Junos® OS Release 12.1X47 Feature Guide

Junos OS Release 12.1X47-D20
3 March 2015
Revision 1

This feature guide accompanies Junos OS Release 12.1X47-D20. This guide contains detailed information about new or enhanced functionality introduced in Junos OS Release 12.1X47-D20 that is summarized in the Release Notes.

Contents

New Features in Junos OS Release 12.1X47-D20

Junos OS Release 12.1X47-D20 introduces the following features:

Management

TCP/TLS Support for Real-Time Logging

log (Security)

Syntax

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  mode (event | stream);
  rate-cap rate-cap-value;
  (source-address source-address | source-interface interface-name);
  stream stream-name {
    category (all | content-security);
    format (binary | sd-syslog | syslog | welf);
    host {
      ip-address;
      port port-number;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
  }
  transport {
    protocol (udp | tcp | tls);
```

```
    tls-profile tls-profile-name;
    tcp-connections tcp-connections;
  }
  utc-time-stamp;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 9.2.
Support for the **source-interface** option added in Junos OS Release 12.1X46-D25.

Description You can set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

Options **disable**—Disable the security logging for the device.

event-rate *rate*—Limit the rate (0 through 1500) at which logs will be streamed per second.

rate-cap *rate-cap-value*—Limit the rate (0 through 5000) at which data plane logs will be generated per second.

source-address *source-address*—Specify a source IP address or IP address used when exporting security logs.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure **stream**.

NOTE: The **source-address** and **source-interface** are alternate values. Using one of the options is mandatory.

utc-time-stamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately.

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

Related Documentation

- *Application Tracking Feature Guide for Security Devices*
- *Master Administrator for Logical Systems Feature Guide for Security Devices*

[edit security log] Hierarchy Level

```
security {
  log {
    cache {
      exclude exclude-name {
        destination-address destination-address;
        destination-port destination-port;
        event-id event-id;
```

```
            failure;
            interface-name interface-name;
            policy-name policy-name;
            process process-name;
            protocol protocol;
            source-address source-address;
            source-port source-port;
            success;
            user-name user-name;
          }
          limit value;
        }
        disable;
        event-rate rate;
        file {
          files max-file-number;
          name file-name;
          path binary-log-file-path;
          size maximum-file-size;
        }
        format (binary | sd-syslog | syslog);
        mode (event | stream);
        source-address source-address | source-interface interface-name;
        stream stream-name {
          category (all | content-security);
          format (binary | sd-syslog | syslog | welf);
          host {
            ip-address;
            port port-number;
          }
          severity (alert | critical | debug | emergency | error | info | notice | warning);
        }
        traceoptions {
          file {
            file-name;
            files max-file-number;
            match regular-expression;
            (no-world-readable | world-readable);
            size maximum-file-size;
          }
          flag flag;
          no-remote-trace;
        }
        transport {
          protocol (udp | tcp | tls);
          tls-profile tls-profile-name;
          tcp-connections tcp-connections;
        }
        utc-time-stamp;
      }
    }
```

Related Documentation

- *Security Configuration Statement Hierarchy*
- *Application Tracking Feature Guide for Security Devices*

- *Master Administrator for Logical Systems Feature Guide for Security Devices*

transport (Security Log)

Syntax

```
transport {
  protocol (udp | tcp | tls);
  tls-profile tls-profile-name;
  tcp-connections tcp-connections;
}
```

Hierarchy Level [edit security log]

Release Information Statement introduced in Junos OS Release 12.1X46-D25.

Description Configure security log transport options.

Options **protocol**—Specify the type of transport protocol to be used to log the data.

- **UDP**—Set the transport protocol to UDP.
- **TCP**—Set the transport protocol to TCP.
- **TLS**—Set the transport protocol to TLS.

tls-profile *tls-profile-name*—Specify the TLS profile name.

tcp-connections *tcp-connections*—Specify the number of TCP connections per SPU.

Range: 1 through 5.

Default: 1.

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

Related Documentation

- *Application Tracking Feature Guide for Security Devices*

System Log Messages

RTLOG System Log Messages

RTLOG_CONN_OPEN

System Log Message args stream-name transport-proto source-address source-port destination-address destination-port;

Description RTLOG connection was established.

Type Event: This message reports an event, not an error

RTLOG_CONN_CLOSE

System Log Message args stream-name transport-proto source-address source-port destination-address destination-port;

Description RTLOG connection was closed.

Type Event: This message reports an event, not an error

RTLOG_CONN_ERROR

System Log Message args stream-name error-message;

Description RTLOG connection was aborted.

Type Event: This message reports an event, not an error

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

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: http://kb.juniper.net/InfoCenter/
- 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.

Revision History

3 March 2015—Revision 1, Junos OS Release 12.1X47-D20 Feature Guide