### 클러스터

#### 개요

로그프레소 소나는 클러스터 구성을 지원합니다. 클러스터는 독립적인 노드들이 협력하여 수집, 분석, 전달 등의 역할을 수행하며, 시스템 안정성과 가용성을 높이기 위해 노드별 이중화 구성을 제공합니다.

로그프레소 클라우드에서 로그프레소 소나 인스턴스는 클러스터가 자동으로 구성되어 제공됩니다. 온프레미스 환경에서는 운영 환경에 맞게 단독실행형 또는 클러스터 형태로 구성되어 제공되므로 클러스터 설정의 변경을 권장하지 않습니다.

아키텍처

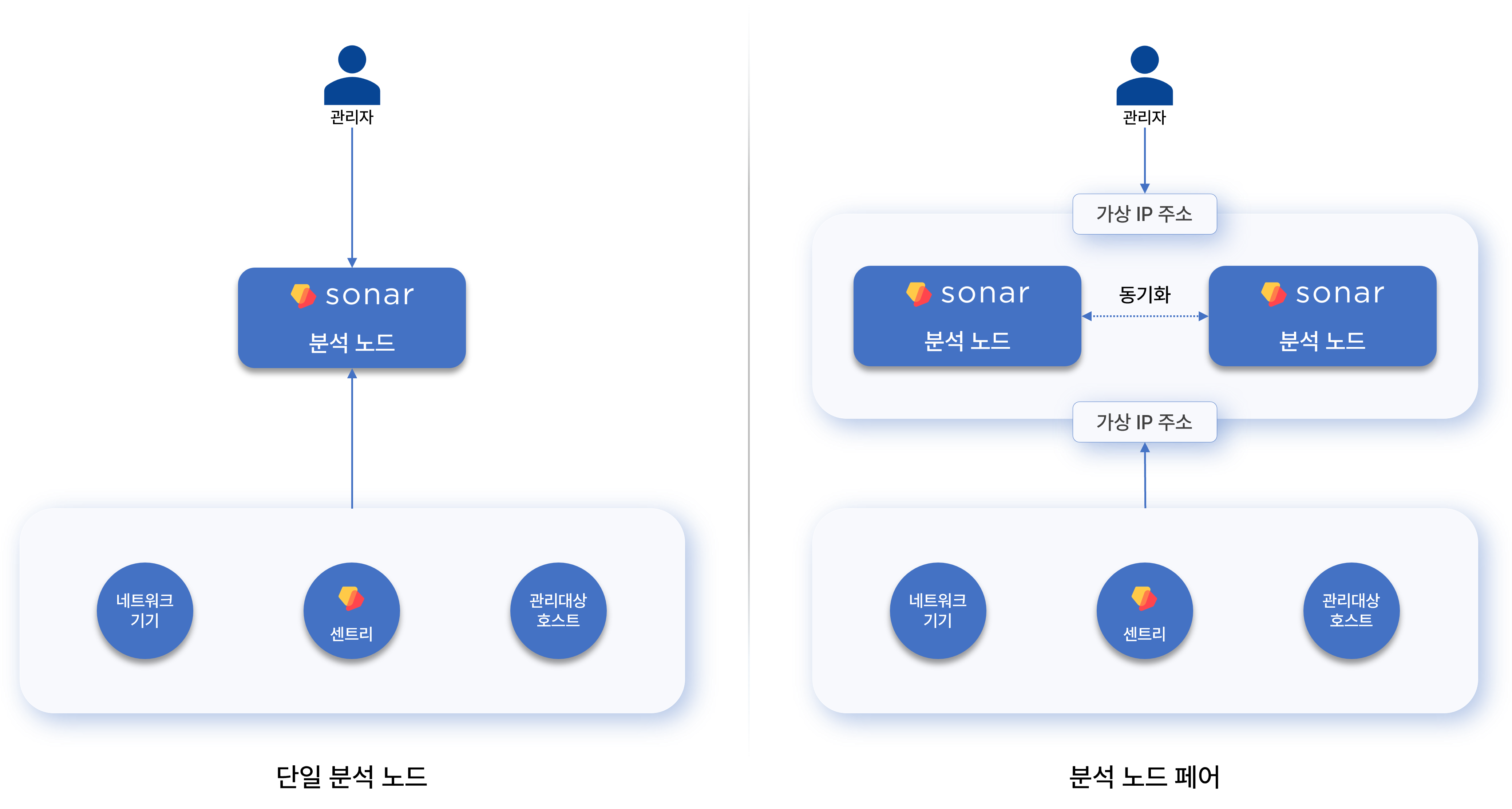
로그프레소 클러스터는 구성하는 티어에 따라 다음과 같이 나누어 볼 수 있습니다.

* **1 티어**: 분석 노드만으로 구성되는 티어
* **2 티어**: 전달 노드 - 분석 노드
* **2 티어(레거시)**: 수집 노드 - 분석 노드
* **3 티어**: 전달 노드 - 수집 노드 - 분석 노드

하루에 수집되는 원본 로그의 양에 따라 적절한 티어 구성을 선택해서 사용할 수 있습니다. 로그프레소가 **권장하는 아키텍처는 3티어 구성**입니다.

1 티어: 분석 노드 티어

1 티어 구성을 그림으로 표현하면 다음과 같습니다. 좌측은 단일 분석 노드, 우측은 분석 노드 페어입니다. 로그프레소의 레퍼런스 하드웨어를 기준으로 하루 최대 200GB의 데이터를 처리할 수 있습니다.



**단일 분석 노드**

수집할 데이터가 적을 경우, **단일 서버**에서 **수집 노드와 분석 노드의 기능을 동시에 수행**할 수 있습니다. 그러나 노드 장애 시 데이터 유실이 발생할 수 있습니다.

**분석 노드 페어**

가용성 문제에 대응할 수 있도록 **분석 노드를 이중화**한 1티어 구성입니다.

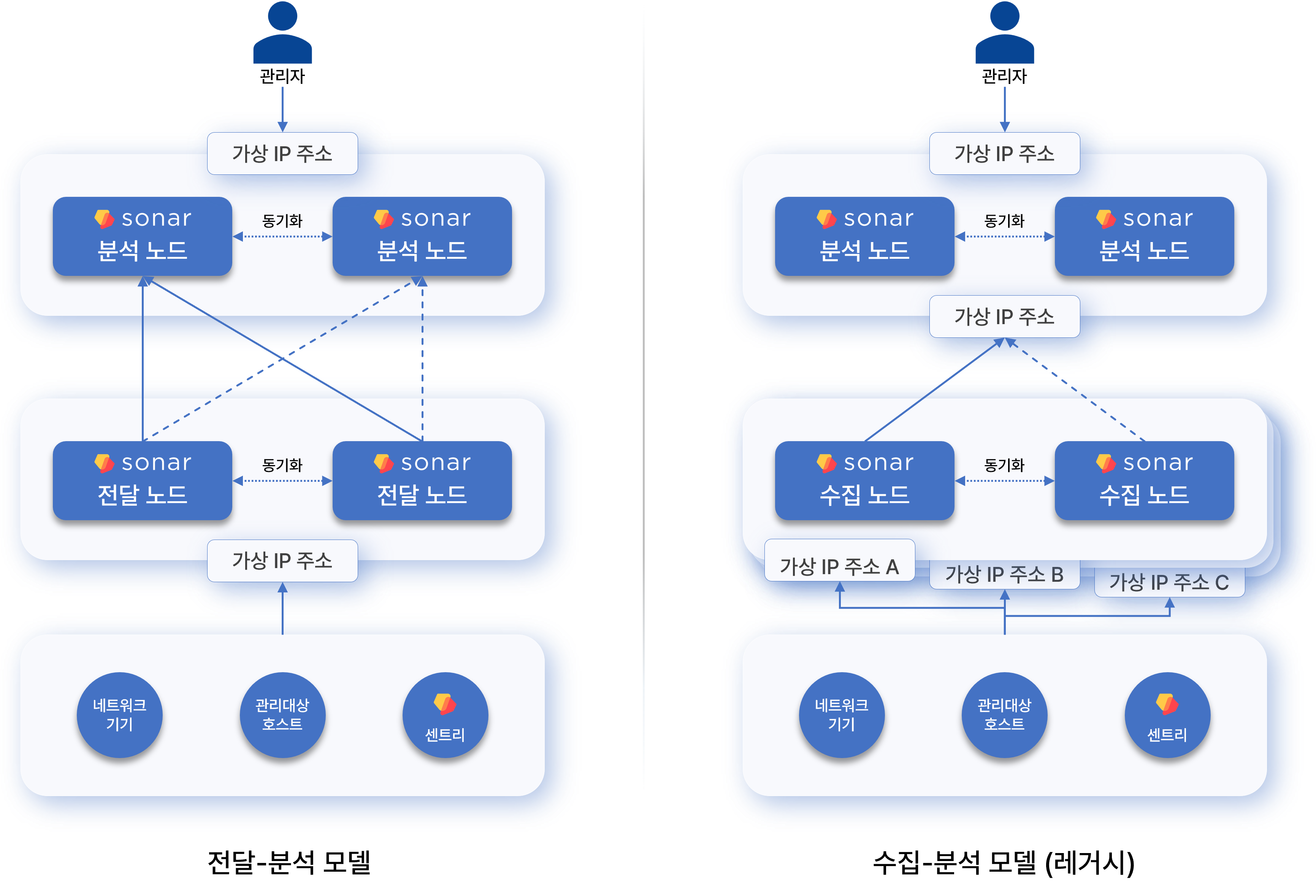
**각 노드는 가상 IP 주소를 공유**하므로 외부에서 클러스터에 접속하려면 분석 노드의 가상 IP 주소나 도메인 주소를 이용하면 됩니다.

* 네트워크 기기, 관리대상 호스트, 센트리가 데이터를 전송하면 액티브 상태인 노드가 데이터 수신
* 관리자의 분석 노드 접속이 액티브 노드가 웹 콘솔 제공

분석 노드 페어는 수평 확장할 수 없으므로 수집할 데이터가 증가하면 3 티어 구성으로 변경하는 것이 좋습니다.

2 티어: 전달-분석 / 수집-분석 (레거시)

2티어 구성은 데이터를 수집하는 노드와 데이터를 보관하는 노드를 나누는 방식입니다. 2티어는 다음 그림에서 좌측은 전달-분석 모델, 우측은 수집-분석 모델(레거시)입니다.



**전달-분석 모델**

분석 노드로 구성된 1 티어 아키텍처에 전달 노드 페어가 추가된 형태로 [로그프레소 클라우드](https://logpresso.cloud/)에서 볼 수 있는 기본 구성입니다. 전달 노드는 4.0.2404.0 버전에서 도입되어 데이터 게이트웨이 및 로드밸런서로서 동작합니다([관련 문서](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/sonar/4.0/issues/SNR2070)). 전달 노드, 분석 노드 모두 가용성을 고려해 이중화를 권장합니다.

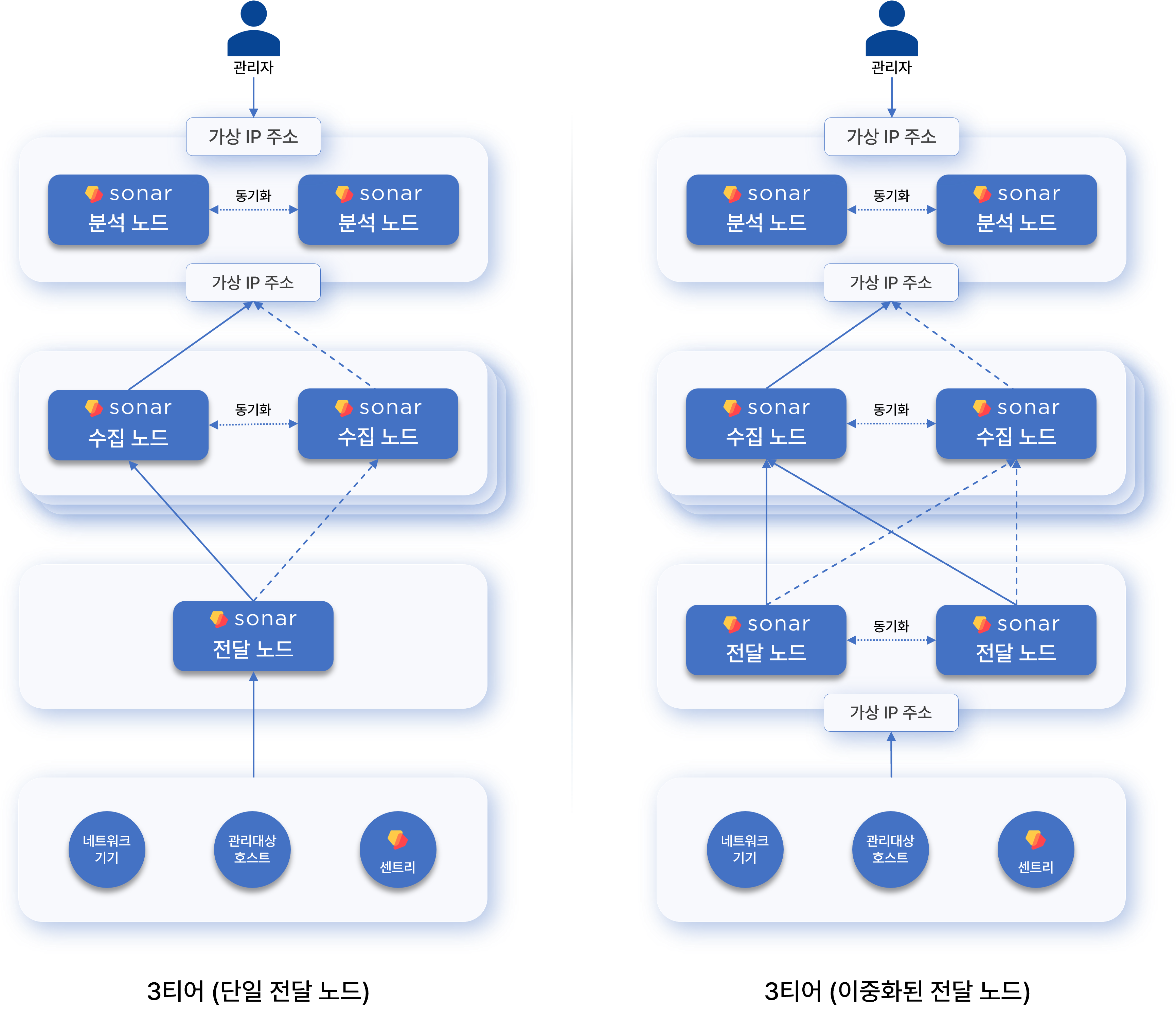
전달 노드는 후위 노드의 수평 확장을 고려해 사용되므로 이 구성은 3 티어 구성의 과도기적인 형태라 할 수 있습니다. 분석 노드는 하나의 페어만 이용할 수 있으므로 수평 확장하려면 3 티어 구성으로 전체 구성을 변경해야 합니다.

**수집-분석 모델(레거시)**

4.0.2404.0 버전 이전에 사용하던 아키텍처로, 1 티어 구성에 수집 노드 페어가 추가된 형태입니다. 데이터 수집과 분석을 수행하는 티어를 구분함으로써 수집 노드 페어 단위로 수평 확장할 수 있어 수집할 데이터가 증가하더라도 유연하게 대응할 수 있습니다. 그러나 데이터 원천(네트워크 기기, 관리대상 호스트, 센트리)마다 각각 지정된 수집 노드 페어와 통신해야 하므로 수집 노드 페어가 늘어날수록 네트워크 토폴로지가 복잡해지는 단점이 있어 권장하지 않습니다.

3 티어: 전달-수집-분석 (권장 구성)

3 티어 전달-수집-분석 모델은 2 티어 수집-분석 모델 (레거시)를 대체하는 새로운 아키텍처로, 대규모 데이터 수집 환경에서 권장하는 클러스터 구성입니다.



3 티어 구성은 2 티어 구성의 모든 단점을 극복할 수 있는 구성입니다. 수집 노드 페어가 2개 이상이면 반드시 전달 노드를 구성하세요. 전달 노드는 2 티어 수집-분석 모델의 토폴로지 문제를 해결할 수 있습니다.

레거시에서 3 티어로 전환

레거시 아키텍처에서 3 티어 아키텍처로 전환하려면 다음과 같은 단계가 필요합니다.

**1. 전달 노드 설치**

전달 노드를 운영 환경에 반입하여 설치합니다.

**2. 앱 재설치**

전달 노드애 앱이 설치되지 않으므로, 필요 시 [앱 재설치](https://docs.logpresso.com/ko/sonar/4.0/ui/section-apps)를 통해 전달 서버에 앱을 설치해야 합니다.

**3. 수집기 교체**

[수집기의 수집 방식](https://docs.logpresso.com/ko/sonar/4.0/ui/section-loggers)에 따라 다른 접근이 필요합니다.

**패시브 수집기**

새 수집기 구성 후 레거시 수집기 중지/삭제

수집 위치가 전달 노드 페어, 적재 위치가 수집 노드 페어인 수집기 구성

데이터 원천에서 데이터 전송 목적지를 전달 노드의 가상 IP 주소 또는 도메인 주소로 변경 후 수집 상태 확인

문제 없으면 레거시 수집기의 실행을 중지하거나 제거

**액티브 수집기**

레거시 수집기 중지 후 새 수집기 구성

수집 노드에서 실행 중인 레거시 수집기 중지

수집 위치가 전달 노드 페어, 적재 위치가 수집 노드 페어인 수집기 구성 후 수집 상태 확인

문제 없으면 필요에 따라 레거시 수집기를 제거

노드 유형

로그프레소 클러스터는 분석 노드(control node), 수집 노드(data node), 전달 노드(forwarder node)로 구성됩니다. 단독 실행되는 로그프레소 소나 서버는 수집 노드, 분석 노드의 역할을 모두 수행합니다.

분석 노드

분석 노드는 로그프레소 클러스터의 모든 노드를 제어하는 기능을 수행하고, 사용자가 클러스터에 접근할 수 있도록 웹 콘솔을 제공합니다. 이중화된 분석 노드는 가상 IP 주소를 공유합니다.

**노드 제어**

전달 노드, 수집 노드는 분석 노드의 가상 IP 주소로 설정 및 정책 동기화를 요청하고, 분석 노드는 각 노드의 요청에 따라 변경된 설정이나 정책을 전송하는 폴링(polling) 방식으로 통신합니다.

**사용자 웹 인터페이스**

사용자 또한 분석 노드의 가상 IP 또는 도메인 주소를 이용해 웹 콘솔에 접근할 수 있습니다. 정책 위반으로 소명 요청을 받은 임직원이나 소명을 검토해야 하는 결재자의 웹 접속 주소도 이 가상 IP 주소를 이용합니다.

**데이터 분석 및 보안 위협 및 이상행위 탐지**

분석 노드는 수집 노드에 적재된 데이터를 바탕으로 [실시간 탐지](https://docs.logpresso.com/ko/sonar/4.0/ui/section-stream-rule), [배치 탐지](https://docs.logpresso.com/ko/sonar/4.0/ui/section-batch-rule) 시나리오에 따라 다음과 같은 동작을 수행합니다.

* 보안 위협이나 이상행위 [이벤트](https://docs.logpresso.com/ko/sonar/4.0/ui/section-events) 탐지
* [티켓](https://docs.logpresso.com/ko/sonar/4.0/ui/section-ticket) 발행 및 관리
* [소명](https://docs.logpresso.com/ko/sonar/4.0/ui/section-explanation) 및 결재 관리
* 탐지된 위협에 [자동 대응](https://docs.logpresso.com/ko/sonar/4.0/ui/section-playbook)

사용자가 분석 노드에서 실행하거나, 로그프레소 클러스터에서 주기적으로 실행되는 로그프레소 쿼리는 대부분 수집 노드에 있는 데이터를 읽어와 처리합니다. 분석 노드는 로그프레소 쿼리문의 실행 계획을 수립하고 관리하는 역할을 수행하고, 각 노드에서 분산 처리된 결과를 받은 후 데이터를 가공합니다.

분석 노드는 데이터베이스로 온프레미스 환경에서 MariaDB, 클라우드에서 매니지드 데이터베이스를 사용합니다.

수집 노드

수집 노드는 수집기를 통해 수집된 데이터를 파싱하고 정규화, 인덱싱하여 [테이블](https://docs.logpresso.com/ko/sonar/4.0/ui/section-table)에 저장하고 관리합니다.

**데이터 적재 및 쿼리 실행**

[파서](https://docs.logpresso.com/ko/sonar/4.0/ui/section-parsers)에 의한 원본 데이터 파싱과 [수집 모델](https://docs.logpresso.com/ko/sonar/4.0/ui/section-logger-models)에 정의된 정규화는 모두 수집 노드에서 이뤄집니다.

모든 수집 노드는 각각 동일한 이름을 갖는 테이블에 원본 데이터와 정규화된 데이터를 함께 저장합니다. 분석 노드에서 로그프레소 쿼리를 실행하면 [table](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/table-command), [fulltext](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/query/fulltext-command)와 같은 데이터 조회 명령은 각 수집 노드에서 병렬로 처리됩니다.

**생명주기 관리**

수집 노드는 테이블에 정의된 [보관 주기](https://docs.logpresso.com/ko/sonar/4.0/ui/section-table)와 [데이터 생명주기](https://docs.logpresso.com/ko/sonar/4.0/ui/subsection-lifecycle)에 따라 데이터를 관리합니다.

전달 노드

전달 노드는 4.0.2404.0 버전에서 도입되었습니다([관련 문서](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/sonar/4.0/issues/SNR2070)). 이중화된 전달 노드도 분석 노드처럼 가상 IP 주소를 공유합니다. 역할은 크게 두 가지입니다.

- 수집 노드 페어가 2개 이상일 때, 전달 노드의 구성을 권장합니다.- 수집 노드 페어를 액티브-액티브 방식으로 운영하려면 L4 스위치나 네트워크 로드밸런서가 필요합니다.

**데이터 게이트웨이**

[수집기](https://docs.logpresso.com/ko/sonar/4.0/ui/section-loggers)는 전달 노드에서 실행되고, 전달 노드는 로그프레소 클러스터의 데이터 송수신 게이트웨이가 됩니다. 전달 노드의 가상 IP 주소 또는 도메인 주소가 게이트웨이 주소로 사용됩니다.

전달 노드 대신에 수집 노드가 데이터 게이트웨이 역할을 수행할 수 있지만 권장하지 않습니다. 수집 노드 페어 개수만큼 데이터 게이트웨이가 늘어나고, 데이터 원천은 그 중에서 하나만 지정해 데이터를 전송해야 하므로 네트워크 구조가 복잡해집니다.

**부하 분산**

전달 노드가 수신/수집한 데이터는 수집 노드로 전송됩니다. 전달 노드는 [수집기](https://docs.logpresso.com/ko/sonar/4.0/ui/section-loggers)에 정의된 전송 방식에 따라 여러 수집 노드 페어에 균등하게 데이터가 적재되도록 로드 밸런싱을 수행하거나, 특정한 노드 페어로 데이터를 전송합니다.

전달 노드는 수집 노드와 통신 중 장애를 감지하면 전송할 데이터를 메모리와 로컬 디스크에 임시 보관하고, 장애가 복구되면 보관한 데이터를 수집 노드로 재전송합니다. 전달 노드는 전송을 완료한 후 로컬에 남아 있는 데이터를 제거합니다.

구성 순서

클러스터를 구성할 때 다음과 같은 순서로 노드를 구성하세요.

분석 노드 및 이중화

수집 노드 및 이중화

전달 노드 및 이중화

이 설명서는 웹 콘솔의 사용법만 다루고, 실제 설치 과정은 별도의 문서를 제공합니다.

* 분석 노드, 수집 노드의 설치 과정은 별도의 문서를 제공할 예정입니다.
* 전달 노드의 설치 및 설정 과정은 [이 문서](https://docs.logpresso.com/ko/sonar/4.0/ui/ko/sonar/4.0/forwarder)를 참고하세요.

데이터 생명주기

데이터 생명주기는 일반적으로 데이터의 생성부터 삭제까지 일련의 과정을 의미합니다. 로그프레소 소나는 데이터 원천으로부터 수집하는 데이터는 로그, PCAP 파일과 같은 것으로, 시간순으로 생성되는 특징이 있습니다. 이러한 데이터는 '현재'와 가까울수록 중요도가 높다는 특징이 있습니다.

저장하는 데이터의 용량이 늘어남에 따라 보관 비용 역시 증가하게 됩니다. 스토리지 생명주기 기능은 자주 접근하는 최근 데이터는 빠르지만 비싼 스토리지에, 드물게 접근하는 오래된 데이터는 느리지만 저렴한 스토리지에 나눠 저장할 수 있게 해줌으로써 성능과 비용 사이의 균형점을 찾을 수 있는 방법을 제공합니다.

저장된 데이터의 위치가 변경되거나, 변경 중일 때에도 데이터의 조회/분석 기능은 단일 스토리지를 사용할 때와 동일하게 동작하므로 시스템 운영과 사용에는 전혀 영향이 없습니다.

데이터 생명주기는 수집된 데이터에만 적용되고, 클러스터를 구성하는 노드들의 시스템 데이터에는 적용되지 않습니다.

스토리지 계층

로그프레소 소나는 접근 빈도가 높은 최근 데이터를 가장 성능이 좋은 스토리지(SSD)에 저장하고, 접근 빈도가 낮은 오래된 데이터를 상대적으로 성능은 낮지만 저렴한 스토리지(NAS, 클라우드 오브젝트 스토리지)에 저장하는 스토리지 계층화를 지원합니다.

로그프레소 소나의 스토리지는 3 계층으로 구성됩니다.

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | Hot (제1계층) | Warm (제2계층) | Cold (제3계층) |
| 장치 유형 | NVMe, SSD | HDD, WORM | WORM, NAS, 클라우드 오브젝트 스토리지 |
| 검색 성능 | 매우 높음 | 보통 | 낮음 |
| 통계 성능 | 높음 | 보통 | 낮음 |
| 복제 계수 | 2 | 2 | 1 |
| 단위 비용 | 높음 | 보통 | 낮음 |
| 구성 목적 | 검색 성능 극대화 | 범용 분석 | 데이터 아카이빙, 컴플라이언스 준수 |

**Hot**

수집된 데이터를 가장 먼저 저장하는 최상위 계층 고비용 고성능 스토리지. 설정한 기간이 지나면 하위 계층(Warm 또는 Cold)으로 데이터를 롤오버합니다.

**Warm**

Hot 계층에서 롤오버된 데이터를 저장하는 중간 비용 중간 성능 스토리지. 노드가 이중화되어 있으면 **노드 A, 노드 B가 각각 롤오버를 수행**하므로 동일한 데이터가 한 벌씩 복제됩니다.

**Cold**

Hot, Warm같은 상위 계층에서 롤오버된 데이터를 저장하는 저비용 저성능 스토리지. 노드가 이중화되어 있어도 **데이터는 한 벌만 롤오버**됩니다.

Cold 계층은 보통 컴플라이언스를 준수하는데 요구되는 오래된 데이터를 저장하거나, 활용 가치가 낮고 검색 빈도가 매우 적은 데이터를 보관하는 용도로 사용됩니다.

운영 환경과 목적에 따라 Warm, Cold 계층은 선택적으로 적용할 수 있습니다. WORM 스토리지를 사용하려면 로그프레소 스토어에서 WORM 드라이버

Warm, Cold 디렉터리에 NFS 등을 사용하는 경우, 데이터 전송 속도가 충분히 보장되는지 확인하세요.

롤오버

롤오버는 데이터의 보관 기간이나 용량에 따라 데이터를 하위 계층으로 이전하는 동작입니다. 예를 들어 Hot, Warm, Cold 계층에 각각 120일의 보관 기간을 지정했다면, 데이터는 각 계층마다 120일씩 총 360일의 보관 기간을 거칩니다. 데이터가 Cold 계층에서 보관 기간을 다하면 계층에 정의된 설정에 따라 삭제되거나, 영구 보관됩니다.



* 롤오버는 수집된 데이터를 대상으로 적용되고 시스템 데이터는 항상 Hot 계층에 보관됩니다.
* [롤 오버 설정](https://docs.logpresso.com/ko/sonar/4.0/ui/subsection-storage)에서 실행 일정과 스토리지 계층 간 데이터 전송 시 속도를 제한할 수 있습니다.
* [스토리지 최대 용량](https://docs.logpresso.com/ko/sonar/4.0/ui/subsection-storage)을 지정할 수 있습니다. 각 노드는 15분 마다 스토리지 최대 용량을 점검하고, 보관 중인 데이터가 최대 용량을 초과하면 하위 스토리지 계청으로 초과된 데이터를 롤오버합니다.

로그프레소 소나는 롤오버할 때 데이터의 손실을 방지하기 위해 다음과 같이 동작합니다.

하위 계층에 전송할 파일과 동일한 임시 파일을 복제합니다.

파일 복제가 완료되면 상위 스토리지에서 파일을 삭제하고, 임시 파일의 이름을 원본과 동일하게 변경합니다.

하위 계층의 스토리지가 WORM이거나 클라우드 스토리지인 경우, 임시 파일 복제 없이 파일을 전송하도록 설정할 수 있습니다.

기존 기능 대비 차이점

데이터 생명주기는 테이블의 [보관 주기](https://docs.logpresso.com/ko/sonar/4.0/ui/section-table), 노드의 [스토리지 관리](https://docs.logpresso.com/ko/sonar/4.0/ui/subsection-node)와 유사하지만 다음과 같은 차이가 있습니다.

|  |  |  |
| --- | --- | --- |
| 구분 | 테이블 보관 주기 | 생명주기 |
| 적용 범위 | 개별 테이블 안에 있는 데이터(지역 설정) | 스토리지에 기록된 모든 데이터(전역 설정) |
| 관리 대상 | 테이블 파티션 단위 데이터 | 테이블 파티션 단위 데이터 |
| 보관 기한 초과 | 데이터 삭제 | 하위 스토리지 계층으로 롤오버 |
| 스토리지 관리 | 오래된 데이터 삭제 또는 수집 중지 | (1차) 롤오버, (2차) 삭제 또는 아카이빙 |

데이터 생명주기와 테이블 보관 주기는 서로 독립적으로 실행됩니다. 두 기능이 지정한 데이터 보관 기한 중에서 먼저 도래한 기한이 적용되어 데이터가 삭제될 수 있으므로 다음 중 한 가지를 선택해 데이터를 관리하세요.

데이터 생명주기만 사용

* 테이블 생성 시 보관 주기 기본 설정인 "영구 저장"을 그대로 사용하세요.
* 생명주기에 기반한 데이터 관리는 전역 설정이므로 테이블 단위의 데이터 관리보다 용이합니다.

데이터 생명주기를 주기능, 테이블의 보관 주기를 보조기능으로 사용

* 전역 설정으로 데이터 생명주기의 보관 기간을 지정하세요.
* 테이블의 보관 주기는 필요할 때만 전역 설정보다 짧게 지정하세요.

생명주기 초기값

생명주기의 초기값은 정의되어 있지 않습니다. 이 상태에서 데이터는 테이블의 보관 주기와 노드의 스토리지 관리 설정에 따라 동작합니다.

**테이블**에 정의된 [보관 주기](https://docs.logpresso.com/ko/sonar/4.0/ui/section-table): 보관 주기가 지난 데이터를 삭제하거나 영구 보관합니다.

**노드**의 [스토리지 관리](https://docs.logpresso.com/ko/sonar/4.0/ui/subsection-node): 로컬 스토리지가 포화되기 전에 오래된 데이터부터 삭제하거나 데이터 수집을 중지합니다. 이때 모니터링하는 스토리지는 로그프레소의 데이터 저장 디렉터리가 있는 파티션입니다.