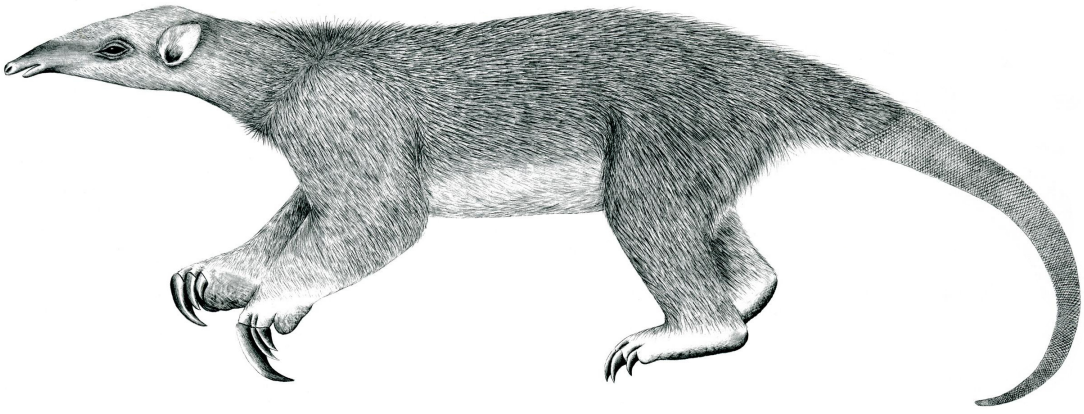
Tranalyzer2

syslogDecode

Syslog



Tranalyzer Development Team

Contents

1 syslogDecode

1.1 Description

The syslogDecode plugin analyzes Syslog traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
SYSL_FSN	0	Format for Syslog severity/facility messages: 0: Numbers, 1: Names	

1.3 Flow File Output

The syslogDecode plugin outputs the following columns:

Column	Type	Description	Flags
syslogStat	H8	Status	
syslogMCnt	U32	message count	
syslogSev_Fac_Cnt	RU8_U8_U32	Number of severity/facility messages	

1.3.1 syslogStat

The syslogStat column is to be interpreted as follows:

syslogStat	Description
0x01	Syslog detected
0x02	—
0x04	—
0x08	—
0x10	—
0x20	—
0x40	—
0x80	Counter for facility/severity overflowed

1.4 Packet File Output

In packet mode (-s option), the syslogDecode plugin outputs the following columns:

Column	Type	Description	Flags
syslogStat	H8	Status	
syslogSev	U8/S	Severity	SYSL_FSN=0/1
syslogFac	U8/S	Facility	SYSL_FSN=0/1

1.5 Plugin Report Output

The following information is reported:

- Aggregated syslogStat
- Number of Syslog packets
- Number of Syslog message types

1.6 TODO

- IPv6 tests

1.7 References

- https://tools.ietf.org/html/rfc5424