

멀티 클라우드 환경에서의 LLM 기반 로그 분석 및 이상 탐지

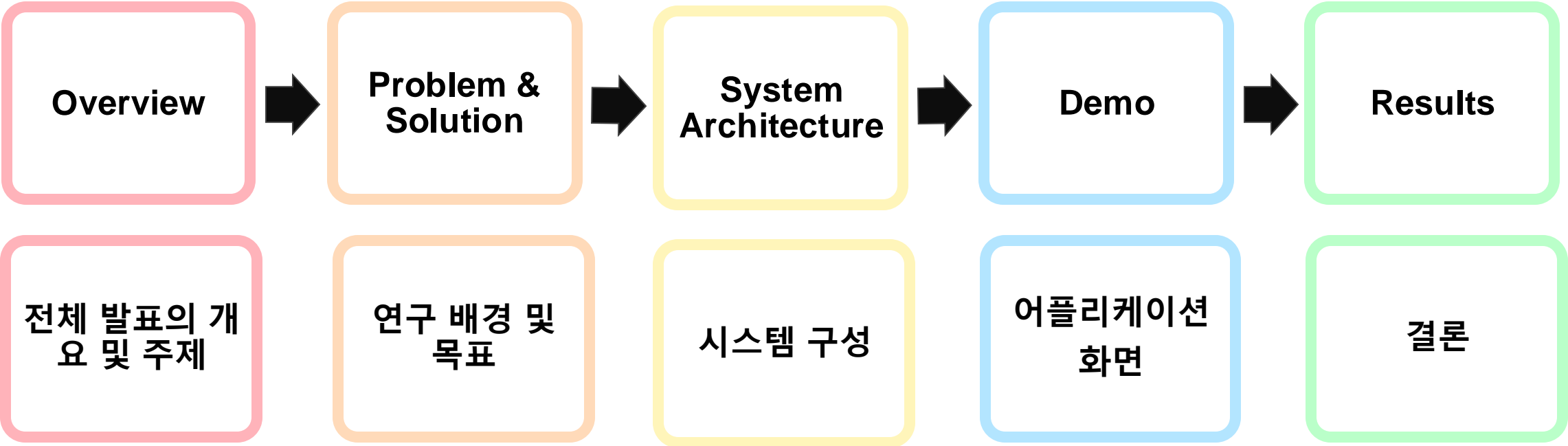
202155595 이한홍

202155590 이종일

201924479 박재홍

지도교수 김호원

2024.11.01.



Problem & Solution

❖ 연구 배경 및 필요성

1. 클라우드 환경에서의 대규모 로그 데이터 처리

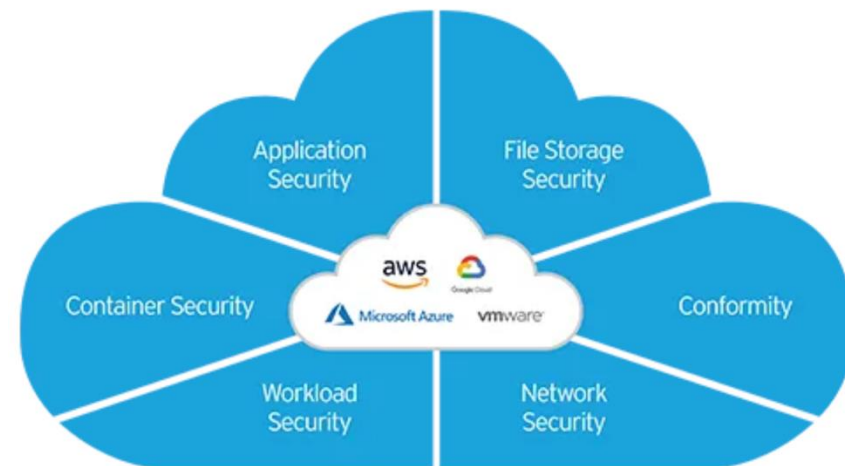
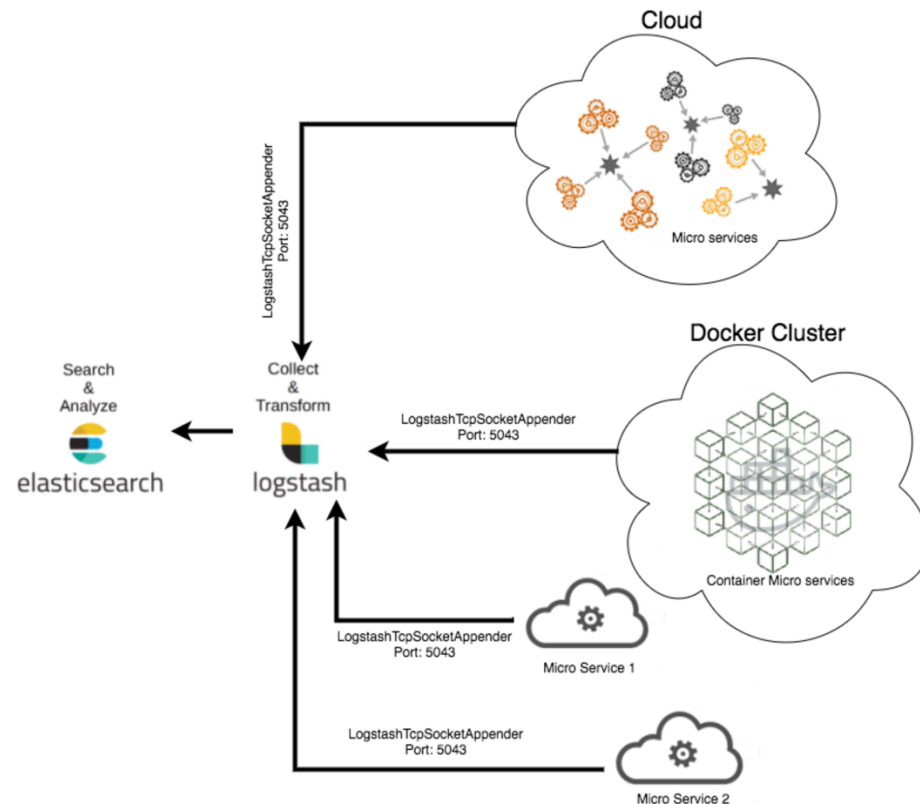
- 멀티 클라우드 환경과 MSA 도입으로 애플리케이션이 여러 인프라에 분산됨에 따라 로그 데이터의 양이 급증했고, 이를 체계적으로 수집하고 신속하게 분석할 수 있는 역량이 중요해짐.

2. 클라우드 환경에서의 보안 위협 증가

- 클라우드 인프라의 복잡성으로 인해 보안 위협이 증가하고 있으며, 로그 데이터를 활용한 실시간 모니터링과 분석을 통해 신속하게 대응하는 능력이 중요해짐.

3. 전통적인 탐지 방식의 한계

- 기존의 규칙 기반 탐지 방식은 고정된 패턴이나 조건에 의존하기 때문에, 새로운 문제나 비정상적인 동작을 탐지하는 데 한계가 있음.



❖ 연구 목표

1. 멀티 클라우드 환경에서 로그 데이터 수집 및 분석

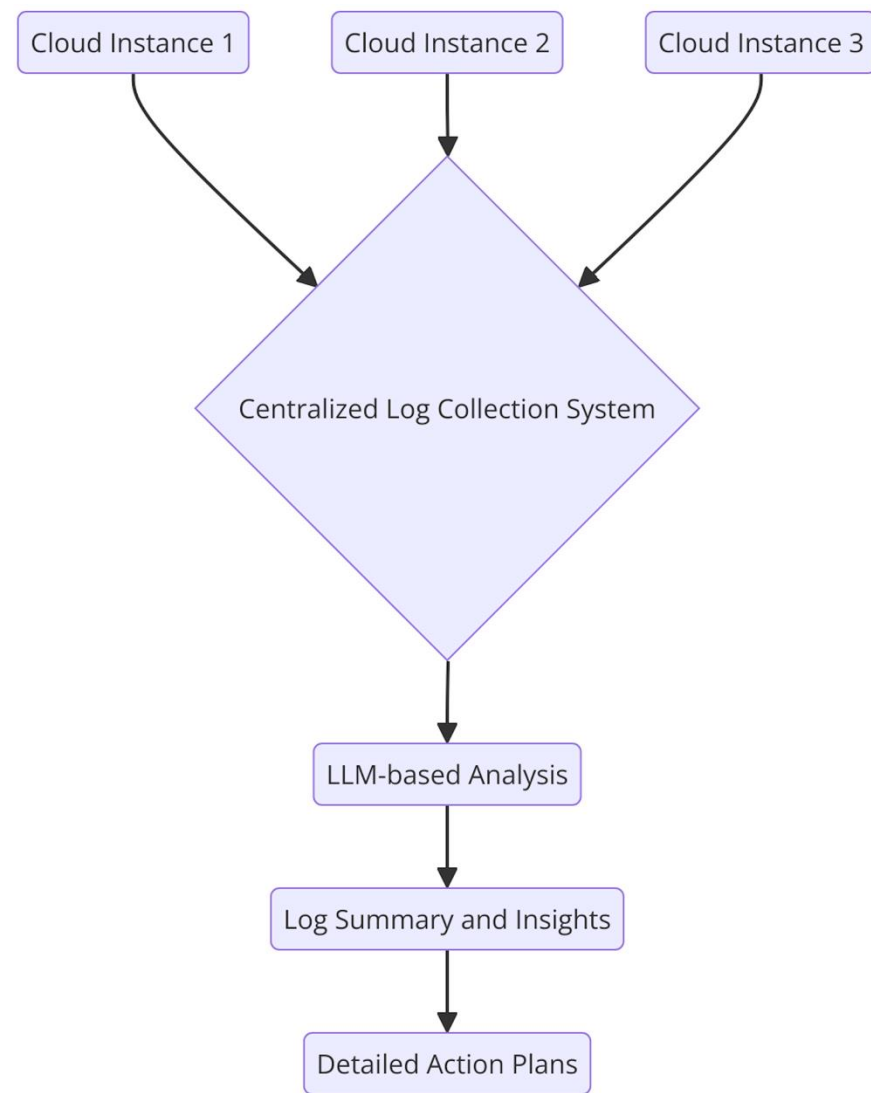
- 멀티 클라우드 환경에서 발생하는 대규모 로그 데이터를 실시간으로 수집하고, LLM을 활용해 이를 요약하고 분석하는 시스템을 구축한다.

2. 계층적 로그 요약 및 중요도 기반 정보 제공

- 로그 데이터를 **계층적**으로 요약하고 **중요도**에 따라 선별적으로 정보를 제공하여, 관리자가 **핵심** 정보에 집중하고 시스템을 보다 효율적으로 모니터링 할 수 있게 한다.

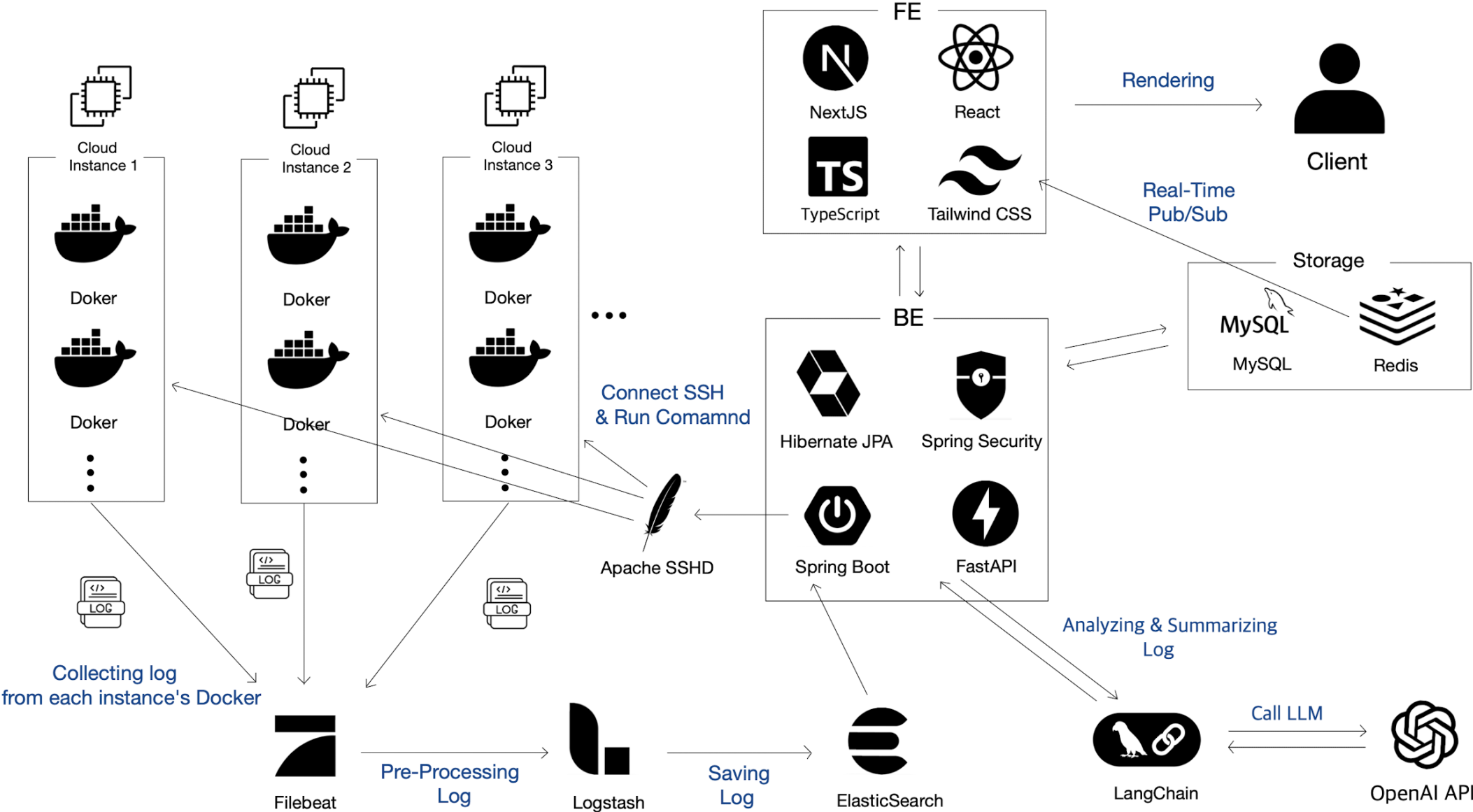
3. 효율적인 문제 해결 및 대응

- 구체적인 대응방안을 제시하고, 관리자가 실시간으로 시스템 상태를 확인하며 필요한 조치를 **원격**으로 신속히 취할 수 있도록 지원한다.



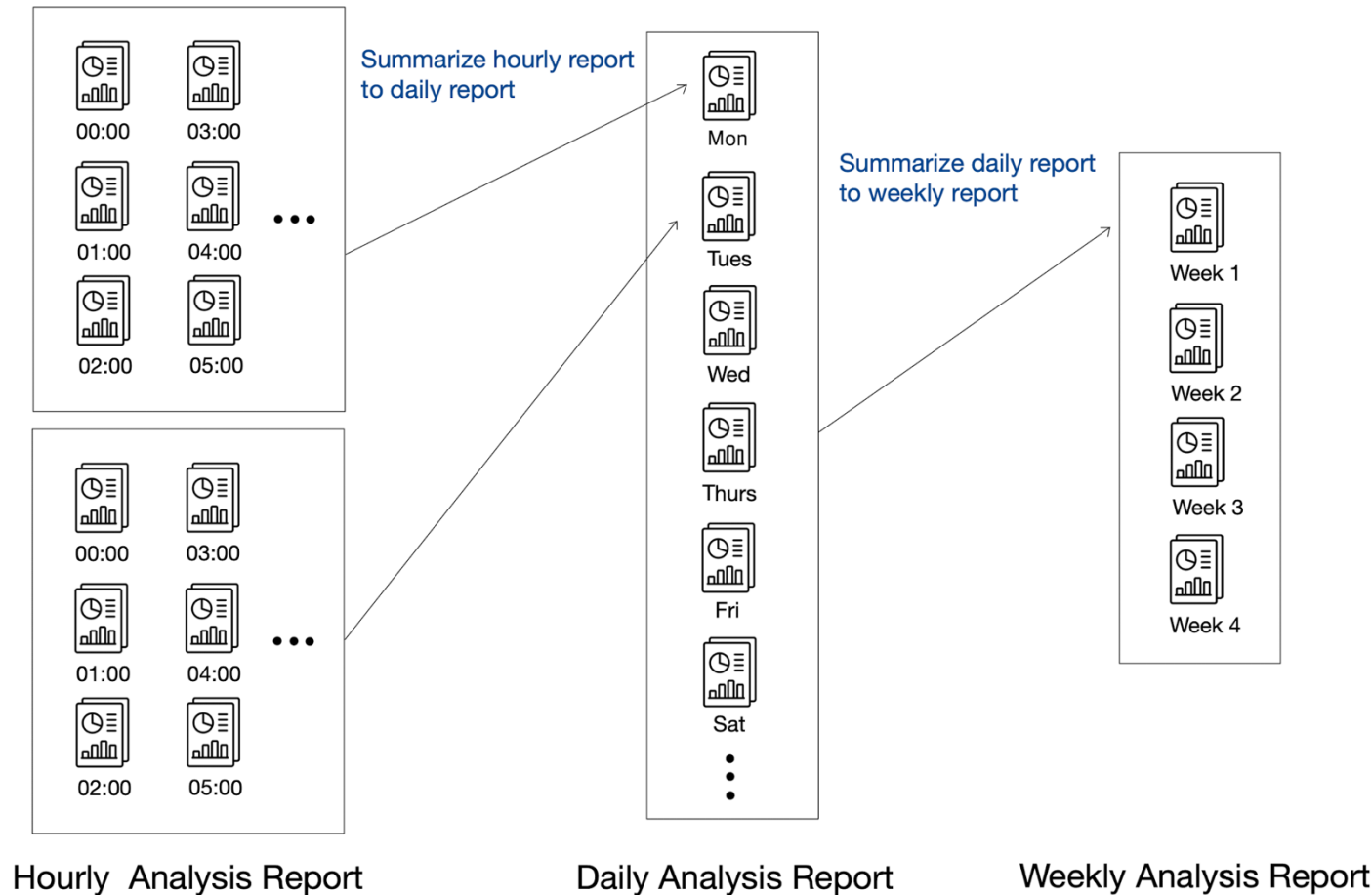
System Architecture

❖ 전체 구성도



System Architecture

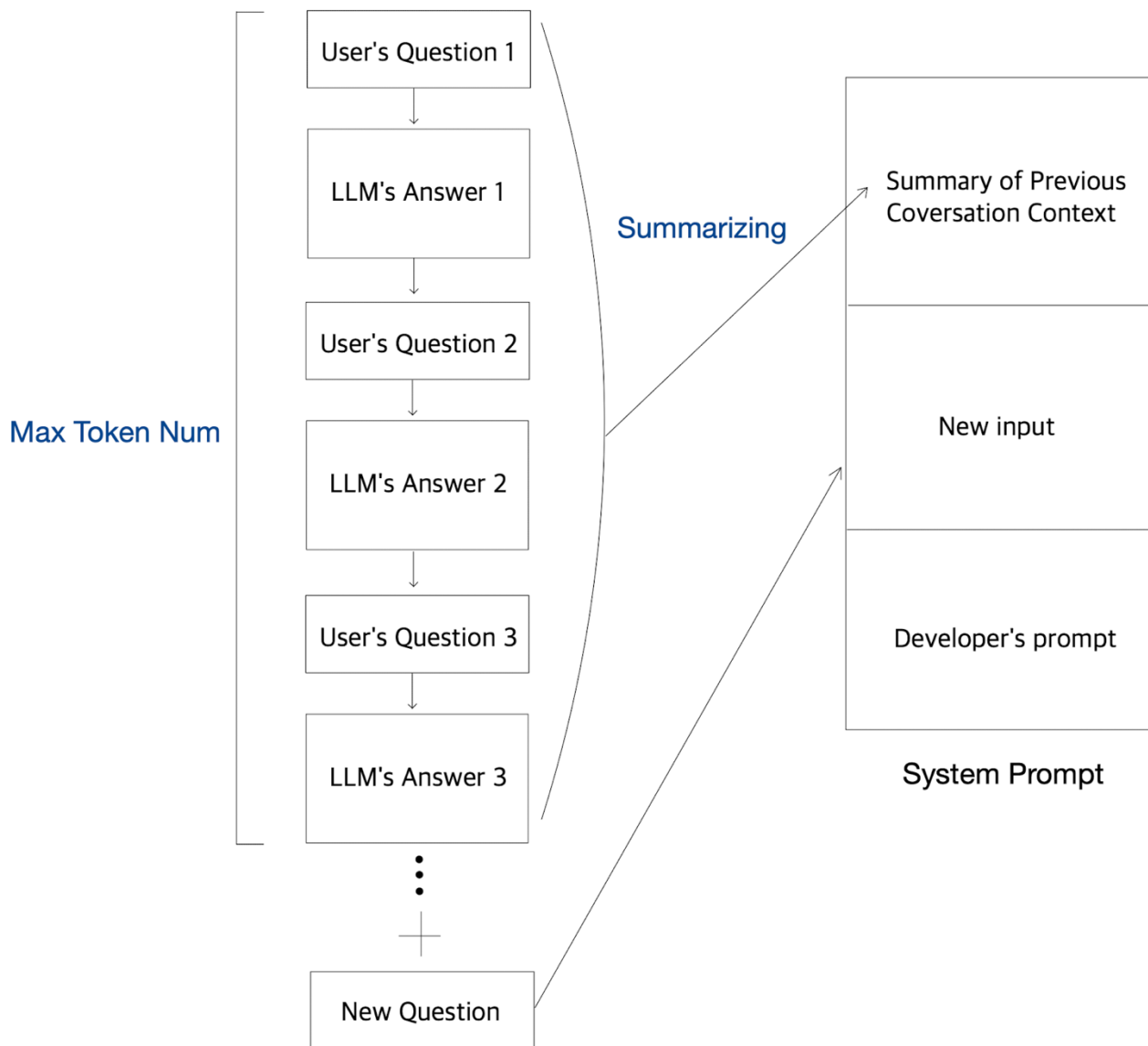
❖ 로그의 계층적 관리



- 수집된 로그 데이터를 LLM을 통해 시간별로 요약한 후, 이를 바탕으로 일일 요약을 생성하고, 주간 요약으로 확장하여 로그를 **계층적**으로 관리.
- 시간별 로그를 단계적으로 확장하는 **다단계** 분석을 통해, **단기적** 이벤트부터 **장기적** 추세까지 모두 파악해 정확한 판단과 조치 가능.

System Architecture

❖ 토큰 한계를 해결하는 대화 맥락 유지 전략



- 대화가 일정량 이상 누적될 때마다 시스템이 이전 대화를 **요약**하여 프롬프트에 포함.
- 요약된 대화는 새로운 질문과 **함께** 시스템 프롬프트에 추가되어, LLM이 이전 대화 맥락을 유지한 상태에서 답변할 수 있도록 지원.

LLMN

검색

1

호애이

로그아웃

새로운 아이템

로그 기록

인사이트

설정

대시보드 54.180.244.93

CPU 사용량 52%

메모리 사용량 32%

네트워크 수신 0.02 MB

네트워크 송신 0.03 MB

요약

[Warning] 2024-09-10 13:45: CPU 사용량이 85% 이상입니다. 시스템 점검이 필요합니다.

[Critical] 2024-09-10 13:30: 네트워크 수신량이 비정상적으로 높습니다. 원인 분석을 권장합니다.

[Warning] 2024-09-10 13:15: 평소보다 네트워크 트래픽이 비정상적으로 높습니다. 이전 7일 평균보다 50% 높은 트래픽이 감지되었습니다.

[Critical] 2024-09-10 13:30: 매일 오전 10시에 메모리 사용량이 급증합니다. 해당 시간대에 불필요한 작업을 줄이거나 리소스 할당을 조정하는 것을 권장합니다.

CPU

40

30

20

10

0

09:00

12:00

15:00

18:00

21:00

| | | | | |
|-------|-------|-------|-------|-------|
| 09:00 | 12:00 | 15:00 | 18:00 | 21:00 |
| 12 | 25 | 18 | 35 | 36 |

Memory

40

30

20

10

0

09:00

12:00

15:00

18:00

21:00

| | | | | |
|-------|-------|-------|-------|-------|
| 09:00 | 12:00 | 15:00 | 18:00 | 21:00 |
| 12 | 25 | 18 | 35 | 36 |

➤ 클라우드 서버의 상태를 실시간으로 모니터링하는 대시보드 화면

+ 새로운 아이템

📄 로그 기록

🔍 인사이트

⚙️ 설정

새로운 아이템

<주의> 컨테이너의 이름을 추후에 변경하면 기능이 정상적으로 작동하지 않을 수 있습니다.

프로젝트 이름

ForPaw - Spring Boot

설명

ForPaw 프로젝트의 스프링 어플리케이션

클라우드 인스턴스

Ubuntu (54.180.244.93)



컨테이너

연결할 컨테이너를 선택해주세요.



Spring

FastAPI

React

연결하지 않음

➤ 모니터링 할 클라우드의 프로젝트(컨테이너)를 등록하는 화면

LLMN

검색

🔔 1

👤 호애이 ▾

🚪 로그아웃

+ 새로운 아이템

📄 로그 기록

🔍 인사이트

⚙️ 설정

프로젝트

🔄

| 상태 | 이름 | 설명 | CPU | Mem | 컨테이너 |
|----|---------|------------------------|-------|---------------------|---------|
| ✔️ | Spring | ForPaw BE - 스프링 | 8.46% | 89.08MiB / 949.2MiB | 실행중 |
| ✔️ | MongoDB | No RDBMS DB | N/A | N/A | 종료됨 |
| ❌ | FastAPI | ForPaw BE - FastAPI... | N/A | N/A | 연결되지 않음 |

➤ 등록된 프로젝트들의 목록과 상태를 조회하는 화면

+ 새로운 아이템

로그 기록

인사이트

설정

Spring

ForPaw BE의 스프링 프로젝트

- 수정하기
- 컨테이너 재시작
- 컨테이너 종료
- 삭제하기

요약

2024.09.10_18

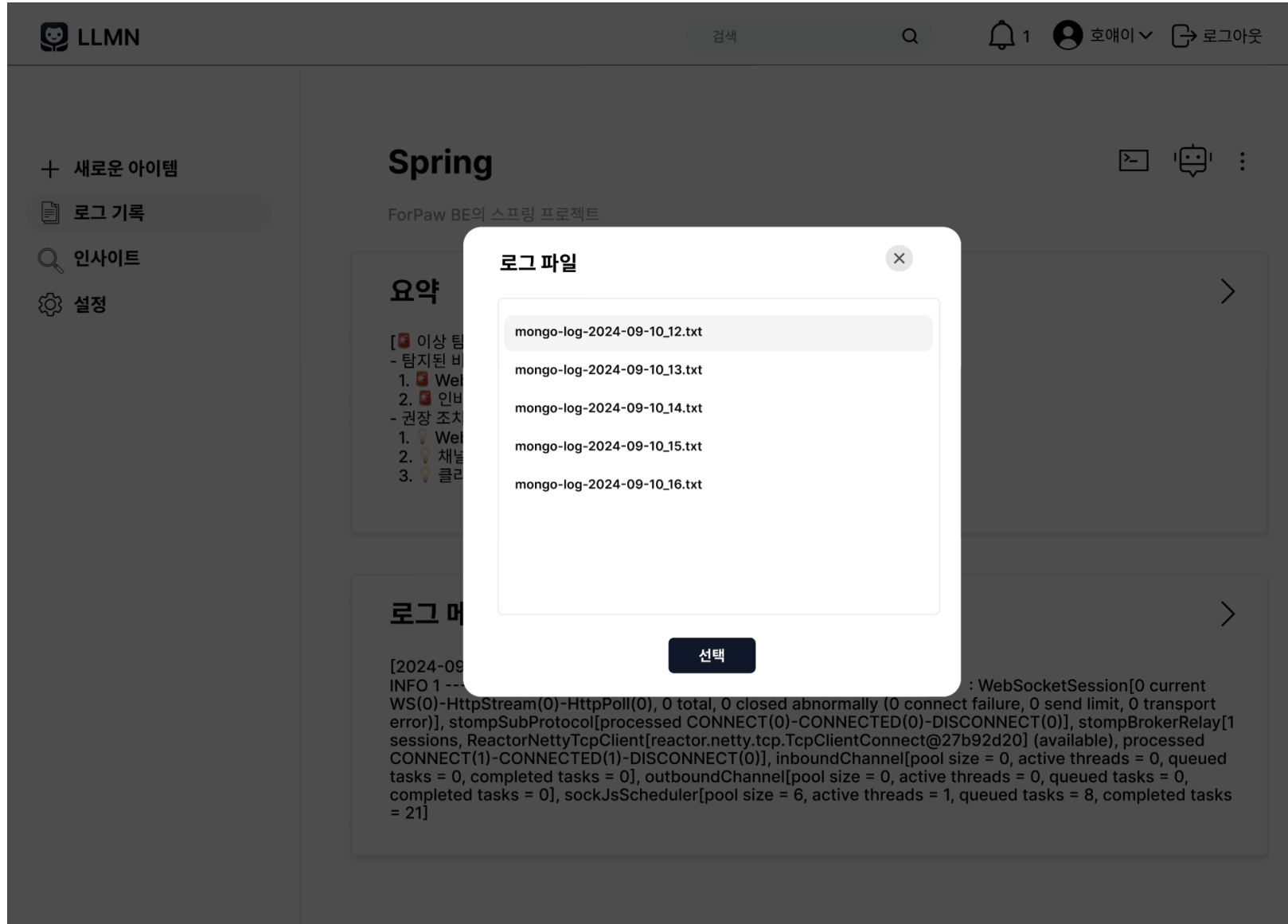
- [🔴 이상 탐지 요약]
- 탐지된 비정상 패턴
 1. 🚫 WebSocket 세션이 전혀 활성화되지 않음 (현재 세션 0개)
 2. 🚫 인바운드 및 아웃바운드 채널의 활성 스레드가 0개로 비정상적으로 낮음
 - 권장 조치
 1. 💡 WebSocket 서버 설정 및 연결 상태 점검
 2. 💡 채널 풀 및 스레드 설정 검토
 3. 💡 클라이언트 연결 요청 확인 및 로그 추가 분석"

로그 메시지

[2024-09-10_10:59]
INFO 1 --- [MessageBroker-3] o.s.w.s.c.WebSocketMessageBrokerStats : WebSocketSession[0 current WS(0)-HttpStream(0)-HttpPoll(0), 0 total, 0 closed abnormally (0 connect failure, 0 send limit, 0 transport error)], stompSubProtocol[processed CONNECT(0)-CONNECTED(0)-DISCONNECT(0)], stompBrokerRelay[1 sessions, ReactorNettyTcpClient[reactor.netty.tcp.TcpClientConnect@27b92d20] (available), processed CONNECT(1)-CONNECTED(1)-DISCONNECT(0)], inboundChannel[pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 0], outboundChannel[pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 0], sockJsScheduler[pool size = 6, active threads = 1, queued tasks = 8, completed tasks = 21]

➤ 확인하고 싶은 프로젝트의 개요를 조회하는 화면

❖ 로그 파일 선택



➤ 조회하고 싶은 프로젝트의 로그 파일을 선택하는 화면

+ 새로운 아이템

로그 기록

인사이드

설정

Spring - 로그 메시지

ForPaw BE의 스프링 프로젝트



mongo-log-2024-09-10_16.txt

```
[2024-09-10_10:59]
INFO 1 --- [MessageBroker-3] o.s.w.s.c.WebSocketMessageBrokerStats : WebSocketSession[0 current
WS(0)-HttpStream(0)-HttpPoll(0), 0 total, 0 closed abnormally (0 connect failure, 0 send limit, 0 transport
error)], stompSubProtocol[processed CONNECT(0)-CONNECTED(0)-DISCONNECT(0)],
stompBrokerRelay[1 sessions, ReactorNettyTcpClient[reactor.netty.tcp.TcpClientConnect@27b92d20]
(available), processed CONNECT(1)-CONNECTED(1)-DISCONNECT(0)], inboundChannel[pool size = 0,
active threads = 0, queued tasks = 0, completed tasks = 0], outboundChannel[pool size = 0, active threads
= 0, queued tasks = 0, completed tasks = 0], sockJsScheduler[pool size = 6, active threads = 1, queued
tasks = 8, completed tasks = 21]
```

```
[2024-09-10_11:29]
INFO 1 --- [MessageBroker-4] o.s.w.s.c.WebSocketMessageBrokerStats : WebSocketSession[0 current
WS(0)-HttpStream(0)-HttpPoll(0), 0 total, 0 closed abnormally (0 connect failure, 0 send limit, 0 transport
error)], stompSubProtocol[processed CONNECT(0)-CONNECTED(0)-DISCONNECT(0)],
stompBrokerRelay[1 sessions, ReactorNettyTcpClient[reactor.netty.tcp.TcpClientConnect@27b92d20]
(available), processed CONNECT(1)-CONNECTED(1)-DISCONNECT(0)], inboundChannel[pool size = 0,
active threads = 0, queued tasks = 0, completed tasks = 0], outboundChannel[pool size = 0, active threads
= 0, queued tasks = 0, completed tasks = 0], sockJsScheduler[pool size = 6, active threads = 1, queued
tasks = 8, completed tasks = 23]
```

```
[2024-09-10_11:51]
Hibernate: select
p1_0.id,p1_0.answer_num,p1_0.comment_num,p1_0.content,p1_0.created_date,p1_0.group_id,p1_0.hot_point
,p1_0.is_blocked,p1_0.post_id,p1_0.post_type,p1_0.read_cnt,p1_0.removed_at,p1_0.title,p1_0.updated_date,
p1_0.user_id from post_tb p1_0 where p1_0.created_date between ? and ? and p1_0.post_type=? and
p1_0.removed_at is null
```

```
[2024-09-10_11:51]
Hibernate: select
p1_0.id,p1_0.answer_num,p1_0.comment_num,p1_0.content,p1_0.created_date,p1_0.group_id,p1_0.hot...
```

➤ 로그 시간대를 선택한 후, 로그 메시지를 조회하는 화면

LLMN

검색

1

호애이

로그아웃

새로운 아이템

로그 기록

인사이트

설정

Spring - 요약

ForPaw BE의 스프링 프로젝트

2024-09-12 19:00

[🔴] 이상 탐지 요약

- 탐지된 비정상 패턴:

1. [🔴] WebSocket 세션이 전혀 활성화되지 않음 (현재 세션 0개)

2. [🔴] 인바운드 및 아웃바운드 채널의 활성 스레드가 0개로 비정상적으로 낮음

- 권장 조치:

1. [💡] WebSocket 서버 설정 및 연결 상태 점검

2. [💡] 채널 풀 및 스레드 설정 검토

3. [💡] 클라이언트 연결 요청 확인 및 로그 추가 분석"

2024-09-12 19:00

[📊] 일반적인 요약

- 주요 이벤트:

1. [ℹ️] WebSocket 세션 상태: 현재 0개의 WebSocket 세션, 1개의 연결 세션이 처리됨.

2. [ℹ️] Hibernate 쿼리: 사용자 정보 조회를 위한 여러 번의 쿼리가 실행됨.

3. [ℹ️] 로그인 시도 기록: 여러 번의 로그인 시도가 데이터베이스에 기록됨.

- 발생 빈도:

- [🔴] ERROR: 0

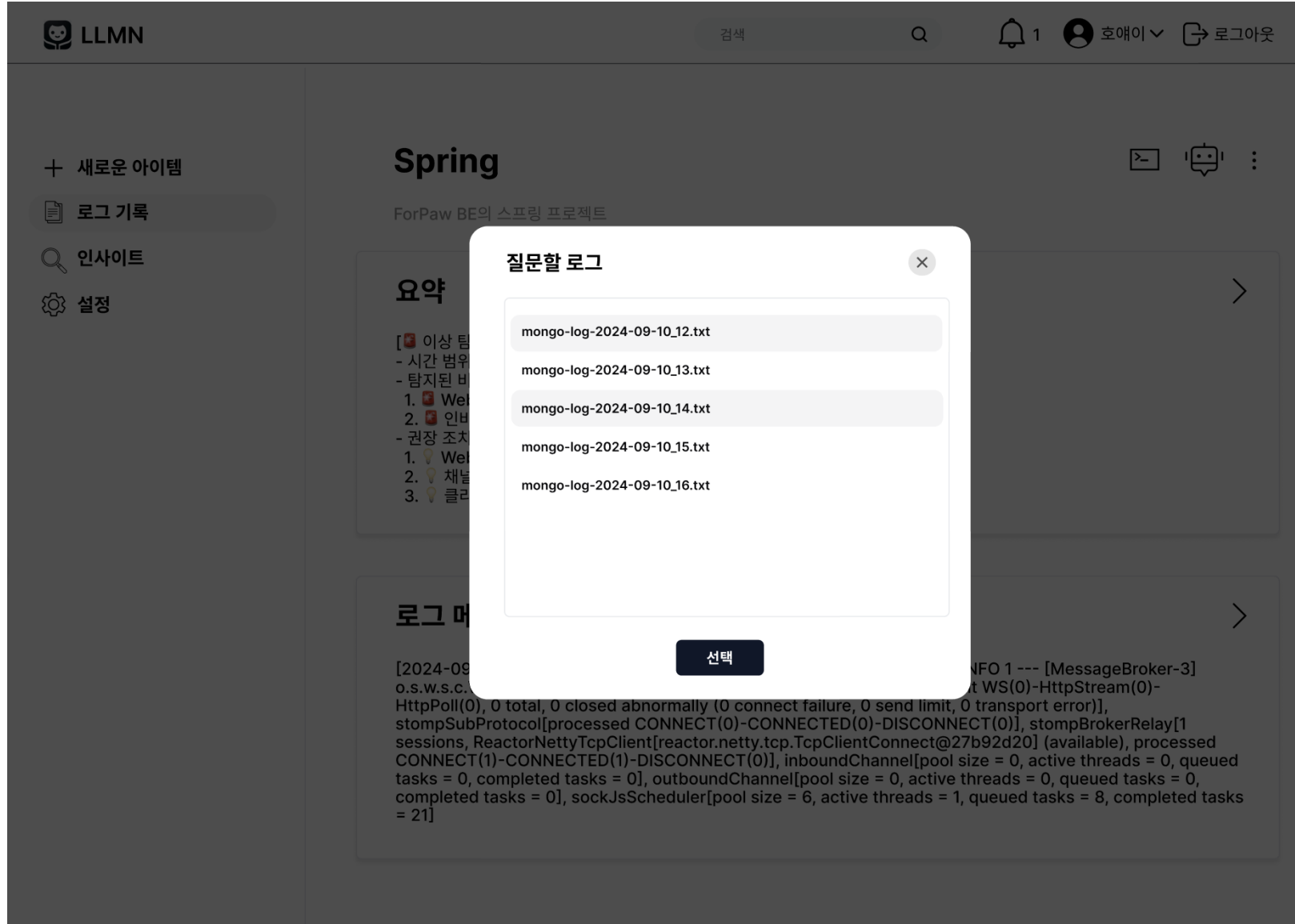
- [⚠️] WARN: 0

- [ℹ️] INFO: 8

2024-09-12 19:30

➤ 프로젝트의 요약 리포트를 조회하는 화면 (LLM에 의해 분석된 리포트)

❖ 질문할 로그 선택



➤ 특정 로그에 대해 궁금한 게 있을 때, 질문할 로그 파일을 선택하는 화면

❖ 챗봇에 질문하기

LLMN

검색

1

호애이

로그아웃

새로운 아이템

로그 기록

인사이드

설정

Spring

질문하기

호애이

2024-10-04 15:45에 Spring 애플리케이션에서 발생한 성능 저하 및 간헐적인 HTTP 503 오류의 원인이 무엇인지 자세히 설명해줘

"2024-10-04 15:45에 발생한 성능 저하 및 간헐적인 HTTP 503 오류는 여러 요소가 복합적으로 작용하여 발생한 문제로 확인되었습니다. 로그를 종합 분석한 결과, 다음과 같은 주요 이슈가 파악되었습니다:

1. 데이터베이스 응답 지연:

- 2024-10-04 15:30: OrderService에서 데이터베이스 요청이 평소보다 오래 걸리는 것이 확인되었습니다. 평균 응답 시간은 500ms에서 3초로 증가했습니다.
- 로그 메시지에서 org.hibernate.QueryTimeoutException: Query timed out after 3000ms 예외가 반복적으로 발생하고 있었습니다. 이는 대용량 쿼리로 인해 데이터베이스가 과부하 상태에 빠진 것으로 보입니다.

2. 스레드 풀 고갈:

- 2024-10-04 15:40: 애플리케이션 스레드 풀에서 ThreadPoolExecutor의 corePoolSize를 초과하여 모든 스레드가 바쁘게 동작하고 있었으며, 대기 큐에 새로운 요청이 쌓이기 시작했습니다.
- 이로 인해 org.springframework.web.context.request.async.AsyncRequestTimeoutException: Request processing failed 오류가 발생하였고, HTTP 503(Service Unavailable) 오류를 반환했습니다.

3. 외부 API 응답 지연:


- 2024-10-04 15:42: 애플리케이션에서 외부 결제 시스템과 통신하는 /api/payment 엔드포인트에서 응답 시간이 5초를 초과하면서, 해당 요청을 처리하는 PaymentService가 더 이상 요청을 처리하지 못하게 되었습니다. 이로 인해 연쇄적인 성능 저하가 발생했습니다.

입력하기

[2024-10-04T11:51:54.743Z] UNKNOWN: Hibernate: select p1_0.id,p1_0.answer_num,p1_0.comment_num,p1_0.content,p1_0.created_date,p1_0.group_id,p1_0.hot...

➤ 선택한 로그 파일에 대해 질문하고, 챗봇의 답변을 받는 화면

❖ 원격 SSH 명령

 LLMN

검색

1

호애이

로그아웃

+ 새로운 아이템

로그 기록

인사이드

설정

셸 커맨드

```
sudo systemctl status nginx
```

● nginx.service - A high performance web server and a reverse proxy server
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2024-10-04 14:21:16 UTC; 1h 5min ago
Docs: man:nginx(8)
Main PID: 1834 (nginx)
Tasks: 5 (limit: 1152)
Memory: 8.2M
CGroup: /system.slice/nginx.service
├─1834 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
├─1835 nginx: worker process
├─1836 nginx: worker process
├─1837 nginx: worker process
└─1838 nginx: worker process

Oct 04 14:21:16 myserver.com systemd[1]: Started A high performance web server and a reverse proxy server.

입력하기

Broker-3]
n(0)-

rRelay[1
, processed
ds = 0, queued
tasks = 0,
completed

Broker-4]
n(0)-

rRelay[1
, processed
ds = 0, queued
tasks = 0,
completed

p1_0.hot_point
p1_0.is_blocked,p1_0.post_id,p1_0.post_type,p1_0.read_cnt,p1_0.removed_at,p1_0.title,p1_0.updated_date,
p1_0.user_id from post_tb p1_0 where p1_0.created_date between ? and ? and p1_0.post_type=? and
p1_0.removed_at is null

[2024-10-04T11:51:54.743Z] UNKNOWN: Hibernate: select
p1_0.id,p1_0.answer_num,p1_0.comment_num,p1_0.content,p1_0.created_date,p1_0.group_id,p1_0.hot...

➤ 문제를 해결하기 위해 해당 클라우드에 원격으로 접속해, 명령어를 입력하는 셸 커맨드 화면

LLMN

검색

1

호애이

로그아웃

+ 새로운 아이템

로그 기록

인사이트

설정

인사이트

성능 요약

2024.09.10_18 업데이트됨

성능 개요

CPU

평균 사용량: 17.10%

최대 사용량: 18.40% (발생 시간: 14:56)

메모리

평균 사용량: 25,696 MB

최대 사용량: 25,886 MB (발생 시간: 14:56)

네트워크 수신

평균 수신량: 20.50 KB

최대 수신량: 39.00 KB (발생 시간: 14:56)

네트워크 송신

평균 송신량: 3.50 KB

최대 송신량: 7.00 KB (발생 시간: 14:56)

탐지된 비정상 패턴

1. 네트워크 수신량 급감: 14:56에서 15:00 사이에 수신량이 39.00 MB에서 2.00 MB로 급격히 감소함.

2. 네트워크 송신량 중단: 15:00에 송신량이 0.00 MB로 감소하여 비정상적인 상태를 나타냄.

권장 조치

1. 네트워크 연결 상태 점검 및 장애 여부 확인.

2. 서버 방화벽 또는 보안 설정 검토.

3. 네트워크 트래픽 모니터링을 강화하여 추가적인 이상 징후 탐지.

일일 요약

2024.09.10_18 업데이트됨

[Spring]

[Critical] 2024-09-10 11:30: /api/orders 엔드포인트에서 HTTP 500 에러 발생. 응답 시간 5초 이상 지연.

[Warning] 2024-09-10 15:00: /api/users 요청 200회 중 10회 실패 (서버 연결 끊김).

[MongoDB]

➤ 성능 요약, 일일 요약, 장기 트렌드 분석, 추천 등 여러가지 분석 리포트를 조회하는 화면

❖ 로그 혹은 리포트 검색

LLMN

+

 새로운 아이템

📄

 로그 기록

🔍

 인사이트

⚙️

 설정

검색

🔍

🔔 1

👤 호애이 ▾

🚪 로그아웃

기간

시작일

~

종료일

키워드

mongo

검색

검색 결과

mongo

로그 파일

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

📄 LOG

mongo-log-2024-09-10_12.txt

●

○

○

인사이트 기록

Mongo

-

2024-09-12 19:00

-

일반요약

➤ 로그 파일이나 리포트를 빠르게 찾고 싶을 때, 이를 검색하는 화면

알람 조회

LLMN

검색

1

호애이

로그아웃

새로운 아이템

로그 기록

인사이트

설정

대시보드

CPU 사용량 52% 메모리 사용량 72%

요약

[▲ Warning] 2024-09-10 13:45: CPU 사용량이 85% 이상 증가했습니다.

[! Critical] 2024-09-10 13:30: 네트워크 수신량이 비정상적으로 높습니다.

[▲ Warning] 2024-09-10 13:15: 평소보다 네트워크 트래픽이 감지되었습니다.

[! Critical] 2024-09-10 13:30: 매일 오전 10시에 메모리 사용량이 급증합니다. 해당 시간대에 불필요한 작업을 줄이거나 리소스 할당을 조정하는 것을 권장합니다.

CPU

Memory

알림

업데이트

새로운 요약이 업데이트 되었습니다.

2024-09-20 16:45

업데이트

새로운 요약이 업데이트 되었습니다.

2024-09-20 16:45

업데이트

새로운 요약이 업데이트 되었습니다.

2024-09-20 16:45

업데이트

새로운 요약이 업데이트 되었습니다.


2024-09-20 16:45


업데이트




새로운 요약이 업데이트 되었습니다.

2024-09-20 16:45


➤ 알람이 생성됐을 때, 이를 조회하는 화면


 LLMN


검색 

 1  호애이  로그아웃


+ 새로운 아이템


 로그 기록

 인사이트

 **설정**


설정






알람 설정 

닉네임

호애이

클라우드 인스턴스 

| | | | |
|--|---------------|--------|---|
|  ubuntu | 54.180.244.93 | 정상 |  |
| Amazon Linux | 72.180.244.93 | 재연결 필요 |  |

수정

➤ 알람 수신을 변경하거나, 모니터링 할 인스턴스를 추가 혹은 수정하는 화면

❖ 결론

- **LLM**을 적용한 로그 분석 시스템은 로그를 요약하고 이상 패턴을 탐지하는 기능을 제공하여, 로그 분석의 효율성을 크게 개선.
- 관리자가 실시간 성능 지표를 모니터링하고, SSH를 통해 **원격 서버**를 제어할 수 있게 하여, 문제 발생 시 신속하게 대응할 수 있는 환경을 마련.
- 단순한 로그 모니터링을 넘어, **중요한** 정보를 **직관적**이고 **신속**하게 제공하여 관리자의 실시간 대응 능력을 향상.

Thank you

