Discover

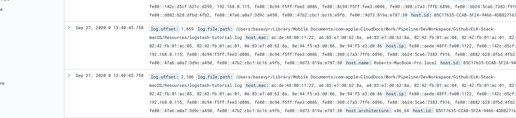
New Save Open Share Inspect

Search KQL Last 15 minutes Show dates Refresh

+ Add filter

71,651 hits

Sep 27, 2020 @ 13:27:33.191 - Sep 27, 2020 @ 13:42:33.191 Auto



filter

Search field names

Filter by type

Selected fields

_source

Available fields

_id
_index
_score
_type
@timestamp
@version
host.ephemeral_id
agent.id
agent.name
agent.type
agent.version
container.id
ecs.version
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
input.type
log.file.path
log.offset
message
tags

Time _source

```
> Sep 27, 2020 @ 13:40:45.750  log.offset: 1,153  log.file.path: /Users/beasley/Library/Mobile Documents~com~apple~CloudDocs/Work/Pipeline/Overkkopass/GitHub/ELK-Stack-mac05/Resources/logstash-tutorial.log  host.mac: ac:de:48:00:11:22,  ab:03:a7:d0:62:8a,  ab:03:a7:d0:62:8a,  82:42:fb:91:ae:00,  82:42:fb:91:ae:00,  82:42:fb:91:ae:00,  82:42:fb:91:ae:00,  82:42:fb:91:ae:00,  86:03:a7:d0:62:8a,  9e:94:f5:a3:d0:9e,  9e:94:f5:a3:d0:9e  host.architecture: x86_64  host.id: fe8d:ae6e:4ff:fe88:7122,  fe8d:1a2c:d5cf:b21c:d599,  192.168.0.115,  fe80:8c94:f5ff:fed2:d886,  fe80:8c94:f5ff:fed2:d886,  fe80:8c94:f5ff:fed2:d886,  fe80:3ab:c7f6:6896,  fe80:3ab:c7f6:6896,  fe80:8c94:f5ff:fed2:d886
```