*— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **authentication**—Trace authentication events.
- **configuration**—Trace configuration events.
- **database**—Trace database events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **profile**—Trace dynamic profile events.
- **rtsock**—Trace routing socket events.
- **statistics**—Trace statistics events.
- **subscriber**—Trace subscriber events.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.

- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size ***maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Static Subscriber Operations on page 123

username-include (Static Subscribers)

Syntax

```
username-include {
  domain-name domain-name;
  interface;
  logical-system-name;
  routing-instance-name;
  user-prefix user-prefix-string;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication],
[edit logical-systems *logical-system-name* system services static-subscribers authentication],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication],
[edit system services static-subscribers authentication],
[edit system services static-subscribers group *group-name* authentication]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Specify the information included in the username created for all static subscribers or for static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

user-prefix (Static Subscribers)

Syntax user-prefix *user-prefix-string*;

Hierarchy Level
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers authentication username-include],
[edit logical-systems *logical-system-name* system services static-subscribers group *group-name* authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers authentication username-include],
[edit routing-instances *routing-instances-name* system services static-subscribers group *group-name* authentication username-include],
[edit system services static-subscribers authentication username-include],
[edit system services static-subscribers group *group-name* authentication username-include]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify that a string is included as the beginning of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.

Options ***user-prefix-string***—String that begins the username. The string can include the following characters: a through z, A through Z, 0 through 9, "-", or ".".

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring Subscribers over Static Interfaces on page 35
- Configuring the Static Subscriber Global Username on page 39
- Configuring the Static Subscriber Group Username on page 43

PART 3

Administration

CHAPTER 10

Monitoring the JSRC Function and Diameter

Verifying Diameter Node, Instance, and Route Information

Purpose View Diameter node information:

Action

- To display summary information about all Diameter nodes:

  user@host> **show diameter**

- To display summary information about all Diameter nodes and add information about Diameter functions, instances, network elements, and peers:

  user@host> **show diameter brief**

- To display brief information about all Diameter nodes and add information about Diameter routes:

  user@host> **show diameter detail**

- To display summary information about all Diameter instances:

  user@host> **show diameter instance**

- To display detailed information about all Diameter instances:

  user@host> **show diameter instance detail**

- To display information about a specific Diameter instance, add the instance name to the command:

  user@host> **show diameter instance master**

  user@host> **show diameter instance detail master**

- To display summary information about all Diameter routes:

  user@host> **show diameter route**

- To display detailed information about all Diameter routes:

  user@host> **show diameter route detail**

- To display information about a specific Diameter route, add the route name to the command:

  user@host> **show diameter route dne-route2**

  user@host> **show diameter route detail dne-route2**

Related Documentation

- *Configuring Diameter*
- *Configuring Gx-Plus*
- *Junos OS Operational Mode Commands*

Verifying and Managing Diameter Function Information

Purpose View or clear Diameter function information:

Action

- To display summary information about all functions associated with Diameter:

  user@host> **show diameter function**

- To display detailed information about all functions associated with Diameter:

  user@host> **show diameter function detail**

- To display information about a specific function associated with Diameter, add the function name to the command:

  user@host> **show diameter function jsrc**

  user@host> **show diameter function detail ptsp**

- To display summary statistics about all functions associated with Diameter:

  user@host> **show diameter function statistics**

- To display detailed statistics about all functions associated with Diameter:

  user@host> **show diameter function statistics detail**

- To display statistics about a specific function associated with Diameter, add the function name to the command:

  user@host> **show diameter function statistics gx-plus**

  user@host> **show diameter function statistics detail jsrc**

- To delete current statistics for all functions associated with Diameter:

  user@host>**clear diameter function statistics**

- To delete current statistics for a specific function associated with Diameter:

  user@host>**clear diameter function gx-plus statistics**

Related Documentation

- *Configuring Diameter*
- *Configuring Gx-Plus*
- *Junos OS Operational Mode Commands*

CHAPTER 11

Manually Managing Subscribers on Static Interfaces

Forcing a Static Subscriber to Be Logged Out

You can force a static subscriber to be logged out on an interface. After you do so, no subscriber can subsequently log in on that interface until the interface state is reset either by a router reset or by entering the **request services static-subscribers login interface** command.

- To forcibly log out a static subscriber on a static interface:

  user@host> request services static-subscribers logout interface **ge-2/0/1.5**

Related Documentation

- Resetting the State of an Interface for Static Subscriber Login on page 83

Resetting the State of an Interface for Static Subscriber Login

When a static subscriber has been forcibly logged out on an interface with the **request services static-subscribers logout interface** command, you can reset the state of the interface. This action enables a static subscriber to log in on the interface. If you do not reset the state manually, then no static subscribers can log in on the interface until the state is reset by a router reset.

- To reset the state of a static interface:

  user@host> request services static-subscribers login interface **ge-2/0/1.5**

Related Documentation

- Forcing a Static Subscriber to Be Logged Out on page 83

Forcing a Group of Static Subscribers to Be Logged Out

You can force the static subscribes on all interfaces in a group to be logged out. After you do so, no subscriber can subsequently log in on an interface in that group until the interface state is reset either by a router reset or by entering the **request services static-subscribers login group** command.

- To forcibly log out all static subscribers on a static interface group:

  user@host> request services static-subscribers logout group **boston**

Related Documentation

- Resetting the State of an Interface Group for Static Subscriber Login on page 84

Resetting the State of an Interface Group for Static Subscriber Login

When static subscribers have been forcibly logged out on an interface group with the **request services static-subscribers logout group** command, you can reset the state of the group. This action enables static subscribers to log in on the interfaces in the group. If you do not reset the state manually, then no static subscribers can log in on any interface in the group until the state is reset by a router reset.

- To reset the state of a static interface group:

  user@host> request services static-subscribers login group **boston**

Related Documentation

- Forcing a Group of Static Subscribers to Be Logged Out on page 84

CHAPTER 12

Monitoring Subscriber Sessions on Static Interfaces

Verifying Information about Subscriber Sessions on Static Interfaces

Purpose View information about subscriber sessions on static interfaces:

Action

- To display information about all static subscriber sessions:

  user@host> **show static-subscribers sessions**

- To display information about the subscriber sessions for the specified group of static interfaces:

  user@host> **show static-subscribers sessions group boston**

- To display information about the subscriber session for the specified interface:

  user@host> **show static-subscribers sessions interface ge-0/0/1.1**

Related Documentation

- For more information, see the *Junos OS Operational Mode Commands*
- Configuring Subscribers over Static Interfaces on page 35
- Subscribers on Static Interfaces Overview on page 23

CHAPTER 13

Administrative Commands for Static Subscriber Interfaces

request services static-subscribers login group

Syntax **request services static-subscribers login group** ***group-name***

Release Information Command introduced in Junos OS Release 9.6.

Description Resets the state of an interface group on which static subscribers were forcibly logged out by the **request services static-subscribers logout group** command. This action enables static subscriber to login on the interfaces in the group.

Options **group** ***group-name***—Group of static subscriber interfaces on which static subscribers have been created.

Required Privilege Level view

Related Documentation
- Resetting the State of an Interface Group for Static Subscriber Login on page 84
- request services static-subscribers logout group on page 89

List of Sample Output request services static-subscribers login group on page 88

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers login group

```
user@host> request services static-subscribers login group boston
```

request services static-subscribers logout group

Syntax **request services static-subscribers logout group** *igroup-name*

Release Information Command introduced in Junos OS Release 9.6.

Description Force static subscribers on the interfaces in the group to be logged out. No subscriber can subsequently log in on the interface group until the interface state is reset by a router reset or the **request services static-subscribers login group** command.

Options **group** *group-name*—Group of static subscriber interfaces on which static subscribers have been created.

Required Privilege Level view

Related Documentation
- Forcing a Group of Static Subscribers to Be Logged Out on page 84
- request services static-subscribers login group on page 88

List of Sample Output request services static-subscribers logout group on page 89

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers logout group

```
user@host> request services static-subscribers logout group boston
```

request services static-subscribers login interface

Syntax **request services static-subscribers login interface** ***interface-name***

Release Information Command introduced in Junos OS Release 9.6.

Description Resets the state of an interface on which a static subscriber was forcibly logged out by the **request services static-subscribers logout interface** command. This action enables a static subscriber to login on the interface.

Options **interface** ***interface-name***—Static interface on which a static subscriber has been created.

Required Privilege Level view

Related Documentation
- Resetting the State of an Interface for Static Subscriber Login on page 83
- request services static-subscribers logout interface on page 91

List of Sample Output request services static-subscribers login interface on page 90

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers login interface

```
user@host> request services static-subscribers login interface ge-2/0/1.5
```

request services static-subscribers logout interface

Syntax **request services static-subscribers logout interface** ***interface-name***

Release Information Command introduced in Junos OS Release 9.6.

Description Force static subscriber on the interface to be logged out. No subscriber can subsequently log in on the interface until the interface state is reset by a router reset or the **request services static-subscribers login interface** command.

Options **interface** ***interface-name***—Static interface on which a static subscriber has been created.

Required Privilege Level view

Related Documentation
- Forcing a Static Subscriber to Be Logged Out on page 83
- request services static-subscribers login interface on page 90

List of Sample Output request services static-subscribers logout interface on page 91

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers logout interface

```
user@host> request services static-subscribers logout interface ge-2/0/1.5
```

CHAPTER 14

Monitoring Commands

clear diameter function statistics

Syntax **clear diameter function <*function-name*> statistics**

Release Information Command introduced in Junos OS Release 9.6.
Support for PTSP introduced in Junos OS Release 10.2.
Support for Gx-Plus introduced in Junos OS Release 11.2.

Description Clear current statistics accumulated for a specified function (application) or for all functions associated with the Diameter instance.

Options ***function-name***—(Optional) Clear statistics for the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions.

Required Privilege Level clear

Related Documentation

- *Gx-Plus for Provisioning Subscribers Overview*
- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 3
- *PTSP Overview*
- show diameter on page 95
- show diameter function on page 101
- show diameter function statistics on page 105

List of Sample Output clear diameter function statistics on page 94

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear diameter function statistics

```
user@host> clear diameter function jsrc statistics
```

show diameter

Syntax **show diameter**
<brief | detail | summary>

Release Information Command introduced in Junos OS Release 9.6.

Description Display information about the Diameter node.

Options **brief | detail | summary**—(Optional) Display the specified level of output. The **summary** output is displayed by default and includes Diameter node status. The **brief** output adds summary information about functions, instances, network elements, and peers. The **detail** output adds summary information about routes.

Required Privilege Level view

Related Documentation

- clear diameter function statistics on page 94
- *clear diameter peer*
- show diameter function on page 101
- *show diameter instance*
- *show diameter network-element*
- *show diameter peer*
- show diameter route on page 108

List of Sample Output
show diameter brief on page 98
show diameter detail on page 99
show diameter summary on page 99

Output Fields Table 7 on page 95 lists the output fields for the **show diameter** command. Output fields are listed in the approximate order in which they appear.

Table 7: show diameter Output Fields

Field Name	Field Description	Level of Output
Diameter process id	ID number of the Diameter process.	All levels
Functions	Number of functions associated with Diameter.	All levels
Connected functions	Number of functions with active Diameter connections.	All levels
Instances	Number of configured Diameter instances.	All levels

Table 7: show diameter Output Fields *(continued)*

Field Name	Field Description	Level of Output
Network elements (NEs)	Number of configured Diameter network elements.	All levels
Connected NEs	Number of Diameter network elements with active connections.	All levels
Peers	Number of Diameter peer nodes.	All levels
Activated peers	Number of Diameter peers with active connections.	All levels
Open peers	Number of peers in the open state, without active network element connections but available for a connection.	All levels
Transports	Number of transports configured.	All levels
Requests queued for network transmit	Number of requests waiting to be sent to the Diameter peers.	All levels
Answers queued for network transmit	Number of replies waiting to be sent to the Diameter peers.	All levels
Expected answers from network	Number of replies expected to be received from the Diameter peers.	All levels
Requests queued for function transmit	Number of requests waiting to be sent to the functions associated with Diameter.	All levels
Answers queued for function transmit	Number of replies waiting to be sent to the functions associated with Diameter.	All levels
Expected answers from functions	Number of replies expected to be received from the functions associated with Diameter.	All levels
Memory used by network transmit queues	Amount of memory consumed by network transmit queues.	All levels
Memory used by function transmit queues	Amount of memory consumed by function transmit queues.	All levels
Origin-state-id	Value of the Origin-State-ID AVP.	All levels
Function	Name of the function for which information is displayed.	**brief detail**
State	State of the Diameter connection with the function: **Connected** or **Disconnec** (disconnected).	**brief detail**

Table 7: show diameter Output Fields *(continued)*

Field Name	Field Description	Level of Output
Upstream Transaction Utilization	Percent of upstream traffic used for this function.	**brief detail**
Downstream Transaction Utilization	Percent of downstream traffic used for this function.	**brief detail**
Net Queue Buffer Utilization	Percent of network transmission buffer used for this function.	**brief detail**
Func Queue Buffer Utilization	Percent of function transmission buffer used for this function.	**brief detail**
Routed Dests	Number of destinations that have this function associated with their routes.	**brief detail**
Name	Name of the Diameter instance.	**brief detail**
Origin-Realm	Value of Origin-Realm attribute-value pair (AVP).	**brief detail**
Origin Host	Value of Origin-Host AVP.	**brief detail**
NE-Total	Number of configured network elements.	**brief detail**
NE-Connected	Number of network elements with active Diameter connections.	**brief detail**
Name	Name of the Diameter network element.	**brief detail**
Instance	Name of the Diameter instance in which the network element is configured.	**brief detail**
State	State of the network element: • Connecting—None of the network element peers are in the open state and available for connection. • Selecting—One network element peer is connected and the network element is waiting for another peer to reach the open state so that it can be connected. • Partially-Connected—One network element peer is in the open state and connected. • Post-selection-delay—Three or more peers are in the open state and the network element is waiting to deactivate the peers in excess of two. • Fully-connected—Two network element peers are in the open state and connected.	**brief detail**
Primary Peer	Primary peer for the network element, based on the configured peer priority.	**brief detail**
Secondary Peer	Secondary peer for the network element, based on the configured peer priority.	**brief detail**
Peer	Name of the peer.	**brief detail**

Table 7: show diameter Output Fields *(continued)*

Field Name	Field Description	Level of Output
Instance	Name of the Diameter instance in which the peer is configured.	**brief detail**
State	State of the peer: • Bad-Config—Misconfiguration. • Bad-Remote—Remote side does not conform to one of the decisions or is sending malformed messages. • Closed—Normal disconnect due to a request from the remote site or due to excessive watchdog timeouts. • Destructing—Peer to be deleted on the next timer tick. Until then, it performs no actions. • Disabled—Peer is administratively disabled. • Internal-error—Internal error has been detected and the peer is in the process of restarting. • No-Activation—Peer is not used by any Diameter network element. • Rejected—Connection was rejected by remote side of the connection. • Suspended—All other reasons to be suspended.	**brief detail**
NE-Count	Number of network elements associated with the peer.	**brief detail**
Activated Count	Activation status of the peer: • **1**—Peer is activated. • **0**—Peer is not activated.	**brief detail**
Primary Count	Status of the peer: primary (**1**) or secondary (**0**).	**brief detail**
Secondary Count	Status of the peer: secondary (**0**) or primary (**1**).	**brief detail**
Route	Name of the Diameter route.	**detail**
NE	Name of the Diameter network element in which the route is configured	**detail**
Instance	Name of the Diameter instance in which the route is configured.	**detail**
Valid	Determination of whether the route is valid: **yes** or **no**.	**detail**
Up	State of the route: **yes** for an active route, **no** for an inactive route.	**detail**

Sample Output

show diameter brief

```
user@host> show diameter brief

Diameter node:
  Diameter process id                  :      1446
  Functions                            :   4
  Connected functions                  :   2
```

```
  Instances                                :   1
  Network elements(NEs)                    :   1
  Connected NEs                            :   0
  Peers                                    :   2
  Activated peers                          :   1
  Open peers                               :   0
  Transports                               :   1
  Requests queued for network transmit     :         0
  Answers queued for network transmit      :         0
  Expected answers from network            :         0
  Requests queued for function transmit    :         0
  Answers queued for function transmit     :         0
  Expected answers from functions          :         0
  Memory used by network transmit queues   :         0
  Memory used by function transmit queues  :         0
  Origin-state-id                          :         0

Diameter function list:
                     Upstream    Downstream  Net Queue   Func Queue
                     Transaction Transaction Buffer      Buffer      Routed
                     Utilization Utilization Utilization Utilization Dests
  Function  State    %           %           %           %
  charging- Disconnec   0           0           0           0           0
  gx-plus   Connected   0           0           0           0           1
  jsrc      Connected   0           0           0           0           0
  packet-tr Disconnec   0           0           0           0           0

Diameter instances:
  Name         Origin-Realm         Origin-Host          NE-Total  NE-Connected
  master       orrr                 ohhh                        1         0

Diameter network-elements:
                                          Primary      Secondary
  Name         Instance     State          Peer         Peer
  n0           master       Connecting     <NONE>       <NONE>

Diameter peer list:
                                                    Activated Primary Secondary
  Peer         Instance     State          NE-Count Count     Count   Count
  p0           master       Suspended        1        1         0       0
  p100         master       No-Activation    0        0         0       0
```

show diameter detail

```
user@host> show diameter detail
...
Diameter routes:
  Route        NE           Instance     Valid Up
  dne-route1   dne1         master       yes   no
```

show diameter summary

```
user@host> show diameter summary
Diameter node:
  Diameter process id                      :      1446
  Functions                                :   4
  Connected functions                      :   2
  Instances                                :   1
  Network elements(NEs)                    :   1
  Connected NEs                            :   0
  Peers                                    :   2
```

```
Activated peers                         :   1
Open peers                              :   0
Transports                              :   1
Requests queued for network transmit    :         0
Answers queued for network transmit     :         0
Expected answers from network           :         0
Requests queued for function transmit   :         0
Answers queued for function transmit    :         0
Expected answers from functions         :         0
Memory used by network transmit queues  :         0
Memory used by function transmit queues :         0
Origin-state-id                         :         0
```

show diameter function

Syntax
show diameter function
<brief | detail | summary>
<function-name>

Release Information
Command introduced in Junos OS Release 9.6.
Support for PTSP introduced in Junos OS Release 10.2.
Support for Gx-Plus introduced in Junos OS Release 11.2.

Description
Display information about all functions associated with Diameter instances or only the specified function.

Options
brief | detail | summary—(Optional) Display the specified level of output. The **summary** output is displayed by default and includes basic function information. The **brief** output displays the summary information in a different format. The **detail** output adds information to the **brief** output.

function-name—(Optional) Display information for only the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions.

Required Privilege Level
view

Related Documentation
- clear diameter function statistics on page 94
- show diameter on page 95
- show diameter function statistics on page 105

List of Sample Output
show diameter function on page 103
show diameter function brief on page 103
show diameter function detail (JSRC) on page 103
show diameter function detail (Gx-Plus) on page 104

Output Fields
Table 8 on page 101 lists the output fields for the **show diameter function** command. Output fields are listed in the approximate order in which they appear.

Table 8: show diameter function Output Fields

Field Name	Field Description	Level of Output
Function name	Name of the function for which information is displayed.	All levels
State	State of the Diameter connection with the function.	All levels
Upstream transaction utilization	Percent of upstream traffic used for this function.	All levels

Table 8: show diameter function Output Fields *(continued)*

Field Name	Field Description	Level of Output
Downstream transaction utilization	Percent of downstream traffic used for this function.	All levels
Network transmit buffer utilization	Percent of network transmission buffer used for this function.	All levels
Function transmit buffer utilization	Percent of function transmission buffer used for this function.	All levels
Routed destinations	Number of destinations that have this function associated with their routes.	All levels
Requests queued for network tx	Number of requests waiting to be sent to the Diameter peers for this function.	**detail**
Pending answers from network	Number of replies expected from the Diameter peers for this function.	**detail**
Answers queued for function tx	Number of replies waiting to be sent to this function.	**detail**
Total upstream transactions pending	Total number of messages queued for this function.	**detail**
Upstream transactions limit	Total number of messages queued for this function.	**detail**
Requests queued for function tx	Number of requests waiting to be sent to this function.	**detail**
Pending answers from function	Number of replies expected to be received from this function.	**detail**
Answers queued for network tx	Number of replies waiting to be sent to this function.	**detail**
Total downstream transactions pending	Total number of messages queued for the Diameter peers.	**detail**
Downstream transactions limit	Maximum number of messages that can be queued for the Diameter peers.	**detail**
Buffers used by network tx queue	Number of buffers used by messages queued for the Diameter peers.	**detail**
Limit on network tx queue buffers	Maximum buffer capacity available for messages queued for the Diameter peers.	**detail**

Table 8: show diameter function Output Fields *(continued)*

Field Name	Field Description	Level of Output
Buffers used by function tx queue	Number of buffers used by messages queued for this function.	**detail**
Limit on function tx queue buffers	Maximum buffer capacity available for messages queued for this function.	**detail**
Origin-state-id	Value of the Origin-State-ID AVP.	**detail**

Sample Output

show diameter function

```
user@host> show diameter function

Diameter function list:
                     Upstream    Downstream  Net Queue   Func Queue
                     Transaction Transaction Buffer      Buffer      Routed
                     Utilization Utilization Utilization Utilization Dests
  Function  State    %           %           %           %
  jsrc      Disconnec  0           0           0           0             0
```

show diameter function brief

```
user@host> show diameter function brief

Diameter function:
  Function name                        : gx-plus

  State                                : Connected
  Upstream transaction utilization     :   0 %
  Downstream transaction utilization   :   0 %
  Network transmit buffer utilization  :   0 %
  Function transmit buffer utilization :   0 %
  Routed destinations                  :         1

  Function name                        : jsrc
  State                                : Disconnected
  Upstream transaction utilization     :   0 %
  Downstream transaction utilization   :   0 %
  Network transmit buffer utilization  :   0 %
  Function transmit buffer utilization :   0 %
  Routed destinations                  :         0
```

show diameter function detail (JSRC)

```
user@host> show diameter function detail

Diameter function:
  Function name                        : jsrc
  State                                : Disconnected
  Upstream transaction utilization     :   0 %
  Downstream transaction utilization   :   0 %
  Network transmit buffer utilization  :   0 %
```

```
  Function transmit buffer utilization   :   0 %
  Routed destinations                    :         0
  Requests queued for network tx         :         0
  Pending answers from network           :         0
  Answers queued for function tx         :         0
  Total upstream transactions pending    :         0
  Upstream transactions limit            :      1024
  Requests queued for function tx        :         0
  Pending answers from function          :         0
  Answers queued for network tx          :         0
  Total downstream transactions pending  :         0
  Downstream transactions limit          :      1024
  Buffers used by network tx queue       :         0
  Limit on network tx queue buffers      :  10485760
  Buffers used by function tx queue      :         0
  Limit on function tx queue buffers     :  10485760
```

show diameter function detail (Gx-Plus)

```
user@host> show diameter function gx-plus detail

Diameter function:
  Function name                          : gx-plus
  State                                  : Connected
  Upstream transaction utilization       :   0 %
  Downstream transaction utilization     :   0 %
  Network transmit buffer utilization    :   0 %
  Function transmit buffer utilization   :   0 %
  Routed destinations                    :         1
  Requests queued for network tx         :         0
  Pending answers from network           :         0
  Answers queued for function tx         :         0
  Total upstream transactions pending    :         0
  Upstream transactions limit            :      1024
  Requests queued for function tx        :         0
  Pending answers from function          :         0
  Answers queued for network tx          :         0
  Total downstream transactions pending  :         0
  Downstream transactions limit          :      1024
  Buffers used by network tx queue       :         0
  Limit on network tx queue buffers      :  10485760
  Buffers used by function tx queue      :         0
  Limit on function tx queue buffers     :  10485760
  Origin-state-id                        :         0
```

show diameter function statistics

Syntax
show diameter function statistics
<brief | detail | summary>
<function-name>

Release Information
Command introduced in Junos OS Release 9.6.
Support for PTSP introduced in Junos OS Release 10.2.
Support for Gx-Plus introduced in Junos OS Release 11.2.

Description
Display statistics about all functions associated with Diameter instances or only the specified function.

Options
brief | detail | summary—(Optional) Display the specified level of output. The **summary** output is displayed by default and includes basic function statistics. The **brief** output displays the summary information in a different format and adds numbers accumulated since the Diameter node was started. The **detail** output adds information to the **brief** output.

function-name—(Optional) Display information for only the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions. When you specify a function, the **brief** output is displayed by default, even when you explicitly specify **summary**.

Required Privilege Level
view

Related Documentation
- clear diameter function statistics on page 94
- show diameter on page 95
- show diameter function on page 101

List of Sample Output
show diameter function statistics on page 107
show diameter function statistics brief on page 107
show diameter function statistics detail on page 107

Output Fields
Table 9 on page 105 lists the output fields for the **show diameter function statistics** command. Output fields are listed in the approximate order in which they appear.

Table 9: show diameter function statistics Output Fields

Field Name	Field Description	Level of Output
Function	Name of the function for which information is displayed.	All levels
Delivered Requests	Number of requests delivered by Diameter to the application.	All levels
Delivered Answers	Number of answers delivered by Diameter to the application.	All levels
Delivered Messages	Total number of messages delivered by Diameter to the application.	All levels

Table 9: show diameter function statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Forwarded Requests	Number of requests sent by Diameter to the network.	All levels
Forwarded Answers	Number of answers sent by Diameter to the network.	All levels
Forwarded Messages	Number of messages sent by Diameter to the network.	All levels
Function name	Name of the function for which information is displayed.	All levels
Over-limit network requests	Number of requests sent to Diameter peers that exceeded the limit on the network transmit queue.	**detail**
Over-limit network answers	Number of answers sent to Diameter peers that exceeded the limit on the network transmit queue.	**detail**
Over-limit network messages	Total number of messages sent to Diameter peers that exceeded the limit on the network transmit queue.	**detail**
Failed to deliver requests	Number of requests sent by Diameter to its application that were not successfully delivered.	**detail**
Failed to deliver answers	Number of answers sent by Diameter to its application that were not successfully delivered.	**detail**
Failed to deliver messages	Total number of messages sent by Diameter to its application that were not successfully delivered.	**detail**
Over-limit function requests	Number of requests sent to Diameter peers that exceeded the limit on the function transmit queue.	**detail**
Over-limit function answers	Number of answers sent to Diameter peers that exceeded the limit on the function transmit queue.	**detail**
Over-limit function messages	Total number of messages sent to Diameter peers that exceeded the limit on the function transmit queue.	**detail**
Failed to forward requests	Number of requests that were not successfully sent by Diameter to the network.	**detail**
Failed to forward answers	Number of answers that were not successfully sent by Diameter to the network.	**detail**
Failed to forward messages	Total number of messages that were not successfully sent by Diameter to the network.	**detail**

Sample Output

show diameter function statistics

```
user@host> show diameter function statistics
Diameter function statistics:
           Delivered Delivered Delivered Forwarded Forwarded Forwarded
  Function Requests  Answers   Messages  Requests  Answers   Messages
  jsrc             0         0         0         0         0         0
```

show diameter function statistics brief

```
user@host> show diameter function statistics brief

Diameter function statistics:
  Function name               : jsrc

  Delivered requests          :         0         0
  Delivered answers           :         0         0
  Delivered messages          :         0         0
  Forwarded requests          :         0         0
  Forwarded answers           :         0         0
  Forwarded messages          :         0         0
```

show diameter function statistics detail

```
user@host> show diameter function statistics detail

Diameter function statistics:
  Function name               : jsrc

  Delivered requests          :         0         0
  Delivered answers           :         0         0
  Delivered messages          :         0         0
  Forwarded requests          :         0         0
  Forwarded answers           :         0         0
  Forwarded messages          :         0         0
  Over-limit network requests :         0         0
  Over-limit network answers  :         0         0
  Over-limit network messages :         0         0
  Failed to deliver requests  :         0         0
  Failed to deliver answers   :         0         0
  Failed to deliver messages  :         0         0
  Over-limit function requests :        0         0
  Over-limit function answers :         0         0
  Over-limit function messages :        0         0
  Failed to forward requests  :         0         0
  Failed to forward answers   :         0         0
  Failed to forward messages  :         0         0
```

show diameter route

Syntax **show diameter route**
<brief | detail | summary>
<route-name>

Release Information Command introduced in Junos OS Release 9.6.

Description Display information about all routes associated with Diameter instances or only the specified route.

Options **brief | detail | summary**—(Optional) Display the specified level of output. The **summary** output is displayed by default and includes basic function information. The **brief** output displays the summary information in a different format. The **detail** output adds information to the **brief** output.

route-name—(Optional) Display information for only the specified route.

Required Privilege Level view

Related Documentation
- show diameter on page 95
- *show diameter network-element*

List of Sample Output
show diameter route on page 109
show diameter route detail on page 109

Output Fields Table 10 on page 108 lists the output fields for the **show diameter route** command. Output fields are listed in the approximate order in which they appear.

Table 10: show diameter route Output Fields

Field Name	Field Description	Level of Output
Route	Name of the route.	**summary brief**
NE	Name of the network element associated with the route.	**summary brief**
Instance	Name of the Diameter instance in which the route is configured.	**summary brief**
NE name	Name of the network element associated with the route.	**brief detail**
Instance name	Name of the Diameter instance in which the route is configured.	**brief detail**
Valid	Determination whether the route is valid, **yes** or **no**.	All levels
Up	State of the route, **yes** (up) or **no** (down).	All levels
Function	Name of the function associated with the route.	**brief detail**

Table 10: show diameter route Output Fields *(continued)*

Field Name	Field Description	Level of Output
Partition	Partition associated with the function.	**brief detail**
Dest-realm	Destination realm configured for the route.	**brief detail**
Dest-host	Destination hostname configured for the route.	**brief detail**
Metric	Metric associated with the destination and function to create the route.	**brief detail**
Score	Value that represents how a route is configured. The basic score is 0. Points are added according to the following scheme: • Function is specified—Add 3. • Function partition is specified—Add 1. • Destination realm is specified—Add 1. • Destination host is specified—Add 1.	**brief detail**

Sample Output

show diameter route

```
user@host> show diameter route

Diameter routes:
  Route        NE           Instance     Valid Up
  rA           ne0          master       yes   yes
```

show diameter route detail

```
user@host> show diameter route detail

Diameter route:
  Route name        : rA
  NE name           : ne0
  Instance mame     : master
  Valid             : yes
  Up                : yes
  Function          : jsrc
  Partition         : jsrc-a
  Dest-realm        : outer-realm
  Dest-host         : outer-host
  Metric            :        50
  Score             :         6
```

show static-subscribers sessions

Syntax **show static-subscribers sessions**
<group *group-name*>
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.6.

Description Display information about the subscriber sessions for all static subscribers, all static subscribers on an interface group, or a single subscriber on an interface.

Options ***group-name***—(Optional) Display session information for static subscribers on all interfaces in the specified group.

interface-name—(Optional) Display session information for the static subscriber on the specified in the specified group.

Required Privilege Level view

Related Documentation
- Subscribers on Static Interfaces Overview on page 23

List of Sample Output
show static-subscribers sessions on page 111
show static-subscribers sessions group on page 111
show static-subscribers sessions interface on page 111

Output Fields Table 11 on page 110 lists the output fields for the **show static-subscribers sessions** command. Output fields are listed in the approximate order in which they appear.

Table 11: show static-subscribers sessions Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	None specified
State	State of the static subscriber session: • **authenticating**—Subscriber is being authenticated. • **activating client**—Client is being activated. • **activating services**—Subscriber services are being activated. • **deactivating client**—Client is being deactivated. • **deactivating services**—Subscriber services are being deactivated. • **initializing**—Process is initializing. • **logged in**—Subscriber is logged in to the interface. • **logged out**—Subscriber is logged out of the interface. • **processing statistics**—Session statistics are being processed. • **terminating session**—Subscriber session is being terminated.	None specified
Group	Name of the interface group to which the interface belongs.	None specified

Table 11: show static-subscribers sessions Output Fields *(continued)*

Field Name	Field Description	Level of Output
User Name	Username used for the static subscriber. Can be the interface name.	None specified

Sample Output

show static-subscribers sessions

```
user@host> show static-subscribers sessions

Static subscriber information:
Interface          State                Group            User Name
ge-9/1/0.1         logged out           SS1              ge-9-1-0.1
ge-9/1/0.10        logged out           SS1              ge-9-1-0.10
ge-9/1/0.100       logged out           SS1              ge-9-1-0.100
ge-9/1/0.11        logged out           SS1              ge-9-1-0.11
ge-9/1/0.12        logged out           SS1              ge-9-1-0.12
ge-9/1/0.13        logged out           SS1              ge-9-1-0.13
ge-9/1/0.14        logged out           SS1              ge-9-1-0.14
ge-9/1/0.15        logged out           SS1              ge-9-1-0.15
ge-9/1/0.16        logged out           SS1              ge-9-1-0.16
ge-9/1/0.17        logged out           SS1              ge-9-1-0.17
ge-9/1/0.18        logged out           SS1              ge-9-1-0.18
ge-9/1/0.19        logged out           SS1              ge-9-1-0.19
ge-9/1/0.2         logged out           SS1              ge-9-1-0.2
ge-9/1/0.20        logged out           SS1              ge-9-1-0.20
ge-9/1/0.21        logged out           SS1              ge-9-1-0.21
```

show static-subscribers sessions group

```
user@host> show static-subscribers sessions group boston

Interface          State                Group            User Name
ge-0/0/1.1         logged in            boston           ge-0/0/1.1
ge-0/0/1.2         logged in            boston           ge-0/0/1.2
```

show static-subscribers sessions interface

```
user@host> show static-subscribers sessions interface ge-0/0/1.1

Interface          State                Group            User Name
ge-0/0/1.1         logged in            foo              ge-0/0/1.1
```

PART 4

Troubleshooting

CHAPTER 15

Acquiring Troubleshooting Information for JSRC

Tracing General Authentication Service Processes

The Junos OS trace operations feature tracks general authentication service operations and records events in a log file. By default, the tracing operation is inactive. To trace general authentication service processes, you specify flags in the **traceoptions** statement at the **[edit system processes general-authentication-service]** hierarchy level. The default tracing behavior is the following:

- Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename, **authd**. You can specify a different filename, but you cannot change the directory (**/var/log**) in which trace files are located.
- When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

  You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). For more information about how log files are created, see the *Junos OS System Log Messages Reference*.

- By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

The general authentication service tracing operations are described in the following sections:

Configuring the General Authentication Service Processes Trace Log Filename

By default, the name of the file that records trace output for general authentication service is **authd**. You can specify a different name by including the **file** statement at the **[edit system processes general-authentication-service]** hierarchy level:

To configure the filename for general authentication service tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1
```

Configuring the Number and Size of General Authentication Service Processes Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output, by including the **files** and **size** options with the **traceoptions** statement.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1 files 20 size 2097152
```

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can allow all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1 world-readable
```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1 no-world-readable
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events. You can refine the output by including regular expressions (regex) that will be matched.

To configure regular expressions to match:

- Configure the regular expression.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1 match regular-expression
```

Configuring the Trace Operation

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
address-assignment	Trace all address-assignment pool events
all	Trace all tracing operations
configuration	Trace configuration events
framework	Trace authentication framework events
gx-plus	Trace Gx-Plus events

Flag	Description
jsrc	Trace JSRC events
ldap	Trace LDAP authentication events
local-authentication	Trace local authentication events
radius	Trace RADIUS authentication events
user-access	Trace user access events, such as login, logout, and authenticate

To configure the flags for the event to be logged:

- Configure the flags.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set flag address-assignment
  ```

Configuring the General Authentication Service Processes Trace Log Filename

By default, the name of the file that records trace output for general authentication service is **authd**. You can specify a different name by including the **file** statement at the **[edit system processes general-authentication-service]** hierarchy level:

To configure the filename for general authentication service tracing operations:

- Specify the name of the file used for the trace output.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set file aap_logfile_1
  ```

Related Documentation

- Tracing General Authentication Service Processes on page 115
- *Configuring Address-Assignment Pools*

Configuring the Number and Size of General Authentication Service Processes Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output, by including the **files** and **size** options with the **traceoptions** statement.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set file aap_logfile_1 files 20 size 2097152
  ```

Related Documentation

- Tracing General Authentication Service Processes on page 115

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can allow all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set file aap_logfile_1 world-readable
  ```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set file aap_logfile_1 no-world-readable
  ```

Related Documentation

- Tracing General Authentication Service Processes on page 115

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events. You can refine the output by including regular expressions (regex) that will be matched.

To configure regular expressions to match:

- Configure the regular expression.

  ```
  [edit system processes general-authentication-service traceoptions]
  user@host# set file aap_logfile_1 match regular-expression
  ```

Related Documentation
- Tracing General Authentication Service Processes on page 115

Configuring the Trace Operation

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
address-assignment	Trace all address-assignment pool events
all	Trace all tracing operations
configuration	Trace configuration events
framework	Trace authentication framework events
gx-plus	Trace Gx-Plus events
jsrc	Trace JSRC events
ldap	Trace LDAP authentication events
local-authentication	Trace local authentication events
radius	Trace RADIUS authentication events
user-access	Trace user access events, such as login, logout, and authenticate

To configure the flags for the event to be logged:

- Configure the flags.

  [edit system processes general-authentication-service traceoptions]
  user@host# set flag address-assignment

Related Documentation
- Tracing General Authentication Service Processes on page 115

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

   ```
   [edit]
   set system syslog archive size 100m files 25
   set system auto-configuration traceoptions file filename
   set system auto-configuration traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions level all
   set protocols ppp-service traceoptions flag all
   set protocols ppp traceoptions file filename size 100m files 25
   set protocols ppp traceoptions level all
   set protocols ppp traceoptions flag all
   set protocols ppp monitor-session all
   set interfaces pp0 traceoptions flag all
   set demux traceoptions file filename size 100m files 25
   set demux traceoptions level all
   set demux traceoptions flag all
   set system processes dhcp-service traceoptions file filename
   set system processes dhcp-service traceoptions file size 100m
   set system processes dhcp-service traceoptions file files 25
   set system processes dhcp-service traceoptions flag all
   set class-of-service traceoptions file filename
   set class-of-service traceoptions file size 100m
   set class-of-service traceoptions flag all
   set class-of-service traceoptions file files 25
   set routing-options traceoptions file filename
   set routing-options traceoptions file size 100m
   set routing-options traceoptions flag all
   set routing-options traceoptions file files 25
   set interfaces traceoptions file filename
   set interfaces traceoptions file size 100m
   set interfaces traceoptions flag all
   set interfaces traceoptions file files 25
   set system processes general-authentication-service traceoptions file filename
   set system processes general-authentication-service traceoptions file size 100m
   set system processes general-authentication-service traceoptions flag all
   set system processes general-authentication-service traceoptions file files 25
   ```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

Related Documentation

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 16

Acquiring Troubleshooting Information for Static Subscriber Interfaces

Tracing Static Subscriber Operations

The Junos OS trace feature tracks static subscriber operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **jsscd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

   You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB).

(For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure static subscriber tracing operations:

1. (Optional) Configure a trace log filename.

   See "Configuring the Static Subscribers Trace Log Filename" on page 124.

2. (Optional) Configure the number and size of trace logs.

   See "Configuring the Number and Size of Static Subscribers Log Files" on page 124.

3. (Optional) Configure user access to trace logs.

   See a"Configuring Access to the Static Subscribers Log File" on page 125.

4. (Optional) Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for Static Subscriber Messages to Be Logged" on page 125.

5. (Optional) Configure flags to specify which events are logged.

   See "Configuring the Static Subscribers Tracing Flags" on page 126.

6. (Optional) Configure a severity level for messages to specify which event messages are logged.

   See "Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged" on page 126.

Configuring the Static Subscribers Trace Log Filename

By default, the name of the file that records trace output for static subscribers is **jsscd**. You can specify a different name with the **file** option.

To configure the filename for static subscribers tracing operations:

- Specify the name of the file used for the trace output.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set file stat-subs_1
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Configuring the Number and Size of Static Subscribers Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set file stat-subs_1 _logfile_1 files 20 size 2097152
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Configuring Access to the Static Subscribers Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set file stat-subs_1 _logfile_1 world-readable
  ```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set file stat-subs_1 _logfile_1 no-world-readable
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Configuring a Regular Expression for Static Subscriber Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set file stat-subs_1 _logfile match regex
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Configuring the Static Subscribers Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set flag authentication
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages . By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

  ```
  [edit system processes static-subscribers traceoptions]
  user@host# set level severity
  ```

Related Documentation

- Tracing Static Subscriber Operations on page 123

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the

relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

   ```
   [edit]
   set system syslog archive size 100m files 25
   set system auto-configuration traceoptions file filename
   set system auto-configuration traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions file filename size 100m files 25
   set protocols ppp-service traceoptions level all
   set protocols ppp-service traceoptions flag all
   set protocols ppp traceoptions file filename size 100m files 25
   set protocols ppp traceoptions level all
   set protocols ppp traceoptions flag all
   set protocols ppp monitor-session all
   set interfaces pp0 traceoptions flag all
   set demux traceoptions file filename size 100m files 25
   set demux traceoptions level all
   set demux traceoptions flag all
   set system processes dhcp-service traceoptions file filename
   set system processes dhcp-service traceoptions file size 100m
   set system processes dhcp-service traceoptions file files 25
   set system processes dhcp-service traceoptions flag all
   set class-of-service traceoptions file filename
   set class-of-service traceoptions file size 100m
   set class-of-service traceoptions flag all
   set class-of-service traceoptions file files 25
   set routing-options traceoptions file filename
   set routing-options traceoptions file size 100m
   set routing-options traceoptions flag all
   set routing-options traceoptions file files 25
   set interfaces traceoptions file filename
   set interfaces traceoptions file size 100m
   set interfaces traceoptions flag all
   set interfaces traceoptions file files 25
   set system processes general-authentication-service traceoptions file filename
   set system processes general-authentication-service traceoptions file size 100m
   set system processes general-authentication-service traceoptions flag all
   set system processes general-authentication-service traceoptions file files 25
   ```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

Related Documentation

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 17

Troubleshooting Configuration Statements

traceoptions (General Authentication Service)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit system processes general-authentication-service]

Release Information Statement introduced in Junos OS Release 9.0.

Description Configure tracing options for the general authentication service.

Options

file *filename*—Name of the file to receive the output of the tracing operation. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **address-assignment**—Trace address-assignment pool events
- **all**—Trace all tracing operations
- **configuration**—Trace configuration events
- **framework**—Trace authentication framework events
- **gx-plus**—Trace Gx-Plus events
- **jsrc**—Trace JSRC events
- **ldap**—Trace LDAP authentication events
- **local-authentication**—Trace local authentication events
- **radius**—Trace RADIUS authentication events
- **user-access**—Trace user access events, such as login, logout, and authenticate.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing General Authentication Service Processes on page 115

traceoptions (Static Subscribers)

Syntax

```
traceoptions {
  file filename<files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system processes static-subscribers],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system processes static-subscribers],
[edit routing-instances *routing-instances-name* system processes static-subscribers],
[edit system processes static-subscribers]

Release Information

Statement introduced in Junos OS Release 9.6.

Description

Define tracing operations for static subscriber processes.

Options

file *filename*— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **authentication**—Trace authentication events.
- **configuration**—Trace configuration events.
- **database**—Trace database events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **profile**—Trace dynamic profile events.
- **rtsock**—Trace routing socket events.
- **statistics**—Trace statistics events.
- **subscriber**—Trace subscriber events.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.

- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match ***regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size ***maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing Static Subscriber Operations on page 123

PART 5

Index

Index

Symbols

A

B

C

D

F

T

U