Log Management

Fitri Setyorini
D3 PSDKU Sumenep
Workshop Administrasi Jaringan
Semester Genap
2023-2024

Isi

Teori :

- Log
- AWSTAT
- RSYSLOG

Praktikum :

- Statistik Website dengan AWSTATS
- Log Server dengan RSYSLOG
- Statistik Proxy Server berbasis Squid dengan SARG

What is a Log ?

- A log is a type of machine data that is particularly significant for developers and IT professionals.
- In some cases, a log could be in the form of a text file created by various software applications and operating systems.
- It contains specific information about the activities that happen during the execution of an application or operating system.

Log Types

- A log is classified according to the format or data types it handles.
- It is also based on the processing and its protocols. Logs following the same protocols fall under one classification.
- Log Types
  - Event log: This log only takes care of the traffic occurring in the network. This includes keeping track of various user credentials, how many times a user has logged in, etc.
  - System log: A system log is responsible for updating all the operations and activities performed by the operating system.
  - Server log: This is a type of text file that keeps a record of the activities performed by the server and also records activity time periods.

1. Statistik Website dengan AWSTATS

AWSTATS

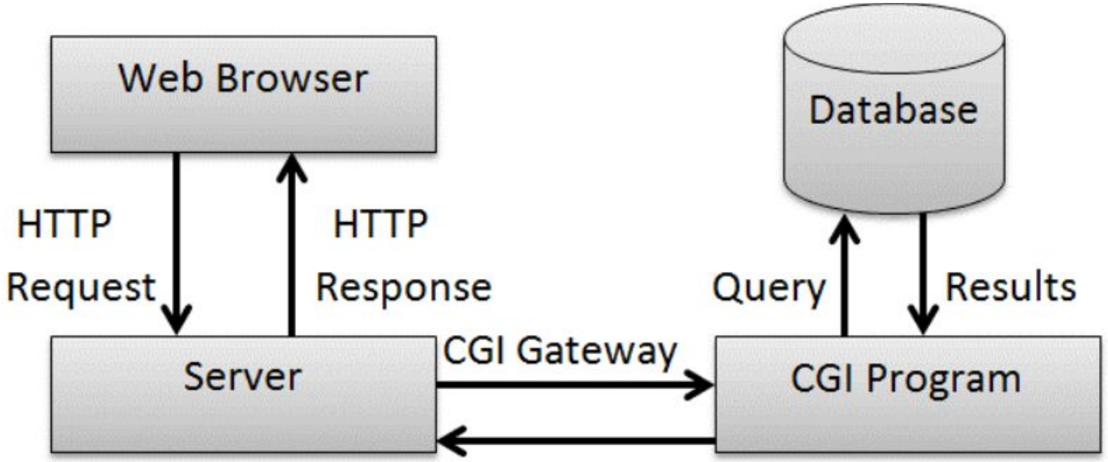
- AWStats kependekan dari Advanced Web Statistics.
- AWStats adalah software log analyzer yang mampu menciptakan report statistic berdasarkan log di server
- AWS compatible untuk web server (Apache2, IIS), ftp server, mail server,proxy server, streaming server
- Data statistic ditampilkan secara grafis sehingga mudah dibaca
- Bersifat free dengan lisensi GNU GPLv3
- AWStats dapat dijalankan lewat cli dan web browser dengan cgi
- AWStats menggunakan Perl, dapat bekerja pada semua Sistem Operasi

File Penting

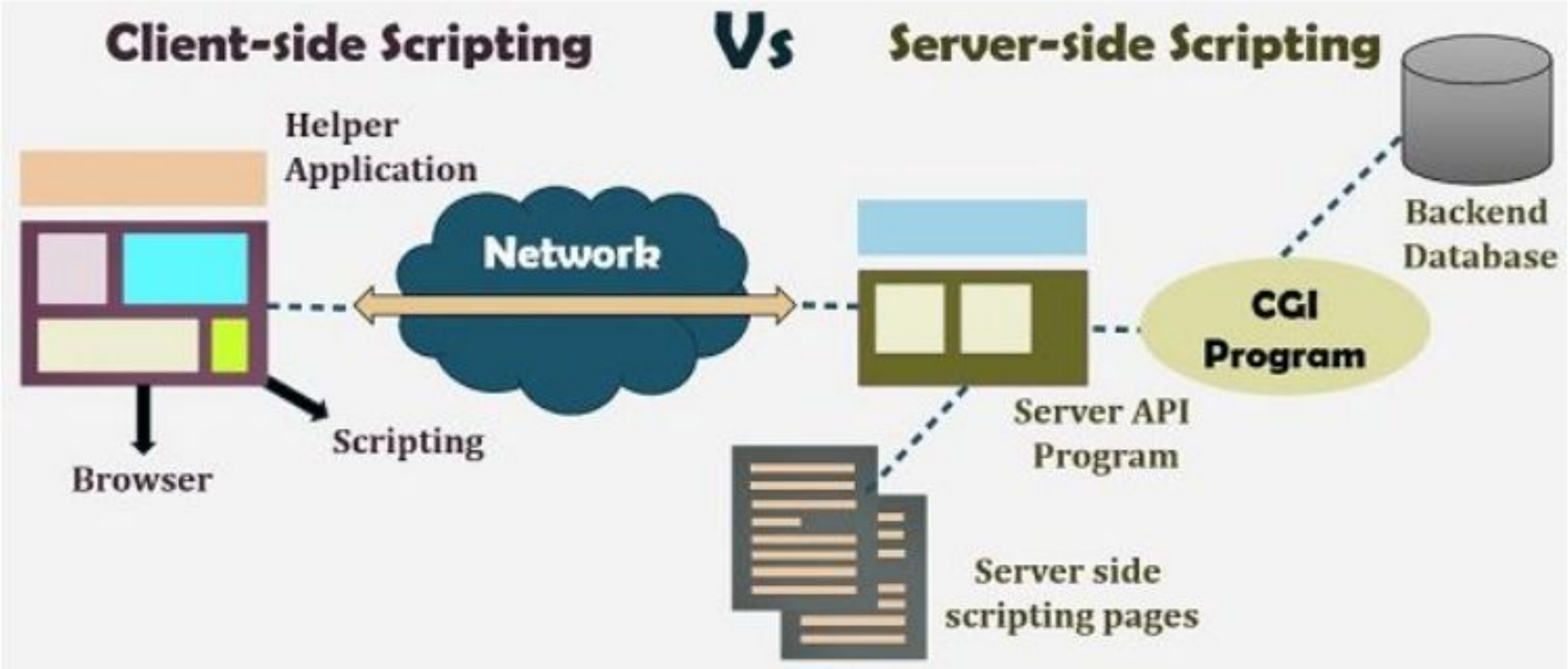
- /etc/awstats/awstats.conf
  - File konfigurasi awstats
- /var/lib/awstats/
  - Direktory tempat menyimpan update statistic terbaru dari awstat
- /usr/lib/cgi-bin/awstats.pl
  - File exe dari awstat. Ketika awstas.pl dipanggil, maka awstats akan mengupdate statistik terbaru
- /var/log/apache2/access.log
  - File log yang akan dianalisa dan ditampilkan awstats. File ini digunakan untuk menyimpan semua request yagn diterima awstats
- /etc/cron.d/awstats
  - File konfigurasi cron.d untuk awstats

Modul CGI

- CGI : Common Gateway Interface
- CGI digunakan oleh web server untuk berinteraksi secara interaktif dengan konten dinamis yang ada di webpage
- CGI termasuk server side script. Selain CGI: asp, phyton, php, javascript termasuk server side script



Client Side v Server Side Script



Bagaimana AWSTATS Bekerja

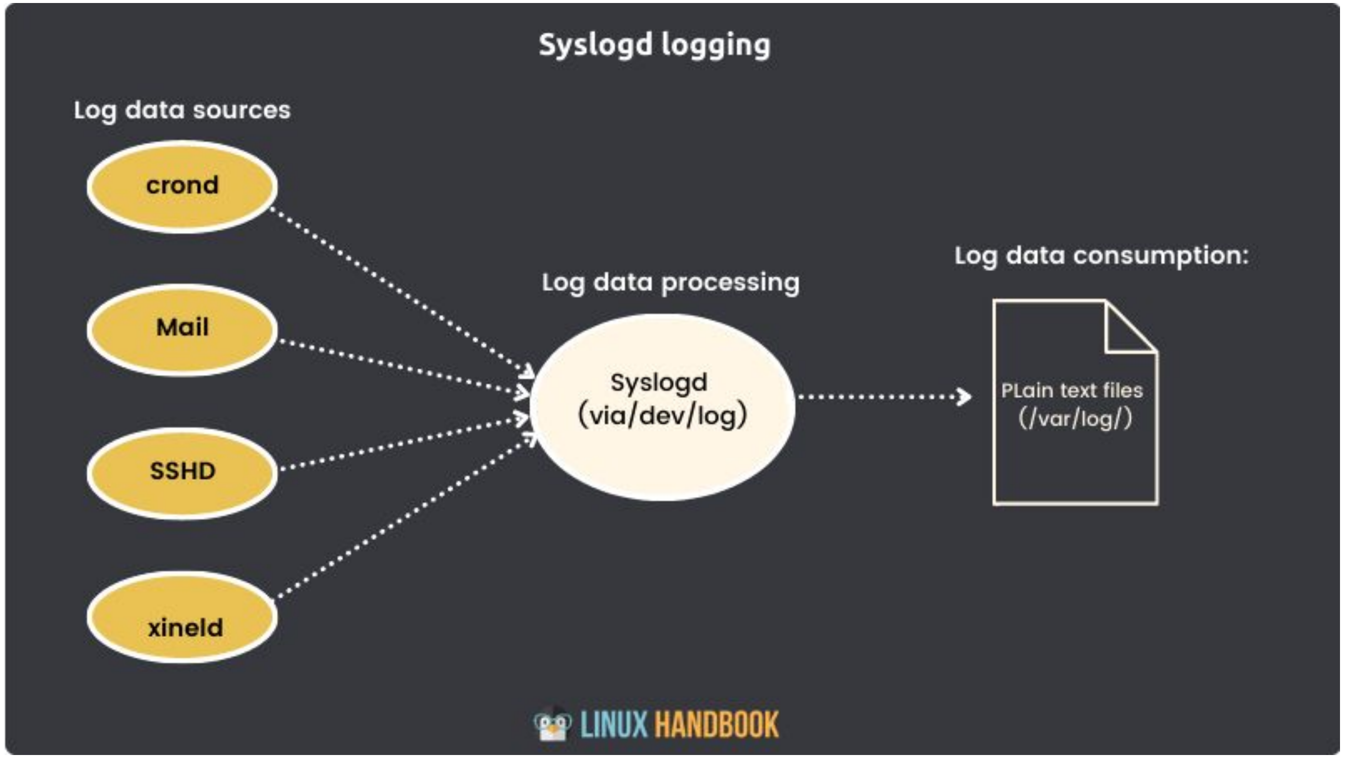
- Setup: Installation and configuration
- Process logs: Building/updating statistics database
- Run Reports: Building and reading reports

1. Statistik Website dengan AWSTATS

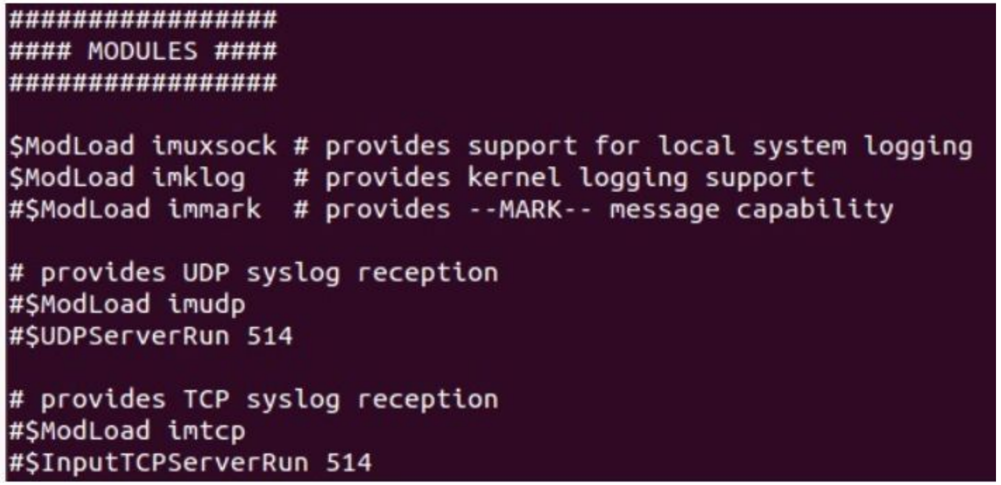
RSYSLOG

- Rsyslog bersifat open source
- Rsyslog menggunakan arsitektur client-server
- Rsyslog server mengumpulkan semua log dari client secara tersentralisasi
- Rsyslog bertugas melakukan logging pesan-pesan r yang dikirim lewat jaringan atau pesan-pesan lokal dari
-
-
- Rsyslog dapat meocan be used to log application e.g SQLServer
- Rsyslog accept inputs from a wide variety of sources, transform them, and output the results to diverse destinations.

How Rsyslog work ?



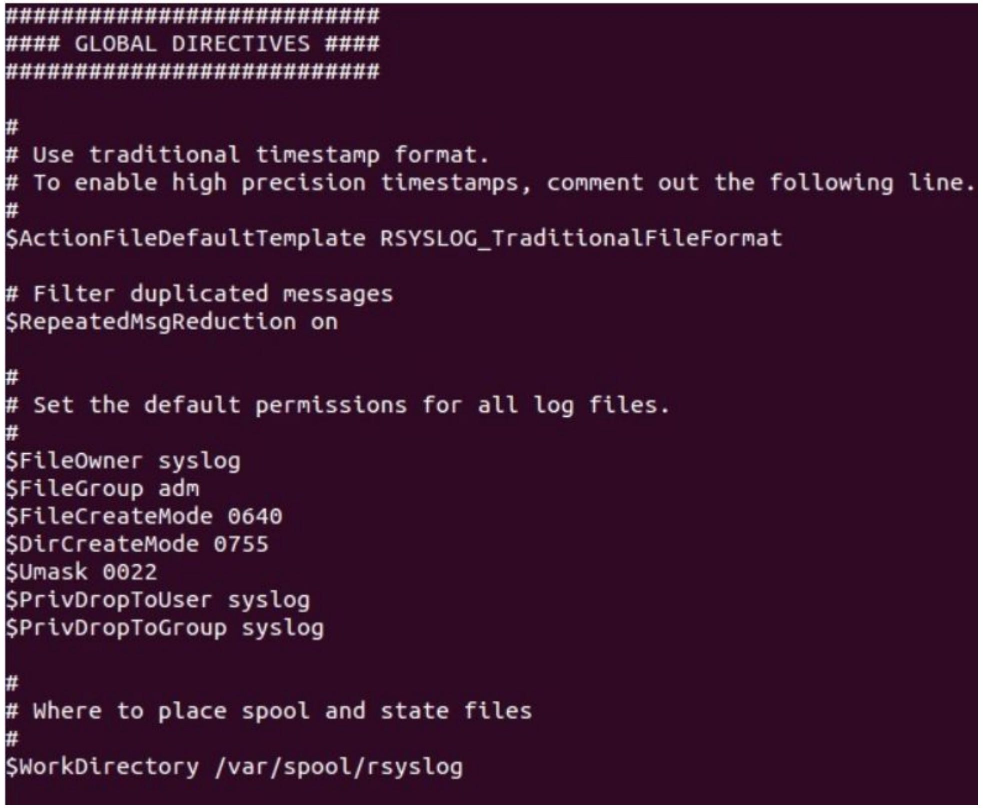
File /etc/rsyslog.conf



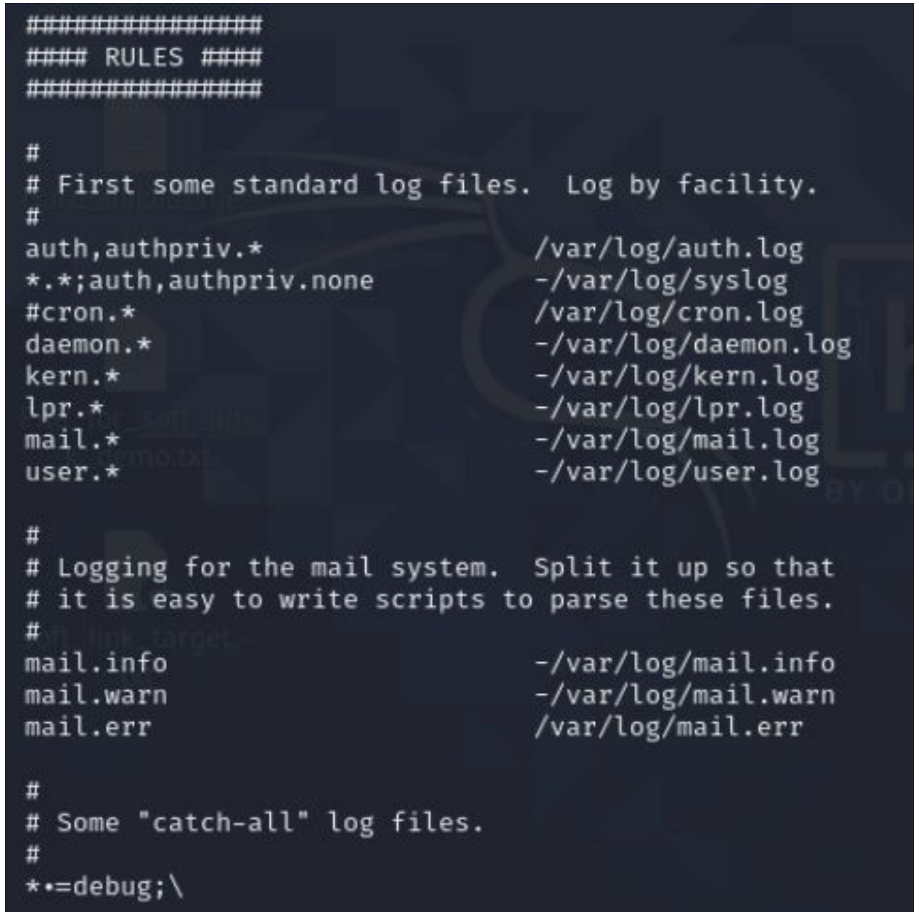
```
#################
#### MODULES ####
#################

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

- File konfigurasi utama: /etc/rsyslog.conf
- Daemon Rsyslog : rsyslogd
- Direktory untuk menyimpan konfigurasi rsyslog tambahan : /etc/rsyslog.d/
- Terdiri dari : module, global directive, dan Rule
- Rsyslog bersifat moduler
  - Hanya modul yang dienable saja yang akan dijalankan oleh Rsyslog
  - 3rd party module dapat ditambahkan ke Rsyslog
  - Jumlah modul dapat bertambah atau berkurang sesuai kebutuhan
  - Secara default, modul yang diaktifkan adalah local system dan kernel

- Global direktif berisi konfigurasi global dari rsyslog
- Rule berisi aturan penulisan log



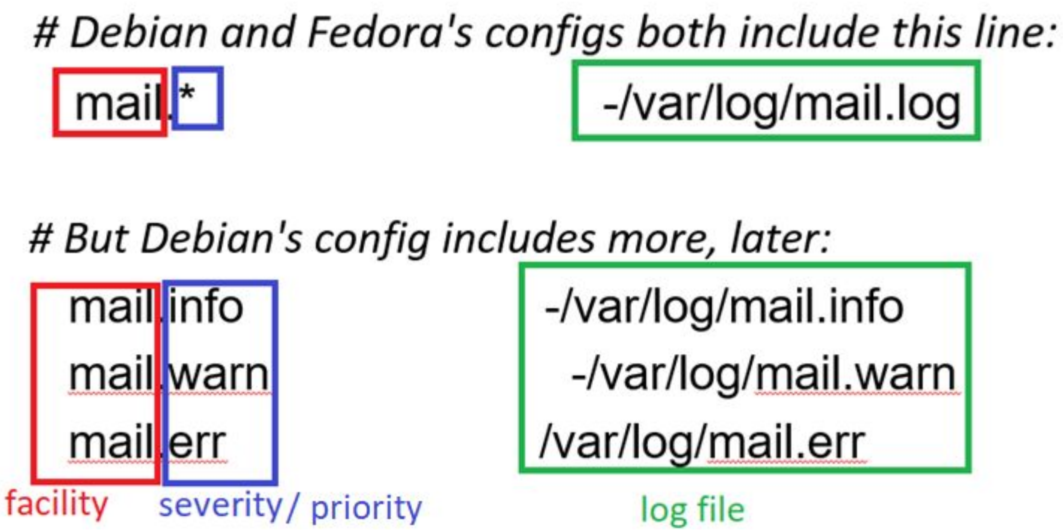
```
###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
```



```
###############
#### RULES ####
###############

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
```

Rule /etc/rsyslog.conf

- Terdiri dari 3 bagian : fasilitas, prioritas dan log file



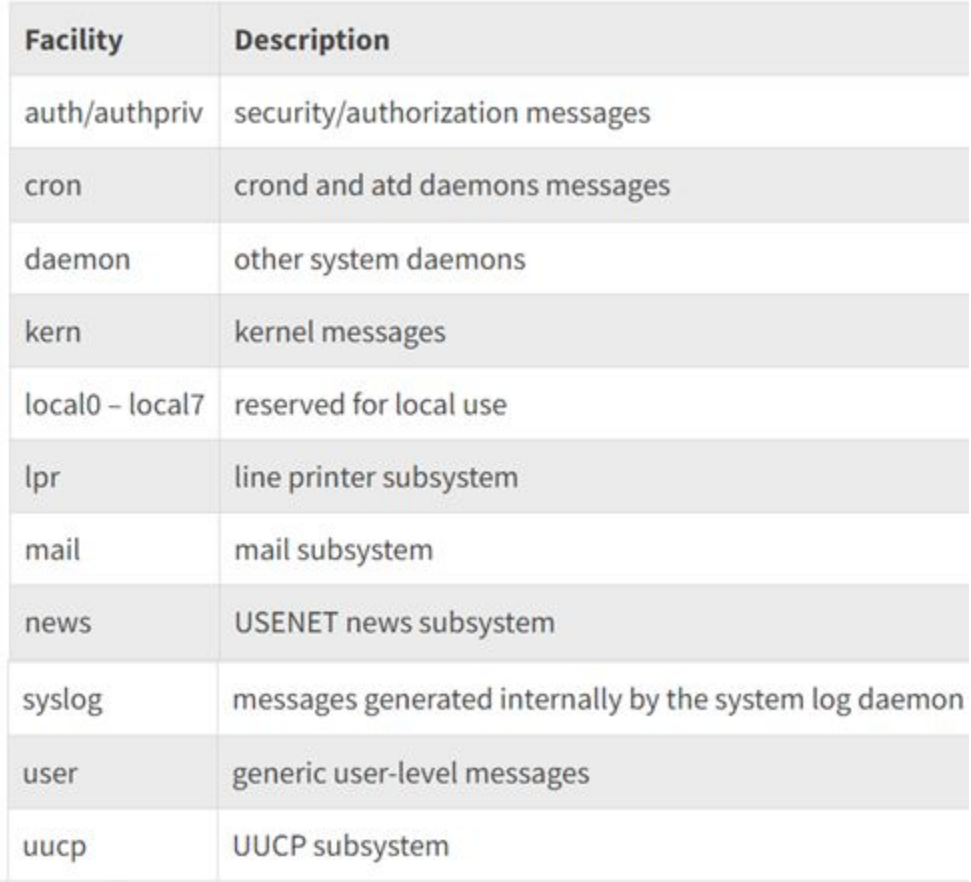
```
# Debian and Fedora's configs both include this line:
 mail.*                   -/var/log/mail.log

# But Debian's config includes more, later:
 mail.info           -/var/log/mail.info
 mail.warn             -/var/log/mail.warn
 mail.err            /var/log/mail.err
```

facility
severity/ priority
log file

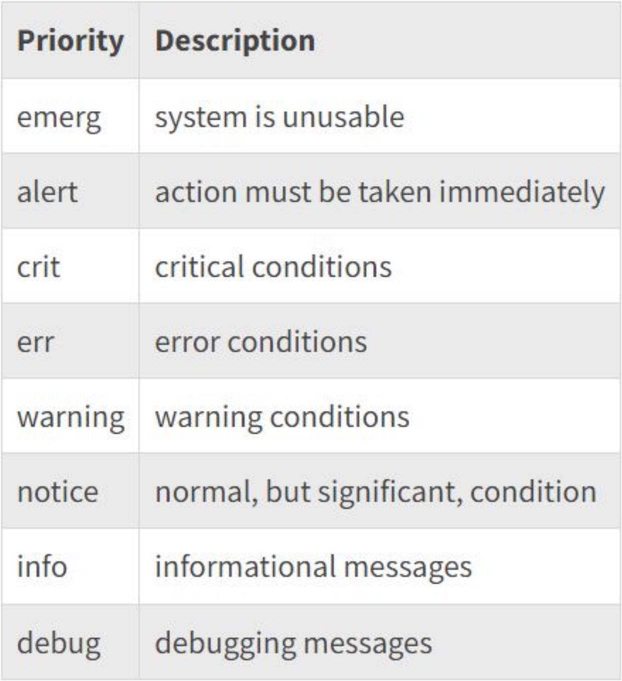
Rules dari Rsyslog.conf

- Facilitas menyatakan sumber dari log
  - Contoh : mail, kernel, local0-7, user, system, dll
- Severity / priority menyatakan tingkat prioritas dari fasilitas
- Ada 7 level dari tertinggi s/d terendah :
  - "emerg", "alert", "crit", "err", "warn", "notice", "info", and "debug“
  - emerg (emergency) memiliki level tertinggi dan debug terendah.

Facilitas dan Prioritas



Facility	Description
auth/authpriv	security/authorization messages
cron	crond and atd daemons messages
daemon	other system daemons
kern	kernel messages
local0 – local7	reserved for local use
lpr	line printer subsystem
mail	mail subsystem
news	USENET news subsystem
syslog	messages generated internally by the system log daemon
user	generic user-level messages
uucp	UUCP subsystem



Priority	Description
emerg	system is unusable
alert	action must be taken immediately
crit	critical conditions
err	error conditions
warning	warning conditions
notice	normal, but significant, condition
info	informational messages
debug	debugging messages

Cara membaca rules dari Rsyslog.conf

- mail.* /var/log/mail.log
  - ‘’Semua pesan dari facility mail dengan prioritas apapun akan dilogging di /var/log/mail.log
- mail.warn /var/log/mail.warn
  - “Semua pesan dari facility 'mail’ yang memiliki prioritas 'warn’ atau lebih tinggi (emerge,alert,crit,err).“ akan dilogging di /var/log/mail.warn
- *.=info;*.=notice;*.=warn; auth,authpriv.none; cron,daemon.none; mail,news.none   -/var/log/messages
  - “Semua facility dengan prioritas info, notice dan warn ; kecuali fasilitas   auth dan authpriv ; kecuali cron dan daemon; kecuali mail dan news; akan dilogging di /var/log/messages

Software yang dibutuhkan

- dnsmasq
- apache2
- awstats
- libgeo-ip-perl
- libgeo-ipfree-perl

Prasyarat

- 1 PC/VM berbasis Debian 12
- PC/VM tersebut telah dilengkapi :
  - DNS Server
  - Web Server

1. Setting DNS

1. Cek ini /etc/hosts

   #nano /etc/hosts

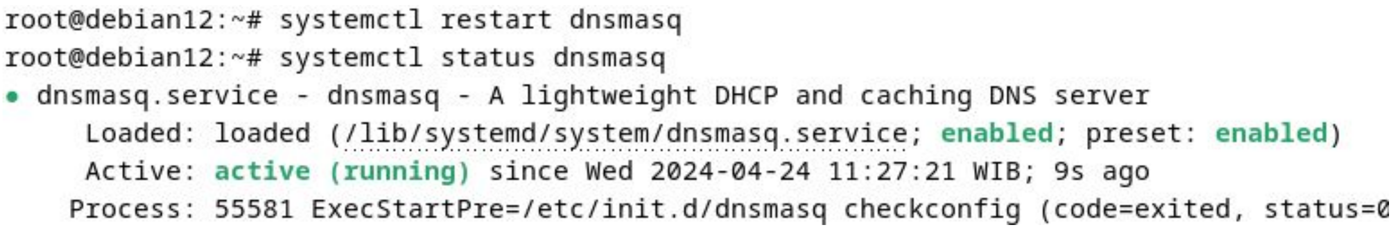
2. Cek isi /etc/resolv.conf

   #nano /etc/resolv.conf

3. Pastikan bahwa DNS anda sudah berjalan dengan baik

   #systemctl restart dnsmasq

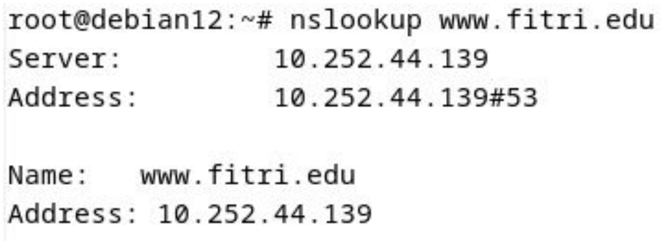
   #systemctl status dnsmasq



```
root@debian12:~# systemctl restart dnsmasq
root@debian12:~# systemctl status dnsmasq
● dnsmasq.service - dnsmasq - A lightweight DHCP and caching DNS server
     Loaded: loaded (/lib/systemd/system/dnsmasq.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-04-24 11:27:21 WIB; 9s ago
    Process: 55581 ExecStartPre=/etc/init.d/dnsmasq checkconfig (code=exited, status=0
```

4. Cek dengan nslookup

   #nslookup www.fitri.edu



```
root@debian12:~# nslookup www.fitri.edu
Server:         10.252.44.139
Address:        10.252.44.139#53

Name:   www.fitri.edu
Address: 10.252.44.139
```

5. Jika nslookup masih gagal, lihat kembali setting dnsmasq di praktikum sebelumnya

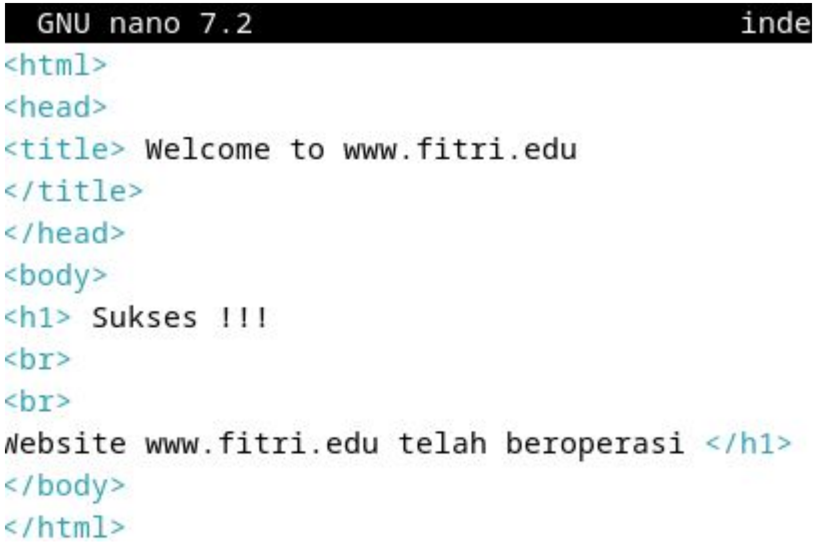
2. Setting Web Page

1. Install dulu apache2
   #apt install apache2
2. Kita menggunakan webserver yang telah dibuat sebelumnya, yaitu www.fitri.edu.
3. Anda akan membuat file html, index.html

   #cd /var/www/html

   #nano index.html

   Simpan dan Exit



```
  GNU nano 7.2                           inde
<html>
<head>
<title> Welcome to www.fitri.edu
</title>
</head>
<body>
<h1> Sukses !!!
<br>
<br>
Nebsite www.fitri.edu telah beroperasi </h1>
</body>
</html>
```

4. Restart apache2

```
#systemctl restart apache2
#systemctl status apache2
```

5. Buka webpage www.fitri.edu
6. Jika gagal muncul, lakukan pembuatan virtual hosting www.fitri.edu. Kemungkinan nomor ip anda telah dipakai oleh mailserver atau website lain
7. Buat 3 directory untuk virtual host, copykan index.html ke direktory baru

```
#cd /var/www/html
#mkdir www.fitri.edu
```

```
#cp index.html www.fitri.edu/
```

8. Masuk ke directory sites-available dan lakukan setting konfigurasi virtual hosting.

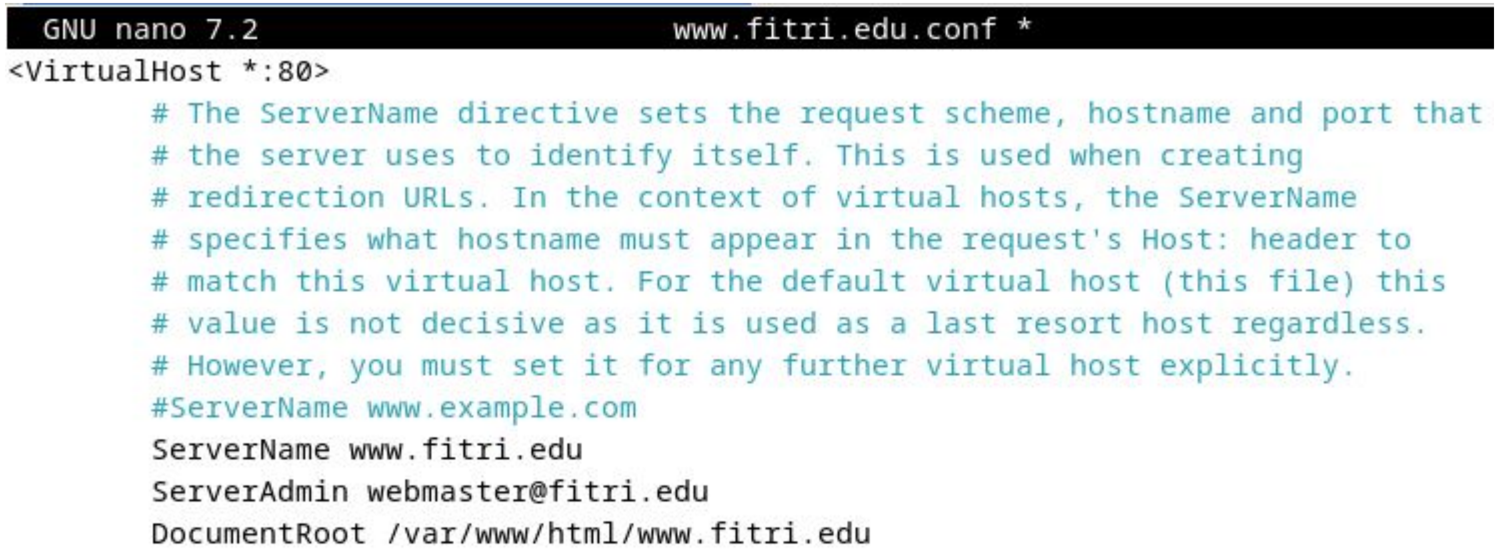
```
# cd /etc/apache2/sites-available
# cp  000-default.conf www.fitri.edu.conf
```

Buka file www.fitri.edu.conf. Edit sebagai berikut

```
#nano www.fitri.edu.conf
```

Simpan dan exit

File www.fitri.edu.conf



```
  GNU nano 7.2                        www.fitri.edu.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com
        ServerName www.fitri.edu
        ServerAdmin webmaster@fitri.edu
        DocumentRoot /var/www/html/www.fitri.edu
```

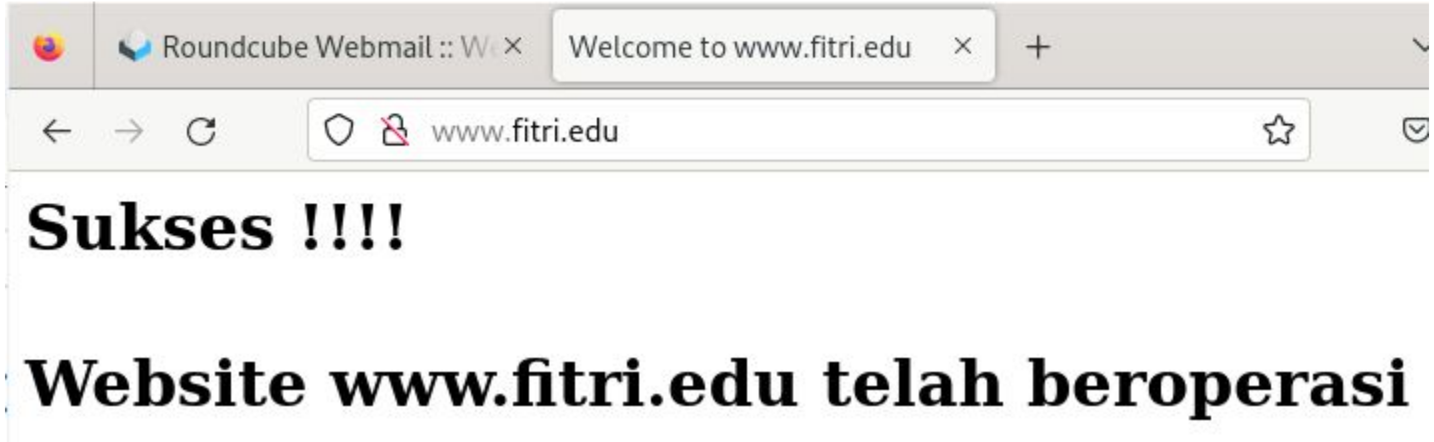
9. Enablekan modul virtual hosting di apache2

```
#a2ensite www.fitri.edu
```

10. Reload web server

```
#systemctl reload apache2
```

11. Buka browser dan ketikkan www.fitri.edu



Sukses !!!!

Website www.fitri.edu telah beroperasi

3. Instalasi awstats

- Update debian anda

  #apt update

- Install awstats

  # apt install awstats

- Install libgeo-ip-perl dan libgeo-ipfree-perl

  # apt install libgeo-ip-perl libgeo-ipfree-perl

4. Konfigurasi awstats

- File konfigurasi awstats diletakkan pada /etc/awstats/awstats.conf
- Backup dulu file tersebut

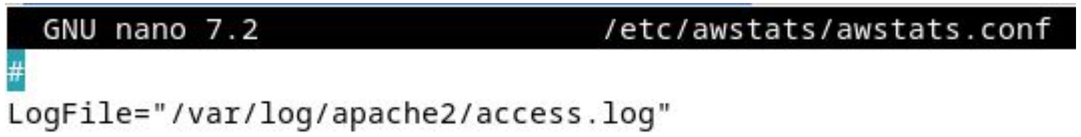
  #cp /etc/awstats/awstats.conf /etc/awstats/awstats.conf.orig

- Edit bagian berikut

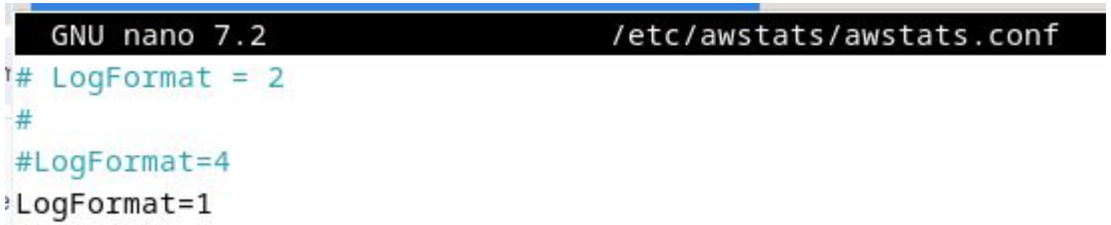
  #nano /etc/awstats/awstats.conf

- Cek pada bagian berikut: LogFile, LogFormat, SiteDomain, HostAliases, DNSLookup, AllowFullYearView, LoadPlugin

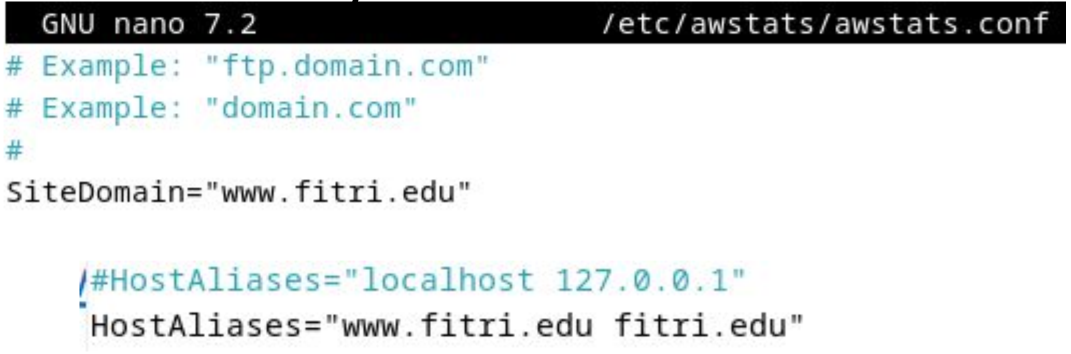
- Pastikan baris bawah telah enable
  LogFile="/var/log/apache2/access.log"
- Beri tanda # pada LogFormat=4 dan ketikkan
  LogFormat=1
- Masukkan nama webserver anda
  SiteDomain="www.fitri.edu"
- Masukkan nama alias webserver. Beri # pada nilai sebelumnya
  HostAliases="www.fitri.edu fitri.edu"



```
 GNU nano 7.2                    /etc/awstats/awstats.conf
#
LogFile="/var/log/apache2/access.log"
```

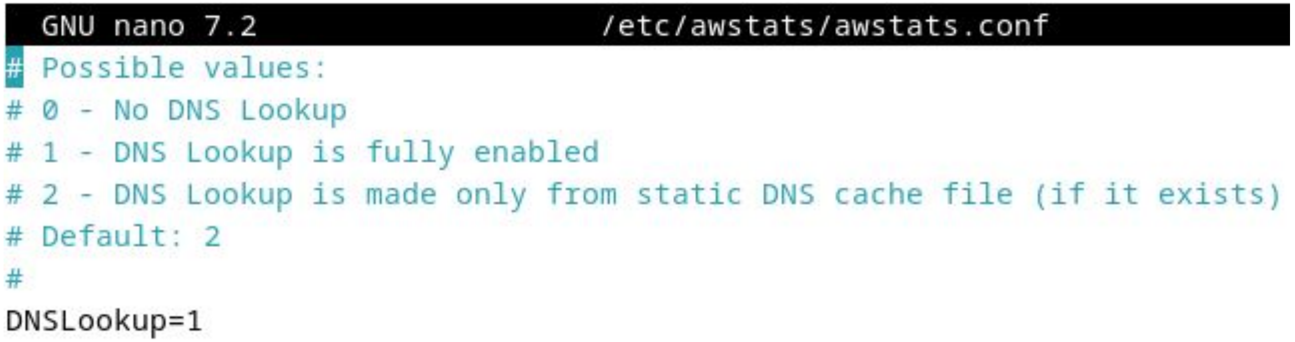


```
 GNU nano 7.2                    /etc/awstats/awstats.conf
# LogFormat = 2
#
#LogFormat=4
LogFormat=1
```

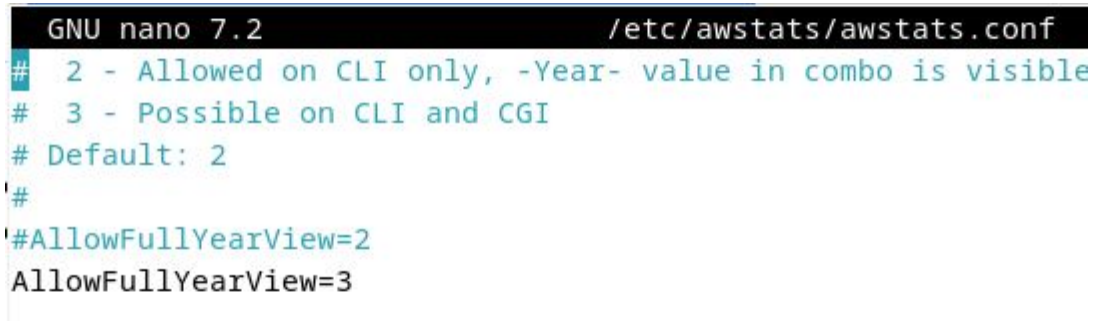


```
 GNU nano 7.2                    /etc/awstats/awstats.conf
# Example: "ftp.domain.com"
# Example: "domain.com"
#
SiteDomain="www.fitri.edu"

   #HostAliases="localhost 127.0.0.1"
   HostAliases="www.fitri.edu fitri.edu"
```

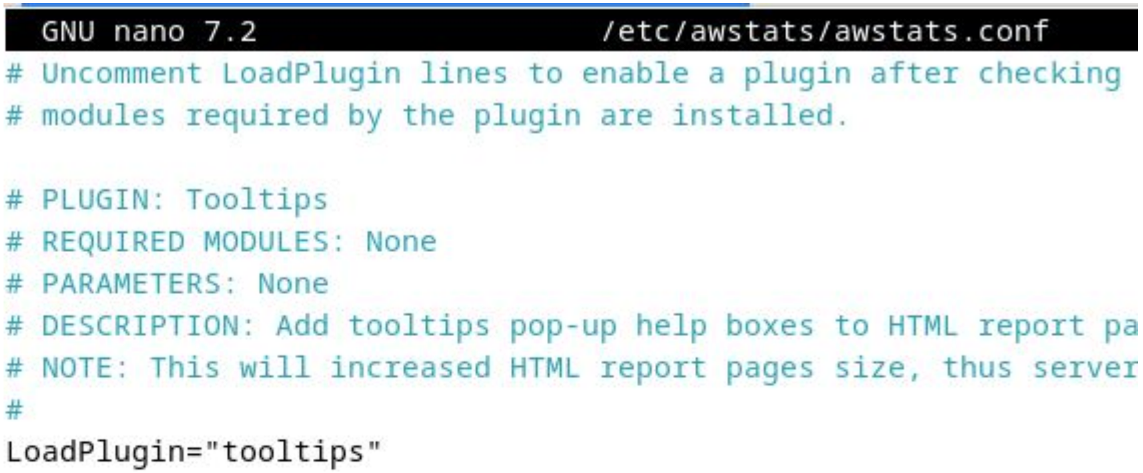
- Karena kita menggunakan dns server, maka pastikan bahwa nilai DNSLookup=1
- Karena kita akan menampilkan data 3 tahun, maka AllowFullYearView=3
- Untuk plugin yang dipakai adalah tooltips LoadPlugin="tooltips"



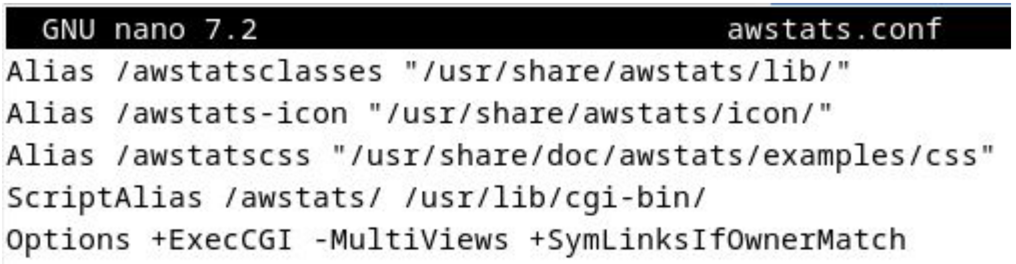
```
  GNU nano 7.2                    /etc/awstats/awstats.conf
# Possible values:
# 0 - No DNS Lookup
# 1 - DNS Lookup is fully enabled
# 2 - DNS Lookup is made only from static DNS cache file (if it exists)
# Default: 2
#
DNSLookup=1
```



```
  GNU nano 7.2                    /etc/awstats/awstats.conf
#   2 - Allowed on CLI only, -Year- value in combo is visible
#   3 - Possible on CLI and CGI
# Default: 2
#
#AllowFullYearView=2
AllowFullYearView=3
```



```
  GNU nano 7.2                    /etc/awstats/awstats.conf
# Uncomment LoadPlugin lines to enable a plugin after checking
# modules required by the plugin are installed.

# PLUGIN: Tooltips
# REQUIRED MODULES: None
# PARAMETERS: None
# DESCRIPTION: Add tooltips pop-up help boxes to HTML report pa
# NOTE: This will increased HTML report pages size, thus server
#
LoadPlugin="tooltips"
```



```
  GNU nano 7.2                                awstats.conf
Alias /awstatsclasses "/usr/share/awstats/lib/"
Alias /awstats-icon "/usr/share/awstats/icon/"
Alias /awstatscss "/usr/share/doc/awstats/examples/css"
ScriptAlias /awstats/ /usr/lib/cgi-bin/
Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
```

- Buat file awstats.conf
  # nano /etc/apache2/conf-available/awstats.conf
- Copy dan paste baris berikut

```
        Alias /awstatsclasses "/usr/share/awstats/lib/"
        Alias /awstats-icon "/usr/share/awstats/icon/"
        Alias /awstatscss "/usr/share/doc/awstats/examples/css"
        ScriptAlias /awstats/ /usr/lib/cgi-bin/
        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
```

- Save and exit file awstats.conf

- Untuk meng-enablekan awstats, buat link file awstats.conf dari antara conf-available/ ke conf-enabled/

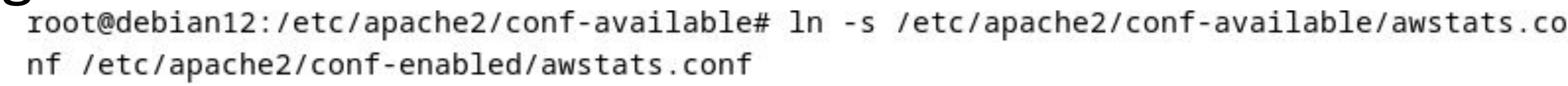
  ```
  # ln -s /etc/apache2/conf-available/awstats.conf
     /etc/apache2/conf-enabled/awstats.conf
  ```

- Enablekan modul cgi

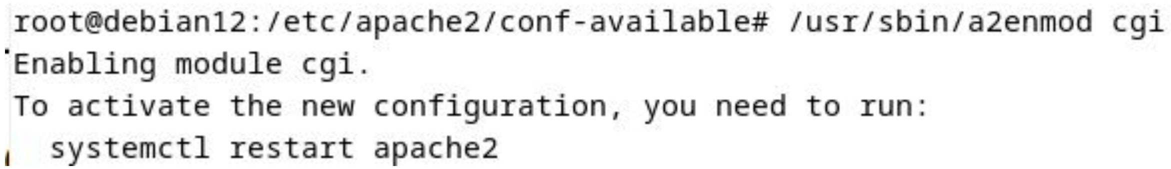
  ```
  # /usr/sbin/a2enmod cgi
  ```

- Restart web server

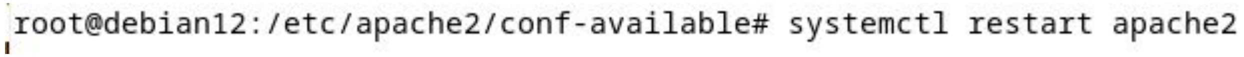
  ```
  # systemctl restart apache2
  ```



```
root@debian12:/etc/apache2/conf-available# ln -s /etc/apache2/conf-available/awstats.co
nf /etc/apache2/conf-enabled/awstats.conf
```

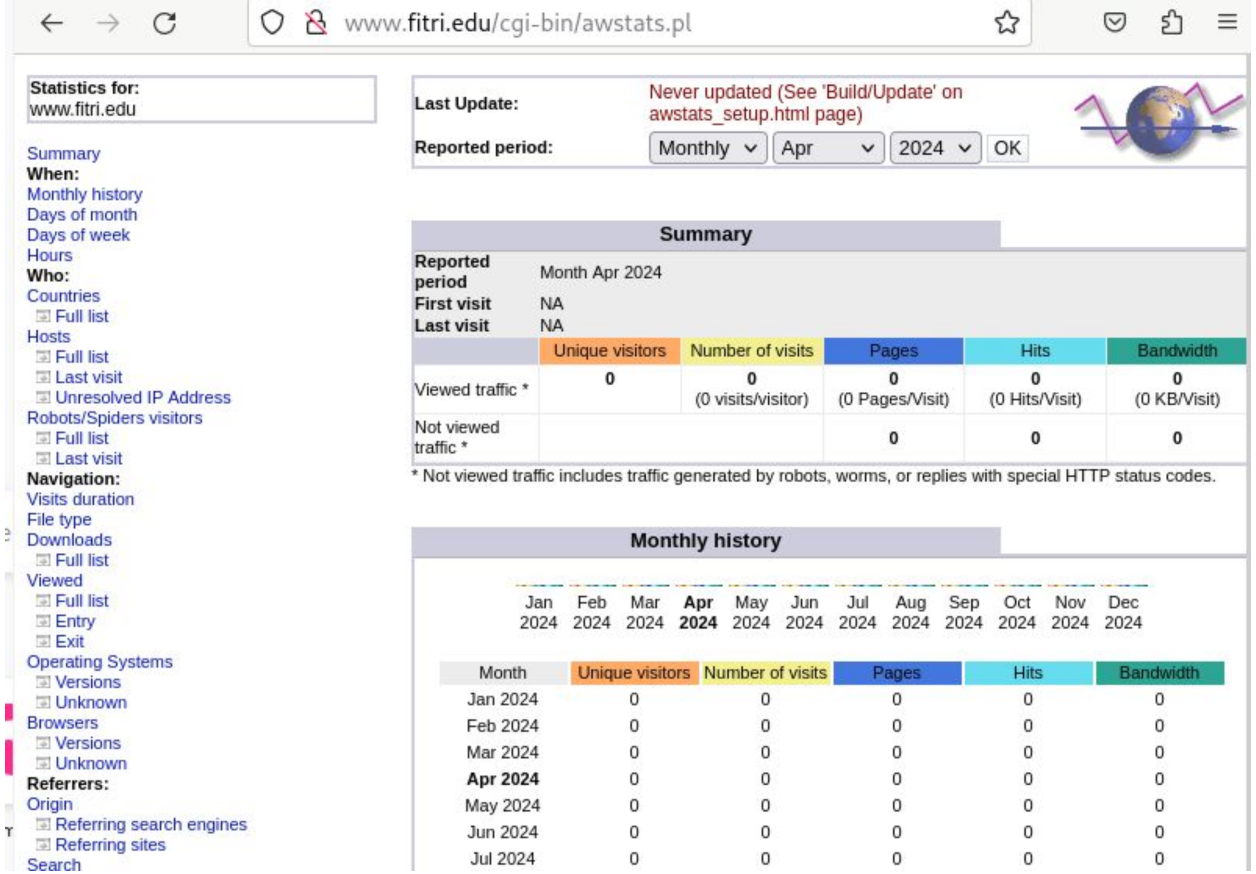


```
root@debian12:/etc/apache2/conf-available# /usr/sbin/a2enmod cgi
Enabling module cgi.
To activate the new configuration, you need to run:
  systemctl restart apache2
```



```
root@debian12:/etc/apache2/conf-available# systemctl restart apache2
```

- Buka browser dan ketikkan berikut http://www.fitri.edu/cgi-bin/awstats.pl



Statistics for:
www.fitri.edu

Last Update: Never updated (See 'Build/Update' on awstats_setup.html page)

Reported period: Monthly Apr 2024

Summary

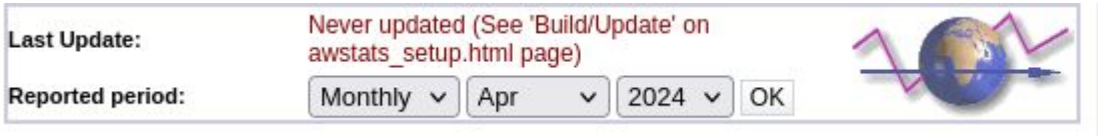
Reported period	Month Apr 2024				
First visit	NA				
Last visit	NA				
	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Viewed traffic *	**0**	**0** (0 visits/visitor)	**0** (0 Pages/Visit)	**0** (0 Hits/Visit)	**0** (0 KB/Visit)
Not viewed traffic *			**0**	**0**	**0**

* Not viewed traffic includes traffic generated by robots, worms, or replies with special HTTP status codes.

Monthly history

Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2024	0	0	0	0	0
Feb 2024	0	0	0	0	0
Mar 2024	0	0	0	0	0
Apr 2024	0	0	0	0	0
May 2024	0	0	0	0	0
Jun 2024	0	0	0	0	0
Jul 2024	0	0	0	0	0

- Jika dilihat, statistik masih 0 dan tertulis di bagian atas : Never updated



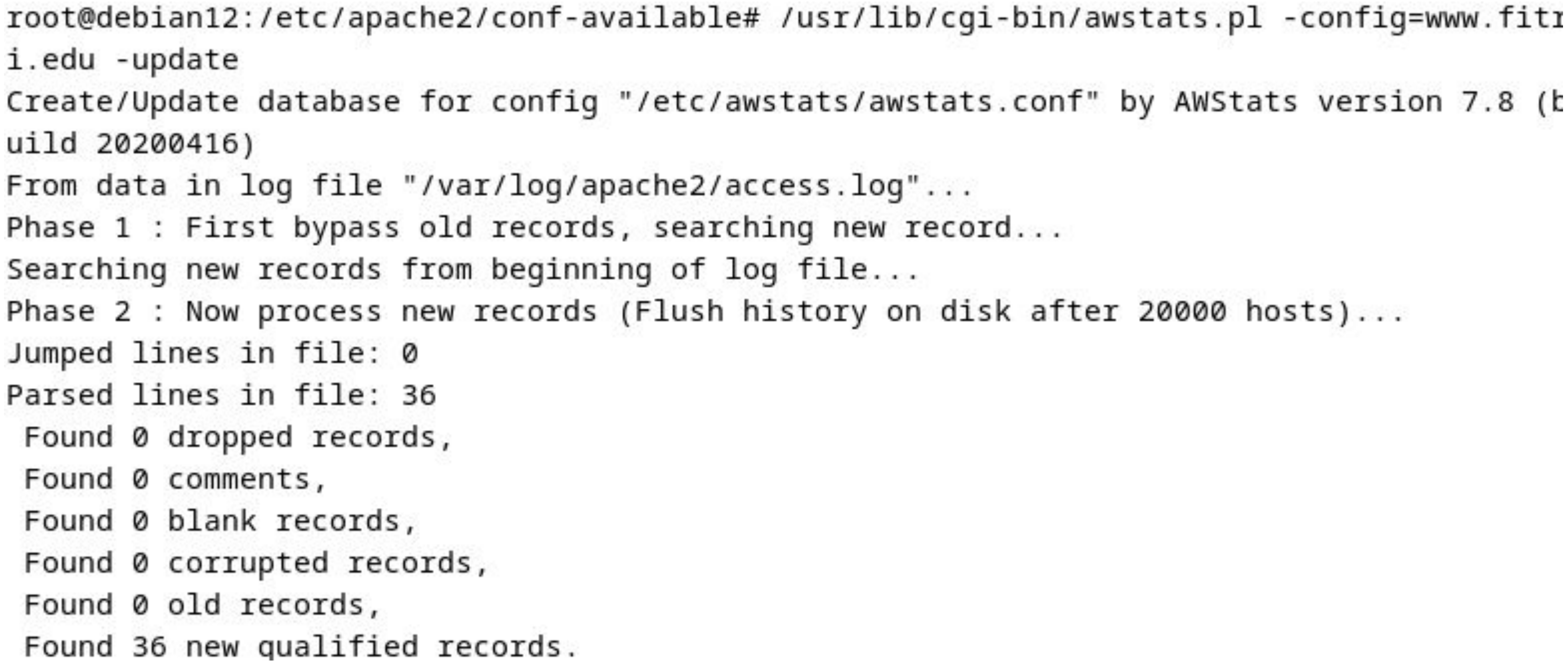
Last Update: Never updated (See 'Build/Update' on awstats_setup.html page)

Reported period: Monthly Apr 2024

- Untuk menyelesaikan itu, anda harus melakukan update secara manual lewat terminal

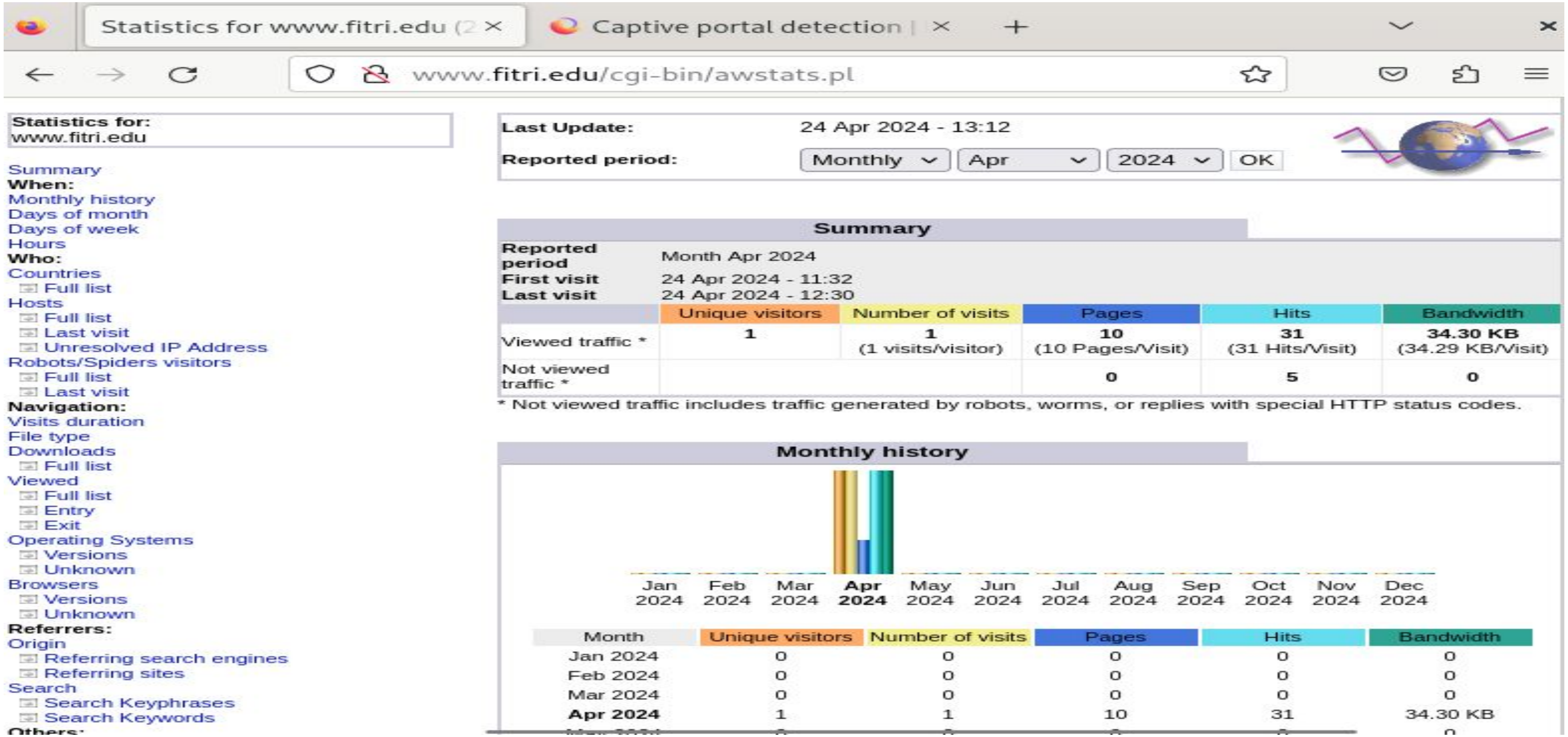
```
# /usr/lib/cgi-bin/awstats.pl -config=www.fitri.edu -update
```

- Buka browser anda dan refresh



```
root@debian12:/etc/apache2/conf-available# /usr/lib/cgi-bin/awstats.pl -config=www.fitr
i.edu -update
Create/Update database for config "/etc/awstats/awstats.conf" by AWStats version 7.8 (b
uild 20200416)
From data in log file "/var/log/apache2/access.log"...
Phase 1 : First bypass old records, searching new record...
Searching new records from beginning of log file...
Phase 2 : Now process new records (Flush history on disk after 20000 hosts)...
Jumped lines in file: 0
Parsed lines in file: 36
 Found 0 dropped records,
 Found 0 comments,
 Found 0 blank records,
 Found 0 corrupted records,
 Found 0 old records,
 Found 36 new qualified records.
```

Output setelah browser direfresh


Statistics for www.fitri.edu (2 ×
Captive portal detection | ×
www.fitri.edu/cgi-bin/awstats.pl

Statistics for:
www.fitri.edu

Summary
When:
Monthly history
Days of month
Days of week
Hours
Who:
Countries
Full list
Hosts
Full list
Last visit
Unresolved IP Address
Robots/Spiders visitors
Full list
Last visit
Navigation:
Visits duration
File type
Downloads
Full list
Viewed
Full list
Entry
Exit
Operating Systems
Versions
Unknown
Browsers
Versions
Unknown
Referrers:
Origin
Referring search engines
Referring sites
Search
Search Keyphrases
Search Keywords
Others:

Last Update: 24 Apr 2024 - 13:12

Reported period: Monthly ⌄ Apr ⌄ 2024 ⌄ OK

Summary

Reported period	Month Apr 2024				
First visit	24 Apr 2024 - 11:32				
Last visit	24 Apr 2024 - 12:30				
	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Viewed traffic *	**1**	**1** (1 visits/visitor)	**10** (10 Pages/Visit)	**31** (31 Hits/Visit)	**34.30 KB** (34.29 KB/Visit)
Not viewed traffic *			**0**	**5**	**0**

* Not viewed traffic includes traffic generated by robots, worms, or replies with special HTTP status codes.

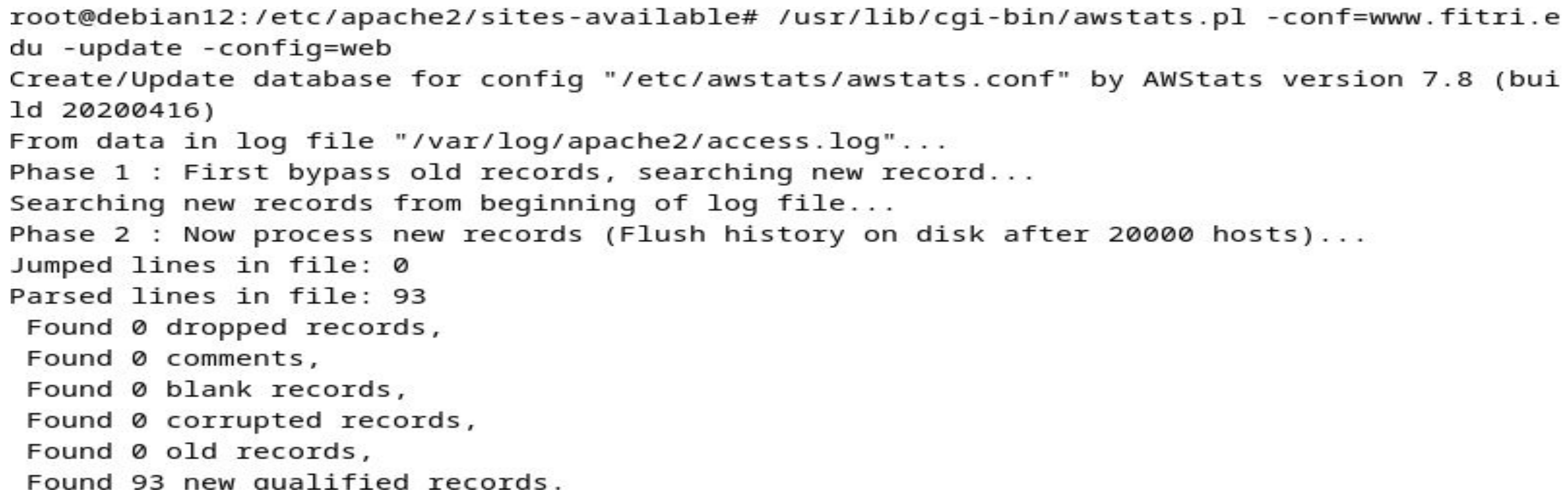
Monthly history

Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2024	0	0	0	0	0
Feb 2024	0	0	0	0	0
Mar 2024	0	0	0	0	0
Apr 2024	1	1	10	31	34.30 KB
May 2024	0	0	0	0	0

- Jika masih belum berhasil, lakukan update ulang

  ```
  # /usr/lib/cgi-bin/awstats.pl -config=www.fitri.edu -update -config=web
  ```

- Buka browser anda dan refresh



```
root@debian12:/etc/apache2/sites-available# /usr/lib/cgi-bin/awstats.pl -conf=www.fitri.e
du -update -config=web
Create/Update database for config "/etc/awstats/awstats.conf" by AWStats version 7.8 (bui
ld 20200416)
From data in log file "/var/log/apache2/access.log"...
Phase 1 : First bypass old records, searching new record...
Searching new records from beginning of log file...
Phase 2 : Now process new records (Flush history on disk after 20000 hosts)...
Jumped lines in file: 0
Parsed lines in file: 93
 Found 0 dropped records,
 Found 0 comments,
 Found 0 blank records,
 Found 0 corrupted records,
 Found 0 old records,
 Found 93 new qualified records.
```

- Jika masih belum berhasil, coba bersihkan cache browser anda dan buka web kembali http://www.fitri.edu/cgi-bin/awstats.pl

Daftar Pustaka

- https://www.linuxtuto.com/how-to-install-awstats-with-apache-on-debian-12/

2. Log Server dengan RSYSLOG

Prasyarat

- 1 PC/VM sebagai Rsyslog server
- 1 PC/VM sebagai Rsyslog client
- Baik server dan client terletak dalam satu network yang sama

1. Server : Install Rsyslog

- Install dulu rsyslog

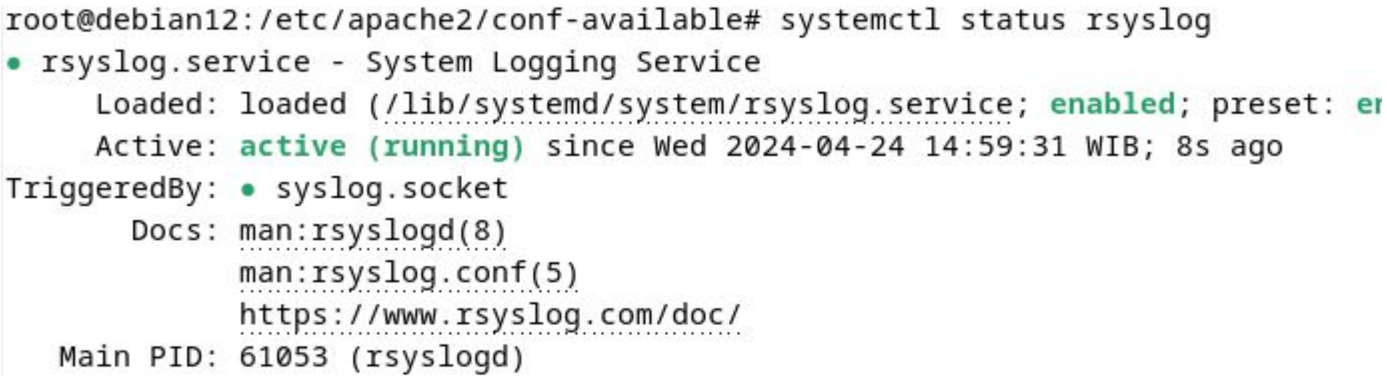
```
#apt install rsyslog
```

2. Server: Cek status Rsyslog

- Cek status rsyslog yang telah diinstall

  #systemctl status rsyslog
- Jika belum aktif, maka servicenya dapat diaktifkan dengan

  #systemctl start rsyslog



```
root@debian12:/etc/apache2/conf-available# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: en
     Active: active (running) since Wed 2024-04-24 14:59:31 WIB; 8s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 61053 (rsyslogd)
```

3. Server : Konfigurasi Rsyslog

- Rsyslog dikonfigurasi lewat file /etc/rsyslog.conf
- Sebelumnya backup dulu file /etc/rsyslog.conf

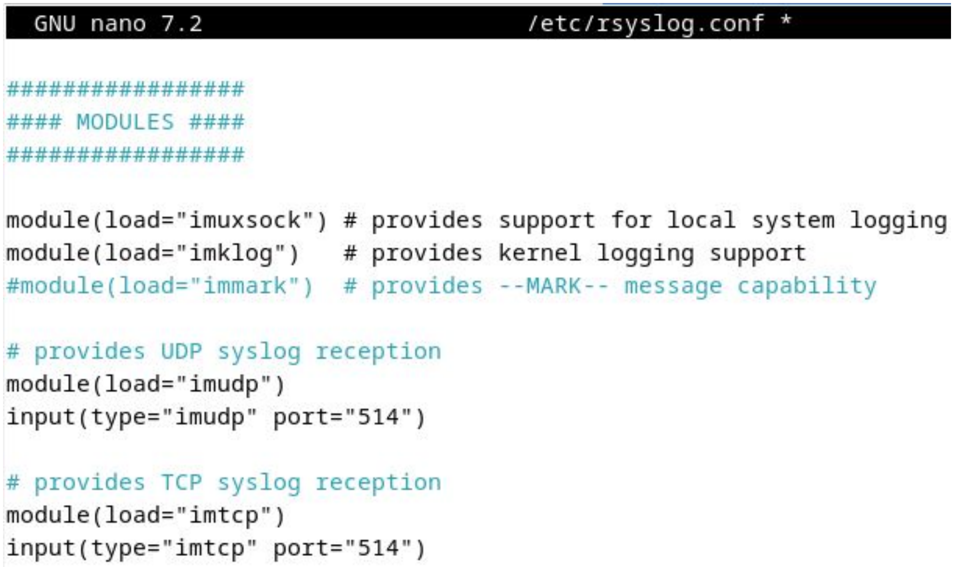
  ```
  #cp  /etc/rsyslog.conf  /etc/rsyslog.conf.orig
  ```

- Edit file /etc/rsyslog.conf

  ```
  #nano /etc/rsyslog.conf
  ```

- Hilangkan tanda # di depan baris

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



```
  GNU nano 7.2                              /etc/rsyslog.conf *

#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

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

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

- Disini, anda meng-enable modul TCP dan UDP dengan port 514 di Rsyslog

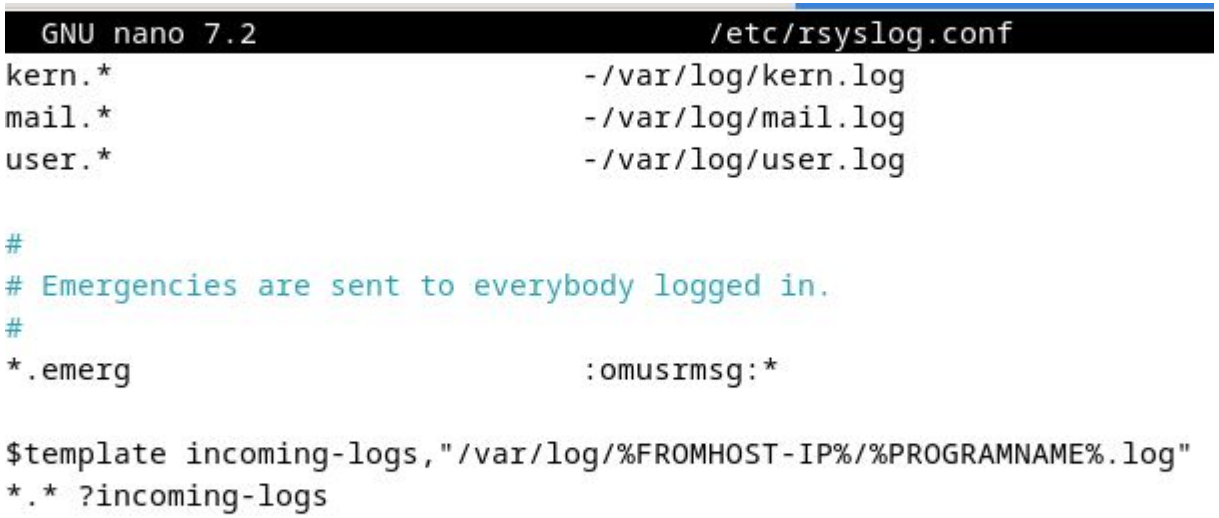
- Tambahkan baris ini di bagian paling bawah

```
$template incoming-logs, "/var/log/%FROMHOST-IP%/%PROGRAMNAME%.log"
*.* ?incoming-logs
```

- Dimana :
  - Anda membuat template bernama Incoming-logs yang diletakkan di directory /var/log/%FROMHOST-IP%/%PROGRAMNAME%/
  - Dimana :

    %FROMHOST-IP% – IP Address dari client

    %PROGRAMNAME% – nama program client yang menciptakan log file
- Artinya : Bila ada client, masing-masing client akan memiliki directory dengan IP addressnya sendiri-sendiri di server
- Di dalam tiap directory, ada nama log file yang berbeda tergantung dari nama program
- Simpan dan Exit



```
  GNU nano 7.2                         /etc/rsyslog.conf
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

$template incoming-logs,"/var/log/%FROMHOST-IP%/%PROGRAMNAME%.log"
*.* ?incoming-logs
```

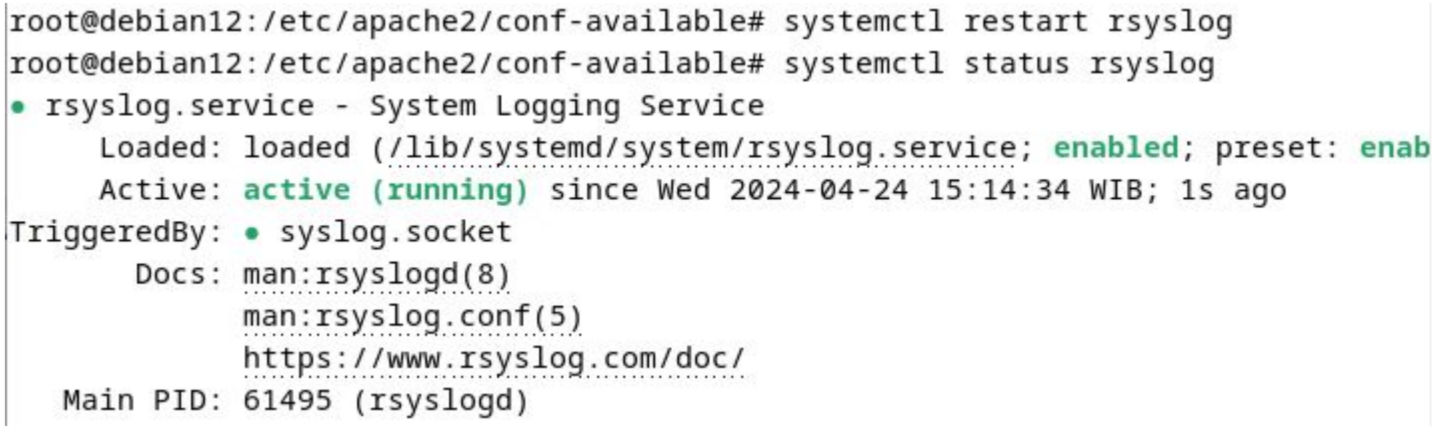
4. Server: Restart Rsyslog

- Setelah mengubah file konfigurasi, anda harus merestart Rsyslog

  #systemctl restart rsyslog

- Cek status rsyslog yang telah direstart. Status seharusnya active

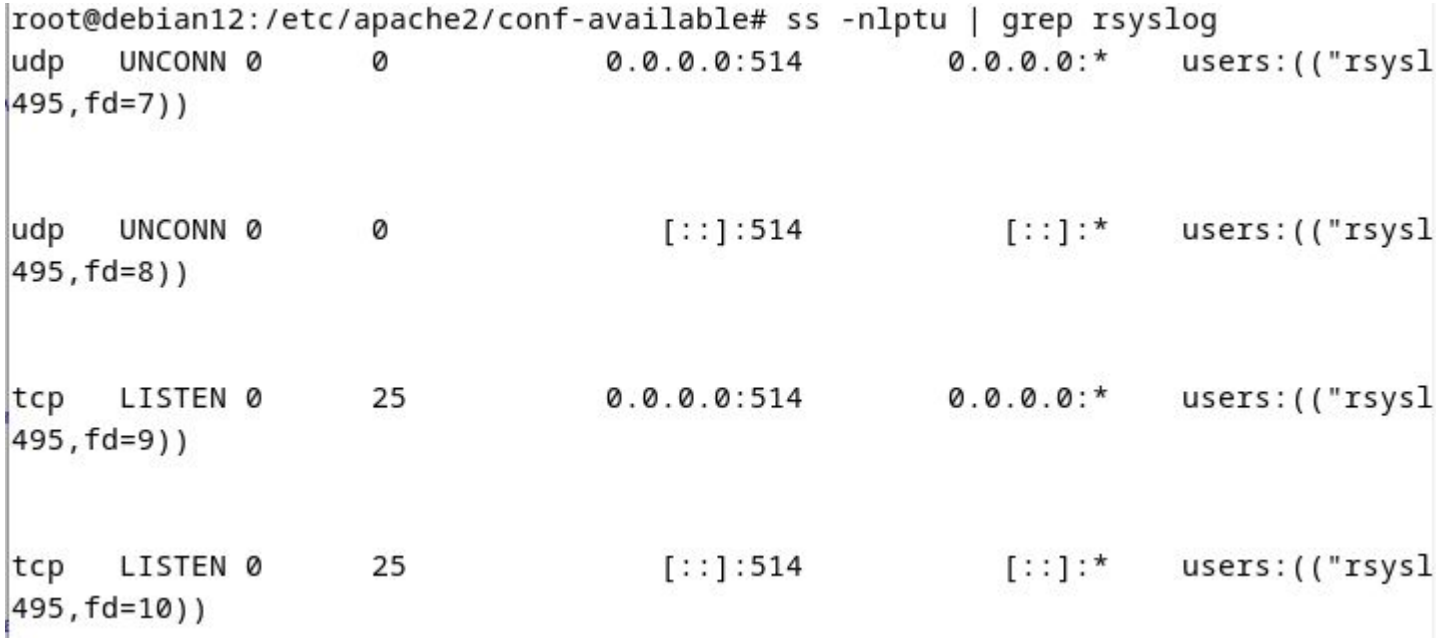
  #systemctl status rsyslog



```
root@debian12:/etc/apache2/conf-available# systemctl restart rsyslog
root@debian12:/etc/apache2/conf-available# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enab
     Active: active (running) since Wed 2024-04-24 15:14:34 WIB; 1s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 61495 (rsyslogd)
```

- Cek port dari rsyslog. Nampak rsyslog bekerja pada port tcp 514 dan udp 514

  #ss -nlptu | grep rsyslog



```
root@debian12:/etc/apache2/conf-available# ss -nlptu | grep rsyslog
udp   UNCONN 0      0            0.0.0.0:514        0.0.0.0:*    users:(("rsysl
495,fd=7))


udp   UNCONN 0      0               [::]:514           [::]:*    users:(("rsysl
495,fd=8))


tcp   LISTEN 0      25           0.0.0.0:514        0.0.0.0:*    users:(("rsysl
495,fd=9))


tcp   LISTEN 0      25              [::]:514           [::]:*    users:(("rsysl
495,fd=10))
```

5. Client : Install Rsyslog

- Berpindahlah dari server ke client
- Update Linux

```
#apt update
```

- Install rsyslog

```
#apt install rsyslog
```

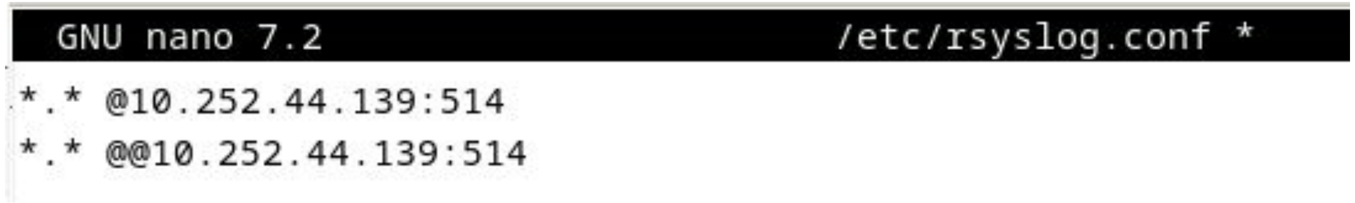
6. Client : Konfigurasi Rsyslog

- Sebelumnya backup dulu file /etc/rsyslog.conf

  #cp /etc/rsyslog.conf /etc/rsyslog.conf.orig

  #nano /etc/rsyslog.conf
- Pada bagian yang paling bawah, tambahkan baris berikut :

```
*.* @[rsyslog-server-ip-address]:514
*.* @@[rsyslog-server-ip-address]:514
```



```
  GNU nano 7.2                      /etc/rsyslog.conf *
*.* @10.252.44.139:514
*.* @@10.252.44.139:514
```

- Arti dari rule diatas :
- *.* @[rsyslog-server-ip-address]:514
  - Semua facility dengan semua prioritas pada modul udp akan dilogging ke ip-address-server, port 514 (@ = udp)
- *.* @@[rsyslog-server-ip-address]:514
  - Semua facility dengan semua prioritas pada modul tcp akan dilogging ke ip-address-server, port 514 (@@ = tcp)
- Untuk mengisi <rsyslog-server-ip-address> anda harus mengecek nomor IP address Rsyslog Server. Pada kasus ini nomor ip server 10.252.44.139

- Tambahkan juga baris berikut

  $ActionQueueFileName queue

  $ActionQueueMaxDiskSpace 1g

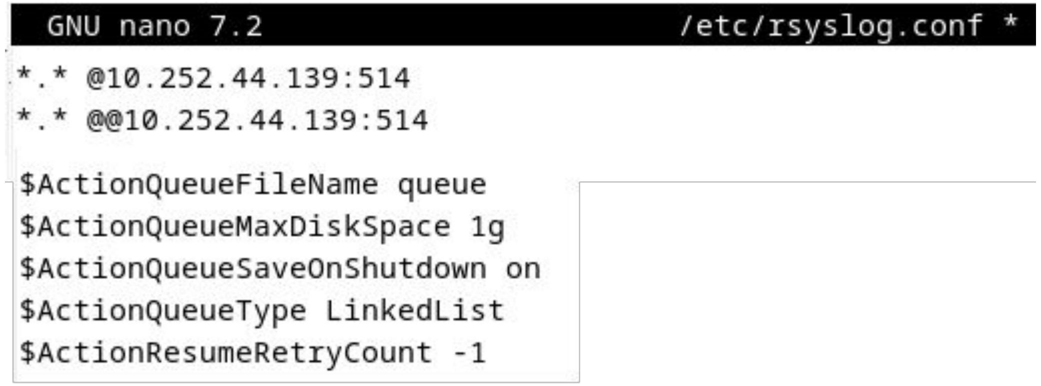
  $ActionQueueSaveOnShutdown on

  $ActionQueueType LinkedList

  $ActionResumeRetryCount -1

- Save dan Exit

- Arti dari perintah diatas :
  - Jika Rsyslog server down, maka Rsyslog client akan membuat file bernama queue, dengan ukuran max 1G.
  - Jika terjadi shutdown, maka queue akan disimpan.
  - Queue bertipe linked list
  - Jika terjadi error, akan dilakukan retry



```
  GNU nano 7.2                                /etc/rsyslog.conf *
*.* @10.252.44.139:514
*.* @@10.252.44.139:514

$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
```

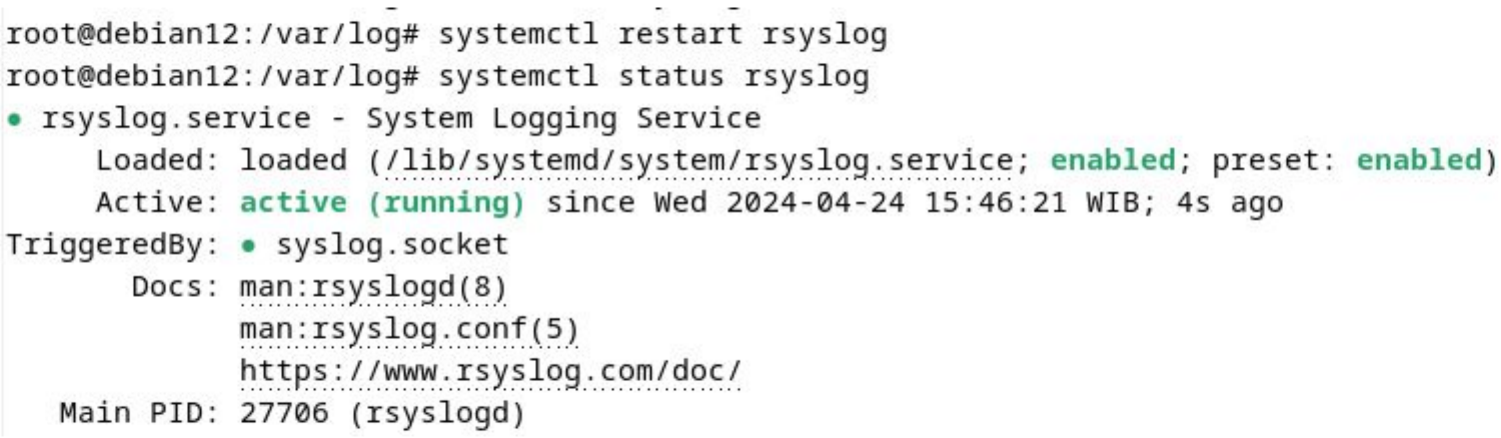
7. Client : Restart Rsyslog

- Setelah mengubah file konfigurasi, anda harus merestart Rsyslog di client

  #systemctl restart rsyslog

- Cek status rsyslog yang telah direstart

  #systemctl status rsyslog



```
root@debian12:/var/log# systemctl restart rsyslog
root@debian12:/var/log# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-04-24 15:46:21 WIB; 4s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 27706 (rsyslogd)
```

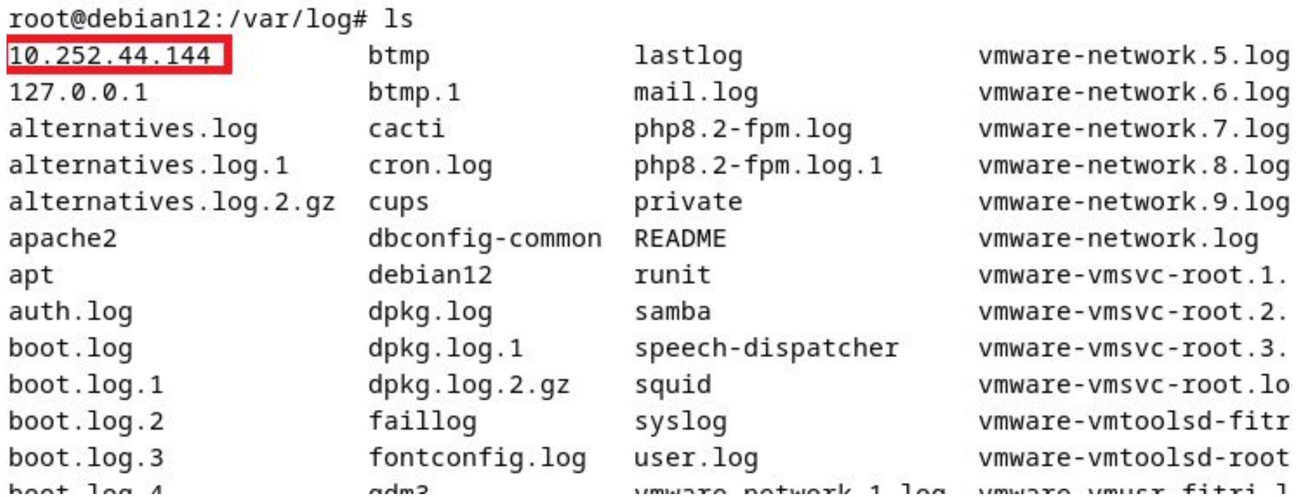
8. Server : Cek file log di /var/log

- Berpindahlah dari client ke server
- File log dari client akan dikirim ke server.
- File ini disimpan di server, pada directory /var/log/*
- Cek apakah ada directory file log

#cd /var/log

#ls

- nomor IP client : 10.252.44.144
- Artinya, log client telah disimpan oleh rsyslog server

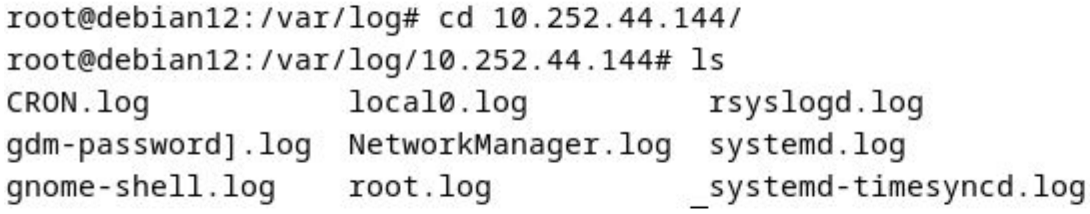


```
root@debian12:/var/log# ls
10.252.44.144          btmp             lastlog               vmware-network.5.log
127.0.0.1              btmp.1           mail.log              vmware-network.6.log
alternatives.log       cacti            php8.2-fpm.log        vmware-network.7.log
alternatives.log.1     cron.log         php8.2-fpm.log.1      vmware-network.8.log
alternatives.log.2.gz  cups             private               vmware-network.9.log
apache2                dbconfig-common  README                vmware-network.log
apt                    debian12         runit                 vmware-vmsvc-root.1.
auth.log               dpkg.log         samba                 vmware-vmsvc-root.2.
boot.log               dpkg.log.1       speech-dispatcher     vmware-vmsvc-root.3.
boot.log.1             dpkg.log.2.gz    squid                 vmware-vmsvc-root.lo
boot.log.2             faillog          syslog                vmware-vmtoolsd-fitr
boot.log.3             fontconfig.log   user.log              vmware-vmtoolsd-root
boot.log.4             gdm3             vmware-network.1.log  vmware-vmusr-fitri.l
```

- Jika ada, masuk ke directory tersebut dan cek isi file log yang terbentuk

  #cd 10.252.44.144

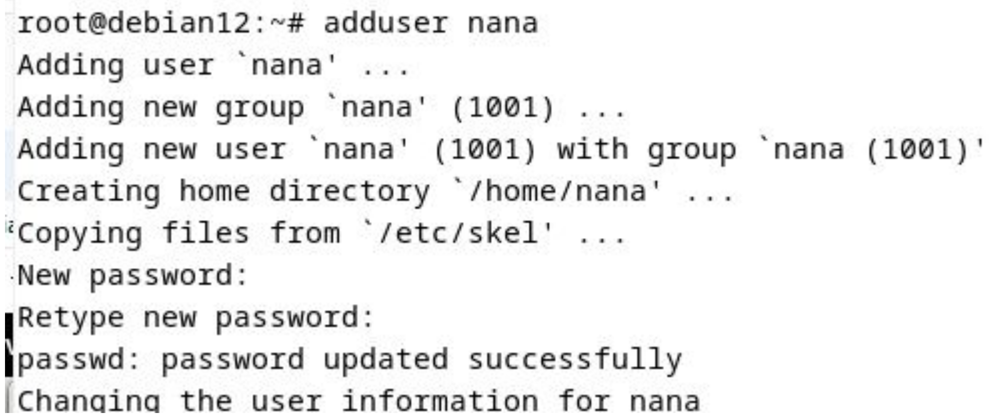
  #ls



```
root@debian12:/var/log# cd 10.252.44.144/
root@debian12:/var/log/10.252.44.144# ls
CRON.log           local0.log          rsyslogd.log
gdm-password].log  NetworkManager.log  systemd.log
gnome-shell.log    root.log           _systemd-timesyncd.log
```

9. Client : Testing Rsyslog

- Buatlah user baru di client



```
root@debian12:~# adduser nana
Adding user `nana' ...
Adding new group `nana' (1001) ...
Adding new user `nana' (1001) with group `nana (1001)'
Creating home directory `/home/nana' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for nana
```

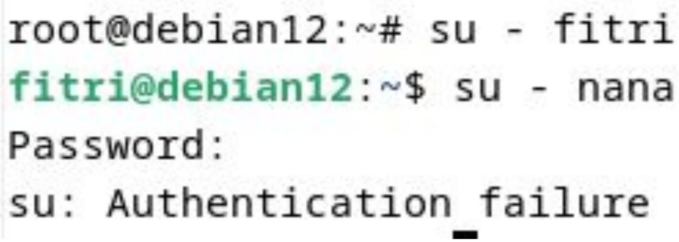
- Jika sudah, masuklah ke salah satu user

  #su - fitri

- Kemudian, masuklah sebagai user baru

  #su - nana

- Anda telah membuat password untuk user baru. Masukkan password yg salah
-



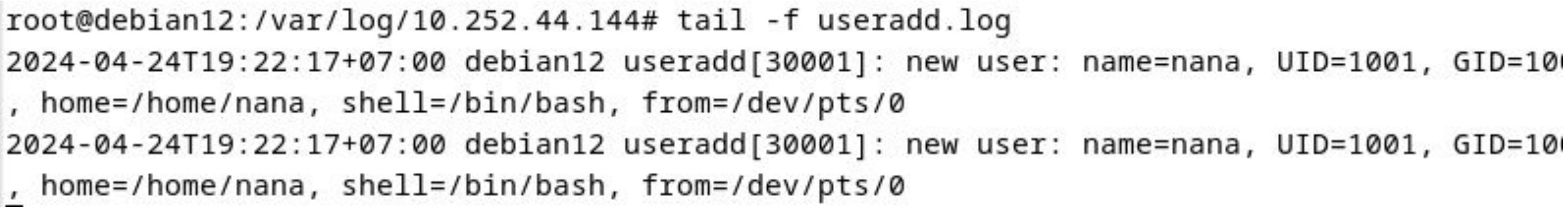
```
root@debian12:~# su - fitri
fitri@debian12:~$ su - nana
Password:
su: Authentication failure
```

10. Server: Testing Rsyslog

- Di Server, lihatlah ke isi direktory /var/log/10.252.44.144

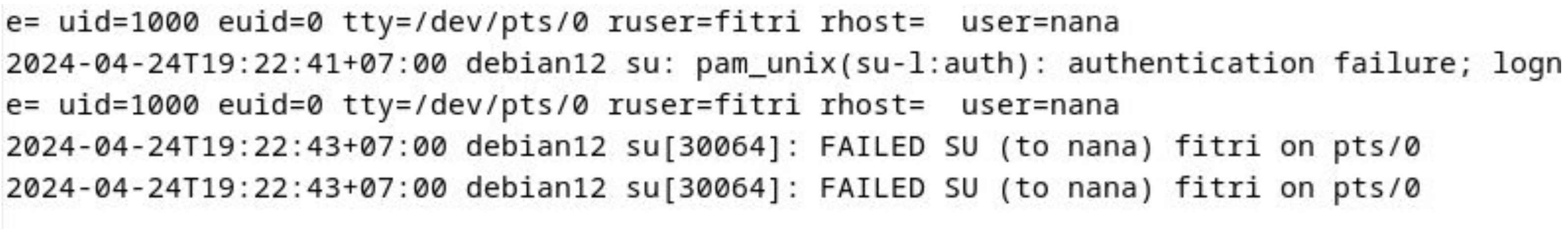
  #cd /var/log/10.252.44.144

  #ls
- Bukalah file useradd.log dengan tail -f
- Nampak, VM client membuat user baru dengan nama nana



```
root@debian12:/var/log/10.252.44.144# tail -f useradd.log
2024-04-24T19:22:17+07:00 debian12 useradd[30001]: new user: name=nana, UID=1001, GID=10
, home=/home/nana, shell=/bin/bash, from=/dev/pts/0
2024-04-24T19:22:17+07:00 debian12 useradd[30001]: new user: name=nana, UID=1001, GID=10
, home=/home/nana, shell=/bin/bash, from=/dev/pts/0
```

- Buka file su.log. Nampak terjadi error saat melakukan login dengan perintah su



```
e= uid=1000 euid=0 tty=/dev/pts/0 ruser=fitri rhost=  user=nana
2024-04-24T19:22:41+07:00 debian12 su: pam_unix(su-l:auth): authentication failure; logn
e= uid=1000 euid=0 tty=/dev/pts/0 ruser=fitri rhost=  user=nana
2024-04-24T19:22:43+07:00 debian12 su[30064]: FAILED SU (to nana) fitri on pts/0
2024-04-24T19:22:43+07:00 debian12 su[30064]: FAILED SU (to nana) fitri on pts/0
```

- Selamat !!!

  Anda telah berhasil menyimpan log dari client di server ☺️

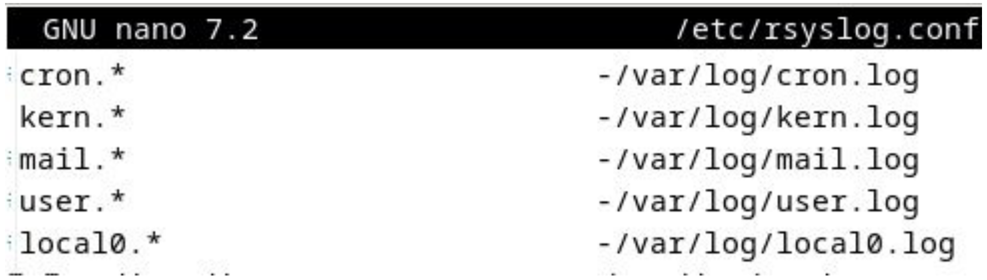
11. Client : Konfigurasi /etc/rsyslog.conf untuk Logger

- Pada tahap ini, kita akan menambahkan log dengan logger.
- Logger sendiri akan diinstall pada langkah berikutnya
- Log akan disimpan di fasilitas rsyslog yaitu local0.log
- Pada Client, buka file /etc/rsyslog.conf

  #nano /etc/rsyslog.conf

  Tambahkan baris berikut

  local0.* -/var/log/local0.log
- Perhatikan bahwa urutan penulisan mempengaruhi output log.
- Arti : Untuk fasilitas local0 dengan semua prioritas, tuliskan log file ke /var/log/local0.log
- Simpan dan exit



```
  GNU nano 7.2                          /etc/rsyslog.conf
cron.*                                  -/var/log/cron.log
kern.*                                  -/var/log/kern.log
mail.*                                  -/var/log/mail.log
user.*                                  -/var/log/user.log
local0.*                                -/var/log/local0.log
```

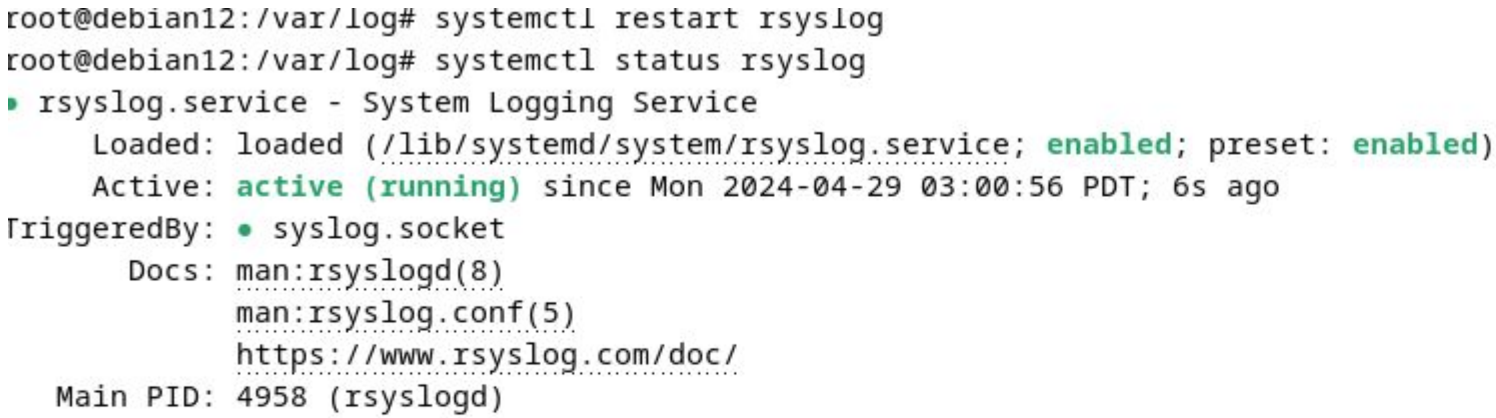
12. Client : Restart Rsyslog

- Restart rsyslog client

  #systemctl restart rsyslog

- Cek status rsyslog client

  #systemctl status rsyslog



```
root@debian12:/var/log# systemctl restart rsyslog
root@debian12:/var/log# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-04-29 03:00:56 PDT; 6s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 4958 (rsyslogd)
```

13. Client : Testing dengan logger

- Berpindahlah dari server ke client
- Install logger di client
  #apt install bsdutils
- Ketikkan baris berikut

$ logger -p local0.notice -t local0 “TEST logging test 0“

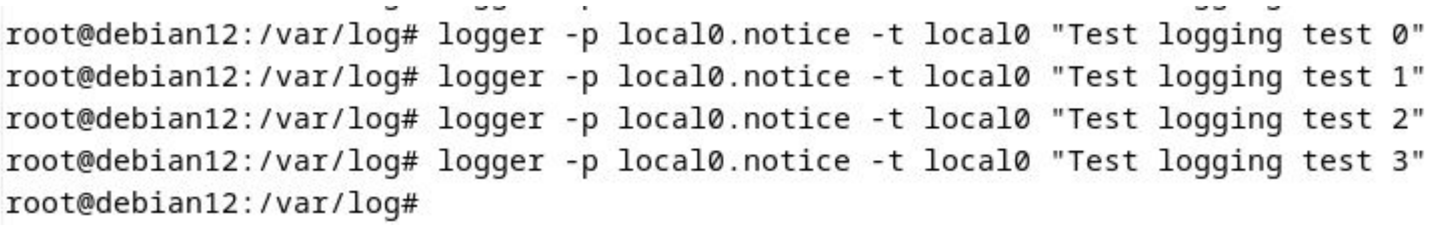
$ logger -p local0.notice -t local0 “TEST logging test 1“

$ logger -p local0.notice -t local0 “TEST logging test 2“

$ logger -p local0.notice -t local0 “TEST logging test 3“

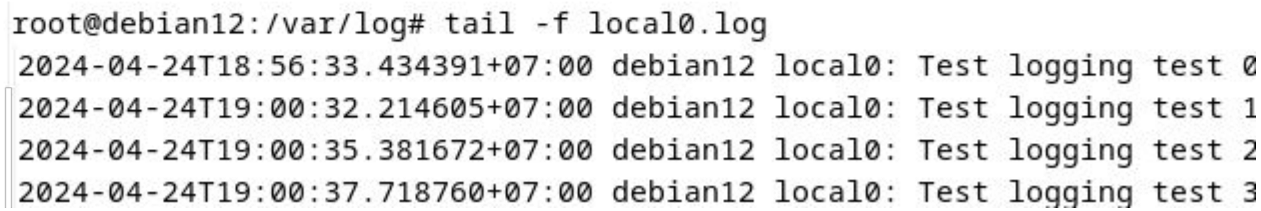
Disini, client mengirim pesan internal “TEST logging test 1“ ke /var/log/local0.log

Fasilitas yang digunakan : local0, prioritas : notice



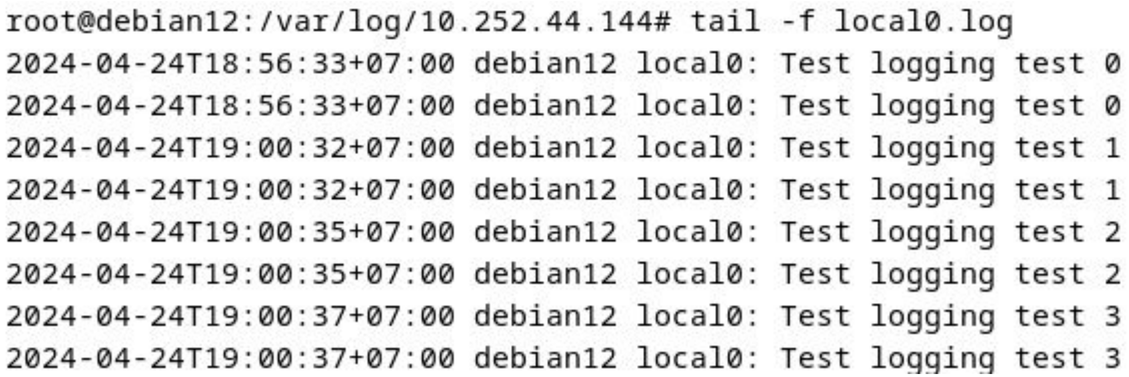
```
root@debian12:/var/log# logger -p local0.notice -t local0 "Test logging test 0"
root@debian12:/var/log# logger -p local0.notice -t local0 "Test logging test 1"
root@debian12:/var/log# logger -p local0.notice -t local0 "Test logging test 2"
root@debian12:/var/log# logger -p local0.notice -t local0 "Test logging test 3"
root@debian12:/var/log#
```

- Kita ingin, agar file log diletakkan di /var/log/local0.log di client dan /var/log/debian11-server/local0.log
- Sekarang cek di client :



```
root@debian12:/var/log# tail -f local0.log
2024-04-24T18:56:33.434391+07:00 debian12 local0: Test logging test 0
2024-04-24T19:00:32.214605+07:00 debian12 local0: Test logging test 1
2024-04-24T19:00:35.381672+07:00 debian12 local0: Test logging test 2
2024-04-24T19:00:37.718760+07:00 debian12 local0: Test logging test 3
```

- Cek di server



```
root@debian12:/var/log/10.252.44.144# tail -f local0.log
2024-04-24T18:56:33+07:00 debian12 local0: Test logging test 0
2024-04-24T18:56:33+07:00 debian12 local0: Test logging test 0
2024-04-24T19:00:32+07:00 debian12 local0: Test logging test 1
2024-04-24T19:00:32+07:00 debian12 local0: Test logging test 1
2024-04-24T19:00:35+07:00 debian12 local0: Test logging test 2
2024-04-24T19:00:35+07:00 debian12 local0: Test logging test 2
2024-04-24T19:00:37+07:00 debian12 local0: Test logging test 3
2024-04-24T19:00:37+07:00 debian12 local0: Test logging test 3
```

- Selamat !!!
- Anda telah berhasil menyimpan log logger dari client ke server 😊

Daftar Pustaka

1. https://ioflood.com/blog/install-logger-command-linux/#:~:text=Usage%20and%20Verification-,Using%20Logger,notice'.
2. https://kifarunix.com/install-and-setup-rsyslog-server-on-ubuntu-22-04/?expand_article=1
3. https://kifarunix.com/enable-rsyslog-logging-on-debian-12/
4. https://www.rsyslog.com/doc/troubleshooting/troubleshoot.html

3. Statistik Squid Proxy Server dengan SARG

SARG

- SARG is an open source tool that allows you to analyse the squid log files
- SARG can generate reports in HTML format with informations about :
  - users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, daily reports, weekly reports and monthly reports.
- The SARG is very handy tool to view how much internet bandwidth is utilized by individual machines on the network and can watch on which websites the network’s users are accessing.

Sebelumnya ….

- Pastikan anda sudah melakukan instalasi dan konfigurasi squid
- Pastikan bahwa squid telah berjalan dengan baik

```
#systemctl status squid
```

- Jika squid mati, nyalakan squid terlebih dahulu

```
#systemctl restart squid
```

SARG

1. Update Linux

   #apt update

2. Install sarg

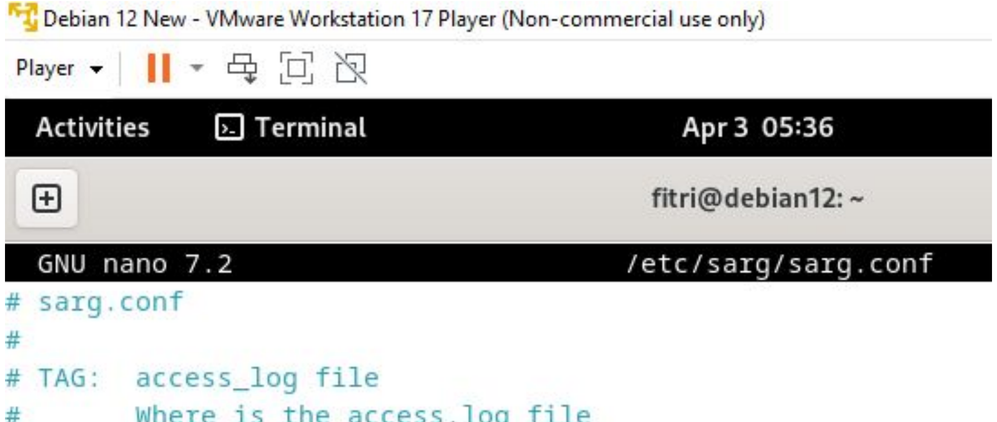
   #apt install sarg

3. Edit file konfigurasi sarg /etc/sarg/sarg.conf

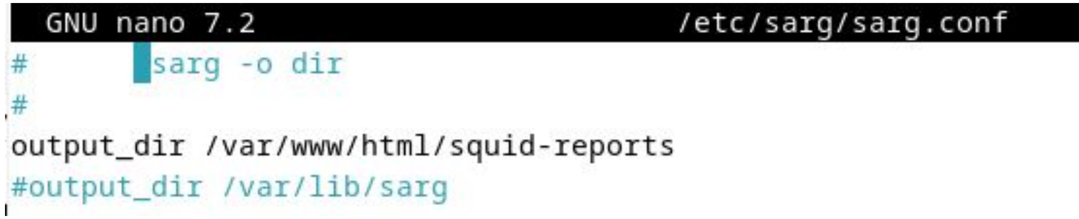
   Jika anda menggunakan date_format default yaitu Amerika, maka formatnya adalah bulan/tanggal/tahun

   Jika anda menggunakan date_format Eropa, maka formatnya adalah tanggal/bulan/tahun

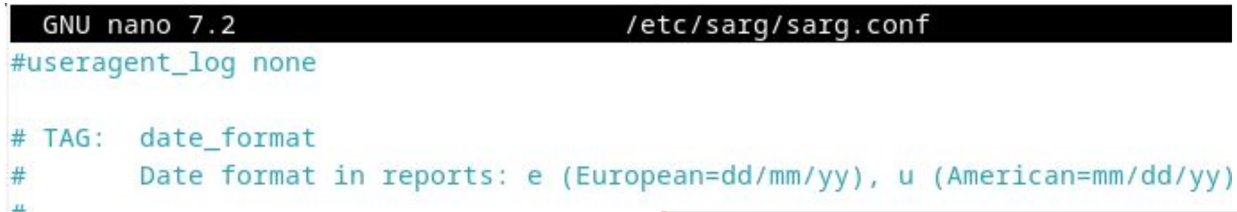
   Pilih sesuai yang anda lebih suka, disini saya menggunakan format Amerika


Debian 12 New - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Apr 3 05:36
fitri@debian12: ~

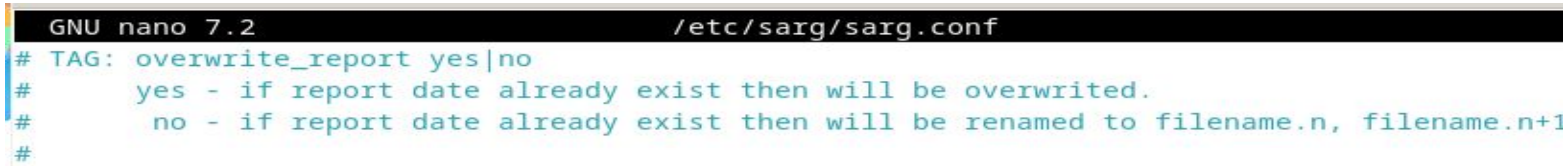
```
  GNU nano 7.2                                /etc/sarg/sarg.conf
# sarg.conf
#
# TAG:  access_log file
#       Where is the access.log file
#       sarg -l file
#
access_log /var/log/squid/access.log
```



```
  GNU nano 7.2                                        /etc/sarg/sarg.conf
#       sarg -o dir
#
output_dir /var/www/html/squid-reports
#output_dir /var/lib/sarg
```



```
  GNU nano 7.2                                /etc/sarg/sarg.conf
#useragent_log none

# TAG:  date_format
#       Date format in reports: e (European=dd/mm/yy), u (American=mm/dd/yy)
#
date_format u
```

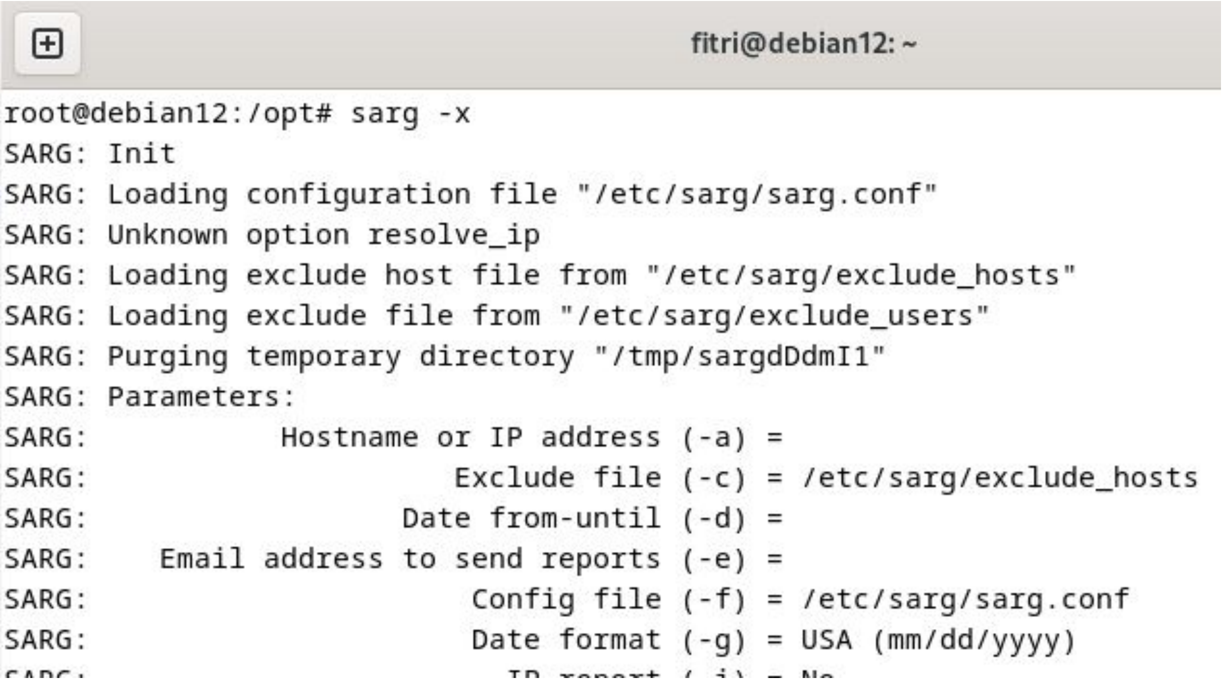


```
  GNU nano 7.2                                /etc/sarg/sarg.conf
# TAG: overwrite_report yes|no
#       yes - if report date already exist then will be overwrited.
#        no - if report date already exist then will be renamed to filename.n, filename.n+1
#
```

- Save dan exit
- Jalankan sarg

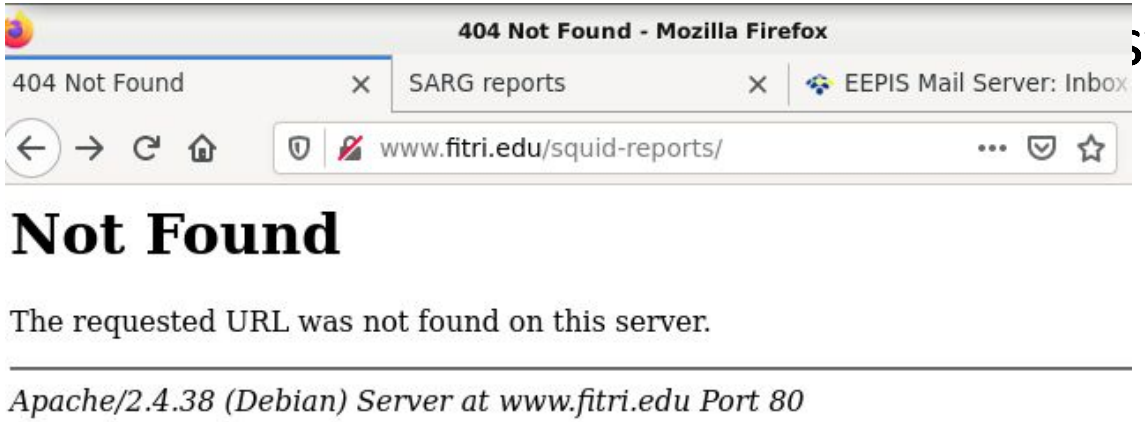
  #sarg -x

- Anda sukses mengenerate repor



```
root@debian12:/opt# sarg -x
SARG: Init
SARG: Loading configuration file "/etc/sarg/sarg.conf"
SARG: Unknown option resolve_ip
SARG: Loading exclude host file from "/etc/sarg/exclude_hosts"
SARG: Loading exclude file from "/etc/sarg/exclude_users"
SARG: Purging temporary directory "/tmp/sargdDdmI1"
SARG: Parameters:
SARG:           Hostname or IP address (-a) =
SARG:                    Exclude file (-c) = /etc/sarg/exclude_hosts
SARG:                 Date from-until (-d) =
SARG:    Email address to send reports (-e) =
SARG:                     Config file (-f) = /etc/sarg/sarg.conf
SARG:                     Date format (-g) = USA (mm/dd/yyyy)
SARG:                       IP report (-i) = No
```

- Buka browser, ketikkan http://www.fitri.edu/squid-reports
- Keluar output berikut :
- sting belum bekerja dengan baik


404 Not Found - Mozilla Firefox

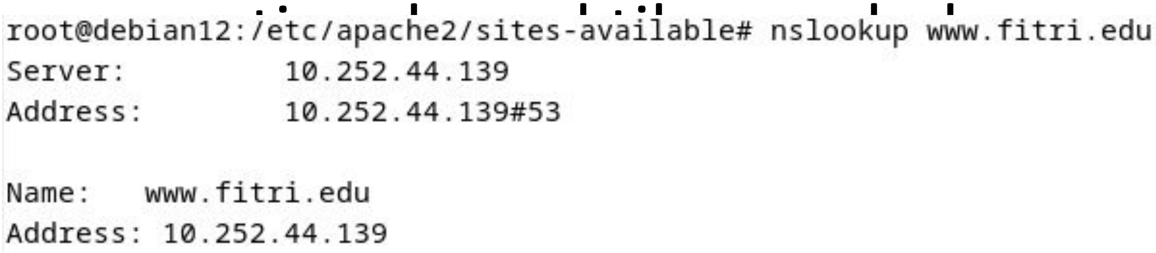
Not Found

The requested URL was not found on this server.

Apache/2.4.38 (Debian) Server at www.fitri.edu Port 80

Cek DNS Server

- Pastikan dulu bahwa dns server anda telah bekerja dg nslookup
- Jika belum, cek dulu file /etc/hosts, /etc/resolv.conf dan /etc/dnsmasq.c



```
root@debian12:/etc/apache2/sites-available# nslookup www.fitri.edu
Server:         10.252.44.139
Address:        10.252.44.139#53

Name:   www.fitri.edu
Address: 10.252.44.139
```

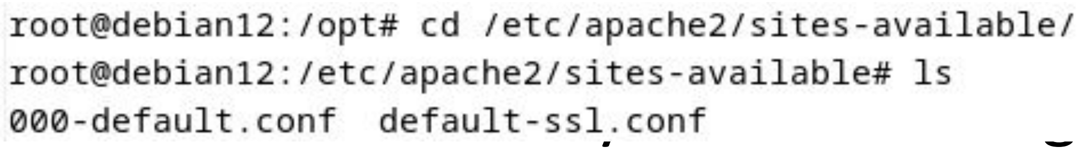
nslookup

Cek Virtual hosting

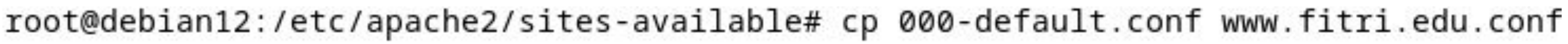
- Anda boleh menskip langkah ini jika virtual hosting telah bekerja dengan s/d ppt slide 13)
- Pastikan anda telah menginstall apache2

  #apt list apache2

- irtual hosting

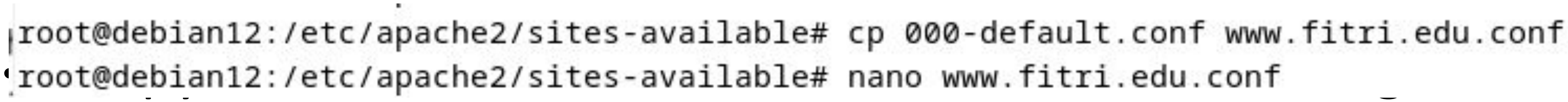


```
root@debian12:/opt# cd /etc/apache2/sites-available/
root@debian12:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf
```

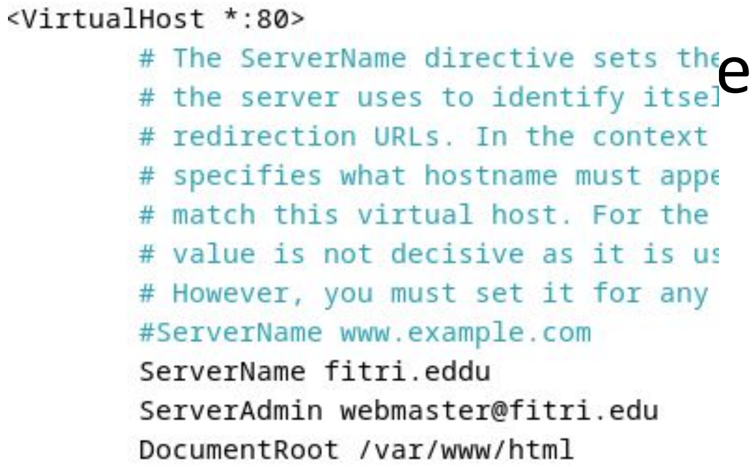


```
root@debian12:/etc/apache2/sites-available# cp 000-default.conf www.fitri.edu.conf
```

- Kopikan file 000.default ke file www.fitri.edu.conf



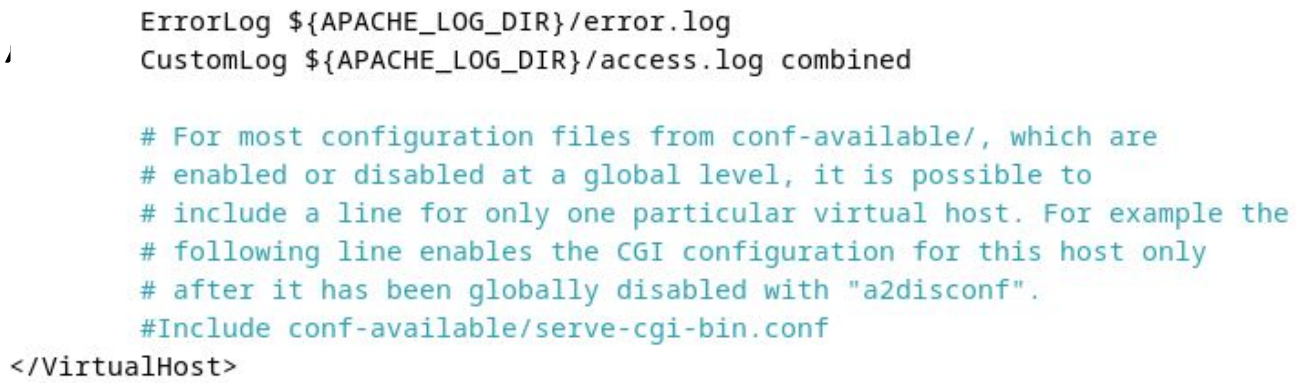
```
root@debian12:/etc/apache2/sites-available# cp 000-default.conf www.fitri.edu.conf
root@debian12:/etc/apache2/sites-available# nano www.fitri.edu.conf
```



```
<VirtualHost *:80>
        # The ServerName directive sets the
        # the server uses to identify itsel
        # redirection URLs. In the context
        # specifies what hostname must appe
        # match this virtual host. For the
        # value is not decisive as it is us
        # However, you must set it for any
        #ServerName www.example.com
        ServerName fitri.eddu
        ServerAdmin webmaster@fitri.edu
        DocumentRoot /var/www/html
```

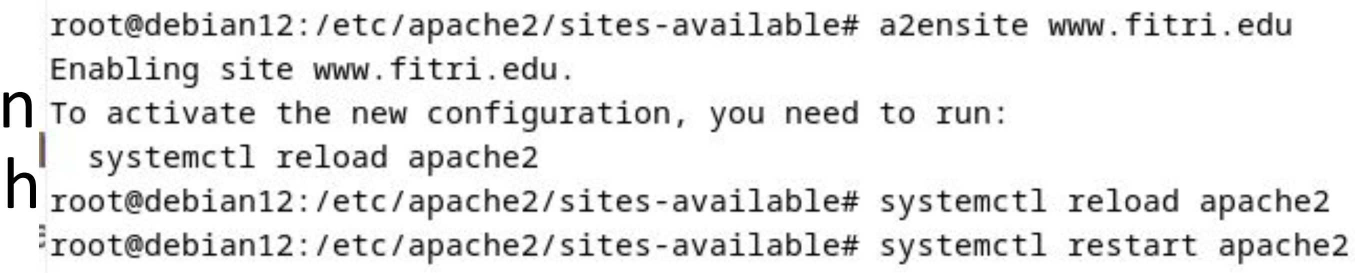
- erName, ServerAdmin dan DocumentRoot

- Dibagian bawah, ne2

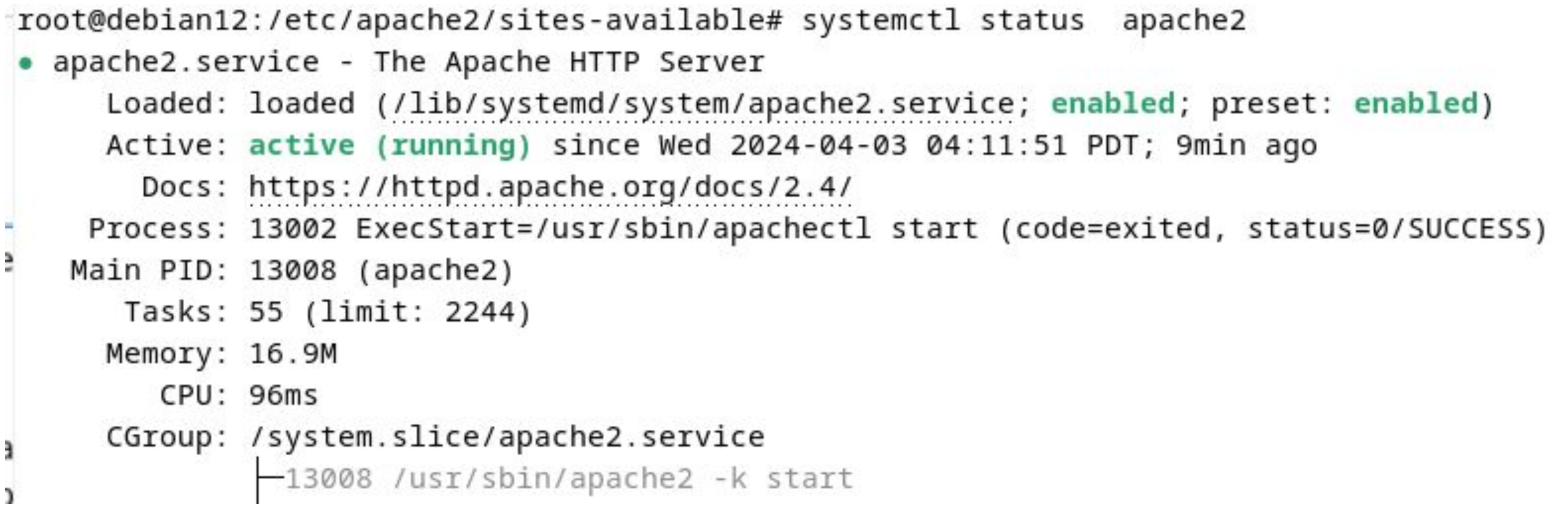


```
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

- Save dan exit
- Enable-kan virtual hostin
- Reload dan restart apach

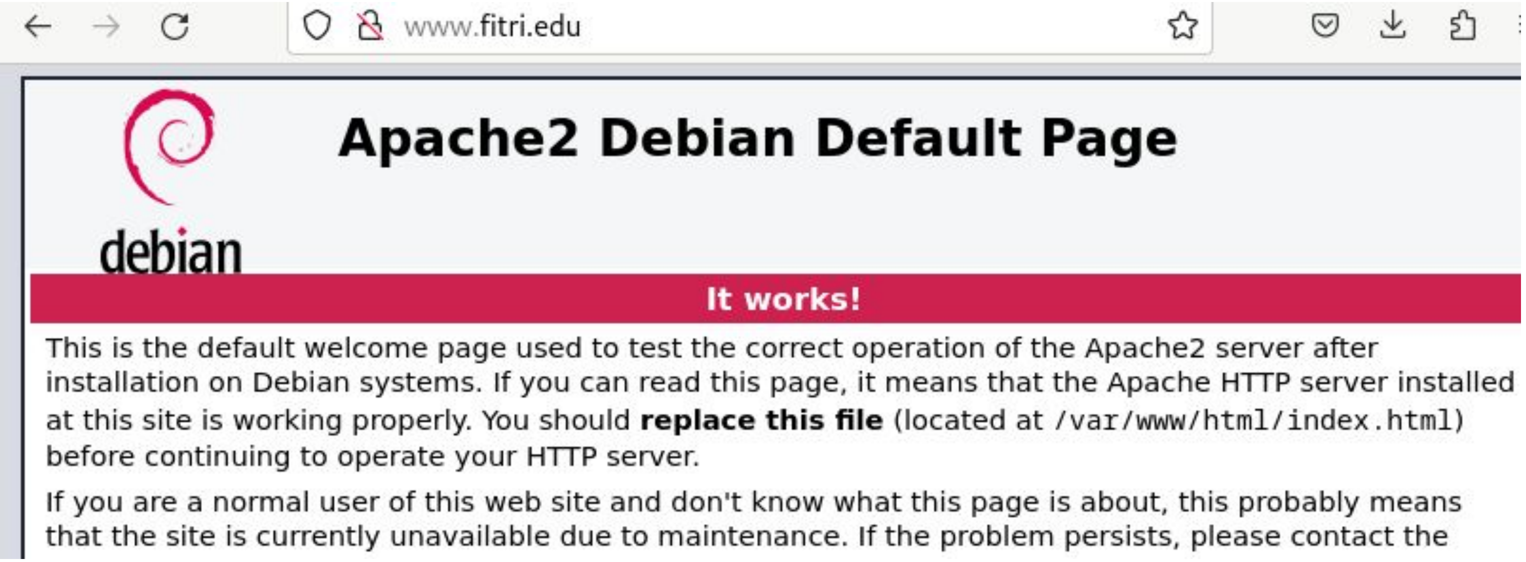


```
root@debian12:/etc/apache2/sites-available# a2ensite www.fitri.edu
Enabling site www.fitri.edu.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@debian12:/etc/apache2/sites-available# systemctl reload apache2
root@debian12:/etc/apache2/sites-available# systemctl restart apache2
```



```
root@debian12:/etc/apache2/sites-available# systemctl status  apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-04-03 04:11:51 PDT; 9min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 13002 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 13008 (apache2)
      Tasks: 55 (limit: 2244)
     Memory: 16.9M
        CPU: 96ms
     CGroup: /system.slice/apache2.service
             ├─13008 /usr/sbin/apache2 -k start
```

- ini.



Apache2 Debian Default Page

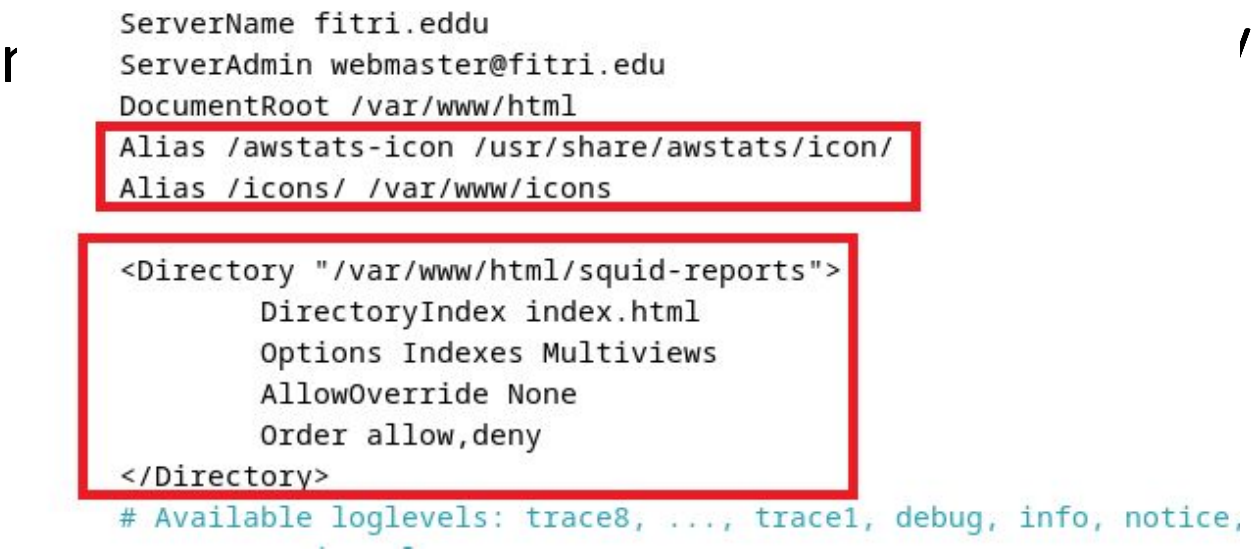
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the

- Ini adalah tanda virtual hosting telah bekerja.

- Sekarar 'www.fitri.edu.conf dan e



```
ServerName fitri.eddu
ServerAdmin webmaster@fitri.edu
DocumentRoot /var/www/html
Alias /awstats-icon /usr/share/awstats/icon/
Alias /icons/ /var/www/icons

<Directory "/var/www/html/squid-reports">
        DirectoryIndex index.html
        Options Indexes Multiviews
        AllowOverride None
        Order allow,deny
</Directory>
# Available loglevels: trace8, ..., trace1, debug, info, notice,
```

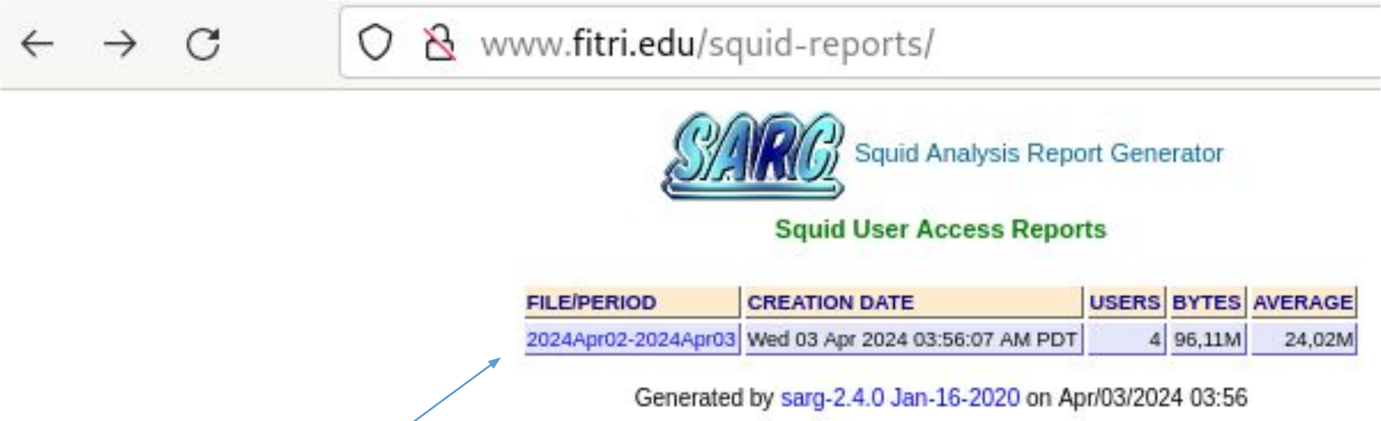
- Save dan exit

- Sekarang, reload dan restart apache2

```
#systemctl reload apache2
#systemctl restart apache2
 #systemctl status apache2
```

19. Buka browser, ketikkan http://www.fitri.edu/squid-reports

Keluar output berikut:



Squid Analysis Report Generator

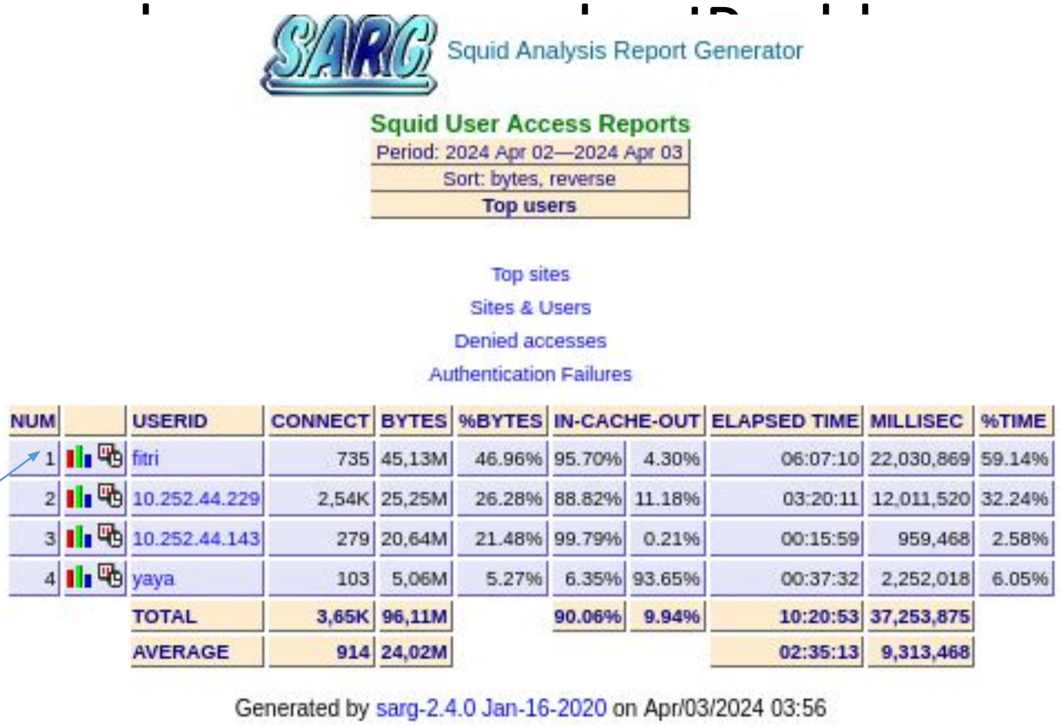
Squid User Access Reports

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2024Apr02-2024Apr03	Wed 03 Apr 2024 03:56:07 AM PDT	4	96,11M	24,02M

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56

- Klik salah satu link yang ditunjuk panah, maka akan muncul output berikut

- Na ng menggunakan proxy



Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sort: bytes, reverse

Top users

Top sites

Sites & Users

Denied accesses

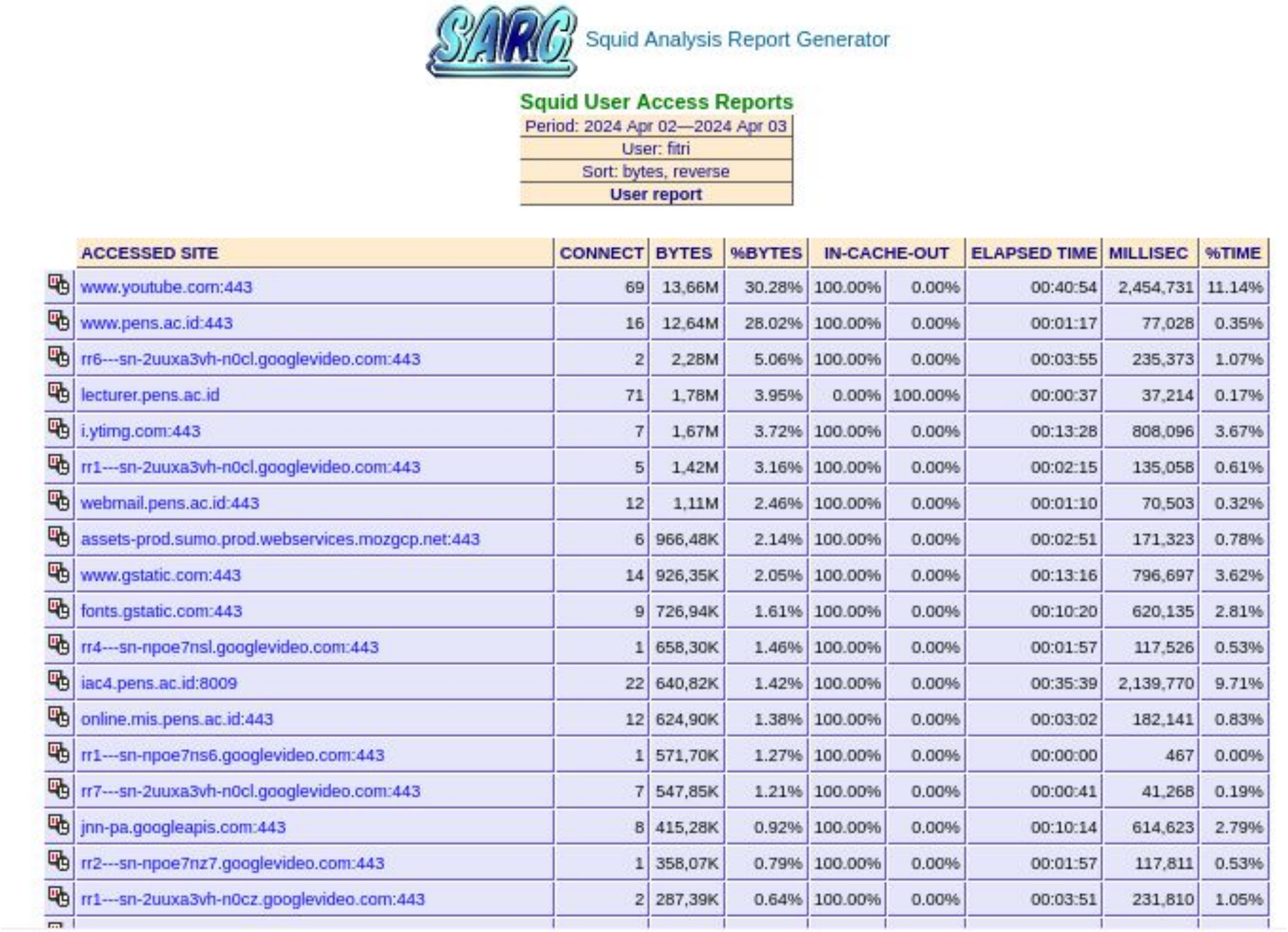
Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		fitri	735	45,13M	46.96%	95.70%	4.30%	06:07:10	22,030,869	59.14%
2		10.252.44.229	2,54K	25,25M	26.28%	88.82%	11.18%	03:20:11	12,011,520	32.24%
3		10.252.44.143	279	20,64M	21.48%	99.79%	0.21%	00:15:59	959,468	2.58%
4		yaya	103	5,06M	5.27%	6.35%	93.65%	00:37:32	2,252,018	6.05%
		TOTAL	**3,65K**	**96,11M**		**90.06%**	**9.94%**	**10:20:53**	**37,253,875**	
		AVERAGE	**914**	**24,02M**				**02:35:13**	**9,313,468**	

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56

Klik

- Semua website yang diakses oleh user fitri akan nampak di dashboard sarg



Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

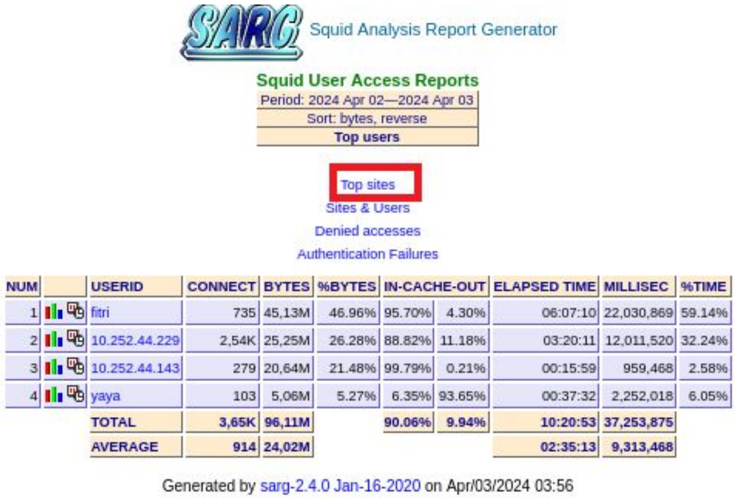
User: fitri

Sort: bytes, reverse

User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
www.youtube.com:443	69	13,66M	30.28%	100.00%	0.00%	00:40:54	2,454,731	11.14%
www.pens.ac.id:443	16	12,64M	28.02%	100.00%	0.00%	00:01:17	77,028	0.35%
rr6---sn-2uuxa3vh-n0cl.googlevideo.com:443	2	2,28M	5.06%	100.00%	0.00%	00:03:55	235,373	1.07%
lecturer.pens.ac.id	71	1,78M	3.95%	0.00%	100.00%	00:00:37	37,214	0.17%
i.ytimg.com:443	7	1,67M	3.72%	100.00%	0.00%	00:13:28	808,096	3.67%
rr1---sn-2uuxa3vh-n0cl.googlevideo.com:443	5	1,42M	3.16%	100.00%	0.00%	00:02:15	135,058	0.61%
webmail.pens.ac.id:443	12	1,11M	2.46%	100.00%	0.00%	00:01:10	70,503	0.32%
assets-prod.sumo.prod.webservices.mozgcp.net:443	6	966,48K	2.14%	100.00%	0.00%	00:02:51	171,323	0.78%
www.gstatic.com:443	14	926,35K	2.05%	100.00%	0.00%	00:13:16	796,697	3.62%
fonts.gstatic.com:443	9	726,94K	1.61%	100.00%	0.00%	00:10:20	620,135	2.81%
rr4---sn-npoe7nsl.googlevideo.com:443	1	658,30K	1.46%	100.00%	0.00%	00:01:57	117,526	0.53%
iac4.pens.ac.id:8009	22	640,82K	1.42%	100.00%	0.00%	00:35:39	2,139,770	9.71%
online.mis.pens.ac.id:443	12	624,90K	1.38%	100.00%	0.00%	00:03:02	182,141	0.83%
rr1---sn-npoe7ns6.googlevideo.com:443	1	571,70K	1.27%	100.00%	0.00%	00:00:00	467	0.00%
rr7---sn-2uuxa3vh-n0cl.googlevideo.com:443	7	547,85K	1.21%	100.00%	0.00%	00:00:41	41,268	0.19%
jnn-pa.googleapis.com:443	8	415,28K	0.92%	100.00%	0.00%	00:10:14	614,623	2.79%
rr2---sn-npoe7nz7.googlevideo.com:443	1	358,07K	0.79%	100.00%	0.00%	00:01:57	117,811	0.53%
rr1---sn-2uuxa3vh-n0cz.googlevideo.com:443	2	287,39K	0.64%	100.00%	0.00%	00:03:51	231,810	1.05%

- Sarg mampu menampilkan top accessed sites (situs terbanyak yang diakses user)



SARG Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sort: bytes, reverse

Top users

Top sites

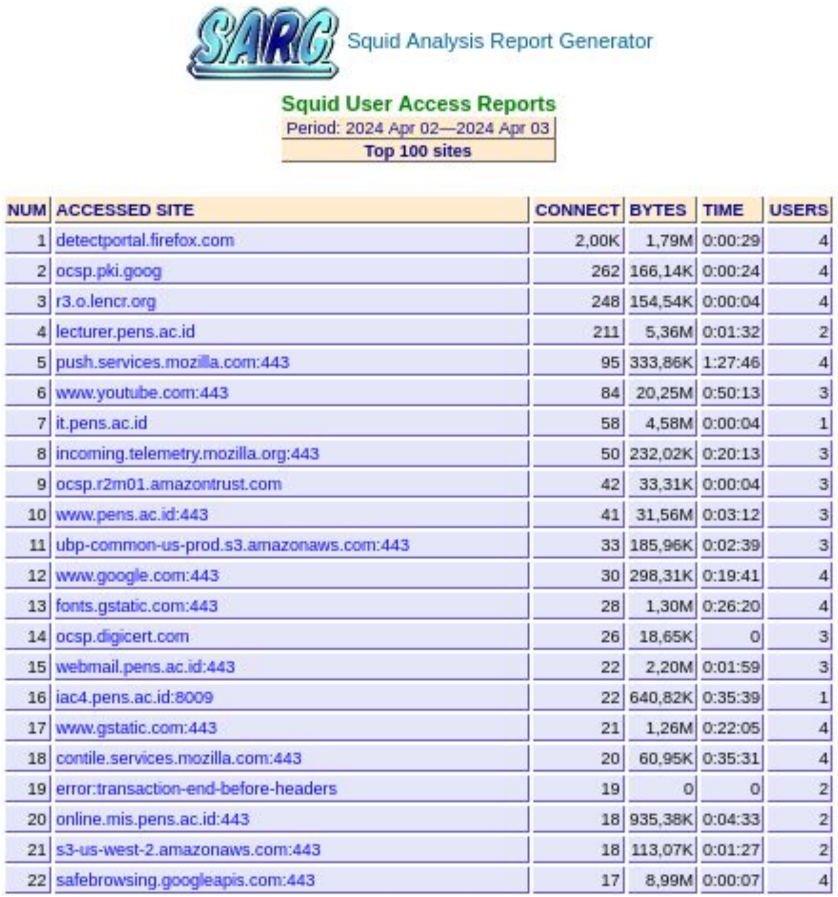
Sites & Users

Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		fitri	735	45,13M	46.96%	95.70%	4.30%	06:07:10	22,030,869	59.14%
2		10.252.44.229	2,54K	25,25M	26.28%	88.82%	11.18%	03:20:11	12,011,520	32.24%
3		10.252.44.143	279	20,64M	21.48%	99.79%	0.21%	00:15:59	959,468	2.58%
4		yaya	103	5,06M	5.27%	6.35%	93.65%	00:37:32	2,252,018	6.05%
		TOTAL	**3,65K**	**96,11M**		**90.06%**	**9.94%**	**10:20:53**	**37,253,875**	
		AVERAGE	**914**	**24,02M**				**02:35:13**	**9,313,468**	

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56



SARG Squid Analysis Report Generator

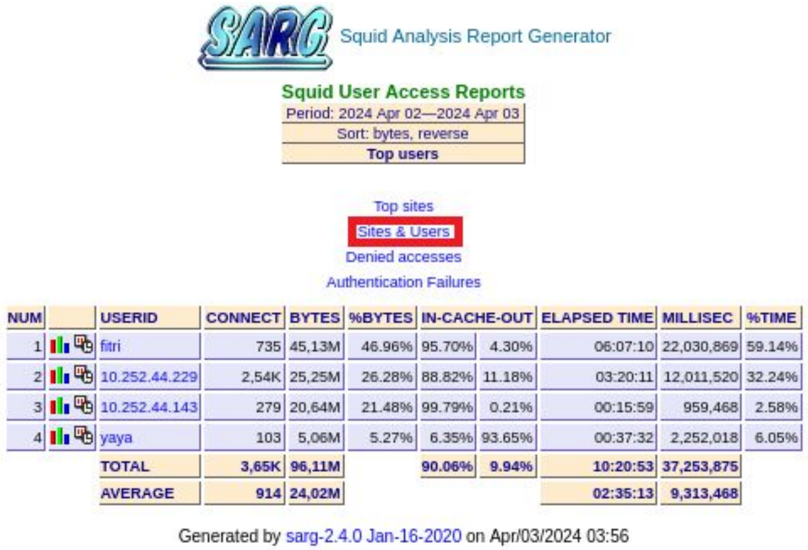
Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Top 100 sites

NUM	ACCESSED SITE	CONNECT	BYTES	TIME	USERS
1	detectportal.firefox.com	2,00K	1,79M	0:00:29	4
2	ocsp.pki.goog	262	166,14K	0:00:24	4
3	r3.o.lencr.org	248	154,54K	0:00:04	4
4	lecturer.pens.ac.id	211	5,36M	0:01:32	2
5	push.services.mozilla.com:443	95	333,86K	1:27:46	4
6	www.youtube.com:443	84	20,25M	0:50:13	3
7	it.pens.ac.id	58	4,58M	0:00:04	1
8	incoming.telemetry.mozilla.org:443	50	232,02K	0:20:13	3
9	ocsp.r2m01.amazontrust.com	42	33,31K	0:00:04	3
10	www.pens.ac.id:443	41	31,56M	0:03:12	3
11	ubp-common-us-prod.s3.amazonaws.com:443	33	185,96K	0:02:39	3
12	www.google.com:443	30	298,31K	0:19:41	4
13	fonts.gstatic.com:443	28	1,30M	0:26:20	4
14	ocsp.digicert.com	26	18,65K	0	3
15	webmail.pens.ac.id:443	22	2,20M	0:01:59	3
16	iac4.pens.ac.id:8009	22	640,82K	0:35:39	1
17	www.gstatic.com:443	21	1,26M	0:22:05	4
18	contile.services.mozilla.com:443	20	60,95K	0:35:31	4
19	error:transaction-end-before-headers	19	0	0	2
20	online.mis.pens.ac.id:443	18	935,38K	0:04:33	2
21	s3-us-west-2.amazonaws.com:443	18	113,07K	0:01:27	2
22	safebrowsing.googleapis.com:443	17	8,99M	0:00:07	4

- Sarg mampu menampilkan ser er berikut userny


Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sort: bytes, reverse

Top users

Top sites

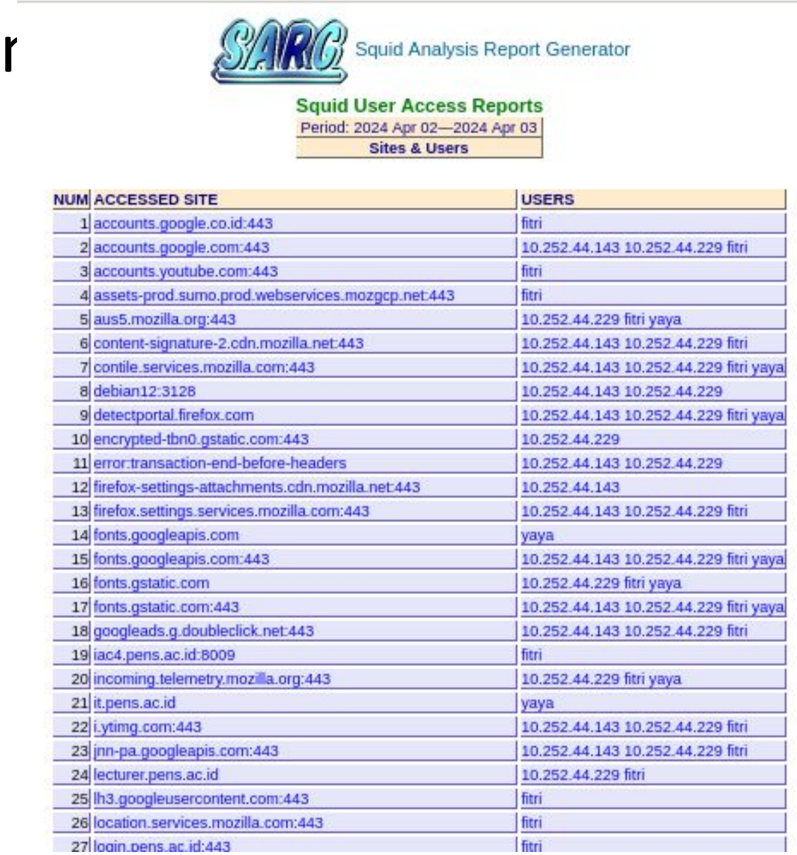
Sites & Users

Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		fitri	735	45,13M	46.96%	95.70%	4.30%	06:07:10	22,030,869	59.14%
2		10.252.44.229	2,54K	25,25M	26.28%	88.82%	11.18%	03:20:11	12,011,520	32.24%
3		10.252.44.143	279	20,64M	21.48%	99.79%	0.21%	00:15:59	959,468	2.58%
4		yaya	103	5,06M	5.27%	6.35%	93.65%	00:37:32	2,252,018	6.05%
		TOTAL	**3,65K**	**96,11M**		**90.06%**	**9.94%**	**10:20:53**	**37,253,875**	
		AVERAGE	**914**	**24,02M**				**02:35:13**	**9,313,468**	

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56


Squid Analysis Report Generator

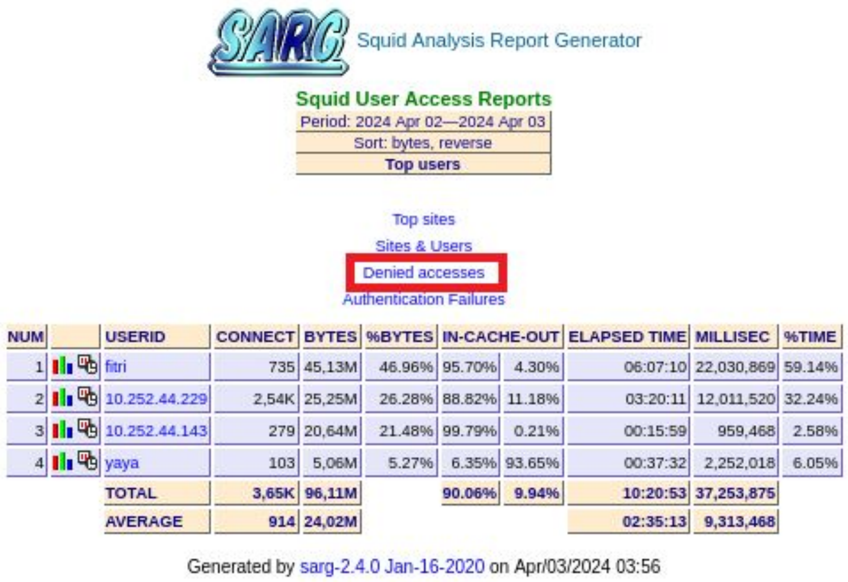
Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sites & Users

NUM	ACCESSED SITE	USERS
1	accounts.google.co.id:443	fitri
2	accounts.google.com:443	10.252.44.143 10.252.44.229 fitri
3	accounts.youtube.com:443	fitri
4	assets-prod.sumo.prod.webservices.mozgcp.net:443	fitri
5	aus5.mozilla.org:443	10.252.44.229 fitri yaya
6	content-signature-2.cdn.mozilla.net:443	10.252.44.143 10.252.44.229 fitri
7	contile.services.mozilla.com:443	10.252.44.143 10.252.44.229 fitri yaya
8	debian12:3128	10.252.44.143 10.252.44.229
9	detectportal.firefox.com	10.252.44.143 10.252.44.229 fitri yaya
10	encrypted-tbn0.gstatic.com:443	10.252.44.229
11	error:transaction-end-before-headers	10.252.44.143 10.252.44.229
12	firefox-settings-attachments.cdn.mozilla.net:443	10.252.44.143
13	firefox.settings.services.mozilla.com:443	10.252.44.143 10.252.44.229 fitri
14	fonts.googleapis.com	yaya
15	fonts.googleapis.com:443	10.252.44.143 10.252.44.229 fitri yaya
16	fonts.gstatic.com	10.252.44.229 fitri yaya
17	fonts.gstatic.com:443	10.252.44.143 10.252.44.229 fitri yaya
18	googleads.g.doubleclick.net:443	10.252.44.143 10.252.44.229 fitri
19	iac4.pens.ac.id:8009	fitri
20	incoming.telemetry.mozilla.org:443	10.252.44.229 fitri yaya
21	it.pens.ac.id	yaya
22	i.ytimg.com:443	10.252.44.143 10.252.44.229 fitri
23	jnn-pa.googleapis.com:443	10.252.44.143 10.252.44.229 fitri
24	lecturer.pens.ac.id	10.252.44.229 fitri
25	lh3.googleusercontent.com:443	fitri
26	location.services.mozilla.com:443	fitri
27	login.pens.ac.id:443	fitri

- Sarg mampu menampilkan semua host yang pernah diblok
- Kita pernah mengeblok network address 10.252.44.0/24



Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sort: bytes, reverse

Top users

Top sites

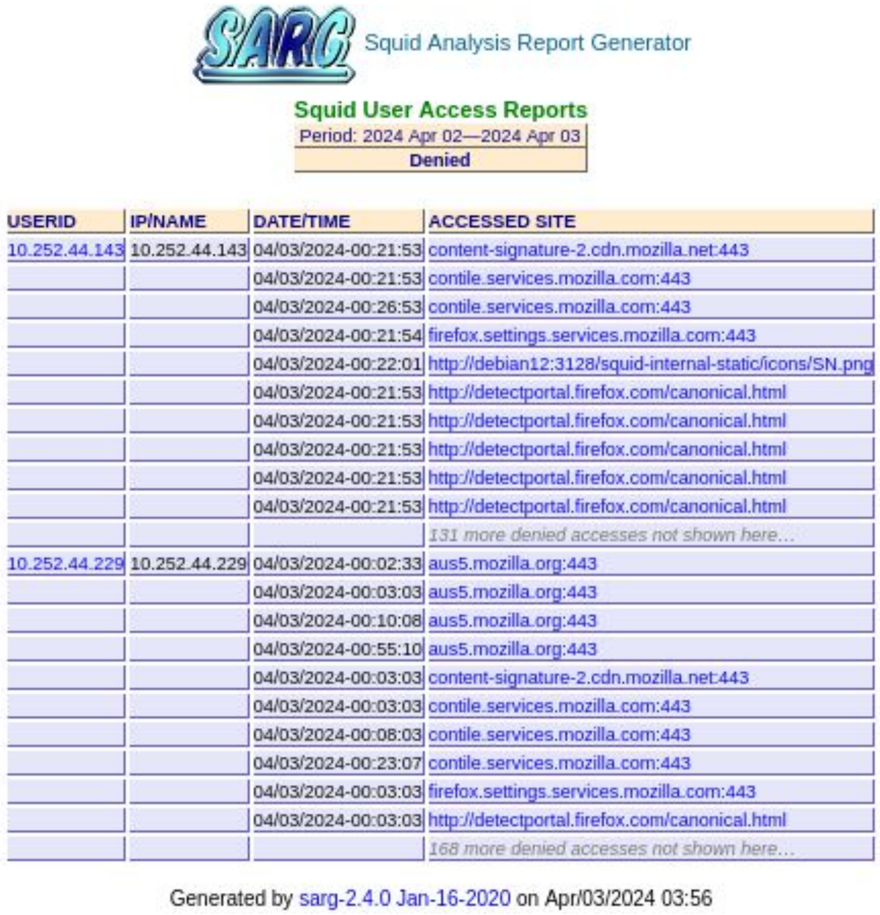
Sites & Users

Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		fitri	735	45,13M	46.96%	95.70%	4.30%	06:07:10	22,030,869	59.14%
2		10.252.44.229	2,54K	25,25M	26.28%	88.82%	11.18%	03:20:11	12,011,520	32.24%
3		10.252.44.143	279	20,64M	21.48%	99.79%	0.21%	00:15:59	959,468	2.58%
4		yaya	103	5,06M	5.27%	6.35%	93.65%	00:37:32	2,252,018	6.05%
		TOTAL	**3,65K**	**96,11M**		**90.06%**	**9.94%**	**10:20:53**	**37,253,875**	
		AVERAGE	**914**	**24,02M**				**02:35:13**	**9,313,468**	

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56



Squid Analysis Report Generator

Squid User Access Reports

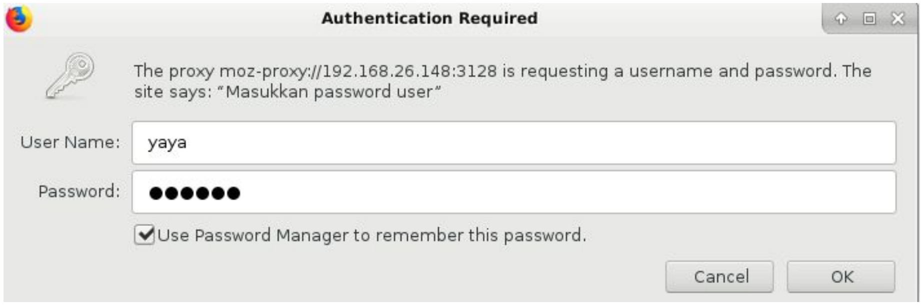
Period: 2024 Apr 02—2024 Apr 03

Denied

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
10.252.44.143	10.252.44.143	04/03/2024-00:21:53	content-signature-2.cdn.mozilla.net:443
		04/03/2024-00:21:53	contile.services.mozilla.com:443
		04/03/2024-00:26:53	contile.services.mozilla.com:443
		04/03/2024-00:21:54	firefox.settings.services.mozilla.com:443
		04/03/2024-00:22:01	http://debian12:3128/squid-internal-static/icons/SN.png
		04/03/2024-00:21:53	http://detectportal.firefox.com/canonical.html
		04/03/2024-00:21:53	http://detectportal.firefox.com/canonical.html
		04/03/2024-00:21:53	http://detectportal.firefox.com/canonical.html
		04/03/2024-00:21:53	http://detectportal.firefox.com/canonical.html
		04/03/2024-00:21:53	http://detectportal.firefox.com/canonical.html
			131 more denied accesses not shown here…
10.252.44.229	10.252.44.229	04/03/2024-00:02:33	aus5.mozilla.org:443
		04/03/2024-00:03:03	aus5.mozilla.org:443
		04/03/2024-00:10:08	aus5.mozilla.org:443
		04/03/2024-00:55:10	aus5.mozilla.org:443
		04/03/2024-00:03:03	content-signature-2.cdn.mozilla.net:443
		04/03/2024-00:03:03	contile.services.mozilla.com:443
		04/03/2024-00:08:03	contile.services.mozilla.com:443
		04/03/2024-00:23:07	contile.services.mozilla.com:443
		04/03/2024-00:03:03	firefox.settings.services.mozilla.com:443
		04/03/2024-00:03:03	http://detectportal.firefox.com/canonical.html
			168 more denied accesses not shown here…

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56

- Sarg mampu menampilkan semua otentikasi yang error karena passwor
- Untuk ini, anda bisa mencoba dengan memasukkan password yang salah proxy
- Masukkan password yang salah untuk user yaya



Authentication Required

The proxy moz-proxy://192.168.26.148:3128 is requesting a username and password. The site says: "Masukkan password user"

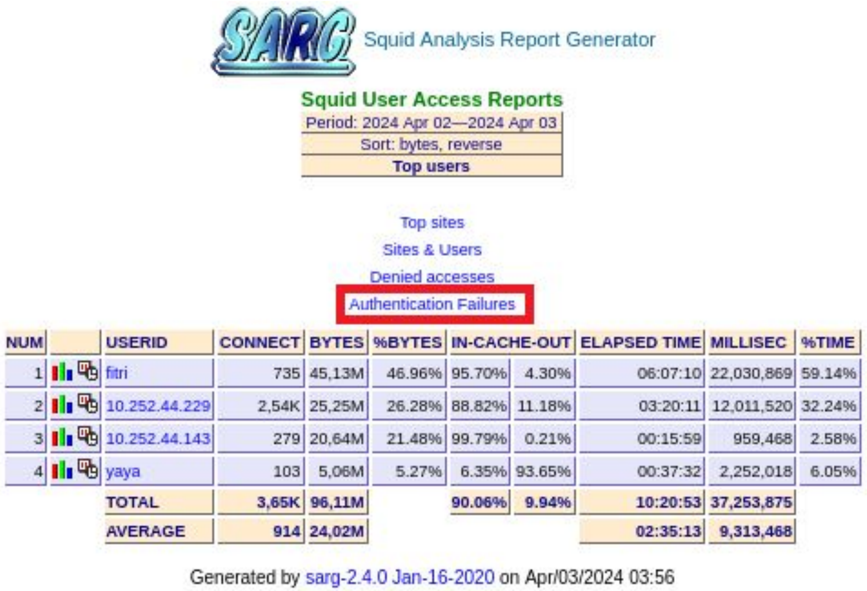
User Name: yaya

Password: ●●●●●●

☑ Use Password Manager to remember this password.

Untuk menampilkan semua kesalahan otentikasi , klik Authenticated Failures

Tampak user yaya pernah melakukan kesalahan otentikasi



Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Sort: bytes, reverse

Top users

Top sites

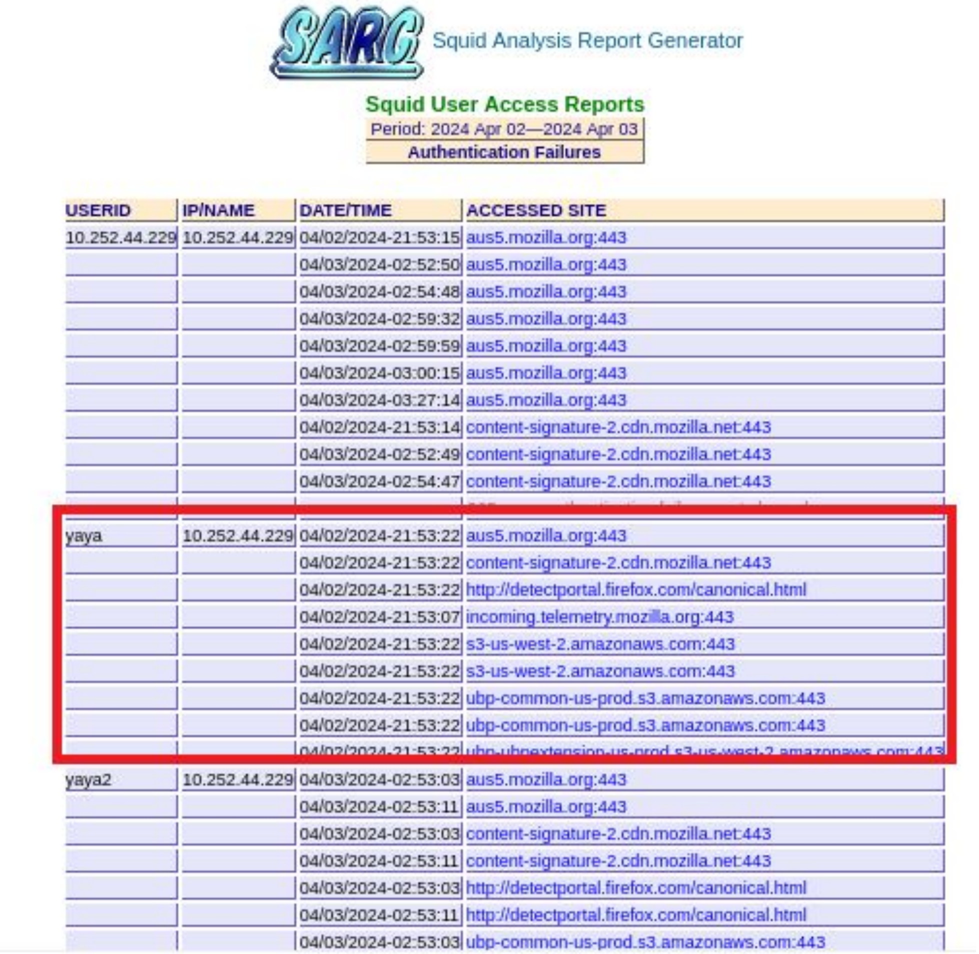
Sites & Users

Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		fitri	735	45,13M	46.96%	95.70%	4.30%	06:07:10	22,030,869	59.14%
2		10.252.44.229	2,54K	25,25M	26.28%	88.82%	11.18%	03:20:11	12,011,520	32.24%
3		10.252.44.143	279	20,64M	21.48%	99.79%	0.21%	00:15:59	959,468	2.58%
4		yaya	103	5,06M	5.27%	6.35%	93.65%	00:37:32	2,252,018	6.05%
		TOTAL	**3,65K**	**96,11M**		**90.06%**	**9.94%**	**10:20:53**	**37,253,875**	
		AVERAGE	**914**	**24,02M**				**02:35:13**	**9,313,468**	

Generated by sarg-2.4.0 Jan-16-2020 on Apr/03/2024 03:56



Squid Analysis Report Generator

Squid User Access Reports

Period: 2024 Apr 02—2024 Apr 03

Authentication Failures

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
10.252.44.229	10.252.44.229	04/02/2024-21:53:15	aus5.mozilla.org:443
		04/03/2024-02:52:50	aus5.mozilla.org:443
		04/03/2024-02:54:48	aus5.mozilla.org:443
		04/03/2024-02:59:32	aus5.mozilla.org:443
		04/03/2024-02:59:59	aus5.mozilla.org:443
		04/03/2024-03:00:15	aus5.mozilla.org:443
		04/03/2024-03:27:14	aus5.mozilla.org:443
		04/02/2024-21:53:14	content-signature-2.cdn.mozilla.net:443
		04/03/2024-02:52:49	content-signature-2.cdn.mozilla.net:443
		04/03/2024-02:54:47	content-signature-2.cdn.mozilla.net:443
		[illegible]	[illegible]
yaya	10.252.44.229	04/02/2024-21:53:22	aus5.mozilla.org:443
		04/02/2024-21:53:22	content-signature-2.cdn.mozilla.net:443
		04/02/2024-21:53:22	http://detectportal.firefox.com/canonical.html
		04/02/2024-21:53:07	incoming.telemetry.mozilla.org:443
		04/02/2024-21:53:22	s3-us-west-2.amazonaws.com:443
		04/02/2024-21:53:22	s3-us-west-2.amazonaws.com:443
		04/02/2024-21:53:22	ubp-common-us-prod.s3.amazonaws.com:443
		04/02/2024-21:53:22	ubp-common-us-prod.s3.amazonaws.com:443
		04/02/2024-21:53:22	ubp-ubpextension-us-prod.s3-us-west-2.amazonaws.com:443
yaya2	10.252.44.229	04/03/2024-02:53:03	aus5.mozilla.org:443
		04/03/2024-02:53:11	aus5.mozilla.org:443
		04/03/2024-02:53:03	content-signature-2.cdn.mozilla.net:443
		04/03/2024-02:53:11	content-signature-2.cdn.mozilla.net:443
		04/03/2024-02:53:03	http://detectportal.firefox.com/canonical.html
		04/03/2024-02:53:11	http://detectportal.firefox.com/canonical.html
		04/03/2024-02:53:03	ubp-common-us-prod.s3.amazonaws.com:443

Sumber :

https://www.tecmint.com/sarg-squid-analysis-report-generator-and-internet
oring-tool/

Daftar Pustaka

- https://www.linuxtechi.com/setup-rsyslog-server-on-debian/
- https://linuxhandbook.com/syslog-guide/
- https://adamtheautomator.com/rsyslog-configuration/
- https://www.loggly.com/use-cases/rsyslog-manual-configuration-and-troubleshooting/
- https://www.gilesorr.com/blog/rsyslog-filtering.html
- https://www.gilesorr.com/blog/rsyslog-facility-severity.html
- https://www.howtoforge.com/how-to-setup-rsyslog-server-on-debian-11/

- https://medium.com/@matteo.mattei/monitor-ssh-access-and-send-email-when-someone-logins-f269830dda33
- https://devconnected.com/monitoring-linux-logs-with-kibana-and-rsyslog/
- https://www.redhat.com/sysadmin/log-aggregation-rsyslog
- https://www.linuxtechi.com/manage-linux-log-files-using-logrotate/