Discover

New Save Open Share Inspect

KQL Last 15 minutes Show dates Refresh

Search

+ Add filter

metricbeat*

Search field names

Filter by type

0

Selected fields

_source

Available fields

_id
_index
_score
_type
@timestamp
@version
@version.keyword_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
ecs.version
event.dataset
event.duration
event.module
host.architecture
host.hostname
host.id
host.ip
host.mac
host.name
host.os.build
host.os.family
host.os.kernel
host.os.name
host.os.platform
host.os.version
metricset.name
metricset.period
process.args
process.executable
process.name
process.pgid
process.pid
process.ppid
service.type
system.cpu.cores
system.cpu.idle.pct
system.cpu.iowait.norm.pct
system.cpu.iowait.pct
system.cpu.nice.norm.pct
system.cpu.nice.pct
system.cpu.system.norm.pct
system.cpu.softirq.pct
system.cpu.steal.norm.pct
system.cpu.steal.pct
system.cpu.system.norm.pct
system.cpu.system.pct
system.cpu.total.norm.pct
system.cpu.total.pct
system.cpu.user.norm.pct
system.cpu.user.pct
system.filesystem.available
system.filesystem.device_name
system.filesystem.files
system.filesystem.free
system.filesystem.free_files
system.filesystem.mount_point
system.filesystem.total
system.filesystem.type
system.filesystem.used.bytes
system.filesystem.used.pct
system.fsstat.count
system.fsstat.total_files
system.fsstat.total_size.free
system.fsstat.total_size.total
system.fsstat.total_size.used
system.load.1
system.load.15
system.load.5
system.load.cores
system.load.norm.1
system.load.norm.15
system.load.norm.5
system.memory.actual.free
system.memory.actual.used.bytes
system.memory.actual.used.pct
system.memory.free
system.memory.swap.free
system.memory.swap.total
system.memory.swap.used.bytes
system.memory.swap.used.pct
system.memory.total
system.memory.used.bytes
system.memory.used.pct
system.network.in.bytes
system.network.in.dropped
system.network.in.errors
system.network.in.packets
system.network.name
system.network.out.bytes
system.network.out.dropped
system.network.out.errors
system.network.out.packets
system.process.cmdline
system.process.cpu.start_time
system.process.cpu.total.norm.pct
system.process.cpu.total.pct
system.process.cpu.total.value
system.process.memory.rss.bytes
system.process.memory.rss.pct
system.process.memory.share
system.process.memory.size
system.process.name
system.process.state
system.process.summary.dead
system.process.summary.idle
system.process.summary.running
system.process.summary.sleep
system.process.summary.stopped
system.process.summary.total
system.process.summary.unknown
system.process.summary.zombie
system.process.summary.zombie
system.socket.summary.all.listening
system.socket.summary.tcp.all.count
system.socket.summary.tcp.all.listening
system.socket.summary.tcp.all.orphan
system.socket.summary.tcp.all.tw
system.socket.summary.udp.all.count
tags
user.name

2,134 hits

Sep 27, 2020 @ 11:00:25.535 - Sep 27, 2020 @ 11:15:25.535 Auto

Count

@timestamp per 30 seconds

Time _	_source
> Sep 27, 2020 @ 11:15:18.965	tags: beats_input_raw_event Version: 1 host.ip: fe80::aede:48ff:fe00:1122, fe80::142c:d5cf:b2c:d299, 192.168.0.115, fe80::2845:23ff:fe42:3a9, fe80::2845:23ff:fe42:3a9, fe80::300:7a3:7ff6:689c, fe80::b624:5ba3:7b95:f916, fe80::d882:b20:df6d:4f52, fe80::2845:a8a7:3d9c:a858, fe80::4752:c0c1:bc9:a9fb, fe80::9d73:8f9a:a787:30 host.mac: ac:de:48:00:11:22, a6:83:e7:d0:62:8a, a4:83:e7:d0:62:8a, 42:01:0a:a4:00:06, 02:42:f5:ff:ac:06, 02:42:f5:ff:ac:07, 02:42:f5:ff:ac:08, 02:42:f5:ff:ac:09, 06:83:e7:d0:62:8a, 2a:45:23:42:3e:19, 2a:45:23:42:3e:19 host.name: Roberts-MacBook-Pro.local host.hostname: Roberts-MacBook-Pro.local host.os.version: 10.15.7
> Sep 27, 2020 @ 11:15:18.965	process.args: /usr/local/Cellar/kibana-full/7.9.2/libexec/jdk.app/Contents/Home/bin/java, -Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CmsInitiatingOccupancyFraction=75, -XX:+UseCMSInitiatingOccupancyOnly, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.invokedynamic=true, -Djruby.jit.threshold=0, -Djruby.regexp.interruptible=true, -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Djava.io.tmpdir=/var/folders/_q/_ldqqqqx0ln0ln0ln