N-Partner

N-REPORTER

How to manage Audit log of Squid Syslog

V 1.1.1

Preface

Squid is a common proxy service in Linux. In order to let N-Reporter manage Squid Syslog without problem, please use the following recommended steps to set up your own Syslog.

In this manual, we use Linux Squid 2.7 for example.

Contents

How to set up Output format of Linux Squid

Linux Squid setup steps

►**step1:** Login Linux with root or the user has a property permission.

vi /etc/squid/squid.conf

►**step2:** Search the location of access_log. Add a new line or edit as following.

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

access_log syslog:local4.info squid

Local4.info (Make changes according to your needs.)

►**step3:** Search the location of access_log. Add a new line or edit as following.

logformat

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

►**step4:** Search the location of access_log. Add a new line or edit as following.

/etc/init.d/squid restart

How to set up **Linux rsyslog** forward to **squid syslog**

Linux setup:

►**step1:** Login Linux with root or the user has a proper permission.

vi /etc/rsyslog.conf

►**step2:** Add a new line in the end of rsyslog.conf profile, 192.168.2.3 is an IP of N-Reporter. The setting of local4 must be as the same as squid.conf（access_log syslog:local4.info squid）。

local4.* @192.168.2.3

►**step3:** Restart rsyslog

/etc/init.d/rsyslog restart

►**step4:** After restarting rsyslog, all the squid syslog of Linux will be send to N-Reporter (192.168.2.3)

In this case, N-Reporter can track all the syslog of squid completely.