Discover

New Save Open Share Inspect

Search

KQL Sep 29, 2020 @ 09:04:21.9 → Sep 29, 2020 @ 09:20:30.3 Refresh

+ Add filter

file*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

- message
- tags
- _id
- _index
- _score
- _type
- @timestamp
- @version
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- container.id
- ecs.version
- host.architecture
- host.boot.id
- 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

3,911 hits

Sep 29, 2020 @ 09:04:21.954 - Sep 29, 2020 @ 09:20:30.349 Auto

Time _ source

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 584,493 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 585,593 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 586,722 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 587,643 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 588,764 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 589,853 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 590,959 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 592,027 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 593,229 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 594,179 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 595,383 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 596,509 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 597,643 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 598,757 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 599,494 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 584,477 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 585,571 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 586,685 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 587,799 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 588,874 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 584,577 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 589,680 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 590,783 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 591,869 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 592,944 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 593,923 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 594,864 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 595,937 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 596,509 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 597,081 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 595,025 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorkspace/Github/ELK-Stack-macOS/Resources/logstash-tutorial.log log.offset: 596,141 host.architecture: x86_64 host.os.version: 10.15.7 host.os.platform: darwin host.os.name: Mac OS X host.os.kernel: 19.6.0 host.os.family: darwin host.os.build: 19G2 host.hostname: Roberts-MacBook-Pro.local host.name: Roberts-MacBook-Pro.local host.mac: ac:de:48:00:11:22, a6:83:e7:d8:62:8a, a6:83:e7:d8:62:8b, a6:83:e7:d8:62:9a, a6:83:e7:d8:62:9b, 82:42:f5:91:ac:01, 82:42:f5:91:ac:00, 82:42:f5:91:ac:05, 82:42:f5:91:ac:04, 86:3f:a4:21:f2:1e, ae:7f:fe:21:f2:1e

> Sep 29, 2020 @ 09:19:23.281 @timestamp: Sep 29, 2020 @ 09:19:23.281 tags: [beats_input_codec_plain_applied] @version: 1 container.id: com-apple-CloudDocs log.file.path: /Users/bassery/Library/Mobile Documents/com~apple~CloudDocs/Work/Pipeline/DevWorksp