```
{
  "_index": "auditbeat-7.5.1-2023.02.12-000040",
  "_id": "ddfYt4YBTU-oy5CHN7aF",
  "_version": 1,
  "_score": 0,
  "_source": {
    "@timestamp": "2023-03-06T16:54:04.873Z",
    "process": {
      "pid": 14827
    },
    "service": {
      "type": "system"
    },
    "cloud": {
      "availability_zone": "asia-northeast1-b",
      "instance": {
        "id": "233459340444774954",
        "name": "nicolesstevesghost2"
      },
      "machine": {
        "type": "n1-standard-1"
      },
      "project": {
        "id": "elastic-sa"
      },
      "provider": "gcp"
    },
    "destination": {
      "packets": 5,
      "bytes": 87210,
      "ip": "132.132.132.132",
      "port": 80
    },
    "network": {
      "direction": "outbound",
      "type": "ipv4",
      "transport": "tcp",
      "packets": 9,
      "bytes": 87370,
      "community_id": "1:lLx0NH+yoqWDcbt7wA20U9EU5to="
    },
    "flow": {
      "final": true,
      "complete": false
    },
    "event": {
      "end": "2023-03-06T16:54:03.039Z",
      "duration": 808365,
      "module": "system",
      "dataset": "socket",
      "kind": "event",
      "action": "network_flow",
      "category": "network_traffic",
      "start": "2023-03-06T16:54:03.038Z"
```

```
    },
    "agent": {
      "type": "auditbeat",
      "ephemeral_id": "da569583-3772-465b-b481-478acec831d4",
      "hostname": "nicolesstevesghost2",
      "id": "bd332535-5af4-4c27-8a11-6b9a8060acf9",
      "version": "7.5.1"
    },
    "source": {
      "port": 52316,
      "packets": 4,
      "bytes": 160,
      "ip": "10.146.15.198"
    },
    "server": {
      "port": 80,
      "packets": 5,
      "bytes": 87210,
      "ip": "132.132.132.132"
    },
    "system": {
      "audit": {
        "socket": {
          "kernel_sock_address": "0xffff8d1411f3b000"
        }
      }
    },
    "host": {
      "containerized": false,
      "name": "nicolesstevesghost2",
      "hostname": "nicolesstevesghost2",
      "architecture": "x86_64",
      "os": {
        "version": "16.04.6 LTS (Xenial Xerus)",
        "family": "debian",
        "name": "Ubuntu",
        "kernel": "4.15.0-1052-gcp",
        "codename": "xenial",
        "platform": "ubuntu"
      },
      "id": "15968c8010a2822cccc93ce79efa7afb"
    },
    "ecs": {
      "version": "1.1.0"
    },
    "client": {
      "port": 52316,
      "packets": 4,
      "bytes": 160,
      "ip": "10.146.15.198"
    }
  },
  "fields": {
    "event.category": [
```

```
    "network_traffic"
  ],
  "server.ip": [
    "132.132.132.132"
  ],
  "host.hostname": [
    "nicolesstevesghost2"
  ],
  "process.pid": [
    14827
  ],
  "cloud.availability_zone": [
    "asia-northeast1-b"
  ],
  "service.type": [
    "system"
  ],
  "system.audit.socket.kernel_sock_address": [
    "0xffff8d1411f3b000"
  ],
  "host.os.version": [
    "16.04.6 LTS (Xenial Xerus)"
  ],
  "host.os.name": [
    "Ubuntu"
  ],
  "source.ip": [
    "10.146.15.198"
  ],
  "host.name": [
    "nicolesstevesghost2"
  ],
  "network.community_id": [
    "1:lLx0NH+yoqWDcbt7wA20U9EU5to="
  ],
  "event.kind": [
    "event"
  ],
  "flow.final": [
    true
  ],
  "source.packets": [
    4
  ],
  "network.packets": [
    9
  ],
  "client.ip": [
    "10.146.15.198"
  ],
  "agent.hostname": [
    "nicolesstevesghost2"
  ],
  "host.architecture": [
```

```
    "x86_64"
  ],
  "cloud.provider": [
    "gcp"
  ],
  "cloud.machine.type": [
    "n1-standard-1"
  ],
  "source.port": [
    52316
  ],
  "agent.id": [
    "bd332535-5af4-4c27-8a11-6b9a8060acf9"
  ],
  "client.port": [
    52316
  ],
  "host.containerized": [
    false
  ],
  "ecs.version": [
    "1.1.0"
  ],
  "agent.version": [
    "7.5.1"
  ],
  "host.os.family": [
    "debian"
  ],
  "destination.bytes": [
    87210
  ],
  "event.start": [
    "2023-03-06T16:54:03.038Z"
  ],
  "server.bytes": [
    87210
  ],
  "destination.port": [
    80
  ],
  "client.packets": [
    4
  ],
  "event.end": [
    "2023-03-06T16:54:03.039Z"
  ],
  "destination.packets": [
    5
  ],
  "cloud.instance.id": [
    "2334593404447749 54"
  ],
  "agent.type": [
```

```
    "auditbeat"
  ],
  "event.module": [
    "system"
  ],
  "host.os.kernel": [
    "4.15.0-1052-gcp"
  ],
  "server.port": [
    80
  ],
  "network.bytes": [
    87370
  ],
  "network.direction": [
    "outbound"
  ],
  "host.id": [
    "15968c8010a2822cccc93ce79efa7afb"
  ],
  "network.type": [
    "ipv4"
  ],
  "source.bytes": [
    160
  ],
  "server.packets": [
    5
  ],
  "host.os.codename": [
    "xenial"
  ],
  "destination.ip": [
    "132.132.132.132"
  ],
  "network.transport": [
    "tcp"
  ],
  "event.duration": [
    808365
  ],
  "event.action": [
    "network_flow"
  ],
  "@timestamp": [
    "2023-03-06T16:54:04.873Z"
  ],
  "host.os.platform": [
    "ubuntu"
  ],
  "client.bytes": [
    160
  ],
  "agent.ephemeral_id": [
```

```
      "da569583-3772-465b-b481-478acec831d4"
    ],
    "flow.complete": [
      false
    ],
    "event.dataset": [
      "socket"
    ],
    "cloud.project.id": [
      "elastic-sa"
    ],
    "cloud.instance.name": [
      "nicolesstevesghost2"
    ]
  }
}
```