syslog-ng Premium Edition 7.0.11

Quick Start Guide

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

syslog-ng PE Quick Start Guide
Updated - November 2018
Version - 7.0.11

Contents

3

Introduction

The syslog-ng application is a flexible and highly scalable system logging application that is ideal for creating centralized and trusted logging solutions.

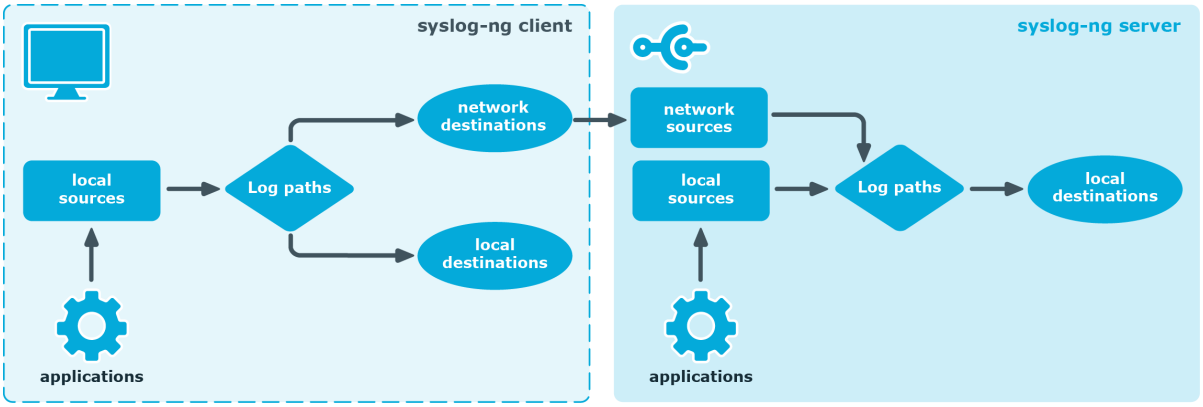
Typically, syslog-ng is used to manage log messages and implement centralized logging, where the aim is to collect the log messages of several devices on a single, central log server. The different devices — called syslog-ng clients — all run syslog-ng, and collect the log messages from the various applications, files, and other sources. The clients send all important log messages to the remote syslog-ng server, which sorts and stores them.

Modes of operation

The syslog-ng Premium Edition application has three distinct operation scenarios: *Client*, *Server*, and *Relay*. The syslog-ng PE application running on a host determines the mode of operation automatically based on the license and the configuration file.

Client mode

Figure 1: Client-mode operation

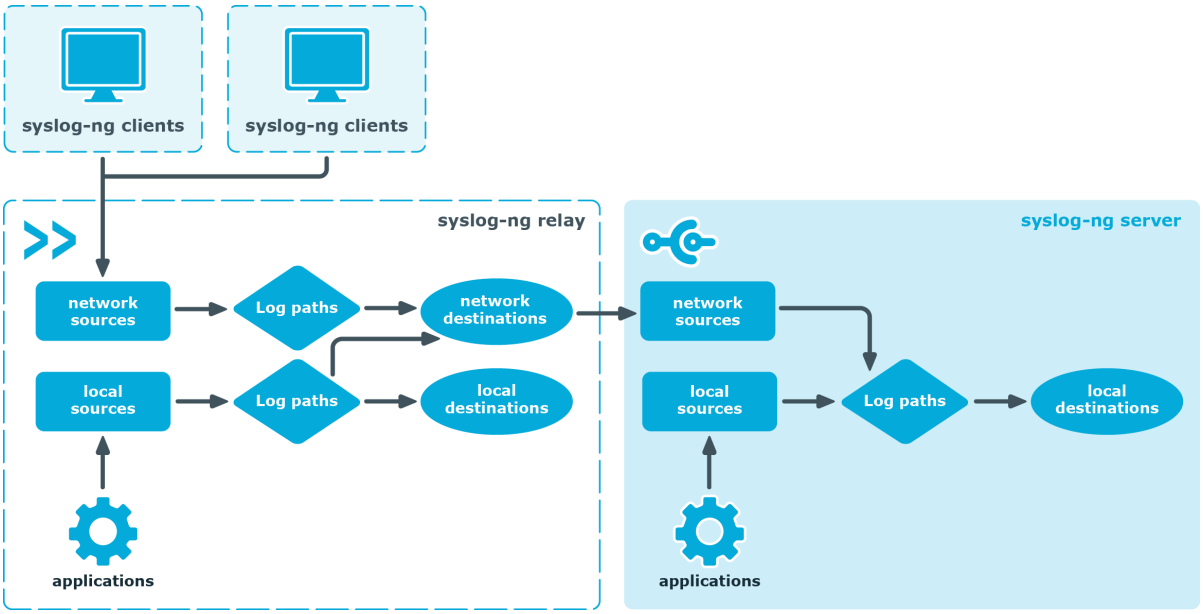


In client mode, syslog-ng collects the local logs generated by the host and forwards them through a network connection to the central syslog-ng server or to a relay. Clients often also log the messages locally into files.

No license file is required to run syslog-ng in client mode.

Relay mode

Figure 2: Relay-mode operation



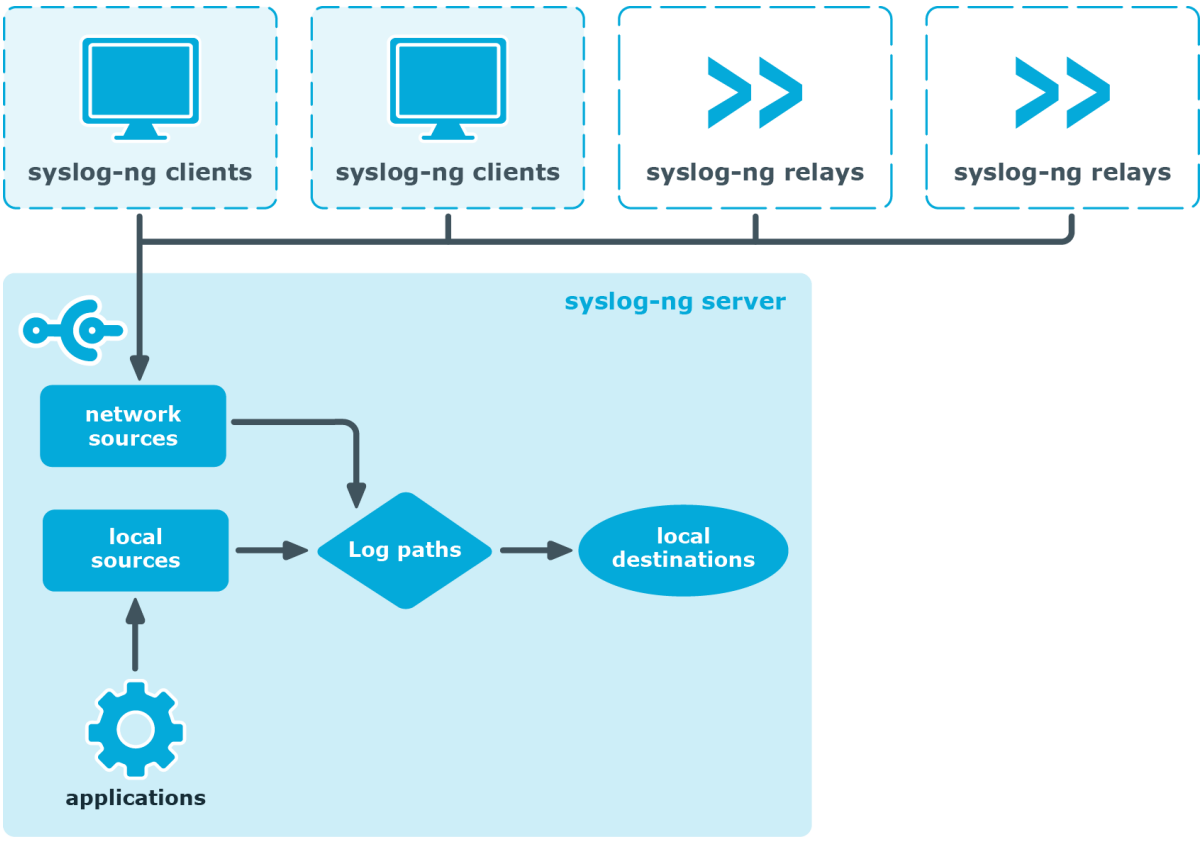
In relay mode, syslog-ng receives logs through the network from syslog-ng clients and forwards them to the central syslog-ng server using a network connection. Relays also log the messages from the relay host into a local file, or forward these messages to the central syslog-ng server.

You cannot use the following destinations in relay mode: `elasticsearch()`, `elasticsearch2()`, `hdfs()`, `kafka()`, `mongodb()`, `pipe()`, `smtp()`, `sql()`. The `file()` and `logstore()` destinations work only for local messages that are generated on the relay.

No license file is required to run syslog-ng in relay mode.

Server mode

Figure 3: Server-mode operation



In server mode, syslog-ng acts as a central log-collecting server. It receives messages from syslog-ng clients and relays over the network, and stores them locally in files, or passes them to other applications, for example log analyzers.

Running syslog-ng Premium Edition in server mode requires a license file. The license determines how many individual hosts can connect to the server. For details on how syslog-ng PE calculates the number of hosts, see Licensing.

Scope

This guide contains instructions for setting up syslog-ng Premium Edition (PE) for evaluation. It covers server installation in Linux, and client installation on Linux and Windows.

In addition, basic configuration options are provided for disk buffering, reliable transfer protocol, macros in filenames, storing messages in encrypted files, and configuring syslog-ng to act as a relay.

This guide is intended as a quick introduction. For evaluating syslog-ng PE in scenarios which exceed the single client-to-server complexity (including, but not limited to usage in domain hosts, complex networks, productive environments, and load testing), refer to Administration Guide.

Supported platforms

The list of supported platforms is available here.

For Windows, the syslog-ng Agent for Windows application is available for all Windows releases starting with Windows XP, including the 64-bit versions of the operating system.

4

Installation

Downloading the Linux installer (server and client)

Purpose:

To obtain the syslog-ng Premium Edition installer from MyBalabit, complete the following steps:

Prerequisites:

The installers are available at the Downloads page. In addition to the installers, a valid license is required to install the syslog-ng PE server. Contact your sales representative for access and license files.

Steps:

1. Navigate to **DOWNLOAD > SYSLOG-NG PREMIUM EDITION**.
2. Choose the latest available version (6.0.3 is used as an example):
    - *Release:* 6 LTS
    - *Component:* syslog-ng Premium Edition
    - *Revision:* 6.0.3
    - *Platform:* Linux glibc2.3.6

3. Click **linux glibc2.3.6 amd64** to download `syslog-ng-premium-edition-6.0.3-linux-glibc2.3.6-amd64.run`.

   The binaries include all required libraries and dependencies of syslog-ng. These components are installed in the `/opt/syslog-ng` directory.

   The installer can reuse existing configuration and license files, and also generate a simple configuration during the installation process. The syslog-ng.conf file is generated into the `/opt/syslog-ng/etc/` directory during the installatino process. If you want to reuse an existing syslog-ng.conf configuration file, the installer will search for it under this directory as well.

   NOTE:

   Existing syslog implementations on Linux systems are replaced during installation.

Downloading the Windows installer (client only)

Purpose:

To obtain the syslog-ng Agent for Windows installer from the syslog-ng PE product page on the Support Portal, complete the following steps:

Prerequisites:

The installers are available through the syslog-ng PE product page on the Support Portal. In addition to the installers, a valid license is required to install the syslog-ng PE server. Contact your sales representative for access and license files.

Steps:

1. Navigate to the Downloads page page.
2. Choose the latest available version (6.0.3 is used as an example):
   - *Release:* 6 LTS
   - *Component:* syslog-ng Agent for Windows
   - *Revision:* 6.0.3
   - *Platform:* Windows 2012
3. Select **syslog-ng Agent with MMC snapin (setup) 64/32bit**
4. Download `syslog-ng-agent-6.0.3-setup.exe`

   Regardless of the path name, the installer contains both the 32-bit and the 64-bit binaries.

5. **Installing the .NET framework**

   The installer requires Microsoft .NET framework version 3.5 or 4.0. For further details, see The syslog-ng Agent for Windows Administration Guide.

Installing the syslog-ng PE server on Linux

Purpose:

To install syslog-ng Premium Edition in server mode, complete the following steps:

Prerequisites:

Running syslog-ng Premium Edition in server mode requires a license file. The license determines how many individual hosts can connect to the server. You can obtain the license from your sales representative.

Steps:

1. Copy the installer and `license.txt` file to the server.
2. Execute the following command as root:

   ```
   sh syslog-ng-premium-edition-6.0.3-linux-glibc2.3.6-amd64.run
   ```
3. Select **Continue** on the Welcome screen, and accept the EULA.
4. Verify that the system summary is correct.

   If false information is displayed, your platform might not be supported. Abort installation, and if necessary, contact One Identity for support.
5. Keep the default installation path and register your installation. Existing syslog implementations on the system are replaced.
6. Provide the full path to the license file (`license.txt`).
7. The installer generates a very basic configuration file during the installation process. Provide the following answers for the following questions:

Question	Answer
Remote source: Do you want to receive log messages from the network?	`Yes`
Remote destination: To forward your log messages to a remote server, enter the address of the server and select OK. Otherwise, select Skip.	`Skip`

Expected outcome

The installer stops the previously installed syslog implementation, and starts the syslog-ng PE server.

8. *Validating the installation*

   Test local logging:

   a. Issue the following commands as root:

      ```
      logger test message
      ```

   b. Verify local log with the following command:

      ```
      tail /var/log/messages
      ```

      ### Expected outcome

      The `test message` line is displayed in the log.

Installing the syslog-ng PE client on Linux

Purpose:

To install syslog-ng Premium Edition in client mode, complete the following steps:

Prerequisites:

No license file is required to run syslog-ng PE in client mode.

Steps:

1. Execute the following command as root:

   ```
   sh syslog-ng-premium-edition-6.0.3-linux-glibc2.3.6-amd64.run
   ```

2. Select Continue on the Welcome screen, and accept the EULA.
3. Verify that the system summary is correct.

   If false information is displayed, your platform might not be supported. Abort installation, and if necessary, contact One Identity for support.

4. Keep the default installation path and register your installation. Existing syslog implementations on the system are replaced.
5. The installer generates a very basic configuration file during the installation process. Provide the following answers for the following questions:

Question	Answer
Remote source: Do you want to receive log messages from the network?	`No`
Remote destination: To forward your log messages to a remote server, enter the address of the server and select OK. Otherwise, select Skip.	`<IP-address-of-destination-syslog-ng PE-server>`

Expected outcome

The installer stops the previously installed syslog implementation, and starts the syslog-ng PE server.

6. *Validating the installation*
    a. Test local logging. Issue the following commands as root:

        ```
        logger test message
        ```

    b. Verify local log with the following command:

        ```
        tail /var/log/messages
        ```

        #### Expected outcome

        The `test message` line is displayed in the log.

    c. Test remote logging. On the client machine, enter the following command:

        ```
        logger remote test message
        ```

    d. Verify the server log. On the syslog-ng PE server, enter:

        ```
        tail /var/log/messages
        ```

        #### Expected outcome

        The host name of the client machine and the message text `remote test message` is displayed in the log.

Troubleshooting

If messages are not forwarded from the client to the server, check if port 514 is blocked by a firewall (protected by default on most Linux servers).

Installing on Windows

Purpose:

The following instructions describe the standalone installation, which is configured locally. For more advanced installation options (using domain group policies, installing by group

policy), refer to The syslog-ng Agent for Windows Administrator Guide.

Steps:

1. Execute the downloaded binary.
2. Accept the EULA.
3. Select the destination folder for syslog-ng Agent for Windows.
4. Choose **Stand alone mode**.
5. The installer generates a simple configuration. Enter the destination IP of the syslog-ng PE server:
    a. Select **Destinations**
    b. Double-click **Add new server**
    c. Enter the server's IP address
    d. Change the port number to `601`
    e. Click **OK**
6. Close the configuration window to finish installation.
7. *Validating the installation*

    Test remote logging:

    a. Log out and back in on the Windows client
    b. Verify the server log. On the syslog-ng PE server, enter the following command:

    ```
    tail /var/log/messages
    ```

Expected outcome

The logout and login events are displayed in the log.

Configuring syslog-ng PE

The syslog-ng application reads incoming messages and forwards them to the selected *destinations*. The syslog-ng application can receive messages from files, remote hosts, and other *sources*.

Log messages enter syslog-ng in one of the defined sources, and are sent to one or more *destinations*.

Sources and destinations are independent objects: *log paths* define what syslog-ng does with a message, connecting the sources to the destinations. A log path consists of one or more sources and one or more destinations, messages arriving from a source are sent to every destination listed in the log path. A log path defined in syslog-ng is called a *log statement*.

There are many other optional elements, like filters, parsers, etc., but in this guide we focus on a core syslog-ng feature: reliable logging.

Advanced Log Transfer Protocol

The syslog-ng PE application can send and receive log messages in a reliable way over the TCP transport layer using the Advanced Log Transfer Protocol (ALTP). ALTP is a proprietary transport protocol that prevents message loss during connection breaks. The transport is used between syslog-ng PE hosts (for example, a client and a server, or a client-relay-server), and interoperates with the flow-control and reliable disk-buffer mechanisms of syslog-ng PE, thus providing the best way to prevent message loss. The sender detects which messages the receiver has successfully received. If messages are lost during the transfer, the sender resends the missing messages, starting from the last successfully received message. Therefore, messages are not duplicated at the receiving end in case of a connection break (however, in failover mode, this is not completely ensured). ALTP also allows for encrypted and non-encrypted connections to be received on the same port, using a single source driver.

To make ALTP work, you have to enable it on the server and on all participating clients as well. In the following example, a minimum working configuration is provided; for additional options, including TLS configuration, refer to "Advanced Log Transfer Protocol " in the Administration Guide.

Enabling disk buffer on the syslog-ng PE client on Linux

Purpose:

The Premium Edition of syslog-ng can store messages on the local hard disk if the central log server or the network connection to the server becomes unavailable. This feature is called the disk buffer and needs to be configured only on the client side.

NOTE:

The log messages on Windows come from files – either eventlog containers or custom log files – which are already stored on the hard disk, so the agent does not use additional disk buffering.

To enable disk buffering on the syslog-ng PE client on Linux, modify its configuration:

Steps:

1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor.
2. Locate the line starting with `destination d_logserver`.
3. Modify it to look like the following line:

   ```
   destination d_logserver {
         tcp("<PEServerIP>" disk-buffer(disk-buf-size(2000000)));
   };
   ```

   Replace `<PEServerIP>` with the hostname or IP address of the syslog-ng PE server.

   For additional disk buffer options, refer to "network() destination options" in the Administration Guide.
4. Save the configuration and restart syslog-ng.

Macros in filenames

Purpose:

On servers where logs of many clients are retained for extended periods of time, log files are usually stored under a directory hierarchy. To help sort incoming log messages to such hierarchies, syslog-ng supports the use of macros. Depending on the needs of your organization, date, source host, or combined solutions can be used.

In the following example, the file destination on the server is modified to also write messages into a directory structure under `/var/log`, where the first level is the year, the second level is the week of the year, followed by a file name based on the sending host.

Steps:

1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor.
2. Locate the line starting with `destination d_messages`.
3. Modify it to look like the following line:

```
destination  d_messages  {
       file("/var/log/messages");
       file("/var/log/$YEAR/$WEEK/$HOST-messages"  create-dirs(yes));
 };
```

4. Save the file and restart syslog-ng

   > NOTE:
   >
   > Collecting to `/var/log/messages` is left there for your convenience, it can be safely removed. Even if the related configuration item is removed, the file stays there, but it is not updated anymore.

   For more details on macros available in syslog-ng, refer to Administration Guide.

Storing messages in encrypted files

Purpose:

The syslog-ng PE application can store log messages securely in encrypted, compressed and timestamped binary files. Timestamps can be requested from an external Timestamping Authority (TSA).

Logstore files consist of individual chunks, every chunk can be encrypted, compressed, and timestamped separately. Chunks contain compressed log messages and header information needed for retrieving messages from the logstore file.

The syslog-ng PE application generates an SHA-1 hash for every chunk to verify the integrity of the chunk. The hashes of the chunks are chained together to prevent injecting chunks into the logstore file. The syslog-ng PE application can encrypt the logstore using various algorithms, using the aes128 encryption algorithm in CBC mode and the hmac-sha1 hashing (HMAC) algorithm as default.

In the following example, a simple logstore destination is added which stores logs with maximum compression.

Steps:

1. Open the `/opt/syslog-ng/etc/syslog-ng.conf` configuration file in a text editor
2. Locate the line starting with `destination d_messages`
3. Add the following line right below:

```
destination d_logstore {
       logstore("/var/log/messages.lgs" compress(9) );
};
```

4. Locate the line containing `destination(d_messages)`
5. Add the following line right below:

   ```
   destination(d_logstore)
   ```

6. Restart syslog-ng for the configuration changes to take effect
7. *Validating the changes*

   You can verify that logs are arriving to the logstore using the following command:

   ```
   /opt/syslog-ng/bin/logcat /var/log/messages.lgs
   ```

syslog-ng PE as a relay

Purpose:

As mentioned earlier, syslog-ng PE can be turned into a relay. This functionality is often used on larger networks, or when logs are collected from network devices using UDP and forwarded to a central location using the more reliable TCP or ALTP protocols. When used as a relay, syslog-ng PE does not store the logs locally, but forwards them immediately to the central syslog-ng PE server.

In this example, a syslog-ng PE Linux client is reconfigured as a relay.

Steps:

1. Open `/opt/syslog-ng/etc/syslog-ng.conf` in a text editor
2. Remove the current log statement: starting with line `log {`, delete everything until the end of the file
3. Add a new UDP source for router logs:

   ```
   source s_udp {udp();};
   ```

4. Add a new log path for storing local logs locally:

   ```
   log { source(s_local); destination(d_messages); };
   ```

5. Add a new log path for sending both local messages and logs collected from the UDP source to the central server:

   ```
   log {
          source(s_local);
          source(s_udp);
          destination(d_logserver);
   };
   ```

6. *Validating the changes*

   Test the relay by executing the following command on the relay machine:

   ```
   /opt/syslog-ng/bin/loggen -i -D localhost 514
   ```

   It generates about a thousand messages a second and sends to the UDP port of the local syslog-ng PE relay. Executing `tail /var/log/messages` should not show any of the generated messages on the relay, but doing the same on the server machine should show a large number of similar lines:

   ```
   Sep 20 21:18:09 relayhost prg00000[1234]: seq: 0000009458, thread: 0000, runid:
   1379704679, stamp: 2013-09-20T21:18:09
   PADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADD
   ```

Example syslog-ng PE configuration

The following is an example configuration that the installer generates during the installation process:

```
@version: 7.0
#Default configuration file for syslog-ng.
#
# For a description of syslog-ng configuration file directives, please read
# the syslog-ng Administrator's guide at:
#
# https://syslog-ng.com/documentation
#
@include "scl.conf"

options {
};

######
# sources
source s_local {
# message generated by Syslog-NG
      internal();
      system();
};


######
# destinations
destination d_messages { file("/var/log/messages"); };

destination d_logserver { tcp("192.168.1.1"); };

log {
      source(s_local);

      destination(d_messages);
      destination(d_logserver);
};
```

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product