

tags: Work

DHCP

Dynamic Host Configuration Protocol

RFC 2131 (<https://datacenter.ietf.org/doc/html/rfc2131>) - The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network.

- 主要功能是讓主機在可以傳送廣播Packet 的網路架構上，運用自己的 MAC Address 藉由網路的廣播位址，向DHCP Server 取得有關IP Address、Network、Mask、Default Gateway、DNS等設定訊息。
- DHCP Server 與 Client 要在相同的Broadcast domain

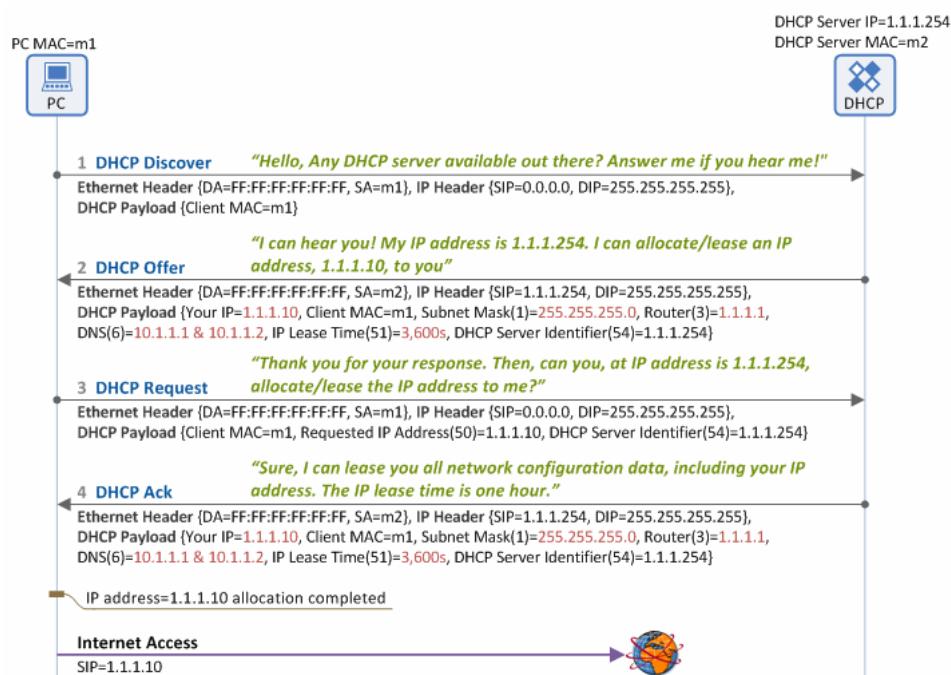
Basic Phases

必看: IP Address Allocation/Lease Procedure

(<https://www.netmanias.com/en/post/techdocs/5998/dhcp-network-protocol/understanding-the-basic-operations-of-dhcp>).

DHCP phases ppt (https://www.cyut.edu.tw/~hcchu/course/MAN_95A/MANCh08.pdf)

As shown in Figure below, the following **four basic phases** are required in DHCP operations between a DHCP server and DHCP client (e.g. a PC) in order for the client to get/lease network configuration data, such as IP address from the DHCP server.



DHCP Discover

要求租用 IP 位址 (DHCP Client 端會傳送 DHCPDISCOVER 封包).

當我們將電腦設定成 DHCP 用戶端後, 第一次啟動電腦時即會進入此階段。

首先由 DHCP 用戶端廣播一個 DHCP Discover (尋找) 封包, 要求任一部 DHCP 伺服器提供 IP 租約。

► Details

DHCP Offer

提供可租用的 IP 位址 (DHCP Server 端會透過傳送 DHCPOFFER 封包來回應).

因為 DHCP Discover 是以廣播方式送出, 所以網路上所有的 DHCP 伺服器都會收到此封包, 而每一台 DHCP 伺服器收到此封包時, 都會從本身的領域中, 找出一個可用的 IP 位址, 設定租約期限後記錄在 DHCP Offer (提議) 封包, 再以廣播方式送給用戶端。

► Details

DHCP Request

確認 IP 租約 (DHCP Client 端會藉由傳送 DHCPREQUEST 來回應 DHCPOFFER).

因為每一台 DHCP 伺服器都會送出 DHCP Offer 封包, 因此 DHCP 用戶端會收到多個 DHCP Offer 封包, 用戶端預設會接受最先收到的 DHCP Offer 封包, 其他陸續收到的 DHCP Offer 封包則不予理會。

用戶端接著以廣播方式送出 DHCP Request (要求) 封包, 除了向選定的伺服器申請租用 IP 位址之外, 也讓其他曾送出 DHCP Offer 封包、但未中選的伺服器知道落選了, 可以租用給其它的用戶端。

► Details

DHCP Ack

同意 IP 租約

當被選中的 DHCP 伺服器收到 DHCP Request 封包時, 假如同意用戶端的租用要求, 便會廣播 DHCP Ack(承認) 封包給 DHCP 用戶端, 告知可以將設定值寫入 TCP/IP 中, 並開始計算租用的時間。

倘若DHCP 伺服器不能給予 DHCP 用戶端所要求的資訊 (例如：要求租用的 IP 已被佔用， 或者不能給予用戶端所要求的租約期限等)， 則會發出 DHCP Nack (拒絕承認) 封包。當用戶端收到 DHCP Nack 封包時， 便直接回到第一階段，重新執行整個流程。

► Details

Example

```
gavin@svrdhcp:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2021-12-12 00:43:12 CST; 4min 2s ago
     Docs: man:dhcpd(8)
    Main PID: 5551 (dhcpd)
      Tasks: 4 (limit: 4639)
     Memory: 4.4M
    CGroup: /system.slice/isc-dhcp-server.service
            └─5551 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhc

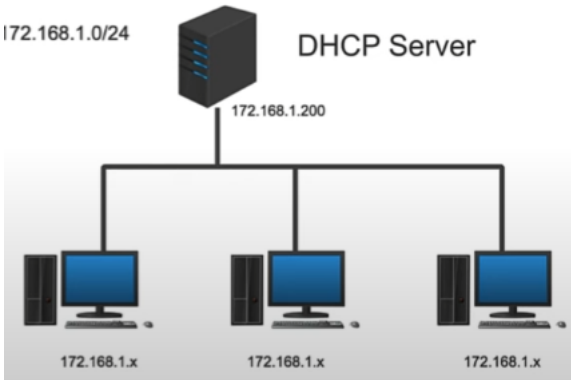
+-- 12 00:43:12 svrdhcp sh[5551]: Sending on LPF/enp0s3/08:00:27:6a:c9:27/172.168.1.0/24
+-- 12 00:43:12 svrdhcp sh[5551]: Sending on Socket/fallback/fallback-net
+-- 12 00:43:12 svrdhcp dhcpd[5551]: Sending on LPF/enp0s3/08:00:27:6a:c9:27/172.168.1.0/24
+-- 12 00:43:12 svrdhcp dhcpd[5551]: Sending on Socket/fallback/fallback-net
+-- 12 00:43:12 svrdhcp dhcpd[5551]: Server starting service.
+-- 12 00:44:08 svrdhcp dhcpd[5551]: DHCPREQUEST for 172.168.1.80 from 08:00:27:2d:d0:93 via enp0s3
+-- 12 00:44:10 svrdhcp dhcpd[5551]: DHCPDISCOVER from 08:00:27:2d:d0:93 via enp0s3
+-- 12 00:44:11 svrdhcp dhcpd[5551]: DHCPOFFER on 172.168.1.81 to 08:00:27:2d:d0:93 (gavin-VirtualB
+-- 12 00:44:11 svrdhcp dhcpd[5551]: DHCPREQUEST for 172.168.1.81 (172.168.1.200) from 08:00:27:2d:
+-- 12 00:44:11 svrdhcp dhcpd[5551]: DHCPACK on 172.168.1.81 to 08:00:27:2d:d0:93 (gavin-VirtualBox
```

Install DHCP server

看這個影片 Setup DHCP Server in Ubuntu Server 20.04

(https://www.youtube.com/watch?v=Q7v4pzQReuo&ab_channel=ErrorAndFix)

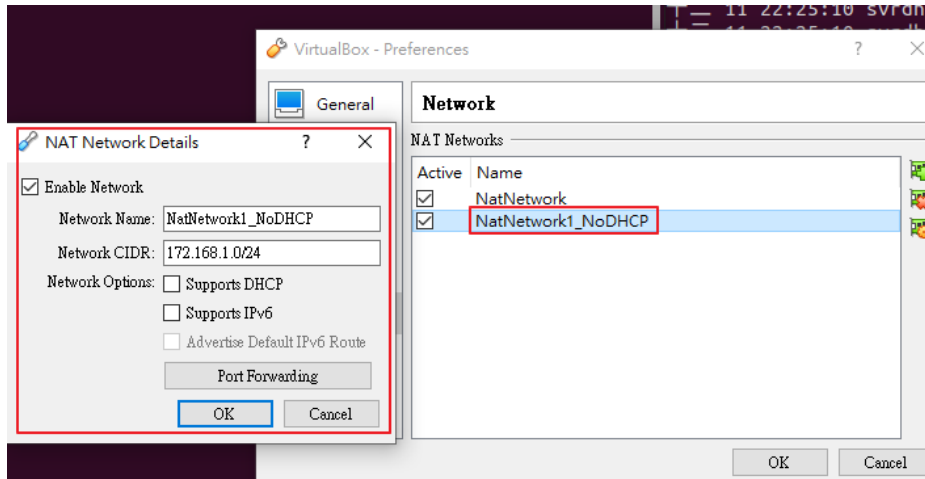
- DHCP Server 架構圖



自己實驗架構:

	DHCP Server	DHCP Client
IP	172.168.1.200	172.168.1.80
MAC	08:00:27:6a:c9:27	08:00:27:2d:d0:93

- 設定 NAT Network, 網卡設定如下



Step 1

```
sudo vim /etc/netplan/00-installer-config.yaml
sudo netplan generate
sudo netplan apply
```

- To use a static IP address 172.168.1.200, I will change the file so that it looks like this afterward:

```
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [172.168.1.200/24]
      gateway4: 172.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Step 2

```
sudo vim /etc/hosts
```

```
127.0.0.1    localhost
127.0.1.1    gavin-VirtualBox
172.168.1.200 svrdhcp.abc.local

# The following lines are desirable for IPv6 capable hosts
::1         ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

- Now, we will change the hostname of our machine as follows:

```
sudo echo svrdhcp /etc/hostname
sudo hostname svrdhcp
```

Step 3

Install a DHCP server:

```
sudo apt-get install isc-dhcp-server
sudo vim /etc/default/isc-dhcp-server
sudo vim /etc/dhcp/dhcpd.conf
```

Add the following lines at the end of the file (replace the IP address to match your network):

```
subnet 172.168.1.0 netmask 255.255.255.0 {
    range 172.168.1.80 172.168.1.90;
    option routers 172.168.1.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option domain-name "abc.local";
}
```

Change the default and max lease time if necessary:

```
default-lease-time 600; #預設租約為 10 分鐘 (單位是 sec)
max-lease-time 7200; #最大租約為 2 小時
```

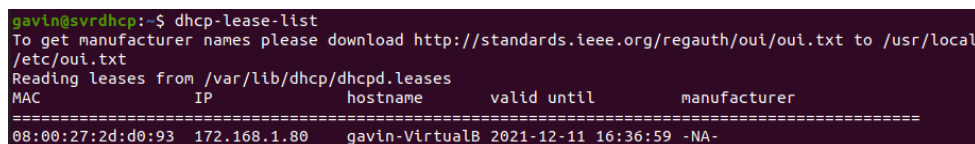
完成

systemctl restart isc-dhcp-server 後即可分配 DHCP IP.

列出分配的dhcp地址的命令

- dhcp-lease-list

```
dhcp-lease-list [options]
```



```
gavin@svrdhcp:~$ dhcp-lease-list
To get manufacturer names please download http://standards.ieee.org/regauth/oui/oui.txt to /usr/local/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
=====
MAC                IP            hostname      valid until    manufacturer
-----
08:00:27:2d:d0:93  172.168.1.80  gavin-VirtualB 2021-12-11 16:36:59 -NA-
```

- lease time 租賃時間
DHCP server用來決定一個 IP address在使用多久之後，就將這個IP回收，轉發給其它的 Client。

- **dhcp-leases** (<https://pypi.org/project/dhcp-leases/>) python library
/var/lib/dhcp/dhcpd.leases

```
1 from dhcp_leases import DhcpLeases
2
3 leases = DhcpLeases('/var/lib/dhcp/dhcpd.leases')
4 leases.get() # Returns the leases as a list of Lease objects
5 dic = leases.get_current() # Returns only the currently valid dhcp leases as dict
6                               # The key of the dict is the device mac address and the
7                               # Value is a Lease object
8 print(dic)
```

Option 66/67

Setting Options 66 and 67 for ISC DHCP Server

(<https://askubuntu.com/questions/874648/setting-options-66-and-67-for-isc-dhcp-server>)

```
sudo vim /etc/dhcp/dhcpd.conf
```

and to add the following entries for activating the option 66 and 67.

```
#option 66
option tftp-server-name "dhcp.server";

#option 67
option bootfile-name "test.cfg";
```

KEA

Kea Administrator Reference Manual

(<https://ftp.stu.edu.tw/Unix/isc/kea/1.7.0/doc/kea-arm.pdf>).

<6.4>

The following commands are supported by keactrl:

- start - starts selected servers.
- stop - stops all running servers.
- reload - triggers reconfiguration of the selected servers by sending the SIGHUP signal to them.
- status - returns the status of the servers (active or inactive) and the names of the configuration files in use.
- version - prints out the version of the keactrl tool itself, together with the versions of the Kea daemons.

Other

journalctl

Systemd Journal有提供一個管理工具 **journalctl**

(<https://qastack.cn/unix/225401/how-to-see-full-log-from-systemctl-status-service>), 我們可以藉由 journalctl 對 Log 進行搜尋。

journalctl 可用於檢索 systemd 日誌(由 systemd-journald.service 記錄)

```
journalctl -u <service-name.service>
```

ex: journalctl -u isc-dhcp-server

FTP

Could find three different TFTP servers:

1. tftpd
2. atftpd
3. tftpd-hpa

[2021.12.19]

FTP parse log ref:

1. <https://gist.github.com/leandrosilva/3651640>

(<https://gist.github.com/leandrosilva/3651640>).

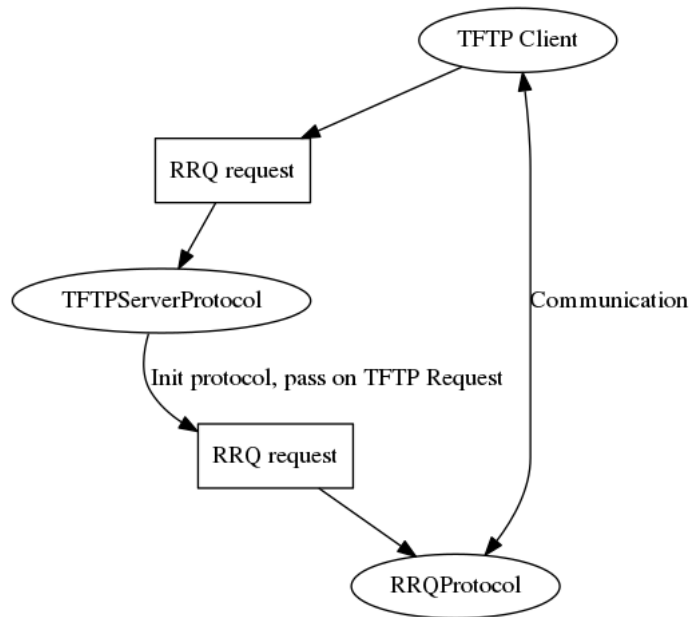
2. <https://github.com/dogoncouch/logdissect>

(<https://github.com/dogoncouch/logdissect>).

DHCP:

The Top 33 Python Dhcp Open Source Projects on Github

(<https://awesomeopensource.com/projects/dhcp/python?categoryPage=11>).



AFTP

Howto Setup advanced TFTP server in Ubuntu

(<https://www.ubuntuugreek.com/howto-setup-advanced-tftp-server-in-ubuntu.html>).

```
sudo apt install atftp atftpd
sudo vim /etc/default/atftpd
```

Setting

参考設定: (<http://myhomelab.blogspot.com/2014/10/installing-tftp-server-atftpd-in-linux.html>).

```
USE_INETD=false
# OPTIONS below are used only with init script
OPTIONS="--tftpd-timeout 300 --retry-timeout 5 --mcast-port 1758 --mcast-addr 239.239.239.239"
```

Make changes to run as a server directly, not through inetd (default)

```
USE_INETD=false
```

Touch /var/log/atftpd.log and set permissions accordingly

```
sudo touch /var/log/atftpd.log
sudo chmod 644 /var/log/atftpd.log
```

Increase logging level by setting to --verbose=7 to capture all messages

Message

Success sent file aa.txt

```
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: socket may listen on any address,
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: Creating new socket: 172.168.1.206
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: Serving aa.txt to 172.168.1.81:35:
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: will do netascii conversion
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: End of transfer
Dec 19 17:02:02 svrdhcp atftpd[6487.140369684129536]: Server thread exiting
```

Failed sent file bb.txt

```
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: socket may listen on any address,
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: Creating new socket: 172.168.1.206
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: Serving bb.txt to 172.168.1.81:58:
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: will do netascii conversion
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: File /srv/tftp/bb.txt not found
Dec 19 17:04:42 svrdhcp atftpd[6487.140369684129536]: Server thread exiting
```

Interrupt sent

```
Dec 19 17:13:14 svrdhcp atftpd[6487.140369684129536]: socket may listen on any address,
Dec 19 17:13:14 svrdhcp atftpd[6487.140369684129536]: Creating new socket: 172.168.1.206
Dec 19 17:13:14 svrdhcp atftpd[6487.140369684129536]: Serving aa.deb to 172.168.1.81:36:
Dec 19 17:13:14 svrdhcp atftpd[6487.140369684129536]: will do netascii conversion
Dec 19 17:13:21 svrdhcp atftpd[6487.140369684129536]: timeout: retrying...
Dec 19 17:13:26 svrdhcp atftpd[6487.140369684129536]: timeout: retrying...
Dec 19 17:13:31 svrdhcp atftpd[6487.140369684129536]: timeout: retrying...
Dec 19 17:13:36 svrdhcp atftpd[6487.140369684129536]: timeout: retrying...
Dec 19 17:13:41 svrdhcp atftpd[6487.140369684129536]: timeout: retrying...
Dec 19 17:13:46 svrdhcp atftpd[6487.140369684129536]: client (172.168.1.81) not responding
Dec 19 17:13:46 svrdhcp atftpd[6487.140369684129536]: End of transfer
Dec 19 17:13:46 svrdhcp atftpd[6487.140369684129536]: Server thread exiting
```

TFTP

Trivial File Transfer Protocol 簡單檔案傳輸協定

Install in Ubuntu (<https://yulun.me/2016/setup-tftp-server-on-ubuntu/>)

Server-Step

1.先安裝好相關套件

```
sudo apt install xinetd tftpd tftp
```

2.新增一組設定檔，放置於 /etc/xinetd.d/tftp


```

service tftp
{
    protocol      = udp
    port          = 69
    socket_type   = dgram
    wait          = yes
    user          = nobody
    server        = /usr/sbin/in.tftpd
    server_args   = /tftpboot
    disable       = no
}

```

#-c: Allow new files to be created

#-s: Change root directory on startup.

#-l: Run the server in standalone (listen) mode, rather than run from inetd.

3.新增 /tftpboot 資料夾，並且修改權限

```

sudo mkdir /tftpboot
sudo chmod -R 777 /tftpboot
sudo chown -R nobody /tftpboot

```

4.將 xinetd 重新啟動

```
sudo service xinetd restart
```

PROBLEM

啟動 error 的話，下面這個原因是缺少 /usr/sbin/in.tftpd 這個文件

```

gavin@svrdhcp:~$ sudo service xinetd status
● xinetd.service - LSB: Starts or stops the xinetd daemon.
   Loaded: loaded (/etc/init.d/xinetd; generated)
   Active: active (running) since Wed 2021-12-15 21:43:45 CST; 3s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 6969 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 4638)
   Memory: 364.0K
    CGroup: /system.slice/xinetd.service
            └─6979 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6

+-- 15 21:43:45 svrdhcp xinetd[6979]: Reading included configuration file: /etc/xinetd.d/servers [fil>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Reading included configuration file: /etc/xinetd.d/services [fi>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Reading included configuration file: /etc/xinetd.d/tftp [file=>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Server /usr/sbin/in.tftpd is not executable [file=/etc/xinetd.d>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Error parsing attribute server - DISABLING SERVICE [file=/etc/>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Reading included configuration file: /etc/xinetd.d/time [file=>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Reading included configuration file: /etc/xinetd.d/time-udp [fi>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Must specify a server in tftp
+-- 15 21:43:45 svrdhcp xinetd[6979]: 2.3.15.3 started with libwrap loadavg labeled-networking option>
+-- 15 21:43:45 svrdhcp xinetd[6979]: Started working: 0 available services

```

Client

```

tftp 172.168.1.200
tftp> get test

```

```

gavin@gavin-VirtualBox:~$ tftp 172.168.1.200
tftp> get aa.txt
Received 14 bytes in 0.0 seconds
tftp>

```

How to input variables in logger formatter? -Ref

(<https://stackoverflow.com/questions/16203908/how-to-input-variables-in-logger-formatter>).

```
1 import logging
2
3 MYVAR = 'gavin'
4
5 class ContextFilter(logging.Filter):
6     """
7     This is a filter which injects contextual information into the log.
8     """
9     def filter(self, record):
10         record.MYVAR = MYVAR
11         return True
12
13 FORMAT = '%(MYVAR)s %(asctime)s - %(levelname)s - %(message)s'
14 logging.basicConfig(format=FORMAT, datefmt='%d/%m/%Y %H:%M:%S')
15
16 logger = logging.getLogger(__name__)
17 logger.addFilter(ContextFilter())
18
19 logger.warning("'Twas brillig, and the slithy toves")
```

Logrotate

logrotate is designed to ease administration of systems that generate large numbers of log files. It allows automatic rotation, compression, removal, and mailing of log files. Each log file may be handled daily, weekly, monthly, or when it grows too large.

原理

linux 日誌切割神器logrotate 原理介紹和配置詳解

(<https://wsgzao.github.io/post/logrotate/>).

logrotate 是怎麼做到切換日誌時不影響程序正常的日誌輸出呢？

logrotate 提供了兩種解決方案。

1. create

- (a). 重命名正在輸出日誌文件，因為重命名只修改目錄以及文件的名稱，而進程操作文件使用的是inode，所以並不影響原程序繼續輸出日誌。
- (b). 創建新的日誌文件，文件名和原日誌文件一樣，注意，此時只是文件名稱一樣，而inode 編號不同，原程序輸出的日誌還是往原日誌文件輸出。
- (c). 最後通過某些方式通知程序，重新打開日誌文件；由於重新打開日誌文件會用到文件路徑而非inode 編號，所以打開的是新的日誌文件。

2. copytruncate

該方案是把正在輸出的日誌拷(copy) 一份出來，再清空(truncate) 原來的日誌；詳細步驟如下：

- (a).將當前正在輸出的日誌文件複製為目標文件，此時程序仍然將日誌輸出到原來文件中，此時，原文件名也沒有變。
- (b).清空日誌文件，原程序仍然還是輸出到預案日誌文件中，因為清空文件只把文件的內容刪除了，而inode 並沒改變，後續日誌的輸出仍然寫入該文件中。

Linux 文件操作機制

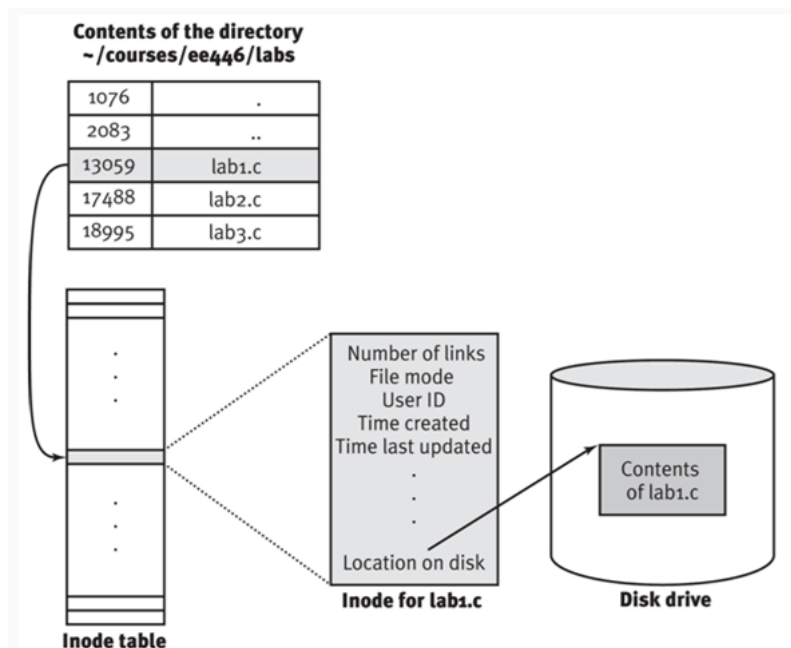
Linux 文件系統里文件和文件名的關係如下圖。

目錄也是文件，文件裡存著文件名和對應的inode 編號。通過這個inode 編號可以查到文件的元數據和文件內容。文件的元數據有引用計數、操作權限、擁有者ID、創建時間、最後修改時間等等。

```
gavin@svrdhcp: /var/log/atftpd$ stat atftpd.log
File: atftpd.log
Size: 0          Blocks: 0          IO Block: 4096   regular empty file
Device: 805h/2053d Inode: 2359331     Links: 1
Access: (0777/-rwxrwxrwx)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2022-01-16 00:00:22.117322174 +0800
Modify: 2022-01-16 00:00:22.117322174 +0800
Change: 2022-01-16 00:00:22.117322174 +0800
Birth: -
```

文件文件名並不在元數據里而是在目錄文件中。因此文件改名、移動，都不會修改文件，而是修改目錄文件

。



運行logrotate

具體logrotate 命令格式如下：

```
logrotate [OPTION...] <configfile>
-d, --debug : debug 模式，測試配置文件是否有錯誤。
-f, --force : 強制轉儲文件。
-m, --mail=command : 壓縮日誌後，發送日誌到指定郵箱。
-s, --state=statefile : 使用指定的狀態文件。
-v, --verbose : 顯示轉儲過程。
```

setting

2022.1.12

云计算网络安全学习教程：Logrotate日志轮转

(<https://www.bilibili.com/video/BV1Lp411d7Zz/>)

寫好的 atftp logrotate 規則放在 /etc/logrotate.d 這個資料夾下

```
/var/log/atftp/atftpd.log {
    missingok #error is ok
    # monthly
    size 30k
    daily
    rotate 3 #保留3份
    create 0777 root root
    su root root
}
```

強制執行一次 rotate - **ref** (<https://blog.csdn.net/p15097962069/article/details/104014961>)

```
sudo logrotate -vf /etc/logrotate.d/atftp
```

方法一：

一樣檔名設置，每次換檔案時，重啟 atftp server，這樣就會繼續 monitor 設置檔名之檔案。

atftp server 重跑一次 setting，所以繼續偵測同個檔名但不同 inode file.

原因: 因為logrotate 頻率不高

```
logger = logging.getLogger()
logger.setLevel(logging.DEBUG)
handler = logging.handlers.SysLogHandler(address = '/dev/log')
handler.setFormatter(
    logging.Formatter("(%(module)s-%(processName)s[%(process)d]: %(name)s: %(message)s")
)
logger.addHandler(handler)
logger.debug('this is debug')
logger.critical('this is critical')
```

syslog

syslog 是一個系統日誌記錄程序，但是由於它已經跟不上時代的腳步，所以rsyslog 替代了它，而且較新的 Ubuntu、Fedora 默認使用的都是 rsyslog。

rsyslog 有兩個配置文件，其一是/etc/rsyslog.conf，是主要的配置環境，另外一個是/etc/rsyslog.d/50-default.conf，主要是配置的 Filter Conditions。

- /etc/rsyslog.d/50-default.conf

```
# 表示將所有facility的info級別,但不包括mail,authpriv,cron相關的信息,
記錄到 /var/log/messages文件
*.info;mail.none;authpriv.none;cron.none /var/log/messages

# 表示將權限,授權相關的所有基本的信息,記錄到/var/log/secure文件中.
這個文件的權限是600
authpriv.* /var/log/secure

# 表示將mail相關的所有基本的信息記錄到/var/log/maillog文件中,
可以看到路徑前面有一個 "-" 而 "-" 表示異步寫入磁碟
mail.* -/var/log/maillog

# 表示將任務計劃相關的所有級別的信息記錄到/var/log/cron文件中
cron.* /var/log/cron

# 表示將所有facility的emerg級別的信息,發送給登錄到系統上的所有用戶
*.emerg *

# 表示將uucp及news的crit級別的信息記錄到/var/log/spooler文件中
uucp,news.crit /var/log/spooler

# 表示將local7的所有級別的信息記錄到/var/log/boot.log文件中上面說過
local0 到local7這8個是用戶自定義使用的,這裡的local7記錄的是系統啟動相關的信息
local7.* /var/log/boot.log
```

分類

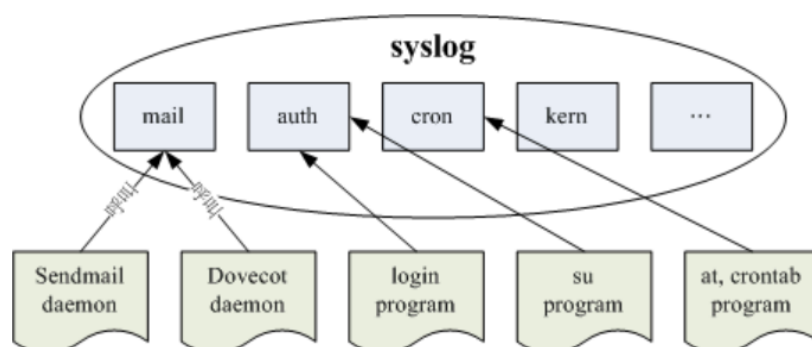
Ref: (https://linux.vbird.org/linux_basic/centos7/0570syslog.php). rsyslogd 主要還是透過 Linux 核心提供的 syslog 相關規範來設定資料的分類的, Linux 的 syslog 本身有規範一些服務訊息, 你可以透過這些服務來儲存系統的訊息。

Linux 核心的 syslog 認識的服務類型主要有底下這些:

相對序號	服務類別	服務類別
0	kern(kernel)	就是核心 (kernel) 產生的訊息，大部分都是硬體偵測以及核心功能的
1	user	在使用者層級所產生的資訊，例如後續會介紹到的用戶使用 <code>logge</code> 指令來記錄登錄檔的功能
2	mail	只要與郵件收發有關的訊息記錄都屬
3	daemon	主要是系統的服務所產生的資訊，例 <code>systemd</code> 就是這個有關的訊息
4	auth	主要與認證/授權有關的機制，例如 <code>ssh</code> , <code>su</code> 等需要帳號/密碼
5	syslog	就是由 <code>syslog</code> 相關協定產生的資訊，其實就是 <code>rsyslogd</code> 這支程式本身產生的資訊！
9	cron	就是例行性工作排程 <code>cron/at</code> 等產生訊息記錄的地方；
11	ftp	與 FTP 通訊協定有關的訊息輸出！
16~23	local0 ~ local7	保留給本機用戶使用的一些登錄檔訊較常與終端機互動。

上面談到的都是 Linux 核心的 `syslog` 函數自行制訂的服務名稱，軟體開發商可以透過呼叫上述的服務名稱來記錄他們的軟體。

- 舉例來說，`sendmail` 與 `postfix` 及 `dovecot` 都是與郵件有關的軟體，這些軟體在設計登錄檔記錄時，都會主動呼叫 `syslog` 內的 `mail` 服務名稱 (`LOG_MAIL`)。所以上述三個軟體 (`sendmail`, `postfix`, `dovecot`) 產生的訊息在 `syslog` 看起來，就會『是 `mail`』類型的服務了



fliter setting

Is there a way to filter syslog entries?

(<https://serverfault.com/questions/15106/is-there-a-way-to-filter-syslog-entries>).

```
:rawmsg,contains,"atftpd" -/var/log/atftp/sys-atftp.log
```