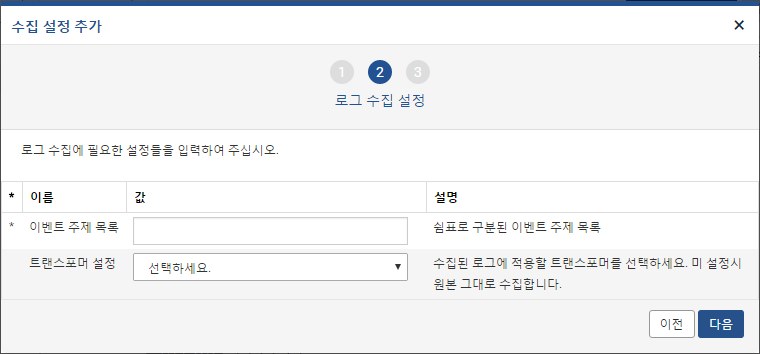
#### 기타

CEP 이벤트 수집기

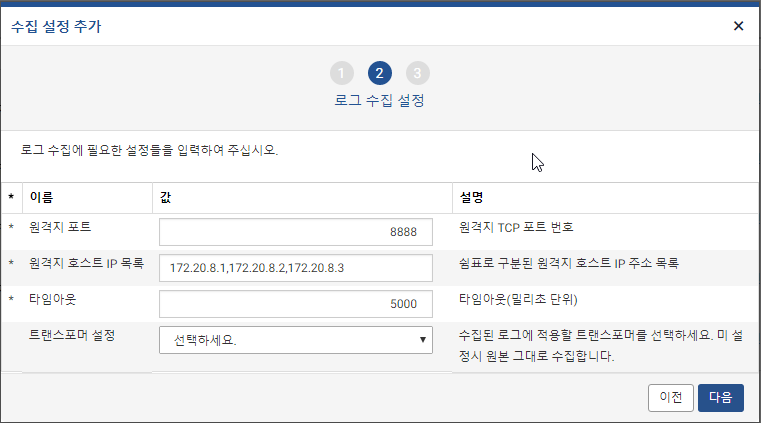
CEP 컨텍스트 이벤트를 수집합니다.



* 이벤트 주제 목록: CEP 이벤트 주제 목록을 입력합니다. 각 항목은 쉼표로 구분합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

TCP 포트 상태 수집기

TCP 포트의 개방 여부를 확인하여 수집합니다.



* 원격지 포트: 원격지 TCP 포트 번호를 입력합니다.
* 원격지 호스트 IP 목록: 원격지 호스트 IP 주소 목록을 입력합니다. 각 IP 주소는 쉼표로 구분합니다.
* 타임아웃: 타임아웃 시간을 설정합니다. 시간단위는 밀리초(ms) 단위 입니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

계정 생성/삭제 탐지 수집기

계정 및 그룹을 추가/삭제 될 때마다 발생하는 로그를 수집합니다.

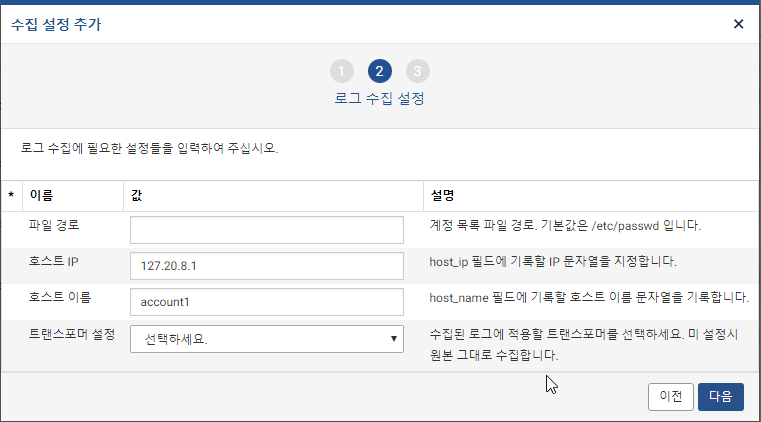


* 파일 경로: 계정 정보가 있는 파일 경로를 입력합니다. 기본 값은 /etc/passwd 입니다.
* 호스트 IP 목록: 로그에 기록된 호스트 IP를 입력합니다.
* 호스트 이름: 로그에 기록될 호스트 이름을 입력합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

리눅스 계정 이벤트 탐지 수집기

리눅스 계정이 추가/삭제 될 때마다 발생하는 로그를 수집합니다.

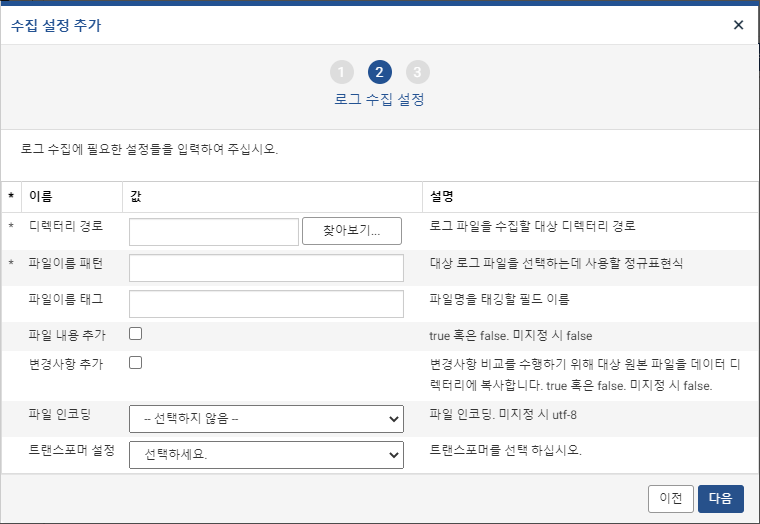
그림 8-77리눅스 계정 이벤트 탐지 수집 설정



* 파일 경로: 계정 정보가 있는 파일 경로를 입력합니다. 기본 값은 /etc/passwd 입니다.
* 호스트 IP 목록: host\_ip 필드에 기록할 IP 문자열을 입력합니다.
* 호스트 이름: host\_name 필드에 기록할 호스트 이름 문자열을 입력합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

설정 파일 변경 탐지 수집기

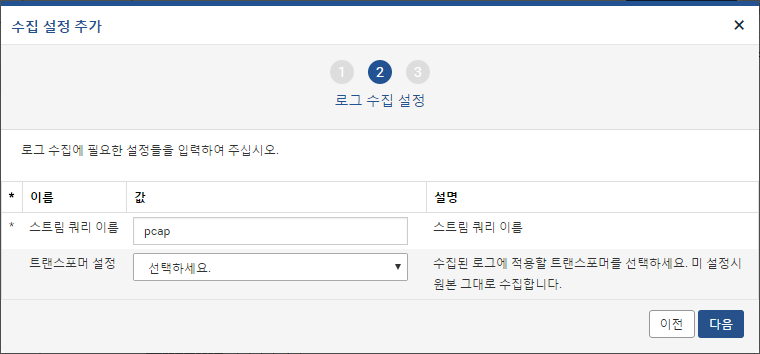
설정 파일이 변경될 때마다 로그를 발생합니다.



* 디렉터리 경로: 로그 파일이 위치하는 파일시스템 경로를 의미합니다.
* 파일이름 패턴: 디렉터리 경로에 존재하는 파일 중 이름이 정규표현식 패턴에 일치하는 경우에만 수집합니다. 정규표현식 그룹을 쓰는 경우 파일 이름에서 날짜 문자열을 추출합니다.
* 파일이름 태그: 수집한 파일명을 태깅할 필드 이름을 입력합니다.
* 파일 내용 추가: 수집 대상 파일 내용을 로그프레소 서버에 저장합니다. 수집 시 file\_content 필드에 파일 내용이 표시됩니다. 변경 내역은 파일 전체에 대해 탐지하지만, 파일 내용은 128KB까지만 저장합니다. 기본값은 false입니다.
* 변경사항 추가: 수집 대상 설정 파일에서 변경된 부분이 어떻게 달라졌는지 확인할 수 있습니다. 기본값은 false입니다. true로 설정 시 변경되기 전 내용과 변경 후 내용을 file\_diff 필드로 보여줍니다. 변경 내역은 최대 128KB까지 기록합니다.
* 파일 인코딩: 수집 대상 파일의 인코딩을 입력합니다. 기본값은 utf-8입니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

스트림 쿼리 출력 수집기

스트림 쿼리의 출력을 수집합니다.



* 스트림 쿼리 이름: 스트림 쿼리의 이름을 입력합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머

트위터 스트림 수집기

트위터 타임라인 스트림으로부터 로그를 생성합니다.



* 컨슈머 키: 애플리케이션의 컨슈머 키(API 키)를 입력합니다.
* 컨슈머 시크릿: 애플리케이션 컨슈머 시크릿(API 시크릿) 정보를 입력합니다.
* 액세스 토큰: 사용자 액세스 토큰을 입력합니다.
* 액세스 토큰 시크릿: 사용자 액세스 토큰 시크릿 정보를 입력합니다.
* 팔로우 계정: 팔로우할 계정 이름을 입력합니다. 각 계정은 쉼표로 구분합니다.
* 검색 키워드: 검색할 키워드를 입력합니다. 각 키워드는 쉼표로 구분합니다.
* 트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 12.2.2 트랜스포머