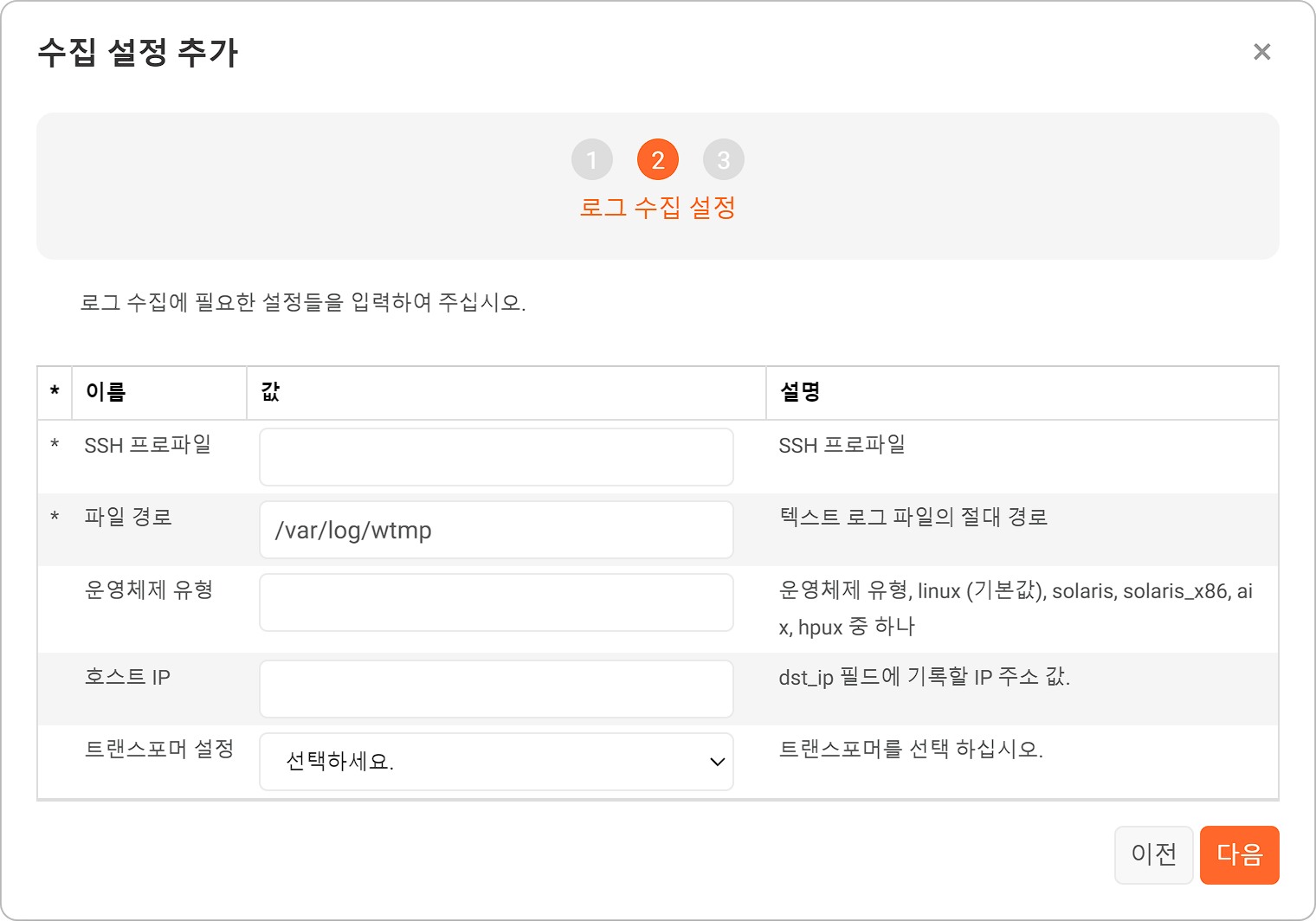
#### SFTP

SFTP 로거들은 SFTP 통신으로 원격 호스트에 접근해 로그 파일을 수집합니다.



SFTP WTMP 파일 로거

SFTP WTMP 파일 로거는 SFTP 통신으로 원격 호스트의 터미널 로그인, 로그아웃 기록을 수집합니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**파일 경로**

wtmp 로그 파일의 경로

**운영체제 유형**

운영체제(미지정 시 기본값: **linux**). **linux**, **solaris**, **solaris\_x86**, **aix**, **hpux** 중에 선택해서 입력하십시오.

**호스트 IP**

dst\_ip 필드에 기록할 IP 주소값. wtmp 로그는 IP 주소나 호스트 정보를 포함하지 않습니다. 하나의 테이블에 여러 wtmp 로그를 기록하는 경우, 호스트를 구분할 수 있도록 호스트 IP를 지정하십시오.

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

SFTP 디렉터리 와처

디렉토리 와처 로거는 로테이션되지 않는 텍스트 로그 파일을 일정 주기마다 수집하려고 할 때 사용합니다. 가령 일자별 혹은 시간대별로 순차 생성되는 로그 파일을 수집할 때 사용합니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**디렉터리 경로**

파일을 수집할 대상 디렉터리 경로

**파일이름 패턴**

수집할 파일의 이름을 검색할 때 사용할 정규표현식

**날짜 정규표현식**

로그에서 날짜 및 시간 정보 문자열 추출에 사용할 정규표현식. 날짜 정규표현식에서 괄호쌍(( ))으로 감싼 문자열 그룹들을 이어붙여서 하나의 날짜 문자열을 만들어냅니다. 이렇게 생성된 날짜 문자열로부터 **날짜 포맷**, **날짜 로케일**에 따라 시간 정보 추출에 사용합니다.

**날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷(예: yyyy-MMM-dd HH:mm:ss). **날짜 로케일**에 따라 파싱하는 형식이 다를 수 있습니다.

**날짜 로케일**

날짜 문자열의 로케일(기본값: **en**). 가령 날짜 파싱 포맷 지시자 중에서 MMM은 로케일에 따라 **Jan**(로케일이 en일 때) 혹은 **1월**(로케일이 ko일 때)로 해석됩니다.

**시간대**

시간대를 목록에서 선택. API를 이용해 로거를 구성하는 경우 **KST** 또는 **Asia/Seoul**와 같은 형식으로 시간대를 지정할 수 있습니다.

**로그 시작 구분 정규표현식**

로그의 시작 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**로그 끝 구분 정규표현식**

로그의 끝 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**문자 집합**

텍스트 파일에 적용할 문자 인코딩 방식을 목록에서 선택(미지정 시 기본값: **UTF-8**)

**파일이름 태그**

수집한 파일 이름을 기록할 필드 이름

**경로 태그**

디렉터리 경로를 기록할 필드 이름

**경로 날짜 추출 포맷**

디렉터리 경로 문자열에서 날짜 문자열 검색에 사용할 정규표현식. 디렉터리가 날짜를 기준 생성될 때(예: /var/log/foo/2022-11-02/bar) 디렉터리 경로 문자열에서 GZIP 파일의 스캔 기준 날짜를 추출할 때 사용합니다.

**모니터링 대상 일수**

파일 경로에서 날짜를 추출한 후 모니터링 대상 일수 이내에 있는 파일만 수집합니다(기본값: 0(기간 제한 없이 파일에 있는 로그 수집)).

**파일 끝 수집 활성화**

로그 끝이 식별되지 않더라도 파일 끝에 도달하면 로그를 수집합니다(기본값: false).

**개행 문자로 CR 사용**

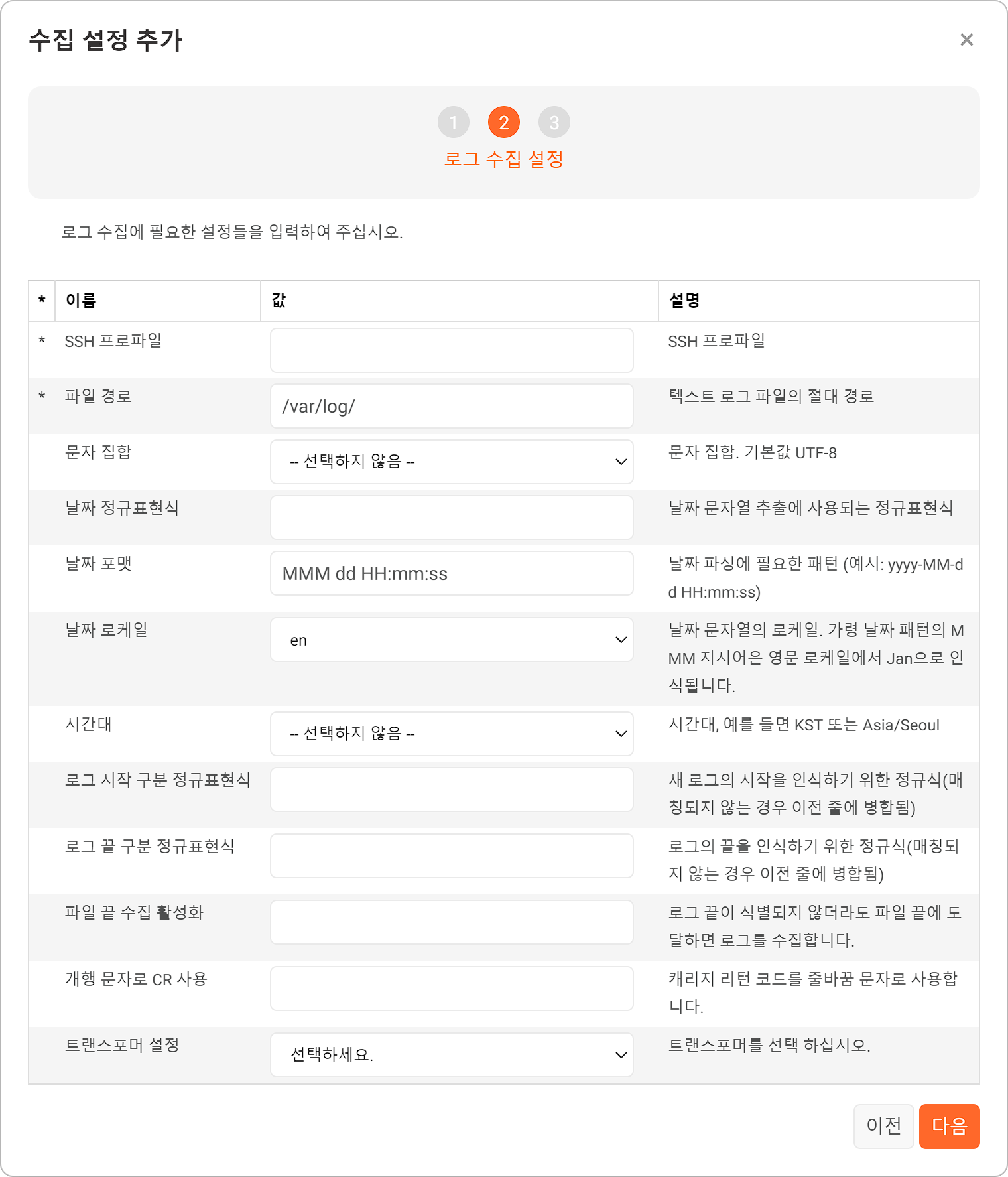
개행 문자로 LF(\n) 대신 CRLF(\r\n)의 사용 여부를 나타내는 불리언 값(미지정 시 기본값: false).

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

SFTP 로테이션 로그 파일

SFTP 로테이션 로거는 주기적으로 다른 경로에 파일을 백업하고 다시 쓰는 단일 로그 파일을 수집할 때 사용합니다. 흔히 리눅스 서버에서는 logrotate를 사용하여 일정 주기로 기존 파일의 이름을 변경하여 백업 보관하고 로그 파일을 새로 생성합니다. SFTP 로테이션 로그 파일 로거는 이런 시나리오에서 사용됩니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**파일 경로**

수집할 대상 로그 파일의 경로(예: /var/log/secure)

**문자 집합**

GZIP 압축을 해제한 후 텍스트 파일에 적용할 문자 인코딩 방식을 목록에서 선택(미지정 시 기본값: **UTF-8**)

**날짜 정규표현식**

로그에서 날짜 및 시간 정보 문자열 추출에 사용할 정규표현식. 날짜 정규표현식에서 괄호쌍(( ))으로 감싼 문자열 그룹들을 이어붙여서 하나의 날짜 문자열을 만들어냅니다. 이렇게 생성된 날짜 문자열로부터 **날짜 포맷**, **날짜 로케일**에 따라 시간 정보 추출에 사용합니다.

**날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷(예: yyyy-MMM-dd HH:mm:ss). **날짜 로케일**에 따라 파싱하는 형식이 다를 수 있습니다.

**날짜 로케일**

날짜 문자열의 로케일(기본값: **en**). 가령 날짜 파싱 포맷 지시자 중에서 MMM은 로케일에 따라 **Jan**(로케일이 en일 때) 혹은 **1월**(로케일이 ko일 때)로 해석됩니다.

**시간대**

시간대를 목록에서 선택. API를 이용해 로거를 구성하는 경우 **KST** 또는 **Asia/Seoul**와 같은 형식으로 시간대를 지정할 수 있습니다.

**로그 시작 구분 정규표현식**

로그의 시작 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**로그 끝 구분 정규표현식**

로그의 끝 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**파일 끝 수집 활성화**

로그 끝이 식별되지 않더라도 파일 끝에 도달하면 로그를 수집합니다(기본값: false).

**개행 문자로 CR 사용**

개행 문자로 LF(\n) 대신 CRLF(\r\n)의 사용 여부를 나타내는 불리언 값(미지정 시 기본값: false).

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

2004.0 이전 버전은 로거의 수집 주기가 도래하기 전에 로그가 로테이션되면 해당 로그 파일이 유실되는 버그가 있습니다. 이 로거를 구성하기 전에 로그프레소 서버가 버전 2004.0 이상인지 확인하십시오.

SFTP 멀티 로테이션 로그 파일

SFTP 멀티 로테이션 로그 파일 로거는 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일들을 수집합니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**디렉터리 경로**

파일을 수집할 대상 디렉터리 경로

**파일이름 패턴**

수집할 파일의 이름을 검색할 때 사용할 정규표현식

**문자 집합**

텍스트 파일에 적용할 문자 인코딩 방식을 목록에서 선택(미지정 시 기본값: **UTF-8**)

**하위 디렉터리 포함**

하위 디렉터리 포함 여부를 나타내는 불리언 값(기본값: false)

**디렉터리 경로 패턴**

로그 파일이 있는 디렉터리를 선택할 때 사용할 정규표현식

**날짜 정규표현식**

로그에서 날짜 및 시간 정보 문자열 추출에 사용할 정규표현식. 날짜 정규표현식에서 괄호쌍(( ))으로 감싼 문자열 그룹들을 이어붙여서 하나의 날짜 문자열을 만들어냅니다. 이렇게 생성된 날짜 문자열로부터 **날짜 포맷**, **날짜 로케일**에 따라 시간 정보 추출에 사용합니다.

**날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷(예: yyyy-MMM-dd HH:mm:ss). **날짜 로케일**에 따라 파싱하는 형식이 다를 수 있습니다.

**날짜 로케일**

날짜 문자열의 로케일(기본값: **en**). 가령 날짜 파싱 포맷 지시자 중에서 MMM은 로케일에 따라 **Jan**(로케일이 en일 때) 혹은 **1월**(로케일이 ko일 때)로 해석됩니다.

**시간대**

시간대를 목록에서 선택. API를 이용해 로거를 구성하는 경우 **KST** 또는 **Asia/Seoul**와 같은 형식으로 시간대를 지정할 수 있습니다.

**로그 시작 구분 정규표현식**

로그의 시작 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**로그 끝 구분 정규표현식**

로그의 끝 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**파일이름 태그**

수집한 파일 이름을 기록할 필드 이름

**경로 태그**

디렉터리 경로를 기록할 필드 이름

**파일 끝 수집 활성화**

로그 끝이 식별되지 않더라도 파일 끝에 도달하면 로그를 수집합니다(기본값: false).

**개행 문자로 CR 사용**

개행 문자로 LF(\n) 대신 CRLF(\r\n)의 사용 여부를 나타내는 불리언 값(미지정 시 기본값: false).

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

2004.0 이전 버전은 로거의 수집 주기가 도래하기 전에 로그가 로테이션되면 해당 로그 파일이 유실되는 버그가 있습니다. 이 로거를 구성하기 전에 로그프레소 서버가 버전 2004.0 이상인지 확인하십시오.

SFTP 일자별 디렉터리

SFTP 일자별 디렉터리 로거는 하루 단위로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**모니터링 기간**

실시간으로 파일 변화를 모니터링할 기간(기본값: 0). 값이 0일 떄, 실시간 수집을 비활성화합니다.

**디렉터리 경로**

파일을 수집할 대상 디렉터리 경로

**파일이름 패턴**

수집할 파일의 이름을 검색할 때 사용할 정규표현식

**디렉터리 날짜 정규표현식**

디렉터리 경로 문자열에서 날짜 문자열 검색에 사용할 정규표현식. 디렉터리 경로에 날짜 정보(예: /var/log/foo/2022-11-02)가 있으면 디렉터리 경로 문자열에서 날짜 정보를 추출해 사용합니다.

**디렉터리 날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷을 설정합니다. (기본값: yyyyMMdd)

**과거 로그 수집 시작 일자**

yyyyMMdd 형식으로 시작 일자를 지정합니다. 지정하지 않으면 과거 로그 수집이 비활성화됩니다.

**과거 로그 수집 끝 일자**

yyyyMMdd 형식으로 끝 일자를 지정합니다. 지정하지 않으면 과거 로그 수집이 비활성화됩니다.

**날짜 정규표현식**

로그에서 날짜 및 시간 정보 문자열 추출에 사용할 정규표현식. 날짜 정규표현식에서 괄호쌍(( ))으로 감싼 문자열 그룹들을 이어붙여서 하나의 날짜 문자열을 만들어냅니다. 이렇게 생성된 날짜 문자열로부터 **날짜 포맷**, **날짜 로케일**에 따라 시간 정보 추출에 사용합니다.

**날짜 포맷**

날짜 문자열을 파싱하는데 사용할 날짜 포맷(예: yyyy-MMM-dd HH:mm:ss). **날짜 로케일**에 따라 파싱하는 형식이 다를 수 있습니다.

**날짜 로케일**

날짜 문자열의 로케일(기본값: **en**). 가령 날짜 파싱 포맷 지시자 중에서 MMM은 로케일에 따라 **Jan**(로케일이 en일 때) 혹은 **1월**(로케일이 ko일 때)로 해석됩니다.

**시간대**

시간대를 목록에서 선택. API를 이용해 로거를 구성하는 경우 **KST** 또는 **Asia/Seoul**와 같은 형식으로 시간대를 지정할 수 있습니다.

**로그 시작 구분 정규표현식**

로그의 시작 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**로그 끝 구분 정규표현식**

로그의 끝 부분을 인식하는 정규표현식. 하나의 로그 항목이 여러 줄에 걸쳐 있을 때 사용합니다(미지정 시 개행 문자를 로그 구분자로 인식).

**문자 집합**

텍스트 파일에 적용할 문자 인코딩 방식을 목록에서 선택(미지정 시 기본값: **UTF-8**)

**파일이름 태그**

수집한 파일 이름을 기록할 필드 이름

**파일 끝 수집 활성화**

로그 끝이 식별되지 않더라도 파일 끝에 도달하면 로그를 수집합니다(기본값: false).

**개행 문자로 CR 사용**

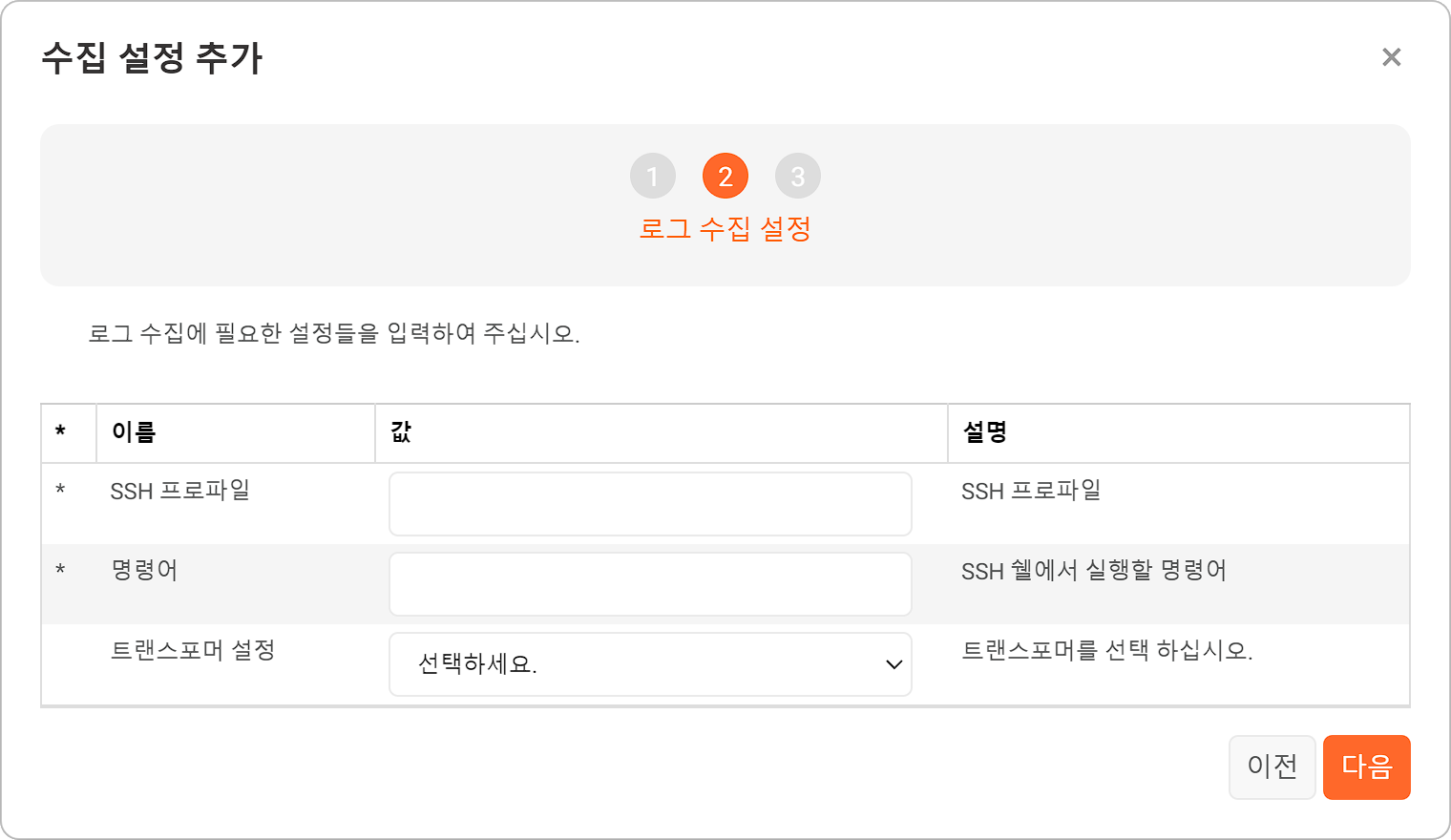
개행 문자로 LF(\n) 대신 CRLF(\r\n)의 사용 여부를 나타내는 불리언 값(미지정 시 기본값: false).

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.

SSH 실행

SSH 실행 로거는 SSH 셸의 표준 출력을 로그로 수집합니다.



**SFTP 프로파일**

연결에 사용할 SFTP 서버 접속 프로파일

**명령어**

SSH 셸에서 실행할 명령어

**트랜스포머 설정**

수집된 로그에 적용할 트랜스포머를 목록에서 선택. 미지정 시 트랜스포머를 적용하지 않고 원본 그대로 수집합니다.