N-Partner

N-REPORTER

How to manage audit log for Linux

V 1.1.2

(01-03-03-005) 2016/04/29

Preface

This manual is mainly describing how to use N-Reporter to receive Linux Audit syslog. This manual focuses on how to set up rsyslog, in order to let Linux can send audit syslog to N-Reporter without problem.

N-Reporter is a product of N-Partner, it is the main Syslog analyzer in the industry. It can analyze received Syslog, and produce many kinds of professional reports.

There are many different versions about Linux OS, such as: Debian 、SUSE 、Redhat、CentOS, etc. In this manual we use Debian 6.X as the environment for example.

How to set up Linux rsyslog to forward audit syslog

Setting up Linux

1. Log in Linux with root or the user has a proper permission.

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

2. Edit /etc/rsyslog.conf, launch UDP model, delete the pound sign # of the following two lines.

```
$ModLoad imudp.so
$UDPServerRun 514
```

3. Add a new line at the end of rsyslog.conf profile. 192.168.2.2 is the IP of N-Reporter.

```
auth, authpriv.*    @192.168.2.2:514
```

4. Restart rsyslog

```
/etc/init.d/rsyslog restart
```

5. After restarting rsyslog, all the audit log about login and logout will be send to N-Reporter. In this case, we can track and execute the audit planning completely through N-Reporter.

Technical Support：

Email: support@npartnertech.com

Skype：support@npartnertech.com

Sales Information：

Email: sales@npartnertech.com

N-Partner