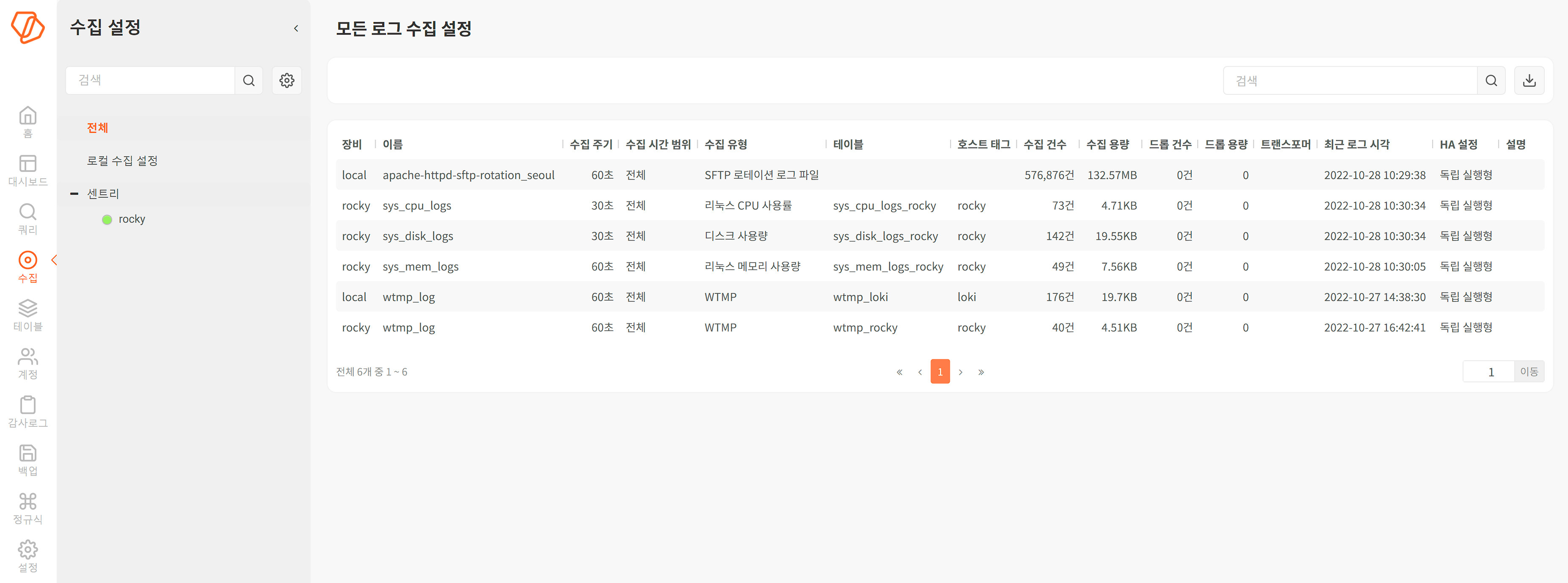
### 개요

로거와 센트리를 포함한 모든 수집 설정은 메뉴에 있는 **수집**에서 확인할 수 있습니다.

#### 로거

로그프레소 플랫폼에서 수행하는 모든 작업은 분석할 데이터의 수집에서 시작됩니다. 로그프레소 플랫폼은 원천 데이터의 종류나 형식을 가리지 않고 원본을 수집해 보존할 수 있도록 여러가지 유형의 로그 로거를 제공합니다. 이러한 로그 로거를 로거(logger)라 합니다.



로그프레소 플랫폼은 로그 수집과 로그 저장 단계가 분리되어 있습니다. 로거는 로그를 실시간으로 수집해서 분석만 수행하고 저장을 하지 않거나, 수집된 모든 로그를 특정한 테이블에 저장하도록 구성할 수 있습니다.

설치 위치에 따른 구분

로거는 로그프레소 서버 또는 센트리에 설치되어 실행됩니다. 로거를 실행하는 위치에 따라 로거는 각각 다른 네임스페이스를 갖습니다.

* 로그프레소 서버의 네임스페이스는 local입니다.
* 센트리는 각 센트리의 식별자(센트리를 등록할 때 지정한 GUID)를 네임스페이스로 사용합니다.

다음 그림은 **수집** 화면에서 확인할 수 있는 네임스페이스의 예시입니다. 예시에서는 센트리의 식별자 black-cat, rocky가 네임스페이스로 사용되고 있습니다.



**수집** 화면 왼편 목록에 열거된 항목을 누르면 설치 위치에 따라 로거 목록 또는 센트리의 정보를 보여줍니다.

* **전체**: 모든 네임스페이스의 로거 목록을 보여줍니다. **전체**는 **수집** 화면에서 보여주는 기본 정보입니다.
* **[로컬 수집 설정](logger-management)**: 로그프레소 서버(local)의 로거 목록을 보여줍니다.
* **[센트리](sentries)**: **센트리**에서는 센트리 목록을, 센트리의 식별자나 별칭을 누르면 해당 센트리의 로거를 비롯해 센트리의 정보를 보여줍니다. 센트리 목록에서 센트리를 임의로 그룹핑할 수 있습니다.

로거의 이름은 네임스페이스 안에서 유일한 것이어야 합니다. 다음 그림은 이름이 wtmp\_log인 로거가 서로 다른 네임스페이스(local, rocky)에 있는 것을 보여줍니다.



쿼리 명령어 중에서 [logger](https://docs.logpresso.com/ko/query/logger-command)는 로거로 수집된 데이터를 실시간으로 출력합니다. 이 명령어의 문법에서 로거의 이름을 네임스페이스\로거\_이름 형식으로 사용합니다.

logger window=INT{y|mon|w|d|h|m|s} NODE\LOGGER[, ...]

실행 방식에 따른 구분

로거는 실행 방식에 따라 액티브 로거와 패시브 로거로 구분됩니다.

**액티브 로거**

데이터 원천에 직접 접근해서 데이터를 수집하는 로거를 액티브 로거라 합니다. 액티브 로거는 주기적으로, 혹은 지정된 일정에 따라 데이터를 반복하여 수집합니다. 가령, 파일에서 로그를 수집하는 경우, 설정된 주기마다 파일의 증가분을 확인하여 로그를 읽어들입니다. 주기적으로 데이터베이스에서 테이블의 데이터를 읽어오는 로거도 액티브 로거입니다.

**패시브 로거**

수신 포트를 열고 대기하고 있다가 해당 포트로 들어오는 데이터를 수집하는 로거를 패시브 로거라 합니다. 패시브 로거는 항상 데이터를 받을 수 있도록 대기하고 있으므로 시스로그, SNMP 트랩과 같이 데이터 원천이 되는 원격 호스트가 전송하는 데이터를 수동적으로 수신합니다.

페데레이션 환경에서 로거 구분

로그프레소 서버를 고가용성(HA, high availability)을 위해 [페데레이션](https://docs.logpresso.com/ko/enterprise/4.0/ui/federation-settings) 형태로 구성해 운용할 수 있습니다. 이 때 로거를 실행하는 위치에 따라 독립실행형/프라이머리 로거, 백업 로거로 구분합니다.

**독립실행형/프라이머리 로거**

단독으로 실행되는 로그프레소 서버나 페데레이션 노드에서 프라이머리로 동작하는 로거

**백업 로거**

프라이머리 로거에 장애가 발생하거나 기타 이유로 동작하지 않을 때 프라이머리 로거를 대신해 실행하도록 지정된 로거

#### 센트리

로그프레소 플랫폼에서 로그프레소 서버는 스스로 데이터를 수집, 분석하는 기능을 수행합니다. 서버와 달리 데이터를 수집하는 기능만 수행하는 노드가 있습니다. 이러한 노드를 센트리(Sentry)라 합니다. 센트리는 데이터를 수집하는 에이전트로 동작하거나, 네트워크 상에서 센트리가 설치되지 않은 다른 호스트로부터 데이터를 수집해 로그프레소 서버로 전송하는 노드로 활용됩니다.

로그프레소 서버가 센트리와 통신에 사용하는 서비스 포트는 tcp 7140입니다. 서버와 센트리 간 통신은 TLS로 암호화되어 있습니다. 통신은 센트리가 먼저 TLS 핸드셰이킹을 하는 것으로 시작합니다. 센트리 인증서가 없는 센트리는 서버에 연결할 수 없습니다.