N-Partner

N-REPORTER

如何管理Squid Syslog稽核记录

V 1.1.1 (简体)

前言

Squid 为 Linux 上常见的 Proxy 服务，为了要让 N-Reporter 顺利管理 Squid Syslog，请按照建议步骤自定义 Syslog 格式。

此文件的范例，是以 Linux Squid 2.7 为范例。

文件章节如下：

连络信息.....1
如何自定义 Linux Squid syslog 输出格式.....2
如何设定 Linux rsyslog 转发 squid syslog.....2

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

如何自定义 Linux Squid syslog 输出格式

Linux Squid 设定的步骤如下：

►**step1:** 登入 Linux 主机。请注意用户权限问题或者使用 root 登入。

vi /etc/squid/squid.conf

►**step2:** 搜寻 access_log 的位置，新增一行或者修改设定如下所示。

#access_log /var/log/squid/access.log squid

access_log syslog:local4.info squid

Local4.info 依据您的需求做适当的修改。

►**step3:** 搜寻 access_log 的位置，新增一行或者修改设定如下所示。

logformat

squid %ts.%03tu %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt

►**step4:** 搜寻 access_log 的位置，新增一行或者修改设定如下所示。

/etc/init.d/squid restart

如何设定 Linux rsyslog 转发 squid syslog

Linux 设定的步骤如下：

►**step1:** 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

►**step2:** 在rsyslog.conf 档的最后面新增一行，其中192.168.2.3 为N-Reporter的IP。local4 必须等于squid.conf 的设定值（access_log syslog:local4.info squid）。

local4.* @192.168.2.3

►**step3:** 重新启动 rsyslog

/etc/init.d/rsyslog restart

►**step4:** rsyslog 重启后，即会将 Linux 系统之后的 squid syslog 送至 N-Reporter(192.168.2.3)

如此，透过 N-Reporter 即可完整的追 squid 所有的 syslog 记录。

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