

Apps to the Rescue

Browse More Apps

CATEGORY

☐ DevOps

☐ IT Operations

☐ Security, Fraud & Compliance

☐ Business Analytics

☐ IoT & Industrial Data

☐ Utilities

CIM VERSION

☐ 4.9

☐ 4.8

☐ 4.7

☐ 4.6

☐ 4.5

☐ 4.4

☐ 4.3

☐ 4.2

☐ 4.1

☐ 4.0

☐ 3.0

Best MatchNewestPopular

2 Apps

TA

Linux Netfilter (iptables) technology add-on

Install

This app provides Linux Netfilter (aka iptables) field extractions and normalisation to the Common Information Model.

N.B. This app was written because the existing TA for iptables on Splunkbase (<https://splunkbase.splunk.com/app/920/>) is no longer being maintained.

Splunk Certified

splunkbase

Search App by keyword, technology

TA

Linux Netfilter (iptables) technology add-on

★★★★★ 1 rating

Splunk Certified

VERSION

0.1.2 ↕

BUILT BY

[Doug Brown](#)

CATEGORY & CONTENTS

Categories: [Security, Fraud & Compliance](#)

App Type: [Add-on](#)

COMPATIBILITY

Products: [Splunk Cloud](#), [Splunk Enterprise](#)

Splunk Versions: [7.0](#), [6.6](#), [6.5](#), [6.4](#), [6.3](#), [6.2](#)

Platform: [Platform Independent](#)

CIM Versions: [4.9](#), [4.8](#), [4.7](#), [4.6](#), [4.5](#), [4.4](#)

LICENSING

[MIT](#)

SUPPORT

[Contact Developer](#)

Developer Supported

[Questions on Splunk Answers](#)

[Flag as inappropriate](#)

What Does the App Give Us?

- Note: the sourcetype changes to "linux:netfilter"

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Close

sourcetype="linux:netfilter" Last 24 hours Q

✓ 958,982 events (4/5/18 9:00:00.000 PM to 4/6/18 9:22:07.000 PM) No Event Sampling Job || ↶ ↷ ⬇ Smart Mode

Events (958,982) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields	All Fields	i	Time	Event
Selected Fields		>	4/6/18 9:22:05.000 PM	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845872] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53370 DF PROTO=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = linux:netfilter
a host 1		>	4/6/18 9:22:05.000 PM	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845865] IN=lo OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53370 DF PROTO=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = linux:netfilter
a source 1		>	4/6/18 9:22:05.000 PM	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845849] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=537 TOS=0x00 PREC=0x00 TTL=64 ID=29176 DF PROTO=TCP SPT=8191 DPT=54904 WINDOW=359 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = linux:netfilter
a sourcetype 1		>	4/6/18 9:22:05.000 PM	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845839] IN=lo OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=537 TOS=0x00 PREC=0x00 TTL=64 ID=29176 DF PROTO=TCP SPT=8191 DPT=54904 WINDOW=359 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = linux:netfilter
Interesting Fields		>	4/6/18 9:22:05.000 PM	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845699] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=139 TOS=0x00 PREC=0x00 TTL=64 ID=53369 DF PROTO=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK PSH URGP=0 host = ip-10-13-133-189 source = /var/log/syslog sourcetype = linux:netfilter
# date_hour 24		>	4/6/18	Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845689] IN=lo OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=139 TOS=0x00 PREC=0x00 TTL=64 ID=53369
# date_mday 2				
# date_minute 60				
a date_month 1				
# date_second 60				
a date_wday 2				
# date_year 1				
a date_zone 1				
a dest 15				

What Does the App Give Us? CIM

4/6/18

Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845872] IN=lo OUT= MAC=00:00:00:00:00:00:00:00:00:00:08:00 SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53370 DF PROTO=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0

Event Actions

Type	Field	Value	Actions
Selected	host	ip-10-13-133-189	
	source	/var/log/syslog	
	sourcetype	linux.netfilter	
Event	DPT	8191	
	DST	127.0.0.1	
	FLAGS	ACK	
	FRAME_TYPE	08:00	
	ID	53370	
	IN	lo	
	LEN	52	
	MAC	00:00:00:00:00:00:00:00:00:00:08:00	
	PREC	0x00	
	PROTO	TCP	
	RES	0x00	
	SPT	54904	
	SRC	127.0.0.1	
	TOS	0x00	
	TTL	64	
	URGP	0	
	WINDOW	3637	
	dest	127.0.0.1	
	dest_ip	127.0.0.1	
	dest_mac	00:00:00:00:00:00	
	dest_port	8191	
	direction	inbound	
	dvc	ip-10-13-133-189	
	dvc_host	ip-10-13-133-189	
	eventtype	linux_netfilter (communicate network)	
		linux_scripted_input (check report)	
		nix-all-logs	
		nix_kernel_attached	
	protocol	ip	
	src	127.0.0.1	

src	127.0.0.1	
src_interface	lo	
src_ip	127.0.0.1	
src_mac	00:00:00:00:00:00	
src_port	54904	
tag	check	
	communicate	
	network	
	report	
tcp_flag	ACK	
tos	0x00	
transport	tcp	
ttl	64	
vendor_product	Linux Netfilter	
Time	_time	2018-04-06T21:22:05.000+00:00
Default	index	os
	linecount	1
	punct	
	splunk_server	ip-10-13-133-189

4/6/18

Apr 6 21:22:05 ip-10-13-133-189 kernel: [286523.845865] IN= OUT=lo SRC=127.0.0.1 DST=127.0.0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53370 DF PROTO=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0