如何設定

SSH audit syslog

V012

2023/10/19

版權聲明

商標

目錄

前言

本文件描述 N-Reporter 使用者如何使用 Rsyslog 或 Syslogd 方式設定 SSH audit syslog。

此文件適用於 RedHat / CentOS / OracleLinux / Debian / Ubuntu / SUSE / Solaris / HP-UX / AIX / FreeBSD。

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

1. Red Hat

1.1 Red Hat 3

1.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@RedHat3 root]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
#obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
[root@RedHat3 root]# service sshd restart && service sshd status
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
sshd (pid 1002 941) is running...
[root@RedHat3 root]#
```

1.1.2 設定 syslog 轉發 SSH log

(1) 查看 syslog 版本

```
# syslogd -v
```

```
[root@RedHat3 root]# syslogd -v
syslogd 1.4.1
[root@RedHat3 root]#
```

(2) 編輯 syslog.conf 設定檔

```
# vi /etc/syslog.conf
```

```
[root@RedHat3 root]# vi /etc/syslog.conf
```

(3) 設定 Facility auth.*;authpriv.* log 存在本機 /var/log/secure 和轉發到 N-Reporter

```
# The authpriv file has restricted access.
authpriv.*;auth.*                                       /var/log/secure
# Send SSH log to N-Reporter
authpriv.*;auth.*                                       @192.168.3.50
```

```
#The authpriv file has restricted access.
authpriv.*;auth.*                                       /var/log/secure
#Send SSH log to N-Reporter
authpriv.*;auth.*                                       @192.168.3.50
```

紅色文字部位請輸入N-Reporter系統IP address

(4) 重啟 syslog 服務和確認 syslog 服務正常

```
# service syslog restart && service syslog status
```

```
[root@RedHat3 root]# service syslog restart && service syslog status
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
syslogd (pid 1035) is running...
klogd (pid 1039) is running...
[root@RedHat3 root]#
```

1.2 Red Hat 5

1.2.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@RedHat5 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
[root@RedHat5 ~]# service sshd restart && service sshd status
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
openssh-daemon (pid  3359) is running...
[root@RedHat5 ~]#
```

1.2.2 安裝 Rsyslog 8 套件

(1) 停用 syslog 服務

```
# service syslog stop
```

```
[root@RedHat5 ~]# service syslog stop
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
[root@RedHat5 ~]#
```

(2) 停用 syslog 開機自動啟動服務和確認 syslog 服務等級都是 off

```
# chkconfig syslog off
# chkconfig syslog --list
```

```
[root@RedHat5 ~]# chkconfig syslog off
[root@RedHat5 ~]# chkconfig syslog --list
syslog          0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@RedHat5 ~]#
```

(3) 下載 rsyslog repository 設定檔

```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```

```
[root@RedHat5 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   227  100   227    0     0    166      0  0:00:01  0:00:01 --:--:--     0
[root@RedHat5 ~]#
```

(4) 安裝 rsyslog 套件

```
# yum -y install rsyslog
```

```
Installed:
  rsyslog.x86_64 0:8.16.0-1.el5.centos

Dependency Installed:
  json-c.x86_64 0:0.11-3.el5.centos          libestr.x86_64 0:0.1.10-1.el5.centos          libgt.x86_64 0:0.3.11-1.el5.centos          liblogging.x86_64 0:1.0.6-1.el5.centos

Replaced:
  sysklogd.x86_64 0:1.4.1-46.el5

Complete!
[root@RedHat5 ~]#
```

(5) 確認 rsyslog 版本

```
# rsyslogd -v
```

```
[root@RedHat5 ~]# rsyslogd -v
rsyslogd 8.16.0, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           No
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat5 ~]#
```

1.2.3 設定 Rsyslog 轉發 SSH log

(1) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@RedHat5 ~]# vi /etc/rsyslog.conf
```

(2) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                              /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                              /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 啟動 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog start && service rsyslog status
```

```
[root@RedHat5 ~]# service rsyslog start && service rsyslog status
Starting system logger:                                    [  OK  ]
rsyslogd (pid  3658) is running...
[root@RedHat5 ~]#
```

(4) 設定 rsyslog 開機自動啟動服務和確認 rsyslog 服務自動啟用等級

```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```

```
[root@RedHat5 ~]# chkconfig rsyslog on
[root@RedHat5 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@RedHat5 ~]#
```

1.3 Red Hat 6

1.3.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@RedHat6 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
[root@RedHat6 ~]# service sshd restart && service sshd status
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
openssh-daemon (pid  6803) is running...
[root@RedHat6 ~]#
```

1.3.2 更新 Rsyslog 8 套件

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

(2) 下載 rsyslog repository 設定檔

```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```

```
[root@RedHat6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0    134      0  0:00:01  0:00:01 --:--:--  1146
[root@RedHat6 ~]#
```

(3) 更新 rsyslog 套件

```
# yum -y install rsyslog
```

```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                 libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@RedHat6 ~]#
```

(4) 確認 rsyslog 版本

```
# rsyslogd -v
```

```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

1.3.3 設定 Rsyslog 轉發 SSH log

(1) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@RedHat6 ~]# vi /etc/rsyslog.conf
```

(2) 註解 imjournal 模組

```
#module(load="imjournal" StateFile="imjournal.state")
```

```
# provides access to the systemd journal and file to store the position in the journal
#module(load="imjournal" StateFile="imjournal.state")
```

(3) 註解 OmitLocalLogging

```
#$OmitLocalLogging on
```

```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
```

(4) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(5) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```

```
[root@RedHat6 ~]# vi /etc/rsyslog.conf
[root@RedHat6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  6893) is running...
[root@RedHat6 ~]#
```

1.4 Red Hat 7

1.4.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@RedHat7 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
[root@RedHat7 ~]# systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 01:13:04 CST; 8ms ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 13840 (sshd)
   CGroup: /system.slice/sshd.service
           └─13840 /usr/sbin/sshd -D

Aug 25 01:13:04 RedHat7.localdomain systemd[1]: Stopped OpenSSH server daemon.
Aug 25 01:13:04 RedHat7.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 25 01:13:04 RedHat7.localdomain sshd[13840]: Server listening on 0.0.0.0 port 22.
Aug 25 01:13:04 RedHat7.localdomain sshd[13840]: Server listening on :: port 22.
Aug 25 01:13:04 RedHat7.localdomain systemd[1]: Started OpenSSH server daemon.
[root@RedHat7 ~]#
```

1.4.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@RedHat7 ~]# rsyslogd -v
rsyslogd 8.24.0-34.el7, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat7 ~]#
```

(2) 編輯 rsyslog.conf 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@RedHat7 ~]# vi /etc/rsyslog.conf
```

(3) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
[root@RedHat7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 01:25:52 CST; 6ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 13855 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─13855 /usr/sbin/rsyslogd -n

Aug 25 01:25:52 RedHat7.localdomain systemd[1]: Stopped System Logging Service.
Aug 25 01:25:52 RedHat7.localdomain systemd[1]: Starting System Logging Service...
Aug 25 01:25:52 RedHat7.localdomain rsyslogd[13855]:  [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid="13855" x-info="http://www.rsysl..."] start
Aug 25 01:25:52 RedHat7.localdomain systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@RedHat7 ~]#
```

1.5 Red Hat 8

1.5.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@RedHat8 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
[root@RedHat8 ~]# systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 16:58:07 CST; 12ms ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 5927 (sshd)
    Tasks: 1 (limit: 23520)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─5927 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,a>

Aug 25 16:58:07 RedHat8 systemd[1]: Stopped OpenSSH server daemon.
Aug 25 16:58:07 RedHat8 systemd[1]: Starting OpenSSH server daemon...
Aug 25 16:58:07 RedHat8 sshd[5927]: Server listening on 0.0.0.0 port 22.
Aug 25 16:58:07 RedHat8 sshd[5927]: Server listening on :: port 22.
Aug 25 16:58:07 RedHat8 systemd[1]: Started OpenSSH server daemon.
[root@RedHat8 ~]#
```

1.5.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@RedHat8 ~]# rsyslogd -v
rsyslogd 8.37.0-13.el8, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat8 ~]#
```

(2) 編輯 rsyslog.conf 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@RedHat8 ~]# vi /etc/rsyslog.conf
```

(3) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
[root@RedHat8 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 17:09:30 CST; 8ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 5951 (rsyslogd)
    Tasks: 3 (limit: 23520)
   Memory: 1.1M
   CGroup: /system.slice/rsyslog.service
           └─5951 /usr/sbin/rsyslogd -n

Aug 25 17:09:30 RedHat8 systemd[1]: Stopped System Logging Service.
Aug 25 17:09:30 RedHat8 systemd[1]: Starting System Logging Service...
Aug 25 17:09:30 RedHat8 rsyslogd[5951]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime  [v8.37.0-13.el8 try http://www.rsyslo>
Aug 25 17:09:30 RedHat8 systemd[1]: Started System Logging Service.
Aug 25 17:09:30 RedHat8 rsyslogd[5951]:  [origin software="rsyslogd" swVersion="8.37.0-13.el8" x-pid="5951" x-info="http://www.rsyslog.com"] start
[root@RedHat8 ~]#
```

2. CentOS

2.1 CentOS 6

2.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@CentOS6 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
[root@CentOS6 ~]# service sshd restart && service ssh status
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
ssh: unrecognized service
[root@CentOS6 ~]#
```

2.1.2 更新 Rsyslog 8 套件

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@CentOS6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@CentOS6 ~]#
```

(2) 下載 rsyslog repository 設定檔

```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```

```
[root@CentOS6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0    137      0  0:00:01  0:00:01 --:--:--  1158
[root@CentOS6 ~]#
```

(3) 更新 rsyslog 套件

```
# yum -y install rsyslog
```

```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                 libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@CentOS6 ~]#
```

(4) 確認 rsyslog 版本

```
# rsyslogd -v
[root@CentOS6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@CentOS6 ~]#
```

2.1.3 設定 Rsyslog 轉發 SSH log

(1) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@CentOS6 ~]# vi /etc/rsyslog.conf
```

(2) 註解 imjournal 模組

```
#module(load="imjournal" StateFile="imjournal.state")
```

```
# provides access to the systemd journal and file to store the position in the journal
#module(load="imjournal" StateFile="imjournal.state")
```

(3) 註解 OmitLocalLogging

```
#$OmitLocalLogging on
```

```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
```

(4) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(5) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```

```
[root@CentOS6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  6321) is running...
[root@CentOS6 ~]#
```

2.2 CentOS 7

2.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@CentOS7 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
[root@CentOS7 ~]# systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 18:29:08 CST; 9ms ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 8242 (sshd)
   CGroup: /system.slice/sshd.service
           └─8242 /usr/sbin/sshd -D

Aug 25 18:29:07 CentOS7.localdomain systemd[1]: Stopped OpenSSH server daemon.
Aug 25 18:29:08 CentOS7.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 25 18:29:08 CentOS7.localdomain sshd[8242]: Server listening on 0.0.0.0 port 22.
Aug 25 18:29:08 CentOS7.localdomain sshd[8242]: Server listening on :: port 22.
Aug 25 18:29:08 CentOS7.localdomain systemd[1]: Started OpenSSH server daemon.
[root@CentOS7 ~]#
```

2.1.2 更新 Rsyslog 套件

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 7.4.7, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes

See http://www.rsyslog.com for more information.
[root@CentOS7 ~]#
```

(2) 更新 rsyslog 套件

```
# yum -y install rsyslog
```

```
Dependency Installed:
  bc.x86_64 0:1.06.95-13.el7                libaio.x86_64 0:0.3.109-13.el7                libfastjson.x86_64 0:0.99.4-3.el7                lz4.x86_64 0:1.8.3-1.el7

Updated:
  centos-release.x86_64 0:7-9.2009.1.el7.centos         dracut.x86_64 0:033-572.el7         initscripts.x86_64 0:9.49.53-1.el7_9.1         lvm2-libs.x86_64 7:2.02.187-6.el7_9.5
  rsyslog.x86_64 0:8.24.0-57.el7_9.1

Dependency Updated:
  cryptsetup-libs.x86_64 0:2.0.3-6.el7                      device-mapper.x86_64 7:1.02.170-6.el7_9.5              device-mapper-event.x86_64 7:1.02.170-6.el7_9.5
  device-mapper-event-libs.x86_64 7:1.02.170-6.el7_9.5      device-mapper-libs.x86_64 7:1.02.170-6.el7_9.5         device-mapper-persistent-data.x86_64 0:0.8.5-3.el7_9.2
  dracut-config-rescue.x86_64 0:033-572.el7                 dracut-network.x86_64 0:033-572.el7                    glib2.x86_64 0:2.56.1-9.el7_9
  kmod.x86_64 0:20-28.el7                                   libgudev1.x86_64 0:219-78.el7_9.3                      lvm2.x86_64 7:2.02.187-6.el7_9.5
  systemd.x86_64 0:219-78.el7_9.3                           systemd-libs.x86_64 0:219-78.el7_9.3                   systemd-sysv.x86_64 0:219-78.el7_9.3

Complete!
[root@CentOS7 ~]#
```

(3) 確認 rsyslog 版本

```
# rsyslogd -v
```

```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 8.24.0-57.el7_9.1, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@CentOS7 ~]#
```

2.1.3 設定 Rsyslog 轉發 SSH log

(1) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@CentOS7 ~]# vi /etc/rsyslog.conf
```

(2) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                                    /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
        action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                                    /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
[root@CentOS7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 22:57:40 CST; 7ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 8284 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─8284 /usr/sbin/rsyslogd -n

Aug 25 22:57:40 CentOS7.localdomain systemd[1]: Starting System Logging Service...
Aug 25 22:57:40 CentOS7.localdomain rsyslogd[8284]:  [origin software="rsyslogd" swVersion="8.24.0-55.el7" x-pid="8284" x-info="http://www.rsyslog..."] start
Aug 25 22:57:40 CentOS7.localdomain systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@CentOS7 ~]#
```

2.3 CentOS 8

2.3.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@CentOS8 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
[root@CentOS8 ~]# systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 23:19:01 CST; 11ms ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 5849 (sshd)
    Tasks: 1 (limit: 23465)
   Memory: 1.1M
   CGroup: /system.slice/sshd.service
           └─5849 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,a>

Aug 25 23:19:01 CentOS8.localdomain systemd[1]: sshd.service: Succeeded.
Aug 25 23:19:01 CentOS8.localdomain systemd[1]: Stopped OpenSSH server daemon.
Aug 25 23:19:01 CentOS8.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 25 23:19:01 CentOS8.localdomain sshd[5849]: Server listening on 0.0.0.0 port 22.
Aug 25 23:19:01 CentOS8.localdomain sshd[5849]: Server listening on :: port 22.
Aug 25 23:19:01 CentOS8.localdomain systemd[1]: Started OpenSSH server daemon.
[root@CentOS8 ~]#
```

2.3.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@CentOS8 ~]# rsyslogd -v
rsyslogd  8.2102.0-8.el8 (aka 2021.02) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@CentOS8 ~]#
```

(2) 編輯 rsyslog.conf 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@CentOS8 ~]# vi /etc/rsyslog.conf
```

(3) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
[root@CentOS8 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 23:23:24 CST; 8ms ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 5900 (rsyslogd)
    Tasks: 3 (limit: 23465)
   Memory: 3.0M
   CGroup: /system.slice/rsyslog.service
           └─5900 /usr/sbin/rsyslogd -n

Aug 25 23:23:24 CentOS8.localdomain systemd[1]: rsyslog.service: Succeeded.
Aug 25 23:23:24 CentOS8.localdomain systemd[1]: Stopped System Logging Service.
Aug 25 23:23:24 CentOS8.localdomain systemd[1]: Starting System Logging Service...
Aug 25 23:23:24 CentOS8.localdomain rsyslogd[5900]: [origin software="rsyslogd" swVersion="8.2102.0-8.el8" x-pid="5900" x-info="https://www.rsyslog.com"] st>
Aug 25 23:23:24 CentOS8.localdomain systemd[1]: Started System Logging Service.
Aug 25 23:23:24 CentOS8.localdomain rsyslogd[5900]: imjournal: journal files changed, reloading...  [v8.2102.0-8.el8 try https://www.rsyslog.com/e/0 ]
[root@CentOS8 ~]#
```

3. OracleLinux

3.1 OracleLinux 6

3.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@OracleLinux6 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
# obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
[root@OracleLinux6 ~]# service sshd restart && service sshd status
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
openssh-daemon (pid  7779) is running...
[root@OracleLinux6 ~]#
```

3.1.2 更新 Rsyslog 8 套件

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@OracleLinux6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@OracleLinux6 ~]#
```

(2) 下載 rsyslog repository 設定檔

```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```

```
[root@OracleLinux6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0     44      0  0:00:05  0:00:05 --:--:--  1182
[root@OracleLinux6 ~]#
```

(3) 更新 rsyslog 套件

```
# yum -y install rsyslog
```

```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                 libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@OracleLinux6 ~]#
```

(4) 確認 rsyslog 版本

```
# rsyslogd -v
```

```
[root@OracleLinux6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@OracleLinux6 ~]#
```

3.1.3 設定 Rsyslog 轉發 SSH log

(1) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@OracleLinux6 ~]# vi /etc/rsyslog.conf
```

(2) 註解 imjournal 模組

```
#module(load="imjournal" StateFile="imjournal.state")
```

```
# provides access to the systemd journal and file to store the position in the journal
#module(load="imjournal" StateFile="imjournal.state")
```

(3) 註解 OmitLocalLogging

```
#$OmitLocalLogging on
```

```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
```

(4) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                                    /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                                    /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(5) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```

```
[root@OracleLinux6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  7868) is running...
[root@OracleLinux6 ~]#
```

3.2 OracleLinux 7

3.2.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
[root@OracleLinux7 ~]# vi /etc/ssh/sshd_config
```

(2) 註解 Facility AUTHPRIV 和 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#SyslogFacility AUTHPRIV
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
[root@OracleLinux7 ~]# systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 15:56:32 CST; 27ms ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 11169 (sshd)
   CGroup: /system.slice/sshd.service
           └─11169 /usr/sbin/sshd -D

Aug 25 15:56:32 OracleLinux7.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 25 15:56:32 OracleLinux7.localdomain sshd[11169]: Server listening on 0.0.0.0 port 22.
Aug 25 15:56:32 OracleLinux7.localdomain sshd[11169]: Server listening on :: port 22.
Aug 25 15:56:32 OracleLinux7.localdomain systemd[1]: Started OpenSSH server daemon.
[root@OracleLinux7 ~]#
```

3.2.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
[root@OracleLinux7 ~]# rsyslogd -v
rsyslogd 8.24.0-38.el7, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@OracleLinux7 ~]#
```

(2) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
[root@OracleLinux7 ~]# vi /etc/rsyslog.conf
```

(3) 註解 authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/secure 並轉發到 N-Reporter

```
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
        action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
[root@OracleLinux7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 15:59:55 CST; 4ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 11180 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─11180 /usr/sbin/rsyslogd -n

Aug 25 15:59:55 OracleLinux7.localdomain systemd[1]: Starting System Logging Service...
Aug 25 15:59:55 OracleLinux7.localdomain rsyslogd[11180]:  [origin software="rsyslogd" swVersion="8.24.0-38.el7" x-pid="11180" x-info="http://www.r...] start
Aug 25 15:59:55 OracleLinux7.localdomain systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@OracleLinux7 ~]#
```

4. Debian 11

4.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
root@Debian11:~# vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart ssh && systemctl status ssh
```

```
root@Debian11:~# systemctl restart ssh && systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-08-25 16:35:24 CST; 10ms ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 526 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 527 (sshd)
      Tasks: 1 (limit: 4668)
     Memory: 1.1M
        CPU: 14ms
     CGroup: /system.slice/ssh.service
             └─527 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 25 16:35:24 Debian11 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 25 16:35:24 Debian11 sshd[527]: Server listening on 0.0.0.0 port 22.
Aug 25 16:35:24 Debian11 sshd[527]: Server listening on :: port 22.
Aug 25 16:35:24 Debian11 systemd[1]: Started OpenBSD Secure Shell server.
root@Debian11:~#
```

4.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@Debian11:~# rsyslogd -v
rsyslogd  8.2102.0 (aka 2021.02) compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Config file:                            /etc/rsyslog.conf
        PID file:                               /run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
root@Debian11:~#
```

(2) 編輯 rsyslog 設定檔

```
# vi /etc/rsyslog.conf
```

```
root@Debian11:~# vi /etc/rsyslog.conf
```

(3) 註解 auth,authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/auth.log 並轉發到 N-Reporter

```
#auth,authpriv.*                                /var/log/auth.log
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
        action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
#
# 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

# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入N-Reporter 系統IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
root@Debian11:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-08-25 16:41:27 CST; 5ms ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 557 (rsyslogd)
      Tasks: 4 (limit: 4668)
     Memory: 848.0K
        CPU: 3ms
     CGroup: /system.slice/rsyslog.service
             └─557 /usr/sbin/rsyslogd -n -iNONE

Aug 25 16:41:27 Debian11 systemd[1]: rsyslog.service: Succeeded.
Aug 25 16:41:27 Debian11 systemd[1]: Stopped System Logging Service.
Aug 25 16:41:27 Debian11 rsyslogd[557]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2102.0]
Aug 25 16:41:27 Debian11 systemd[1]: Starting System Logging Service...
Aug 25 16:41:27 Debian11 rsyslogd[557]: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="557" x-info="https://www.rsyslog.com"] start
Aug 25 16:41:27 Debian11 systemd[1]: Started System Logging Service.
root@Debian11:~#
```

5. Ubuntu

5.1 Ubuntu 18

5.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
root@Ubuntu18:~# vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#LogLevel INFO
Loglevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart ssh && systemctl status ssh
```

```
root@Ubuntu18:~# systemctl restart ssh && systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 09:42:07 UTC; 5ms ago
  Process: 1978 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 1991 (sshd)
    Tasks: 1 (limit: 4590)
   CGroup: /system.slice/ssh.service
           └─1991 /usr/sbin/sshd -D

Aug 25 09:42:07 Ubuntu18 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 25 09:42:07 Ubuntu18 sshd[1991]: Server listening on 0.0.0.0 port 22.
Aug 25 09:42:07 Ubuntu18 sshd[1991]: Server listening on :: port 22.
Aug 25 09:42:07 Ubuntu18 systemd[1]: Started OpenBSD Secure Shell server.
root@Ubuntu18:~#
```

5.1.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@Ubuntu18:~# rsyslogd -v
rsyslogd 8.32.0, compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
root@Ubuntu18:~#
```

(2) 編輯 rsyslog 的 50-default.conf 設定檔

```
# vi /etc/rsyslog.d/50-default.conf
```

```
root@Ubuntu18:~# vi /etc/rsyslog.d/50-default.conf
```

(3) 註解 auth,authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/auth.log 並轉發到 N-Reporter

```
#auth,authpriv.*                        /var/log/auth.log
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
#
# 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

# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入N-Reporter系統IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
root@Ubuntu18:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 09:48:51 UTC; 6ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 2028 (rsyslogd)
    Tasks: 4 (limit: 4590)
   CGroup: /system.slice/rsyslog.service
           └─2028 /usr/sbin/rsyslogd -n
root@Ubuntu18:~#
```

5.2 Ubuntu 20

5.2.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
root@ubuntu20:~# vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart ssh && systemctl status ssh
```

```
root@ubuntu20:~# systemctl restart ssh && systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-08-25 09:55:35 UTC; 8ms ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1051 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1069 (sshd)
      Tasks: 1 (limit: 4580)
     Memory: 1.5M
     CGroup: /system.slice/ssh.service
             └─1069 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 25 09:55:35 ubuntu20 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 25 09:55:35 ubuntu20 sshd[1069]: Server listening on 0.0.0.0 port 22.
Aug 25 09:55:35 ubuntu20 sshd[1069]: Server listening on :: port 22.
Aug 25 09:55:35 ubuntu20 systemd[1]: Started OpenBSD Secure Shell server.
root@ubuntu20:~#
```

5.2.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@ubuntu20:~# rsyslogd -v
rsyslogd  8.2001.0 (aka 2020.01) compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Config file:                            /etc/rsyslog.conf
        PID file:                               /run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
root@ubuntu20:~#
```

(2) 編輯 rsyslog 的 50-default.conf 設定檔

```
# vi /etc/rsyslog.d/50-default.conf
```

```
root@ubuntu20:~# vi /etc/rsyslog.d/50-default.conf
```

(3) 註解 auth,authpriv.*，新增 syslogfacility-text "auth" or "authpriv" 儲存於 /var/log/auth.log 並轉發到 N-Reporter

```
#auth,authpriv.*                                /var/log/auth.log
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
        action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
#
# 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

# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入N-Reporter系統IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```

```
root@ubuntu20:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-08-25 10:00:49 UTC; 8ms ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 1127 (rsyslogd)
      Tasks: 4 (limit: 4580)
     Memory: 1.0M
     CGroup: /system.slice/rsyslog.service
             └─1127 /usr/sbin/rsyslogd -n -iNONE

Aug 25 10:00:49 ubuntu20 systemd[1]: Starting System Logging Service...
Aug 25 10:00:49 ubuntu20 rsyslogd[1127]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2001.0]
Aug 25 10:00:49 ubuntu20 systemd[1]: Started System Logging Service.
Aug 25 10:00:49 ubuntu20 rsyslogd[1127]: rsyslogd's groupid changed to 110
Aug 25 10:00:49 ubuntu20 rsyslogd[1127]: rsyslogd's userid changed to 104
Aug 25 10:00:49 ubuntu20 rsyslogd[1127]: [origin software="rsyslogd" swVersion="8.2001.0" x-pid="1127" x-info="https://www.rsyslog.com"] start
root@ubuntu20:~#
```

6. SUSE 15

6.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
SUSE15:~ # vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 Facility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
LogLevel VERBOSE
```

```
# Logging
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# systemctl restart sshd && systemctl status sshd
```

```
SUSE15:~ # systemctl restart sshd && systemctl status sshd
● sshd.service - OpenSSH Daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
     Active: active (running) since Fri 2022-08-26 01:33:12 UTC; 263ms ago
    Process: 2800 ExecStartPre=/usr/sbin/sshd-gen-keys-start (code=exited, status=0/SUCCESS)
    Process: 2802 ExecStartPre=/usr/sbin/sshd -t $SSHD_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 2803 (sshd)
      Tasks: 1
     CGroup: /system.slice/sshd.service
             └─2803 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 26 01:33:12 SUSE15 systemd[1]: Starting OpenSSH Daemon...
Aug 26 01:33:12 SUSE15 sshd-gen-keys-start[2800]: Checking for missing server keys in /etc/ssh
Aug 26 01:33:12 SUSE15 sshd[2803]: Server listening on 0.0.0.0 port 22.
Aug 26 01:33:12 SUSE15 sshd[2803]: Server listening on :: port 22.
Aug 26 01:33:12 SUSE15 systemd[1]: Started OpenSSH Daemon.
SUSE15:~ #
```

6.2 設定 Rsyslog 轉發 SSH log

(1) 檢查 Rsyslog 版本

```
# rsyslogd -v
```

```
SUSE15:~ # rsyslogd -v
rsyslogd  8.2106.0 (aka 2021.06) compiled with:
        PLATFORM:                               x86_64-suse-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
SUSE15:~ #
```

(2) 新增 rsyslog 的 100-sshd.conf 設定檔

```
# vi /etc/rsyslog.d/100-sshd.conf
```

```
SUSE15:~ # vi /etc/rsyslog.d/110-sshd.conf
```

(3) 設定 SSH log 儲存於 /var/log/auth.log 並轉發到 N-Reporter

```
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入N-Reporter系統IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
SUSE15:~ # systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-08-26 01:43:46 UTC; 15ms ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             http://www.rsyslog.com/doc/
    Process: 3172 ExecStartPre=/usr/sbin/rsyslog-service-prepare (code=exited, status=0/SUCCESS)
   Main PID: 3174 (rsyslogd)
      Tasks: 5
     CGroup: /system.slice/rsyslog.service
             └─3174 /usr/sbin/rsyslogd -n -iNONE

Aug 26 01:43:46 SUSE15 systemd[1]: Starting System Logging Service...
Aug 26 01:43:46 SUSE15 rsyslogd[3174]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2106.0]
Aug 26 01:43:46 SUSE15 systemd[1]: Started System Logging Service.
Aug 26 01:43:46 SUSE15 rsyslogd[3174]: [origin software="rsyslogd" swVersion="8.2106.0" x-pid="3174" x-info="https://www.rsyslog.com"] start
SUSE15:~ #
```

7. Solaris

7.1 Solaris 10

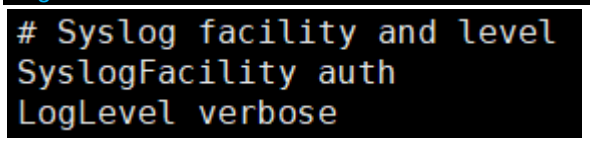
7.1.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

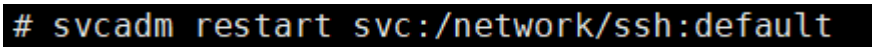
(2) 設定 SyslogFacility 和 LogLevel 詳細訊息

```
SyslogFacility auth
LogLevel verbose
```



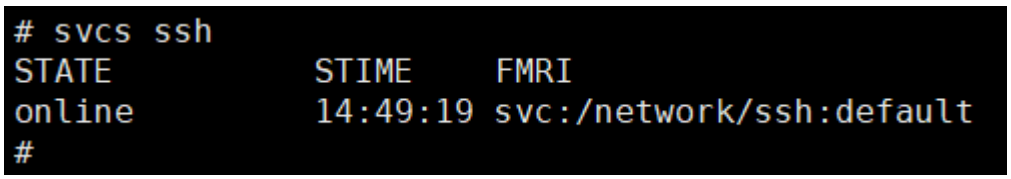
(3) 重啟 SSH 服務

```
# svcadm restart svc:/network/ssh:default
```



(4) 確認 SSH 服務正常

```
# svcs ssh
```



7.1.2 設定 syslog 轉發 SSH log

(1) 顯示 system-log 服務的狀態

```
# svcs system-log
```

```
# svcs system-log
STATE          STIME    FMRI
online         14:40:16 svc:/system/system-log:default
#
```

(2) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

```
# vi /etc/syslog.conf
```

(3) 設定轉發到 N-Reporter

```

#Send SSH log to N-Reporter
auth.debug                                  @192.168.3.50
```

註: facility.severity 後面必須接 <tab>，而非空白 <space>。

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 syslog 服務和確認 syslog 服務正常

```
# svcadm restart system/system-log:default
# svcs system-log
```

```
# svcadm restart system/system-log:default
# svcs system-log
STATE          STIME    FMRI
online         15:06:39 svc:/system/system-log:default
#
```

7.2 Solaris 11

7.2.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
root@Solaris11:~# vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 SyslogFacility auth 和 LogLevel verbose 詳細訊息

```
SyslogFacility auth
#LogLevel INFO
LogLevel verbose
```

```
# Syslog facility and level
SyslogFacility auth
#LogLevel info
LogLevel verbose
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# svcadm restart svc:/network/ssh:default
# svcs ssh
```

```
root@Solaris11:~# svcadm restart svc:/network/ssh:default
root@Solaris11:~# svcs ssh
STATE          STIME    FMRI
online         23:51:12 svc:/network/ssh:default
root@Solaris11:~#
```

7.2.2 查看預設 syslog 或 rsyslog 服務

7.2.2.1 設定 syslog 轉發 SSH log

(1) 顯示 system-log 服務的狀態

```
# svcs system-log
```

```
root@Solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       23:30:15 svc:/system/system-log:rsyslog
online         23:30:58 svc:/system/system-log:default
root@Solaris11:~#
```

(2) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

```
root@Solaris11:~# vi /etc/syslog.conf
```

(3) 設定轉發到 N-Reporter

```
# Send SSH log to N-Reporter
auth.*                                          @192.168.3.50
```

```
#Send SSH log to N-Reporter
auth.*                          @192.168.3.50
```

註: facility.severity 後面必須接 <tab>，而非空白 <space>。

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 syslog 服務

```
# svcadm restart system/system-log:default
# svcs system-log
```

```
root@Solaris11:~# svcadm restart system/system-log:default
root@Solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       23:30:15 svc:/system/system-log:rsyslog
online         23:55:39 svc:/system/system-log:default
root@Solaris11:~#
```

7.2.2.2 設定 rsyslog 轉發 SSH log

(1) 顯示 system-log 服務的狀態

```
# svcs system-log
```

```
root@Solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       23:57:42 svc:/system/system-log:default
online         23:59:58 svc:/system/system-log:rsyslog
root@Solaris11:~#
```

(2) 檢查 rsyslog 版本

```
# /usr/lib/rsyslog/rsyslogd -v
```

```
root@Solaris11:~# /usr/lib/rsyslog/rsyslogd -v
rsyslogd 8.15.0, compiled with:
        PLATFORM:                               x86_64-pc-solaris2.11
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
root@Solaris11:~#
```

(3) 新增 rsyslog 的 100-sshd.conf 設定檔

```
# vi /etc/rsyslog.d/100-sshd.conf
```

```
root@Solaris11:~# vi /etc/rsyslog.d/100-sshd.conf
```

(4) 設定 SSH log 儲存於 /var/log/authlog 並轉發到 N-Reporter

```
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/authlog")
        action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

```
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/authlog")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

紅色文字部位請輸入N-Reporter系統IP address

(5) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# svcadm restart svc:/system/system-log:rsyslog && svcs system-log:rsyslog

# svcs system-log
```

```
root@Solaris11:~# svcadm restart svc:/system/system-log:rsyslog && svcs system-log:rsyslog
STATE          STIME    FMRI
online*        23:59:58 svc:/system/system-log:rsyslog
root@Solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       23:57:42 svc:/system/system-log:default
online          0:05:17 svc:/system/system-log:rsyslog
root@Solaris11:~#
```

8. HP-UX

HP-UX sshd syslog: https://support.hpe.com/hpesc/public/docDisplay?docId=c01965934&docLocale=en_US

(1) 編輯 sshd_config 設定檔

```
# vi /opt/ssh/etc/sshd_config
```

(2) 設定 SyslogFacility AUTH 和 LogLevel VERBOSE

```
SyslogFacility AUTH
LogLevel VERBOSE
```

(3) 停止 SSH 服務

```
# /sbin/init.d/secsh stop
```

(4) 啟動 SSH 服務

```
# /sbin/init.d/secsh start
```

(5) 查看 SSH 運作

```
# ps -ef | grep sshd
```

(6) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

(7) 設定轉發到 N-Reporter

```
# Send SSH log to N-Reporter
auth.info @192.168.8.4
```

註: facility.severity 後面必須接 <tab>，而非空白 <space>。

紅色文字部位請輸入 N-Reporter 系統 IP address

(8) 停止 syslogd 服務和啟動 syslogd 服務

```
# /sbin/init.d/syslogd stop
# /sbin/init.d/syslogd start
```

9. AIX 7

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

(2) 設定 SyslogFacility AUTH 和 LogLevel VERBOSE

```
SyslogFacility AUTH
LogLevel VERBOSE
```

(3) 停止 SSH 服務

```
# stopsrc -s sshd
```

(4) 啟動 SSH 服務

```
# startsrc -s sshd
```

(5) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

(6) 設定轉發到 N-Reporter

```
# Send SSH log to N-Reporter
auth.debug  @192.168.8.184
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(7) 停止 syslog 服務

```
# stopsrc -s syslogd
```

(8) 啟動 syslog 服務

```
# startsrc -s syslogd
```

10. FreeBSD 12

10.1 編輯 SSH 設定檔

(1) 編輯 sshd_config 設定檔

```
# vi /etc/ssh/sshd_config
```

```
root@FreeBSD12:~ # vi /etc/ssh/sshd_config
```

(2) 註解 LogLevel INFO，新增 SyslogFacility AUTH 和 LogLevel VERBOSE 詳細訊息

```
SyslogFacility AUTH
#LogLevel INFO
LogLevel verbose
```

```
# Logging
SyslogFacility AUTH
#LogLevel INFO
LogLevel VERBOSE
```

(3) 重啟 SSH 服務和確認 SSH 服務正常

```
# service sshd restart && service sshd status
```

```
root@FreeBSD12:~ # service sshd restart && service sshd status
Performing sanity check on sshd configuration.
Stopping sshd.
Waiting for PIDS: 957.
Performing sanity check on sshd configuration.
Starting sshd.
sshd is running as pid 998.
root@FreeBSD12:~ #
```

10.2 設定 syslog 轉發 SSH log

(1) 編輯 syslog 設定檔

```
# vi /etc/syslog.conf
```

```
root@FreeBSD12:~ # vi /etc/syslog.conf
```

(2) 設定轉發到 N-Reporter

```
# Send SSH log to N-Reporter
auth.*;authpriv.*                                @192.168.3.50
```

```
#Send SSH log to N-Reporter
auth.*;authpriv.*                       @192.168.3.50
```

註: facility.severity 後面必須接 <tab>，而非空白 <space>。

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 重啟 syslog 服務

```
# service syslogd restart
```

```
root@FreeBSD12:~ # service syslogd restart
Stopping syslogd.
Waiting for PIDS: 459.
Starting syslogd.
root@FreeBSD12:~ #
```

(4) 確認 syslog 服務正常

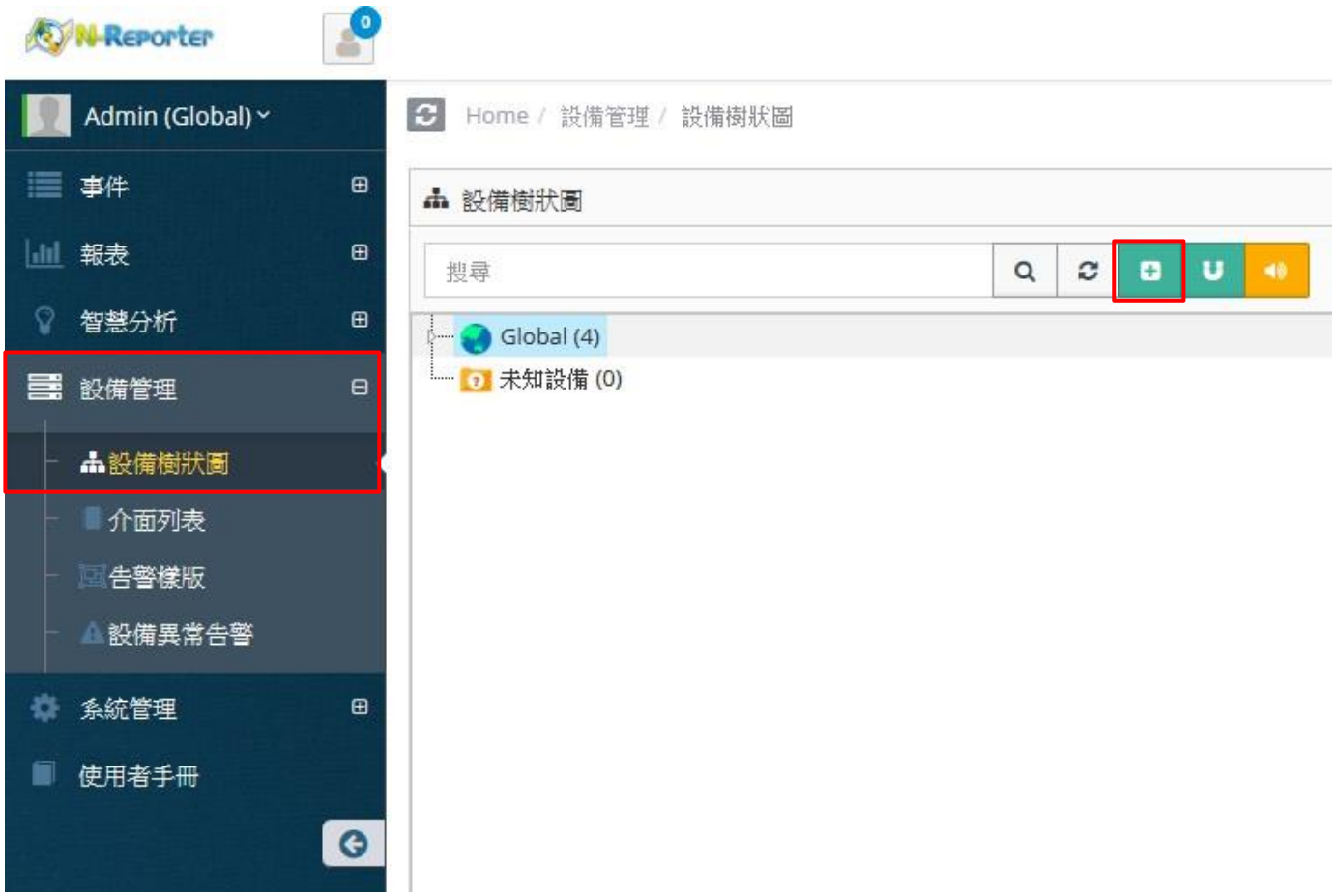
```
# service syslogd status
```

```
root@FreeBSD12:~ # service syslogd status
syslogd is running as pid 1048.
root@FreeBSD12:~ #
```

11. N-Reporter

(1) 新增 SSH audit 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 設定 SSH audit 設備的資料格式

輸入名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [UNIX/Linux/Solaris]、Facility: [(4) security/authorization messages] 和設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

Tel / 04-23752865 Fax / 04-23757458
業務詢問 / sales@npartnertech.com
技術詢問 / support@npartnertech.com