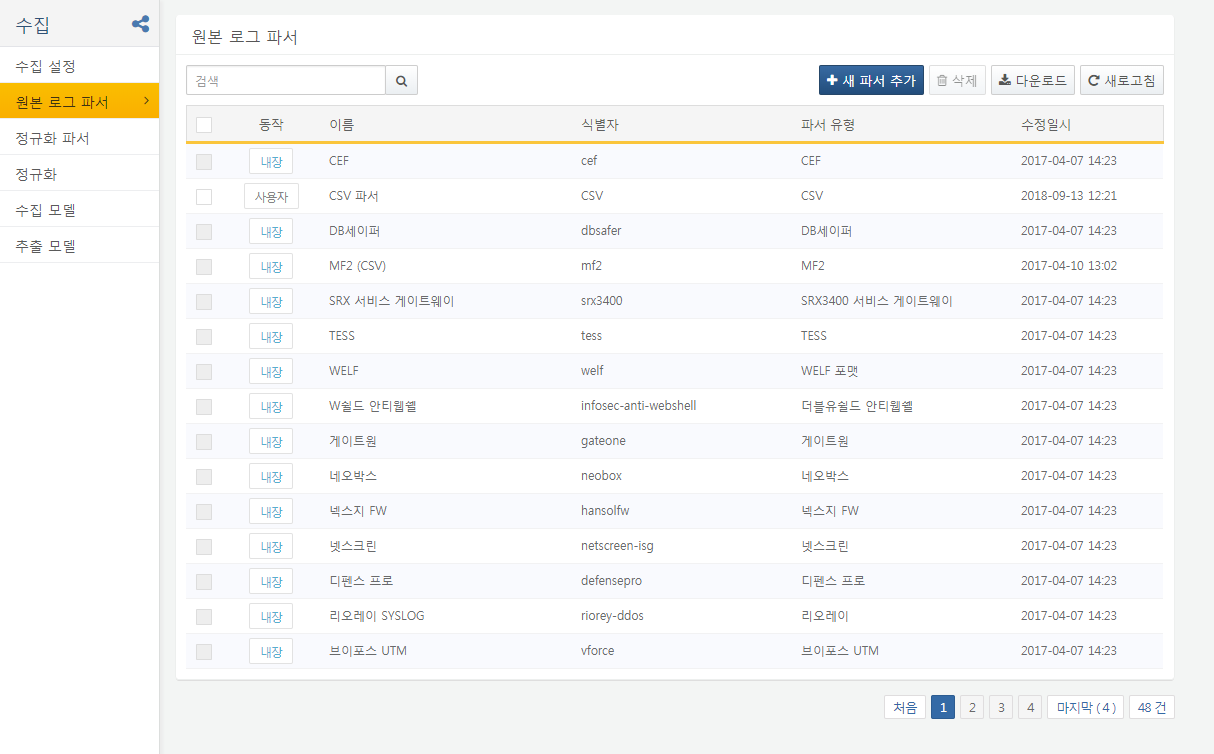
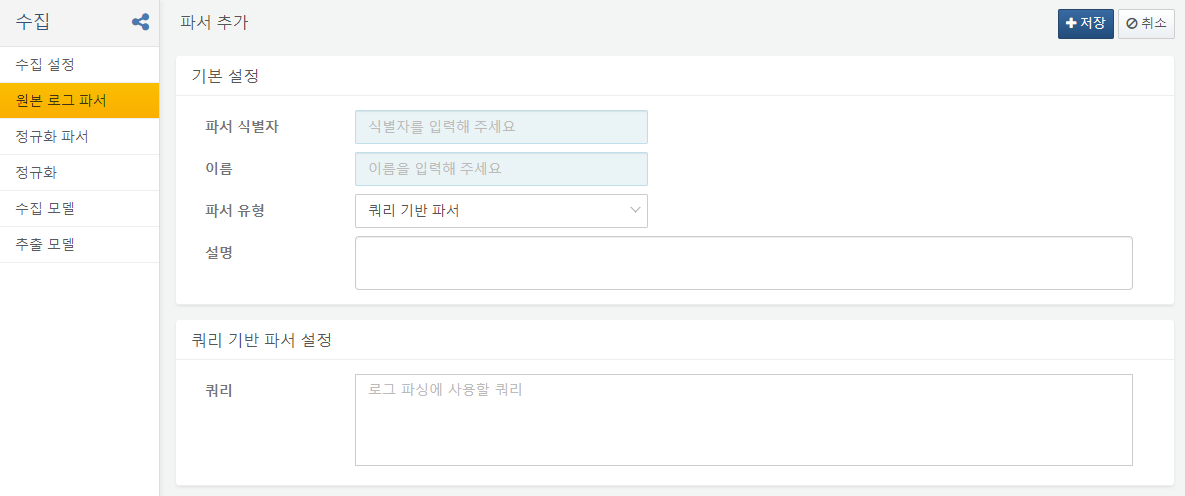
### 원본 로그 파서

원본 로그 파서는 수집 모델에서 원본 로그를 파싱하여 필드를 추출하는데 사용할 파서를 의미합니다. 내장된 파서를 사용하거나, 사용자가 직접 설정한 파서를 생성해서 사용할 수 있습니다. 파서는 클러스터 관리자 권한이나 파서 관리 권한을 가진 계정만 설정할 수 있습니다. 일반 관리자나 사용자 계정은 조회만 가능합니다.



#### 원본 로그 파서 추가

새 파서 만들기 버튼을 클릭하면 사용자 정의 원본 로그 파서를 생성할 수 있습니다.



**파서 식별자**

쿼리에서 사용할 파서 식별자를 입력합니다. 다른 파서 식별자와 겹치지 않는 유일한 이름이어야 합니다.

**이름**

화면에 표시할 파서 이름을 입력합니다. 수집 모델이나 추출 모델에서 설정할 때 이 파서 이름이 목록에 표시됩니다.

**파서 유형**

파서 유형을 선택합니다. 가장 흔히 사용되는 유형은 쿼리 기반 파서이며, 로그가 단순한 경우에는 구분자, 정규표현식 유형이 적합합니다. 다수의 로그 포맷이 복합된 경우 파서 선택기 유형을 사용해서 조건식 매칭에 따라 사용할 파서를 다르게 지정할 수 있습니다.

**설명**

파서에 대한 설명을 입력합니다.

선택할 수 있는 파서 유형은 다음과 같습니다.

* 알려진 로그 포맷에 대해 내장된 파서를 선택할 수 있습니다. 예) 스나이퍼 IPS 등
* 알려진 파일 포맷에 대해 파서를 설정할 수 있습니다. 예) CSV, JSON 등
* 사용자가 직접 파서 동작을 설정할 수 있습니다. 예) 정규표현식, 쿼리 기반 파서 등
* 스크립트 파일로 파서를 정의한 후 사용할 수 있습니다. 예) 그루비, 자바스크립트 등

#### 원본 로그 파서 삭제

체크박스를 선택하고 삭제 버튼을 클릭하면 선택된 파서를 삭제할 수 있습니다. 단, 내장된 파서는 삭제가 불가능합니다.

