

인프라와 서비스 운영을 위한 모니터링

서버부터 사용자 화면까지. 운영의 흐름이 보입니다.

서버 상태, 데이터 흐름, 실제 로그인·조회 결과를 함께 확인합니다.
점검 결과를 실행 근거와 연결하고, 필요한 알림으로 전달합니다.



서버·컨테이너

자원과 실행 상태



데이터·작업

복제와 최신성



사용자 화면

로그인과 조회

수집 → 검증 → 공유

운영 판단에 필요한 것은 연결된 근거입니다

흩어진 신호를 하나의 점검 흐름으로

서버가 응답해도 업무 화면은 실패할 수 있습니다. 각 층의 상태를 같은 흐름에서 확인합니다.

01

수집

지금, 무엇이 실행 중인가

SSH·DB·HTTP 점검으로 서버 자원,
컨테이너, 데이터와 작업 결과를 모읍니다.

서버 / 데이터 / 예약 작업

02

검증

사용자가 실제로 이용하는가

Playwright로 로그인·조회와 API 응답을
확인하고, 단계별 결과와 증거를 남깁니다.

시나리오 / IP 프로필 / 증거

03

공유

누가 어떤 근거를 볼 것인가

장애·복구 기록을 대시보드에서 확인하고,
설정된 범위에 따라 Slack으로 전달합니다.

상태 / 사건 이력 / Slack

정상·주의·장애·알 수 없음·유지보수를 구분하고, 결과가 오래되면 알 수 없음으로 표시합니다.

인프라 상태와 업무 데이터의 연결

운영에서 확인해야 할 여섯 가지 영역

대상별 점검 주기와 임계치를 설정하고, 실제 시험을 거친 항목을 정기 실행합니다.

영역	확인 항목	운영에서 읽는 의미
서버 자원	CPU·메모리·디스크·inode	SSH를 통한 자원 상태와 파일시스템 사용량
Docker	컨테이너 상태·재시작 증가	필요한 컨테이너의 실행 상태와 재시작 변화
파일·백업	파일 날짜·크기·개수·쓰기 안정화	파일명 패턴과 예정 시각을 반영한 생성 여부
크론	시작·종료 코드·소요 시간	heartbeat 보고를 연동한 예약 작업의 결과
데이터베이스	복제 상태·지연·테이블 최신성	MySQL/MariaDB·PostgreSQL의 복제와 시각·커서 변화
HTTP·TLS	상태 코드·본문·응답 시간·인증서	HTTP 기대 응답과 TLS 인증서 만료 시점

사용자 화면 점검은 다음 페이지의 Playwright 시나리오로 연결합니다.

Playwright 시나리오

로그인 이후의 업무 흐름까지 확인

화면 요소·문구·URL과 API 응답을 단계별로 검증합니다. 실패한 지점을 실행 근거와 함께 확인합니다.

01

페이지 접속

시작 URL과 연결 대상 확인

02

로그인

점검용 계정으로 입력·클릭

03

업무 조회

필수 요소·문구·URL 확인

04

응답 검증

API 상태 코드·success 값 확인

...

검증 흐름 · 예시

조회 화면 확인

필수 문구 표시

통과

GET /api/items

200 · success: true

화면·응답·연결 근거를 실행 단위로 기록

실행 요약 / 스크린샷 / 실패 Trace

일반 시나리오는 단계 편집기로 작성합니다. 직접 작성한 코드는 관리자 검토 후 별도 Sandbox에서 실행합니다.

로그인용 POST 외 데이터 변경 요청은 기본 차단합니다. 화면·Trace 원본은 관리자만 접근합니다.

같은 서비스, 서로 다른 노드

도메인은 유지하고 연결 IP를 고정

노드별 IP 실행 프로필로 Web과 API를 함께 매핑합니다. 한 노드의 점검을 다른 노드의 응답으로 대신하지 않습니다.



고정 IP 연결 실패 시 DNS로 우회하지 않습니다. CDN·SSO 등 외부 의존 호스트는 검토한 DNS 예외로 등록하고, 실제 연결 IP를 근거에 남깁니다.

알림을 조절해도 점검과 기록은 계속됩니다

전송 범위와 실행 근거를 함께 관리

Slack 전역·서버별·개별 점검 설정을 분리해 운영 상황에 맞는 전달 범위를 정합니다.

Slack 전송 제어

전체

전체 알림의 전송 여부

서버

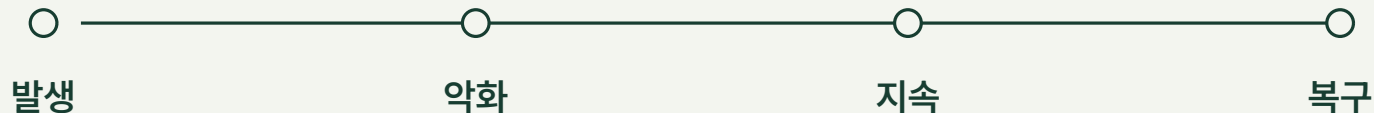
해당 서버와 고정 IP 노드

개별 점검

선택한 점검의 전송 여부

세 범위 중 하나라도 꺼져 있으면 전송하지 않습니다. 다시 켜도 이전 메시지를 몰아서 보내지 않습니다.

사건의 변화



상태와 시각을 확인하고 → 해당 실행을 열고 → 요약·화면·Trace로 근거를 검토합니다.

전송 실패는 재시도합니다. 실행 증거는 권한에 따라 미리보기·원본 다운로드로 확인합니다.

AI Chat · MCP

질문과 도구 실행에도 운영 권한을 적용

한국어 AI Chat과 MCP에서 상태·상세·지표를 조회하고, 허용된 범위에서 점검 작성과 시험을 이어갑니다.

사용자 역할	허용 범위
VIEWER	조회
OPERATOR	조회 · 점검 작성 · 시험
ADMIN	설정 · 자격 증명 · 승인

토큰 범위와 역할의 교집합

MCP 토큰은 사용자 권한과 발급 범위 안에서 동작하며, 만료·폐기를 적용합니다.

승인·자격 증명 권한은 토큰에 발급하지 않습니다.
AI는 운영 변경의 승인을 요청할 수 있습니다.

운영 변경의 승인 흐름

변경 요청 —> 관리자 검토 —> 일회 승인 —> 실행·감사 기록

SSH 변경은 정확한 대상·명령·만료 시각에 묶입니다. AI와 MCP는 직접 승인할 수 없습니다.

AI 공급자·모델은 별도 설정합니다. 도입 시 전송되는 운영 정보와 보안 정책을 함께 검토합니다.

작은 점검 범위에서 시작하는 도입

대상 선정부터 실제 시험, 정기 운영까지

기존 환경의 접근 권한과 점검 기준을 정리하고, 정상·실패 사례를 직접 확인한 뒤 운영에 적용합니다.

01

준비

대상·담당자·접근 권한

SSH·DB·점검용 계정과
관련 Web-API 도메인 정리

02

구성

Docker Compose 배치

Web·Worker·Runner·Sandbox와
PostgreSQL·Redis 연결

03

시험

초안 작성·실제 실행

임계치·시나리오·IP 프로필과
실패 근거·알림 범위 확인

04

운영

활성화·정기 검토

점검 주기·담당자·증거 확인
설정 변경 후 다시 시험

도입 전에 함께 정할 조건

크론의 성공·종료 모니터링에는 heartbeat 보고 연동이 필요합니다.

백업 파일의 존재·크기 점검과 복원 성공 검증은 별도로 설계합니다.

모니터링 저장소의 PostgreSQL·Redis HA와 백업은 별도로 구성합니다.

다음 단계

핵심 업무 한 가지를 정하고, 수집 → 검증 → 공유를 연결해 보세요.