### Source 필드

source 필드는 네트워크 교환/패킷의 발신자에 대한 세부 정보를 캡처합니다. 이러한 필드는 네트워크 이벤트, 패킷 또는 네트워크 트랜잭션의 세부 정보가 포함된 기타 이벤트에서 채워집니다.

source 필드는 일반적으로 destination 필드와 함께 채워집니다. source 및 destination 필드는 기본 요소이므로 이벤트에 네트워크 트랜잭션의 소스 및 대상 세부 정보가 포함된 경우 항상 채워져야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| source.address | src\_addr | 문자열 | 출발지 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| source.bytes | sent\_bytes | 64비트 정수 | 출발지에서 목적지로 전송한 바이트 수 |
| source.domain | src\_host | 문자열 | 출발지 도메인 이름 |
| source.ip | src\_ip | IP 주소 | 출발지 IP 주소 (IPv4 또는 IPv6). |
| source.mac | src\_mac | 문자열 | 출발지 MAC 주소 |
| source.nat.ip | nat\_src\_ip | IP 주소 | NAT 출발지 IP 주소 |
| source.nat.port | nat\_src\_port | 32비트 정수 | NAT 출발지 포트 |
| source.packets | sent\_pkts | 64비트 정수 | 출발지에서 목적지로 전송한 패킷 수 |
| source.port | src\_port | 32비트 정수 | 출발지 포트 |
| source.registered\_domain | src\_eld | 문자열 | 출발지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| source.subdomain | src\_subdomain | 문자열 | 출발지 서브도메인 |
| source.top\_level\_domain | src\_tld | 문자열 | 출발지 TLD |
| source.user.domain | src\_nt\_domain | 문자열 | 출발지 계정이 속한 액티브 디렉터리 또는 LDAP 도메인 이름. |
| source.user.email | mail\_from | 문자열 | 출발지 계정 이메일 |
| source.user.full\_name | src\_emp\_name | 문자열 | 출발지 사용자 성명 |
| source.user.hash | src\_user\_hash | 문자열 | 출발지 계정 익명화 필요 시 계정 해시 값 |
| source.user.id | src\_user\_id | 문자열 | 출발지 계정 식별자. 예: S-1-5-21-202424912787-2692429404-2351956786-1000 |
| source.user.name | src\_user | 문자열 | 출발지 로그인 이름 |
| source.user.roles | src\_user\_roles | 문자열 | 이벤트 발생 시점에 출발지 사용자가 보유한 역할 목록 |