N-Partner

N-REPORTER

如何管理 Linux 登入登出审核

V 1.1.2 (简体)

(01-01-02-005) 2014/01/02

前言

这份文件主要描述如何使用 N-Reporter 接收 Linux Audit syslog。此文件着重于如何设定 Rsyslog ，使得 Linux 可以顺利将 audit syslog 送至 N-Reporter。

N-Reporter 为 N-Partner 所有。为目前业界主要的 Syslog 分析仪。能够统计分析接收的 Syslog，产生各式各样的专业报表。

Linux 目前发行的版本繁多，例如：Debian、 SUSE、 Redhat、CentOS 等。
此文件使用 Debian 6.X 版本作为实际的范例。

文件章节如下

连络信息

N-Partner 公司连络方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有关技术问题请洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有关业务相关问题请洽：

Email: sales@npartnertech.com

如何设定 Linux rsyslog 转发 audit syslog

Linux 设定的步骤如下：

1. 登入 Linux 主机。请注意用户权限问题或者使用 root 登入。

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

2. 编辑/etc/rsyslog.conf，启动 UDP 模块，移去下面两行的註解#

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

3. 在 rsyslog.conf 配置文件的最后面，新增一行。其中 192.168.2.2 为 N-Reporter 的 IP。

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

4. 重新启动 Rsyslog

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

5. Rsyslog 重启后，即会将 Linux 系统之后的登入登出或者尝试登入者的讯息送至 N-Reporter。如此，透过 N-Reporter 即可完整的追踪和执行审核的计划。

采购与销售合作：sales@npartnertech.com
技术咨询：support@npartnertech.com