#### 센트리 로그 수집

센트리에서 진행하는 로그 수집 현황 목록을 볼 수 있습니다. 센트리 서버 파일시스템에 있는 로그 파일을 수집하거나 센트리 서버 성능, 서비스, 이벤트 등을 수집할 수 있습니다.

새로 고침 버튼을 클릭하면 현재 존재하는 로그 수집기 목록과 상태를 새로 고침 합니다.

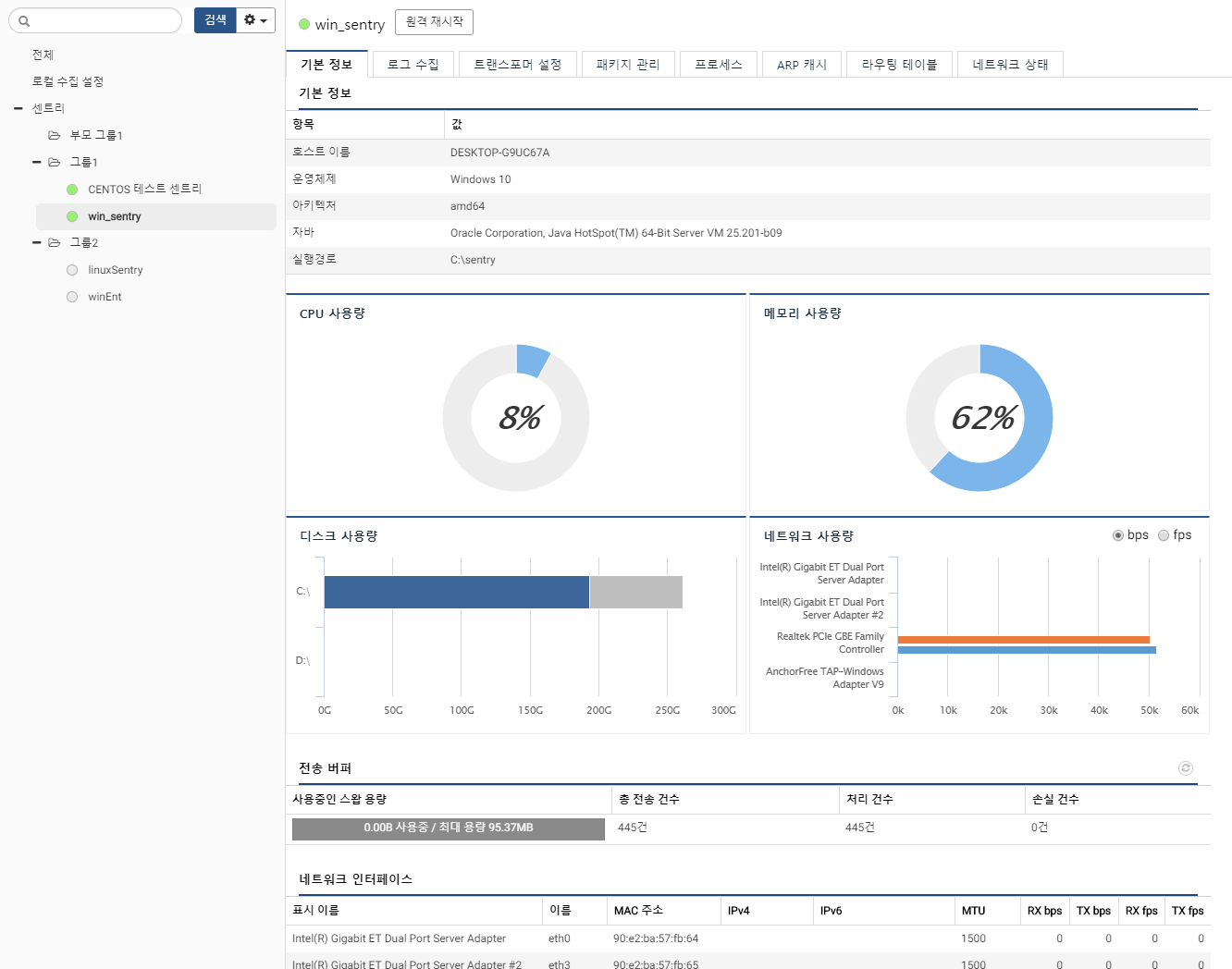
센트리 수집 설정 추가

* 서버의 메인메뉴에서 "수집 설정" 메뉴에서 센트리의 로그 수집을 설정합니다.

단계 1

"수집 설정" 메인메뉴의 왼쪽에서 "센트리" 항목에 연결되어 있는 센트리를 선택합니다. (예시에선 "win\_sentry"을 선택했습니다.)

win\_sentry은 센트리 에이전트의 연결이름입니다.



단계 2

센트리 메인 메뉴에서 "로그 수집" 메뉴를 선택한 후 "수집 설정 추가" 버튼을 클릭합니다.



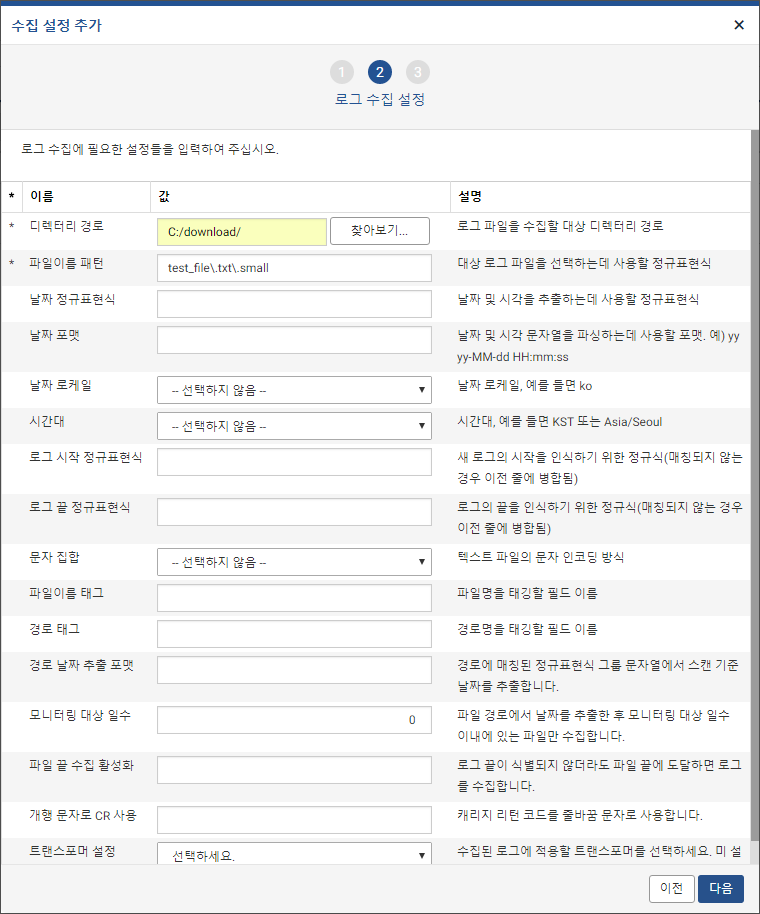
단계 3

수집유형에서 "디렉터리 와처" 유형을 선택한 후 "다음" 버튼을 클릭합니다.



단계 4

디렉터리 와처 입력 값을 입력합니다.

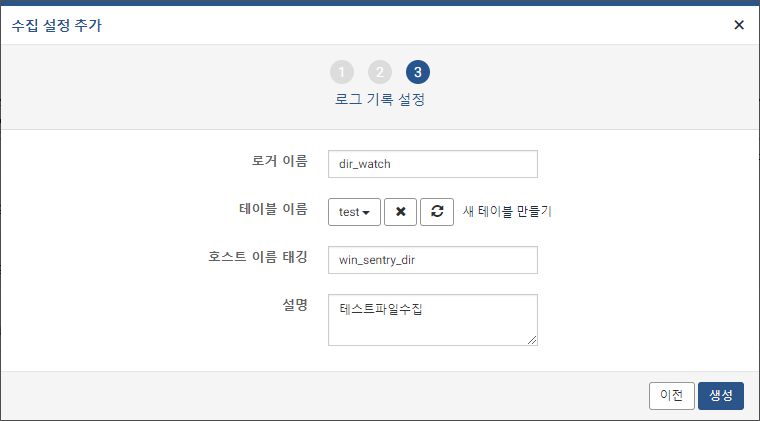


* 디렉터리 경로: 로그 파일이 위치하는 파일시스템 경로를 의미합니다.
* 파일이름 패턴: 디렉터리 경로에 존재하는 파일 중 이름이 정규표현식 패턴에 일치하는 경우에만 수집합니다. 정규표현식 그룹을 쓰는 경우 파일 이름에서 날짜 문자열을 추출합니다.
* 날짜 정규표현식: 로그에서 날짜 문자열을 추출합니다. 정규표현식 그룹으로 묶인 모든 부분을 이어붙여서 하나의 날짜 문자열을 만들어냅니다. 파일이름 정규표현식의 그룹으로 추출된 날짜문자열은 가장 앞 부분에 위치합니다.
* 날짜 포맷: 날짜 문자열을 파싱하는데 사용할 날짜 포맷을 설정합니다. (예: yyyy-MM-dd HH:mm:ss)
* 날짜 로케일: 날짜 문자열의 로케일. 가령 날짜 파싱 포맷의 지시자 중 MMM의 해석은 로케일에 따라 “Jan” 혹은 “1월”로 해석됩니다. 기본값은 en입니다.
* 시간대: 날짜 문자열의 시간대를 입력합니다. (예: KST 또는 Asia/Seoul)
* 로그 시작 정규식: 로그의 시작 부분을 인식하는 정규표현식을 지정합니다. 멀티라인 로그의 경우에 사용되며, 지정하지 않으면 줄 단위로 읽어들입니다.
* 로그 끝 정규식: 로그의 끝 부분을 인식하는 정규표현식을 지정합니다. 멀티라인 로그의 경우에 사용되며, 지정하지 않으면 줄 단위로 읽어들입니다.
* 문자 집합: 텍스트 파일 해석에 사용할 문자집합 코드를 입력합니다. 기본값은 utf-8입니다.
* 파일이름 태그: 파일명을 태깅할 필드 이름을 입력합니다.
* 경로 태그: 경로명을 태깅할 필드 이름을 입력합니다.
* 경로 날짜 추출 포맷: 경로에 매칭된 정규표현식 그룹 문자열에서 스캔 기준 날짜를 추출합니다.
* 모니터링 대상 일수: 파일 경로에서 날짜를 추출한 후 모니터링 대상 일수 이내에 있는 파일만 수집합니다.
* 파일 끝 수집 활성화: 로그 끝이 식별되지 않더라도 파일 끝에 도달하면 로그를 수집합니다. "true"로 입력할 경우 활성화되며, 미설정시 "false"를 기본 값으로 비활성화 됩니다.
* 개행 문자로 CR 사용: 캐리지 리턴 코드를 줄바꿈 문자로 사용합니다. "true"로 입력할 경우 활성화되며, 미설정시 "false"를 기본 값으로 비활성화 됩니다.

트랜스포머 설정: 수집된 로그에 적용할 트랜스포머를 선택합니다. "선택하세요."로 설정할 경우 트랜스포머가 적용되지 않고 원본 그대로 수집합니다. 트랜스포머에 대한 자세한 내용은 다음 항목을 참고하세요. 트랜스포머

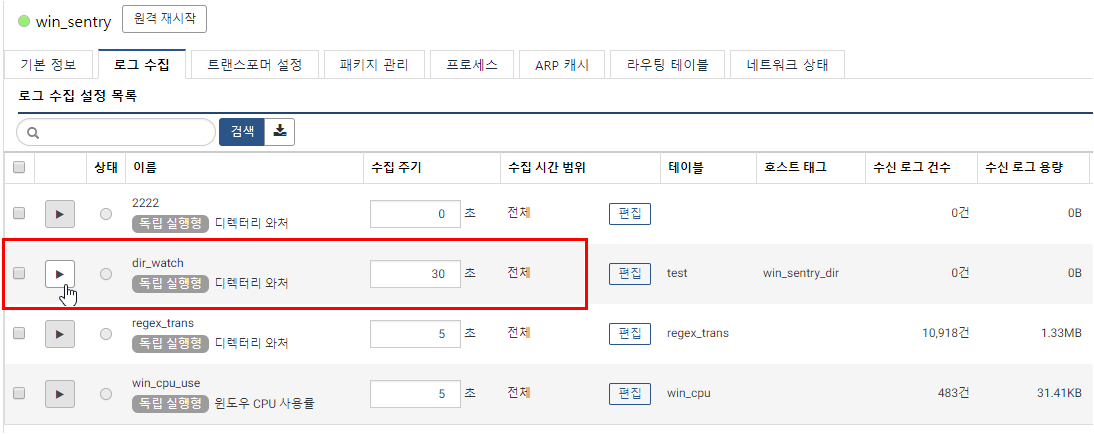
단계 5

로거이름 입력 및 로그를 저장할 테이블을 선택한 후 "생성" 버튼을 클릭하여 완료합니다.



단계 6

수집 주기를 입력한 후 상태 항목의 "시작" 버튼을 클릭해 수집기를 구동시킵니다.



센트리 수집 상태 초기화

센트리 수집기가 지금까지 수집해온 내역을 초기화합니다. 파일 수집기를 초기화 할 경우 기존에 수집한 내역도 다시 수집합니다.

단계 1

센트리 로그 수집 탭에서 수집 상태를 초기화할 수집기를 선택합니다. 만약 수집기가 실행 중이라면 정지시켜야 합니다.



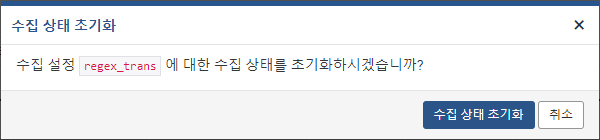
단계 2

수집 상태 초기화 버튼을 클릭합니다.



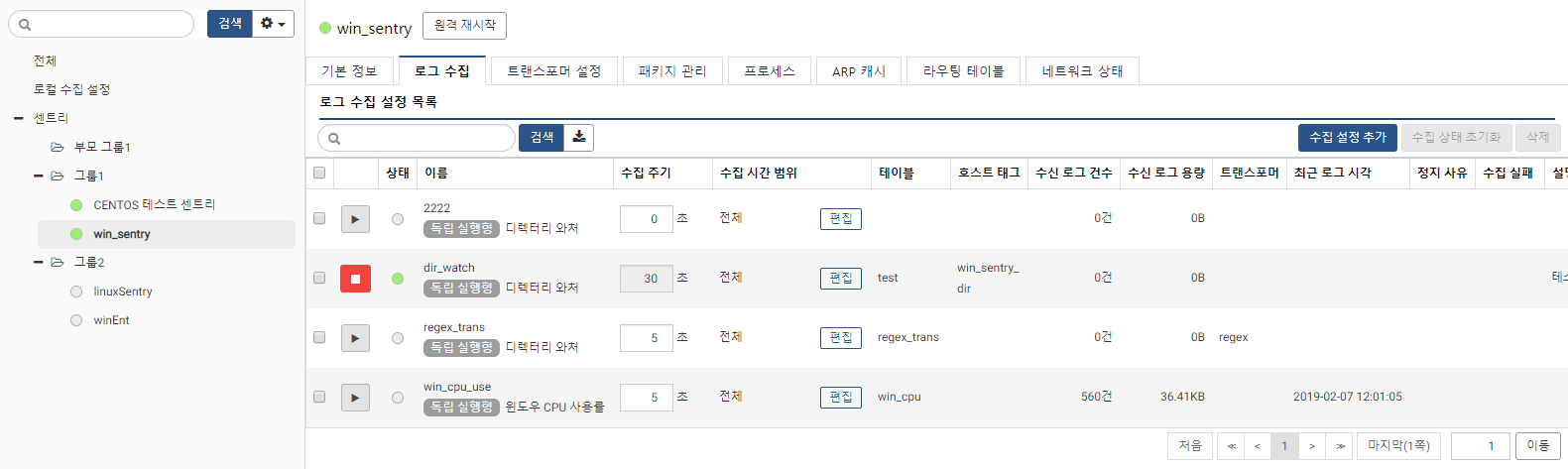
단계 3

수집 상태 초기화 확인 창이 뜨면 수집 상태 초기화 버튼을 클릭하여 진행합니다.



단계 4

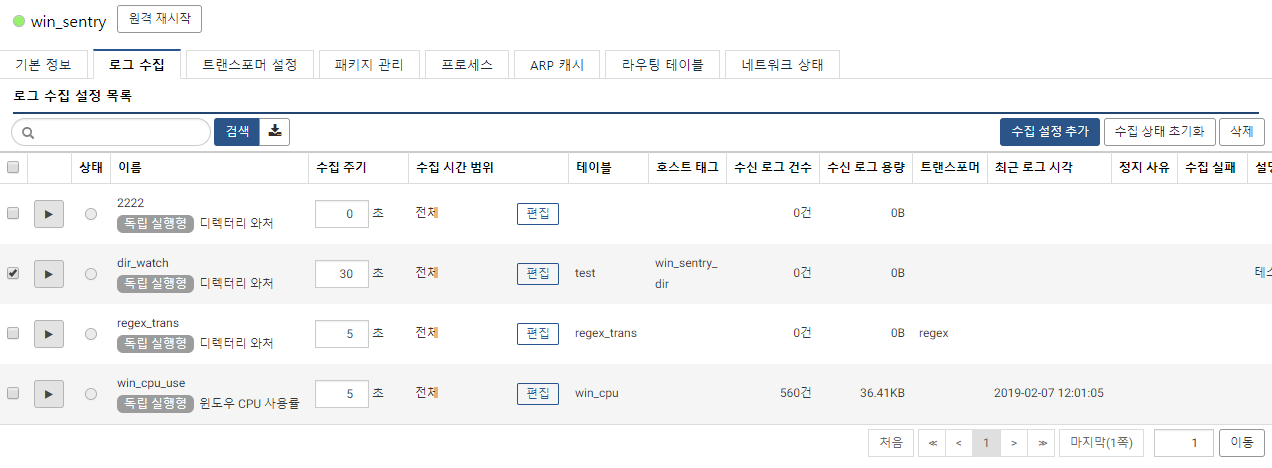
수집기 목록이 새로 고침 되면서 선택한 수집기의 수집 상태가 초기화 된 것을 확인할 수 있습니다. 수신 로그 건수, 수신 로그 용량 등이 0으로 초기화 되었습니다. 화면 우측 하단에 수집 상태 초기화 팝업 알림이 뜹니다.



센트리 수집기 삭제

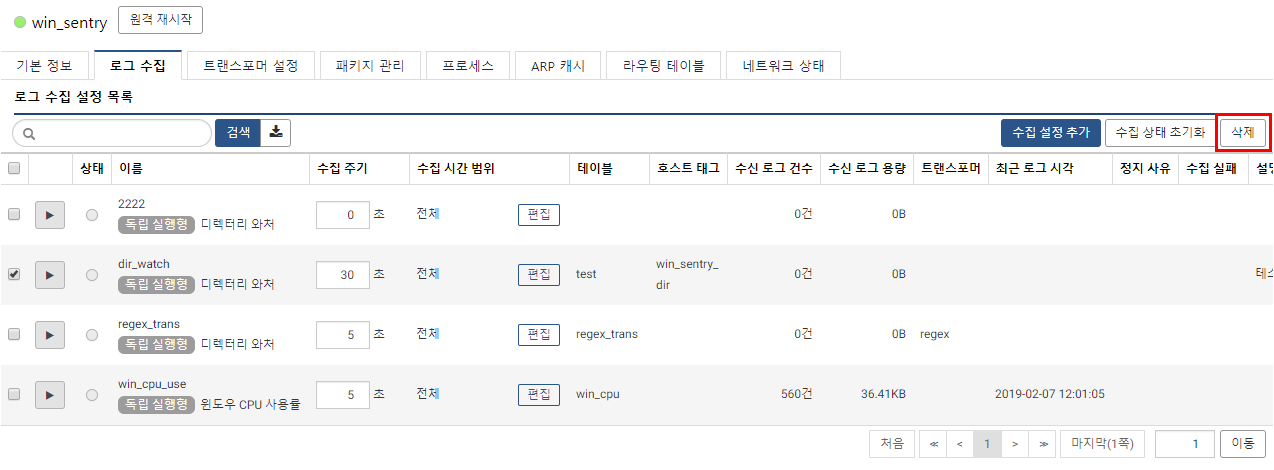
단계 1

삭제할 센트리 수집기를 선택합니다.



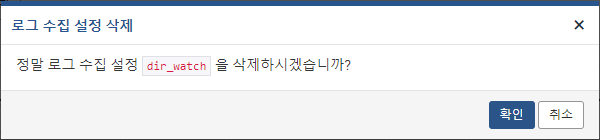
단계 2

삭제 버튼을 클릭합니다.



단계 3

로그 수집 설정 삭제 확인 창에서 확인 버튼을 클릭하여 삭제를 진행합니다.



단계 3

해당 수집기가 삭제되었습니다.

