### Client 필드

클라이언트는 세션, 연결 또는 양방향 플로우 레코드와 관련된 이벤트에 대한 네트워크 연결의 개시자로 정의됩니다.

TCP 이벤트의 경우, 클라이언트는 SYN 패킷을 전송하는 TCP 연결의 개시자입니다. 다른 프로토콜의 경우, 클라이언트는 일반적으로 네트워크 트랜잭션의 개시자 또는 요청자입니다. 일부 시스템에서는 TCP 연결에서 클라이언트를 지칭하기 위해 "발신자"라는 용어를 사용합니다. 클라이언트 필드는 네트워크 이벤트에서 클라이언트 역할을 하는 시스템에 대한 세부 정보를 설명합니다. client 필드는 일반적으로 server 필드와 함께 채워집니다. 클라이언트 필드는 일반적으로 패킷 수준 이벤트에 대해 채워지지 않습니다.

클라이언트/서버 표현은 특정 상황에서 데이터를 시각화하는 데 도움이 되는 의미론적 컨텍스트를 교환에 추가할 수 있습니다. 컨텍스트가 해당 범주에 속하는 경우에도 소스 및 목적지가 적절하게 채워져 있는지 확인해야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| client.address | src\_addr | 문자열 | 클라이언트 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| client.bytes | sent\_bytes | 64비트 정수 | 클라이언트가 서버로 전송한 바이트 수 |
| client.domain | src\_host | 문자열 | 클라이언트 도메인 이름 |
| client.ip | src\_ip | IP 주소 | 클라이언트 IP 주소 (IPv4 또는 IPv6) |
| client.mac | src\_mac | 문자열 | 클라이언트 MAC 주소 |
| client.nat.ip | nat\_src\_ip | IP 주소 | NAT 출발지 주소 |
| client.nat.port | nat\_src\_port | 32비트 정수 | NAT 출발지 포트 |
| client.packets | rcvd\_pkts | 64비트 정수 | 클라이언트가 서버로 전송한 패킷 수 |
| client.port | src\_port | 32비트 정수 | 클라이언트 포트 |
| client.registered\_domain | src\_eld | 문자열 | 출발지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| client.subdomain | src\_subdomain | 문자열 | 출발지 서브도메인 |
| client.top\_level\_domain | src\_tld | 문자열 | 출발지 TLD |