
Section 7 -- Syslog Event and Volume Logs

Formats of log records are as follows. Your syslog daemon will add the date and time, and the name of the NAT (or IP Address, if not in your DNS) at the beginning of each log record. All fields are colon-delimited for easy processing off-line. IP Addresses are 32-bit hexadecimal, flags are 16-bit hexadecimal. All other numeric fields are in decimal.

Mapping Event

This logs initial inbound connection events for port-style service mapping facilities. One should be careful with this, as it could create a lot of log information. It is enabled by setting the msb of the flags field (0x8000 or 0xc000 both have this bit set, 0x0000 and 0x4000 don't).

Log Record Format

`pr:int:srcip:srcport:dstip:dstport:prot`

Log Record Data

Field Name	Description
pr	Log record type indicator for port Mapping events.
int	The name of the interface where the message arrived.
srcip	The source IP Address of the message (who it came from).
srcport	The source Port Number from the message.
dstip	The destination IP Address of the message (who it was sent to).
dstport	The destination Port Number from the message.
prot	A numeric value indicating the communications protocol in use.

Protocol Number	Name
1	ICMP
2	IGMP (used with multicast applications like video conferencing)
4	IP-in-IP Encapsulation (RFC 2003)
6	TCP
17	UDP
47	GRE (used with PPTP, etc.)
55	Minimum IP-in-IP Encapsulation (RFC 2004)
94	Older IP-in-IP Encapsulation

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting events, unless modified with the "syslog facility" and/or "syslog priority" commands.

Default Mapping Event

This logs initial inbound connection events for default-style service mapping facilities. While one should be careful with this, due to the possibility of a massive number of events logged, this one can be very interesting. It logs redirection of protocols that you didn't anticipate. Typical examples are the "Authentication Protocol," where telnet servers attempt to learn more about the client user. It is enabled by setting the msb of the flags field (0x8000 or 0xc000 both have this bit set, 0x0000 and 0x4000 don't).

Log Record Format

df:int:srcip:srcport:dstip:dstport:prot

Log Record Data

Field Name	Description
df	Log record type indicator for default Mapping events.
int	The name of the interface where the message arrived.
srcip	The source IP Address of the message (who it came from).
srcport	The source Port Number from the message.
dstip	The destination IP Address of the message (who it was sent to).
dstport	The destination Port Number from the message.
prot	A numeric value indicating the communications protocol in use.

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting events, unless modified with the "syslog facility" and/or "syslog priority" commands.

Access Denied Mapping Event

This logs initial outbound connection attempts that are rejected because the user has been denied direct access to the Internet by the "access deny" command. It is enabled by appending "log" to the end of the "Access Deny" command. The syslog priority used in the logging of these events is the same as selected for other Reject events. Use the Syslog Reject command to select the desired priority. This logging mode can generate a lot of data, so use it with care.

Log Record Format

ac:int:srcip:srcport:dstip:dstport:prot

Log Record Data

Field Name	Description
ac	Log record type indicator for Access Denied events.
int	The name of the interface where the message arrived.
srcip	The source IP Address of the message (who it came from).
srcport	The source Port Number from the message.
dstip	The destination IP Address of the message (who it was sent to).
dstport	The destination Port Number from the message.
prot	A numeric value indicating the communications protocol in use.

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting "access denied" events, unless modified with the "syslog facility" and/or "syslog reject" commands.

Reject Mapping Event

This logs initial inbound connection events that are rejected because they didn't match any of the pre-established Service Mapping relationships. In other words, this logs deflected queries for services that you did not intend to provide. Typical examples are the "Authentication Protocol," where telnet servers attempt to learn more about the client user. It is enabled by the Syslog Reject command. This logging mode can generate a lot of data, so use it with care.

Log Record Format

rej:int:srcip:srcport:dstip:dstport:prot

Log Record Data

Field Name	Description
rej	Log record type indicator for reject Mapping events.
int	The name of the interface where the message arrived.
srcip	The source IP Address of the message (who it came from).
srcport	The source Port Number from the message.
dstip	The destination IP Address of the message (who it was sent to).
dstport	The destination Port Number from the message.
prot	A numeric value indicating the communications protocol in use.

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting reject events, unless modified with the "syslog facility" and/or "syslog reject" commands.

Service Mapping Statistics

If enabled, this logs data volumes in and out for a service mapping relationship. The log record is sent only when actual data traffic has occurred. It is sent each minute when a non-zero value can be reported. It can generate a lot of data, so use it with care, or be thoughtful in selecting which proxies are monitored.

Log Record Format

```
ps:int:appip:appport:actip:actport:prot:flags:bin:cin:bout:cout
```

Log Record Data

Field Name	Description
ps	Log record type indicator for statistics.
int	The name of the interface where the service occurred.
appip	The apparent IP for this service.
appport	The apparent Port Number for this service.
actip	The actual IP for this service.
actport	The actual Port Number for this service.
prot	A numeric value indicating the communications protocol in use.
flags	The current value of the optional hex flags field for this Mapping.
bin	The number of blocks received from the public net this minute.
cin	The number of characters received from the public net this minute.
bout	The number of blocks sent to the public net this minute.
cout	The number of characters sent to the public net this minute.

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting statistics, unless modified with the "syslog facility" and/or "syslog priority" commands.

NAT UP Message

If a syslog server is defined, the NetNAT will report "up" status via syslog approximately one minute after starting. The delay allows various facilities to settle. The purpose of this is to track the number of reboots, without regard for the reason, since it's almost always too late to find out why. The common reasons for restarting are:

- ◆ The software took a flying leap into nowhere
- ◆ The hardware watchdog timer caught us napping
- ◆ Someone punched the reset button
- ◆ We loaded new software or configuration data

Log Record Format

up:hostname

up:hostname(wd)

Log Record Data

Field Name	Description
up	Log record type indicator for UP event.
hostname	The NetNAT's configured hostname. The setup program assigns the NetNAT a hostname at installation. The hostname global command also allows you to assign a name to the NetNAT.
(wd)	This suffix indicates that the current NetNAT startup was due to a hardware watchdog timer expiration, as opposed to a manual restart.

The NetNAT uses syslog facility "LOCAL2" and priority "INFO" when reporting "up" status, unless modified with the "syslog facility" and/or "syslog priority" commands.