### TLS 필드

TLS 연결과 관련된 필드. 이러한 필드는 TLS 프로토콜 자체에 초점을 맞추며 x.509 인증서 파일과 관련된 필드는 별도로 정의합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| tls.cipher | tls\_cipher | 문자열 | 선택된 암호화 스위트. 예: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| tls.client.certificate | tls\_client\_cert | 문자열 | PEM 인코딩된 클라이언트 인증서 |
| tls.client.certificate\_chain | tls\_client\_cert\_chain | 리스트 | PEM 인코딩된 클라이언트 인증서 체인 |
| tls.client.hash.md5 | tls\_client\_cert\_md5 | 문자열 | 클라이언트 인증서 MD5 지문 |
| tls.client.hash.sha1 | tls\_client\_cert\_sha1 | 문자열 | 클라이언트 인증서 SHA1 지문 |
| tls.client.hash.sha256 | tls\_client\_cert\_sha256 | 문자열 | 클라이언트 인증서 SHA256 지문 |
| tls.client.issuer | tls\_client\_cert\_issuer | 문자열 | 클라이언트 인증서 발급자 |
| tls.client.ja3 | tls\_client\_ja3 | 문자열 | 클라이언트 SSL/TLS 핸드쉐이크에 대한 JA3 해시 |
| tls.client.not\_after | tls\_client\_not\_after | 날짜 | 클라이언트 인증서 유효기간 시작 일시 |
| tls.client.not\_before | tls\_client\_not\_before | 날짜 | 클라이언트 인증서 유효기간 만료 일시 |
| tls.client.server\_name | tls\_client\_sni | 문자열 | 클라이언트 인증서 SNI |
| tls.client.subject | tls\_client\_subject | 문자열 | 클라이언트 인증서 제목 |
| tls.client.supported\_ciphers | tls\_client\_supported\_ciphers | 문자열 | 클라이언트가 지원하는 암호화 스위트 목록 |
| tls.curve | tls\_curve | 문자열 | 커브 암호화 알고리즘. 예: secp256r1 |
| tls.established | tls\_established | 불리언 | TLS 협상 성공 여부 |
| tls.next\_protocol | tls\_next\_protocol | 문자열 | 다음 프로토콜 이름. 예: http/1.1 |
| tls.resumed | tls\_resumed | 불리언 | 기존 TLS 협상 조건으로 통신 재개 여부 |
| tls.server.certificate | tls\_server\_cert | 문자열 | PEM 인코딩된 서버 인증서 |
| tls.server.certificate\_chain | tls\_server\_cert\_chain | 리스트 | PEM 인코딩된 서버 인증서 체인 |
| tls.server.hash.md5 | tls\_server\_cert\_md5 | 문자열 | 서버 인증서 MD5 지문 |
| tls.server.hash.sha1 | tls\_server\_cert\_sha1 | 문자열 | 서버 인증서 SHA1 지문 |
| tls.server.hash.sha256 | tls\_server\_cert\_sha256 | 문자열 | 서버 인증서 SHA256 지문 |
| tls.server.issuer | tls\_server\_issuer | 문자열 | 서버 인증서 발급자. 예: CN=Example Root CA, OU=Infrastructure Team, DC=example, DC=com |
| tls.server.ja3s | tls\_server\_ja3s | 문자열 | 서버 SSL/TLS 핸드쉐이크에 대한 JA3S 해시. 예: 394441ab65754e2207b1e1b457b3641d |
| tls.server.not\_after | tls\_server\_not\_after | 날짜 | 서버 인증서 유효기간 시작 일시 |
| tls.server.not\_before | tls\_server\_not\_before | 날짜 | 서버 인증서 유효기간 만료 일시 |
| tls.server.subject | tls\_server\_subject | 문자열 | 서버 인증서 제목 예: CN=www.example.com, OU=Infrastructure Team, DC=example, DC=com |
| tls.version | tls\_ver | 문자열 | TLS 버전. 예: 1.2 |
| tls.version\_protocol | tls\_protocol | 문자열 | 정규화된 TLS 프로토콜 이름. 예: tls |