

syslogサーバの構築

ルータ機器などからのログを収集する為に、rsyslogサーバを構築した。

rsyslogのインストール

Ubuntu Serverにはrsyslogパッケージはインストール済みだったが、もし入っていなければ下記コマンドを実行しインストール。

```
$ sudo apt install rsyslog
```

rsyslogサービスの設定

下記設定ファイルの以下の行をコメントを外し、外部からのポートアクセスを有効にする。

[/etc/rsyslog.conf](#)

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

記録先フォルダの作成（アクセス権限設定）

```
$ sudo mkdir /var/log/rsyslog_host
$ sudo chown syslog:adm /var/log/rsyslog_host/
```

rsyslogサービスの再起動

```
$ sudo service rsyslog restart
```

rsyslogサービスの起動確認

```
$ sudo service rsyslog status
```

ホスト名別のログファイルを作成

下記のファイルを作成。

[/etc/rsyslog.d/40-fromhost.conf](#)

```
# Default rules for rsyslog.
#
#                               For more information see rsyslog.conf(5) and
#                               /etc/rsyslog.conf

$template logFileName, "/var/log/rsyslog_host/log_%hostname%.log"

#
# First some standard log files.  Log by facility.
#
:fromhost-ip,!isequal, "127.0.0.1" -?logFileName
& stop
```

rsyslogサービスの再起動

```
$ sudo service rsyslog restart
```

これで/var/log/rsyslog_host/フォルダに、ホスト名を含むログファイルが作成されるようになる。

ログローテーションの設定

ログファイル容量が大きくなりすぎないように、ログファイルを定期的に圧縮し削除する。
下記の設定ファイルを作成する。

[/etc/logrotate.d/rsyslog_host](#)

```
/var/log/rsyslog_host/log_*.log
{
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}
```

logrotateサービスの再起動

```
$ sudo service logrotate restart
```

logrotateサービスの起動確認

```
$ sudo service logrotate status
```

ログファイルの確認

syslog権限でファイル作成されるので、内容表示などするには `sudo` が必要。

```
$ ls -al /var/log/rsyslog_host/  
-rw-r----- 1 syslog adm      445  6月 12 09:26 log_192.168.100.250.log  
-rw-r----- 1 syslog adm  695554 6月 12 09:28 log_192.168.100.251.log  
  
$ sudo less /var/log/rsyslog_host/log_log_192.168.100.250.log
```

参考

1. [Ubuntuで syslogサーバを 構築しました](#)
2. [rsyslog でログの出力先を変更する](#)
3. [logrotateの設定ファイル](#)

From:

<https://www.yokoweb.net/dokuwiki/> - 新石器Wiki

Permanent link:

<https://www.yokoweb.net/dokuwiki/software/ubuntu/syslog-server?rev=1749688783>

Last update: 2025/06/12 09:39

