How to Configure SSH Audit Syslog

V013

2025/10/02

Copyright Declaration

Registered Trademark

All company products, names and trademarks mentioned in this manual belongs to their legally registered organizations.

Contents

Preface 2
1. Red Hat 3
1.1 Red Hat 3 3
1.1.1 Edit SSH Configuration File 3
1.1.2 Configure Syslog to Forward SSH Logs 4
1.2 Red Hat 5 5
1.2.1 Edit SSH Configuration File 5
1.2.2 Install Rsyslog 8 Package 6
1.2.3 Configure Rsyslog to Forward SSH Logs 7
1.3 Red Hat 6 8
1.3.1 Edit SSH Configuration File 8
1.3.2 Install Rsyslog 8 Package 9
1.3.3 Configure Rsyslog to Forward SSH Logs 10
1.4 Red Hat 7 11
1.4.1 Edit SSH Configuration File 11
1.4.2 Configure Rsyslog to Forward SSH Logs 12
1.5 Red Hat 8 14
1.5.1 Edit SSH Configuration File 14
1.5.2 Configure Rsyslog to Forward SSH Logs 15
2.CentOS 17
2.1 CentOS 6 17
2.1.1 Edit SSH Configuration File 17
2.1.2 Install Rsyslog 8 Package 18
2.1.3 Configure Rsyslog to Forward SSH Logs 19
2.2 CentOS 7 20
2.2.1 Edit SSH Configuration File 20
2.2.2 Install Rsyslog 8 Package 21
2.2.3 Configure Rsyslog to Forward SSH Logs 22
2.3 CentOS 8 23
2.3.1 Edit SSH Configuration File 23
2.3.2 Configure Rsyslog to Forward SSH Logs 24
3. OracleLinux 26
3.1 OracleLinux 6 26
3.1.1 Edit SSH Configuration File 26
3.1.2 Install Rsyslog 8 Package 27
3.1.3 Configure Rsyslog to Forward SSH Logs 28
3.2 OracleLinux 7 29
3.2.1 Edit SSH Configuration File 29
3.2.2 Configure Rsyslog to Forward SSH Logs 30
4. Debian 11 32
4.1 Edit SSH Configuration File 32
4.2 Configure Rsyslog to Forward SSH Logs 33
5. Ubuntu 35
5.1 Ubuntu 18 35
5.1.1 Edit SSH Configuration File 35
5.1.2 Configure Rsyslog to Forward SSH Logs 36
5.2 Ubuntu 20 38
5.2.1 Edit SSH Configuration File 38
5.2.2 Configure Rsyslog to Forward SSH Logs 39
6. SUSE 15 41
6.1 Edit SSH Configuration File 41
6.2 Configure Rsyslog to Forward SSH Logs 42
7. Solaris 43
7.1 Solaris 10 43
7.1.1 Edit SSH Configuration File 43
7.1.2 Configure Rsyslog to Forward SSH Logs 44
7.2 Solaris 11 45
7.2.1 Edit SSH Configuration File 45
7.2.2 Check the Default syslog or rsyslog Service 46
8. HP-UX 49
9. AIX 7 50
10. FreeBSD 12 51
10.1 Edit SSH Configuration File 51
10.2 Configure Syslog to Forward SSH Logs 52
11. N-Reporter 53
Contact 57

Preface

This document describes how N-Reporter users can configure SSH audit syslog using Rsyslog or Syslogd.

It applies to RedHat / CentOS / OracleLinux / Debian / Ubuntu / SUSE / Solaris / HP-UX / AIX / FreeBSD.

Note: This document is intended solely as a reference for configuring log output. For guidance on the appropriate log export methods, it is recommended to contact the respective device or software vendor.

1. Red Hat

1.1 Red Hat 3

1.1.1 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Syslog to Forward SSH Logs

(1) Enter the command below to check the syslog version:

```
# syslogd -v
```

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

(2) Enter the command below to edit the syslog.conf configuration file:

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

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

(3) Configure the facility auth.* and authpriv. * Logs to be saved locally in /var/log/secure and forwarded to 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
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the syslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Install Rsyslog 8 Package

(1) Enter the command below to stop the syslog service:

```
# service syslog stop
```

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

(2) Enter the commands below to disable the syslog service from starting automatically at boot and verify that all run levels are set to 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) Enter the command below to download the Rsyslog repository configuration file:

```
# 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) Enter the command below to install the Rsyslog package:

```
# 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) Enter the command below to check the Rsyslog version:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the rsyslog configuration file:

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

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

(2) Comment out authpriv.* and add configuration to use syslogfacility-text “auth” or “authpriv”, storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(3) Enter the command below to start the rsyslog service and verify that it is running normally:

```
# 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) Enter the commands below to enable the rsyslog service to start automatically at boot and verify its run levels:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Install Rsyslog 8 Package

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the commands below to download the Rsyslog repository configuration file:

```
# 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) Enter the command below to update the Rsyslog package:

```
# 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) Enter the command below to verify the Rsyslog version:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the rsyslog configuration file:

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

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

(2) Comment out the **imjournal** module:

```
# 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) Comment out **OmitLocalLogging**:

```
# $OmitLocalLogging on
```

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

(4) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(5) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

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

```
[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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the rsyslog configuration file:

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

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

(3) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

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

```
[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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

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

```
[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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the rsyslog configuration file:

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

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

(3) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to N-Reporter:

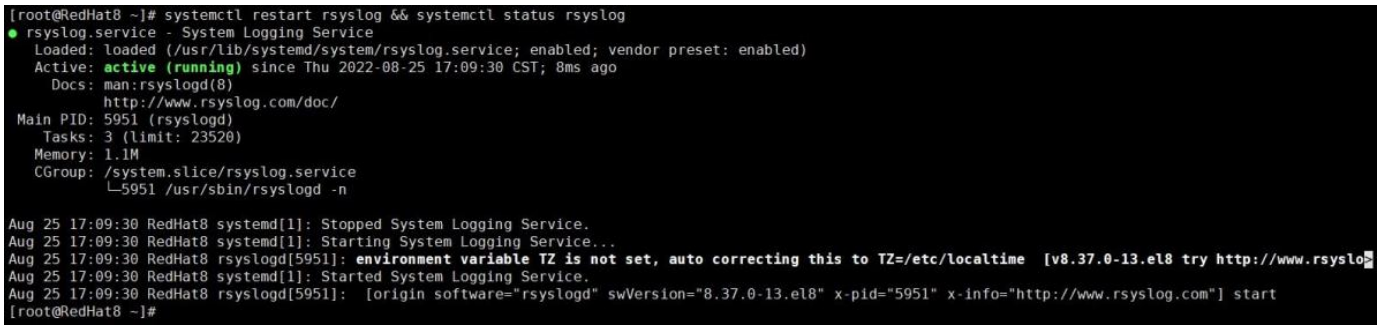
```
    # authpriv.*          /var/log/secure
    # Send SSH log to N-Reporter
    if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
    then { action(type="omfile" File="/var/log/secure")
    action(type="omfwd" Target=" 192.168.3.50" Port="514" Protocol="udp")}
```

```
# 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

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



2. CentOS

2.1 CentOS 6

2.1.1 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Install Rsyslog 8 Package

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the commands below to download the Rsyslog repository configuration file:

```
# 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) Enter the command below to update the Rsyslog package:

```
# 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) Enter the command below to verify the Rsyslog version:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the rsyslog configuration file:

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

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

(2) Comment out the **imjournal** module:

```
# 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) Comment out **OmitLocalLogging**:

```
# $OmitLocalLogging on
```

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

(4) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(5) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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

2.2.1 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 ~]#
```

2.2.2 Install Rsyslog 8 Package

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to update the Rsyslog package:

```
# 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) Enter the command below to verify the Rsyslog version:

```
# 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 ~]#
```

2.2.3 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

```
# 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")}
```

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the rsyslog configuration file:

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

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

(3) Comment out authpriv.* and add configuration to use syslogfacility-text “auth” or “authpriv”, storing logs in /var/log/secure and forwarding them to N-Reporter:

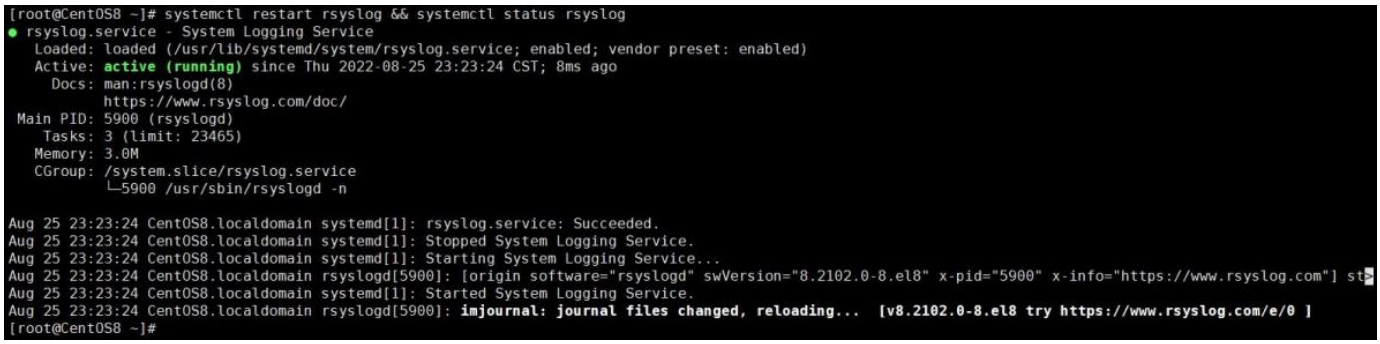
```
# authpriv.*              /var/log/secure
# Send SSH log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
action(type="omfwd" Target=" 192.168.3.50" Port="514" Protocol="udp")}
```

```
# 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

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



3. OracleLinux

3.1 OracleLinux 6

3.1.1 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

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

```
[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 Install Rsyslog 8 Package

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the commands below to download the Rsyslog repository configuration file:

```
# 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) Enter the command below to update the Rsyslog package:

```
# 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) Enter the command below to verify the Rsyslog version:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the rsyslog configuration file:

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

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

(2) Comment out the **imjournal** module:

```
# 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) Comment out **OmitLocalLogging**:

```
# $OmitLocalLogging on
```

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

(4) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(5) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment **SyslogFacility AUTHPRIV** and **LogLevel INFO**, then add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging.

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to edit the sshd_config configuration file:

```
# 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) Enter the command below to edit the rsyslog configuration file:

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

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

(3) Comment out **authpriv.***, and add syslogfacility-text "**auth**" or "**authpriv**" to store logs in /var/log/secure and forward them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment out LogLevel INFO, and add Facility AUTH and LogLevel VERBOSE for detailed logging:

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

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

```
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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the rsyslog configuration file:

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

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

(3) Comment out authpriv.* and add configuration to use syslogfacility-text “auth” or “authpriv”, storing logs in /var/log/secure and forwarding them to 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")}
```

```
#
# 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment out the line **LogLevel INFO**, then add **Facility AUTH** and **LogLevel VERBOSE** to enable detailed logging:

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the 50-default.conf configuration file for rsyslog:

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

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

(3) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment out the line **LogLevel INFO**, then add **Facility AUTH** and **LogLevel VERBOSE** to enable detailed logging:

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to edit the 50-default.conf configuration file for rsyslog:

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

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

(3) Comment out **authpriv.** * and add configuration to use syslogfacility-text "auth" or "authpriv", storing logs in /var/log/secure and forwarding them to 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment out the line **LogLevel INFO**, then add **Facility AUTH** and **LogLevel VERBOSE** to enable detailed logging:

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to check the Rsyslog version:

```
# 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) Enter the command below to create a new rsyslog configuration file named 100-sshd.conf:

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

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

(3) Configure SSH logs to be stored in /var/log/auth.log and forwarded to 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")}
```

Replace the red text with the N-Reporter system IP address.

(4) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Enter the command below to configure **SyslogFacility** and **LogLevel** for detailed logging:

```
SyslogFacility AUTH
LogLevel VERBOSE
```

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

(3) Enter the command below to restart the SSH service:

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

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

(4) Enter the command below to verify that the SSH service is running normally:

```
# svcs ssh
```

```
# svcs ssh
STATE          STIME    FMRI
online         14:49:19 svc:/network/ssh:default
#
```

7.1.2 Configure Rsyslog to Forward SSH Logs

(1) Enter the command below to display the status of the system-log service:

```
# svcs system-log
```

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

(2) Enter the command below to edit the syslog configuration file:

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

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

(3) Configure forwarding to N-Reporter:

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

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

Note: The facility.severity must be followed by <tab>, not a space.

Replace the red text with the N-Reporter system IP address.

(4) Enter the commands below to restart the syslog service and verify that it is running normally:

```
# 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 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Enter the command below to configure **SyslogFacility** and **LogLevel** for detailed logging:

```
SyslogFacility AUTH
LogLevel VERBOSE
```

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

(3) Enter the command below to restart the SSH service verify that it is running normally:

```
# 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 Check the Default syslog or rsyslog Service

7.2.2.1 Configure syslog to Forward SSH Logs

(1) Enter the command below to display the status of the system-log service:

```
# 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) Enter the command below to edit the syslog configuration file:

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

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

(3) Configure forwarding to N-Reporter:

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

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

Note: The facility.severity must be followed by <tab>, not a space.

Replace the red text with the N-Reporter system IP address.

(4) Enter the commands below to restart the syslog service and verify that it is running normally:

```
# 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 Configure rsyslog to Forward SSH Logs

(1) Enter the command below to display the status of the system-log service:

```
# 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) Enter the command below to check the Rsyslog version:

```
# /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) Enter the command below to create a new rsyslog configuration file named 100-sshd.conf:

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

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

(4) Configure SSH logs to be stored in /var/log/auth.log and forwarded to 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/authlog")
       action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp")}
```

Replace the red text with the N-Reporter system IP address.

(5) Enter the command below to restart the rsyslog service and verify that it is running normally:

```
# 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

Reference: HP-UX sshd syslog — HPE Documentation

(1) Enter the command below to edit the sshd_config configuration file:

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

(2) Configure SyslogFacility and LogLevel:

```
SyslogFacility AUTH
LogLevel VERBOSE
```

(3) Enter the command below to stop the SSH service:

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

(4) (4) Enter the command below to start the SSH service:

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

(5) Enter the command below to verify that the SSH service is running:

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

(6) Enter the command below to edit the syslog configuration file:

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

(7) Configure forwarding to N-Reporter:

```
# Send SSH log to N-Reporter
auth.info @192.168.3.88
```

Note: The facility.severity must be followed by <tab>, not a space.

Replace the red text with the N-Reporter system IP address.

(8) Enter the commands below to stop and then start the syslogd service:

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

9. AIX 7

(1) Enter the command below to edit the sshd_config configuration file:

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

(2) Configure SyslogFacility and LogLevel:

```
SyslogFacility AUTH
LogLevel VERBOSE
```

(3) Enter the command below to stop the SSH service:

```
# stopsrc -s sshd
```

(4) Enter the command below to start the SSH service:

```
# startsrc -s sshd
```

(5) Enter the command below to edit the syslog configuration file:

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

(6) Configure forwarding to N-Reporter:

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

Replace the red text with the N-Reporter system IP address.

(7) Enter the command below to stop the syslog service:

```
# stopsrc -s syslogd
```

(8) Enter the command below to start the syslog service:

```
# startsrc -s syslogd
```

10. FreeBSD 12

10.1 Edit SSH Configuration File

(1) Enter the command below to edit the sshd_config configuration file:

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

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

(2) Comment out **LogLevel INFO**, and add **SyslogFacility AUTH** and **LogLevel VERBOSE** for detailed logging:

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

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

(3) Enter the command below to restart the SSH service and verify that it is running normally:

```
# 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 Configure Syslog to Forward SSH Logs

(1) Enter the command below to edit the syslog configuration file:

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

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

(2) Configure forwarding to N-Reporter:

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

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

Note: The facility.severity must be followed by <tab>, not a space.

Replace the red text with the N-Reporter system IP address.

(3) Enter the command below to restart the syslog service:

```
# service syslogd restart
```

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

(4) Enter the command below to verify that the syslog service is running normally:

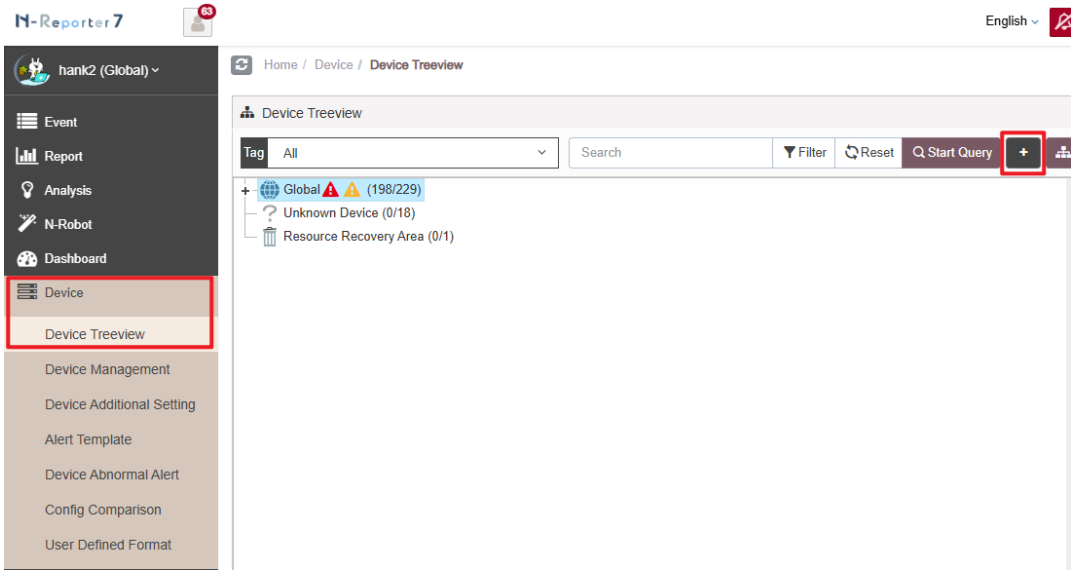
```
# service syslogd status
```

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

11. N-Reporter

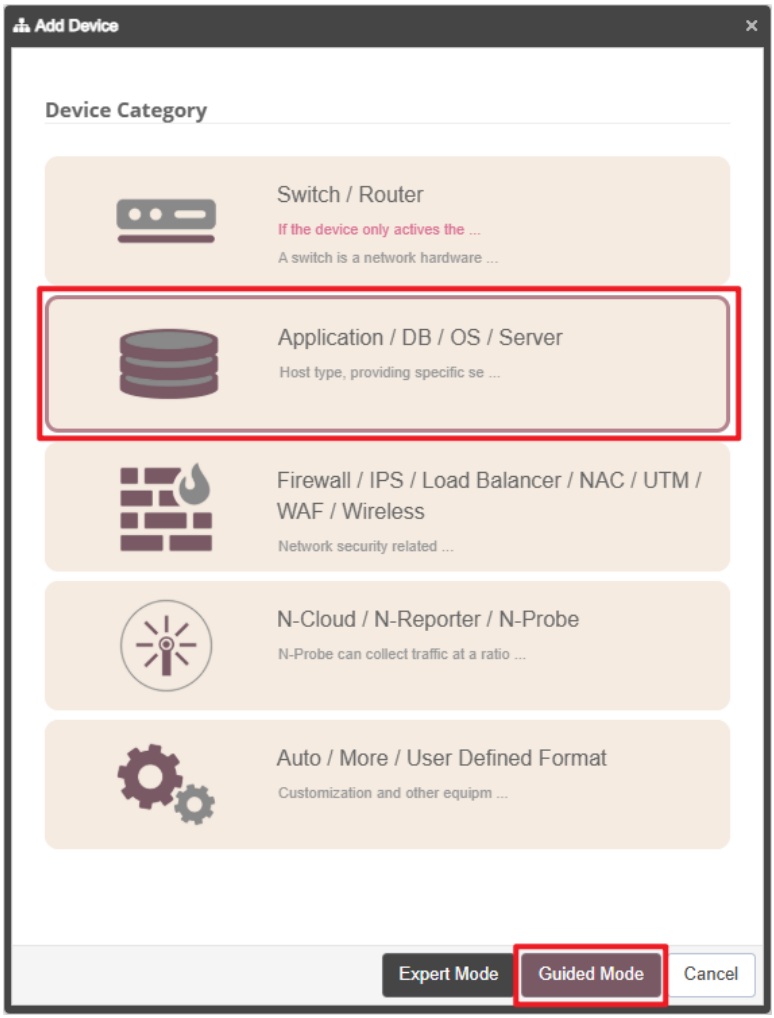
(1) Add an SSH Audit device:

Go to “Device Management” → “Device Treeview” → click “Add.”



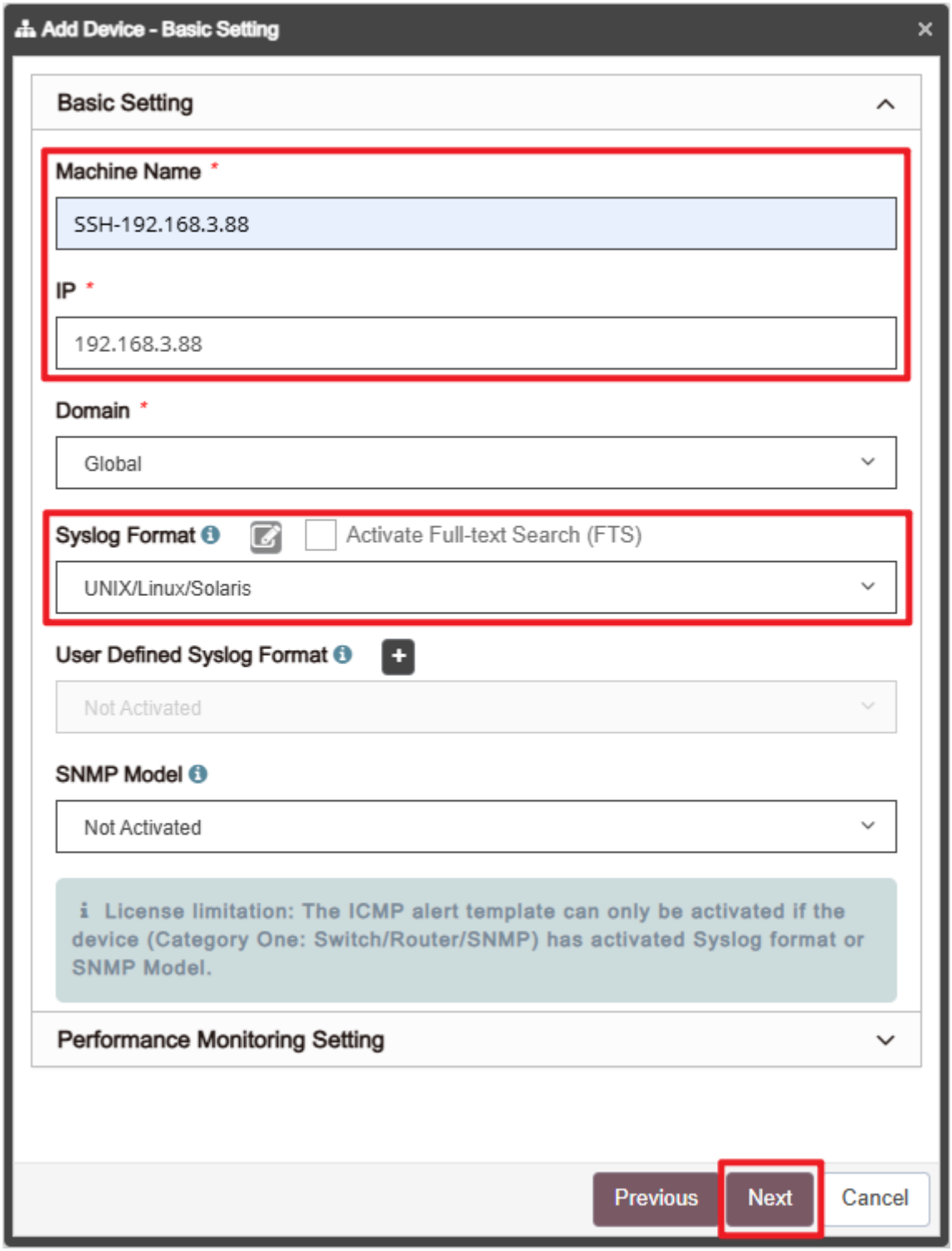
(2) Select the device type:

Choose “Application/DB/OS/Server” → click “Guided Mode.”



(3) Basic Device Settings:

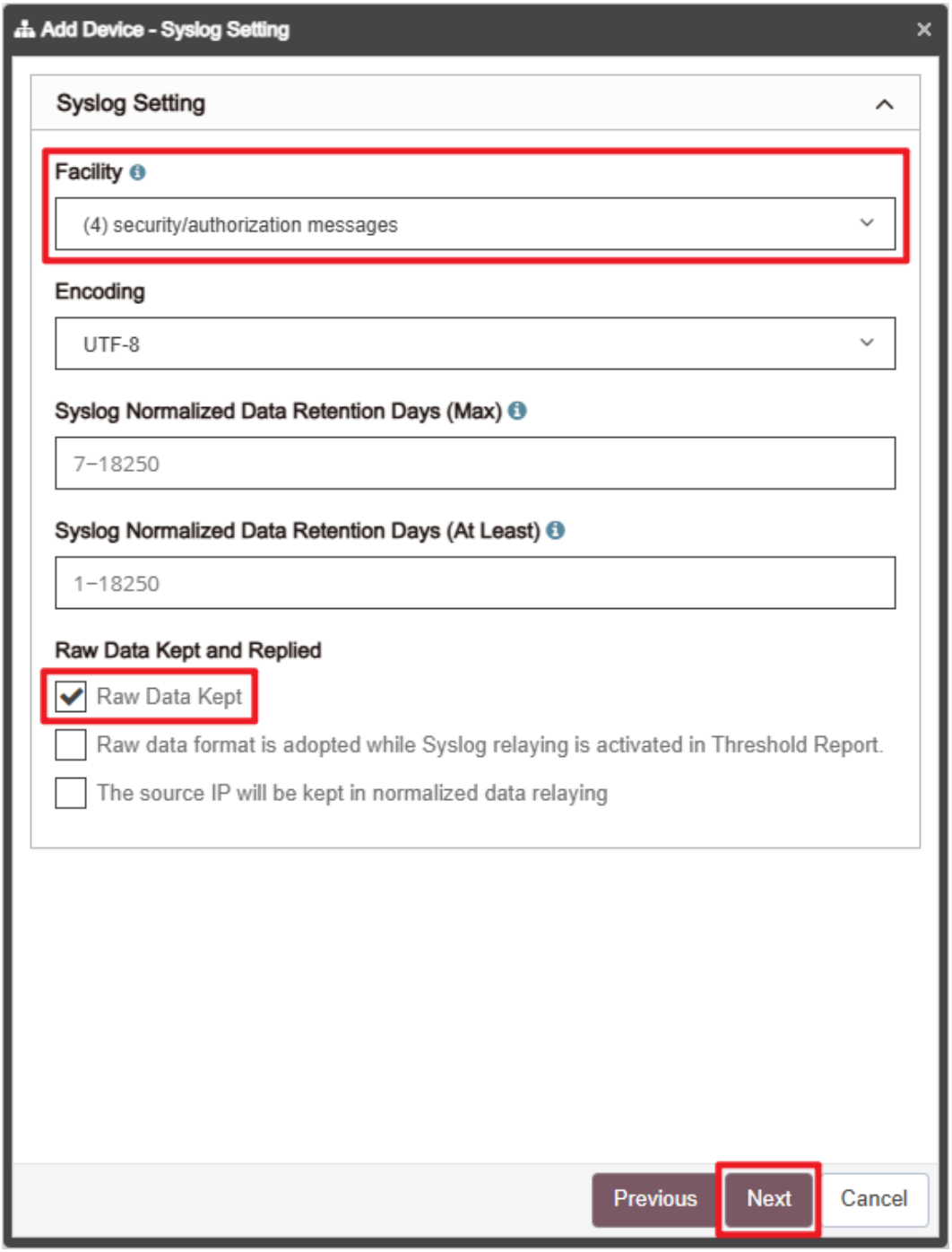
Enter the device name and IP address → For Syslog Data Format, select “UNIX/Linux/Solaris” → click “Next.”



(4) Syslog Settings

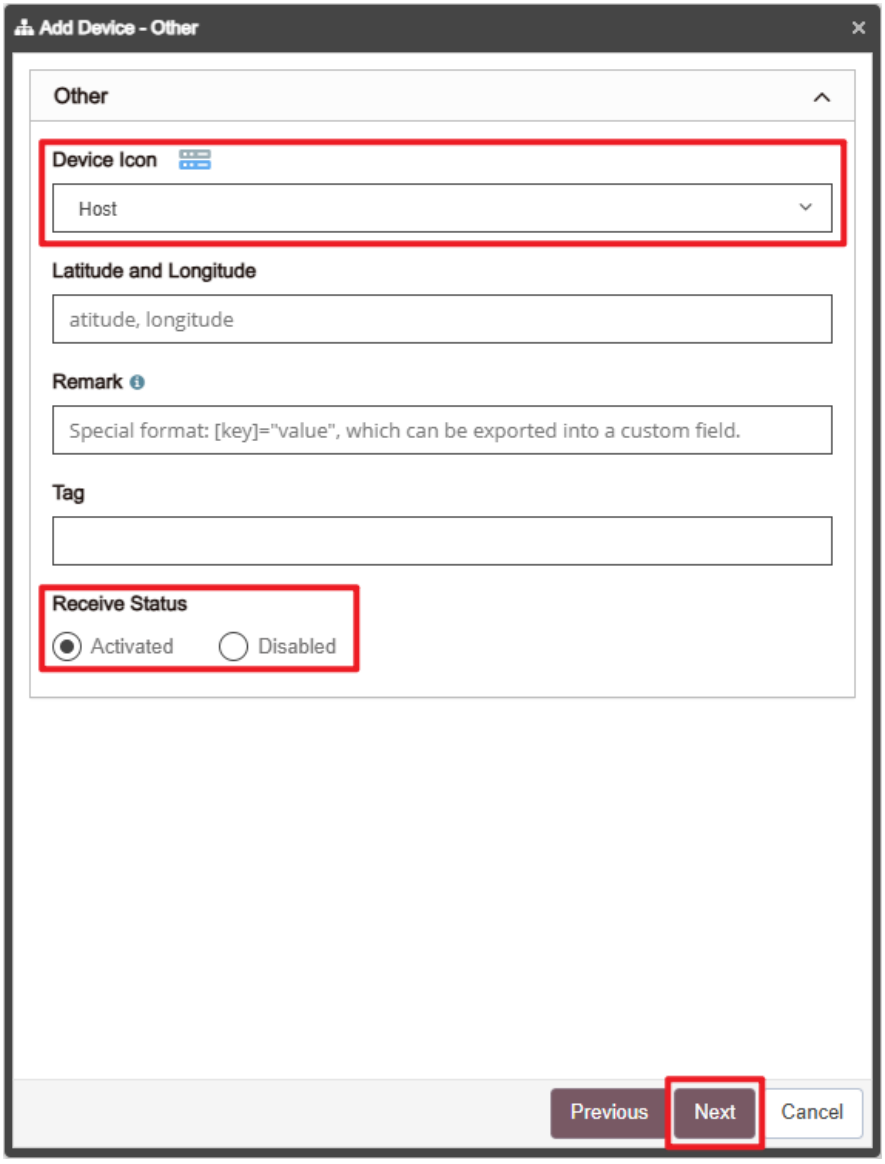
Set “Facility” to “(4) security/ authorization messages” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.

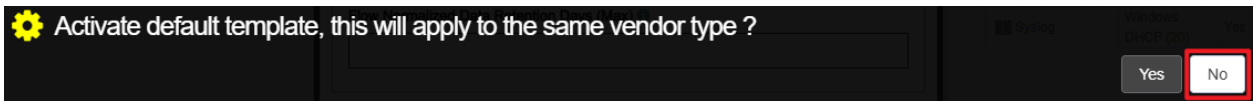


(5) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next” → Confirm.



Activate default templates for devices of the same vendor type, click “No.”



Tel：+886-4-23752865　Fax：+886-4-23757458
Sales Information：sales@npartner.com
Technical Support：support@npartner.com