

● 개인 프로젝트

구축부터 장애 대응까지, Linux 서버 운영 실습

VMware 가상 서버 3대 · Prometheus 모니터링 · Ansible 자동화 · 무작위 장애 10종

조현수

2026.10.7 ~ 10.15

VMware

RHEL 10

nginx

Prometheus

Ansible

프로젝트 개요

VMware 서버 3대로 구축부터 장애 대응까지 진행한 실습

목표

사내 서버 운영을 가정하고, 문제 원인을 찾아 해결하는 실무 흐름 학습

진행 방식

- 단계마다 목적, 명령, 확인 순서로 진행
- 서버 작업은 script 명령으로 기록하고, 화면은 필요한 곳만 캡처
- 막힌 문제는 증상, 원인, 조치 순서로 기록
- 실습 가이드 작성과 오류 해석에 AI(Claude)를 활용
명령 실행과 결과 확인은 직접 진행

서버	IP	역할
web	192.168.100.10	nginx 웹 서버 (HTTPS)
infra	192.168.100.20	내부 DNS, NFS 백업 저장소
mon	192.168.100.30	모니터링, Ansible 관리

사용 기술

RHEL 10

nginx

bind

NFS

LVM

SELinux

firewalld

node_exporter

Prometheus

Alertmanager

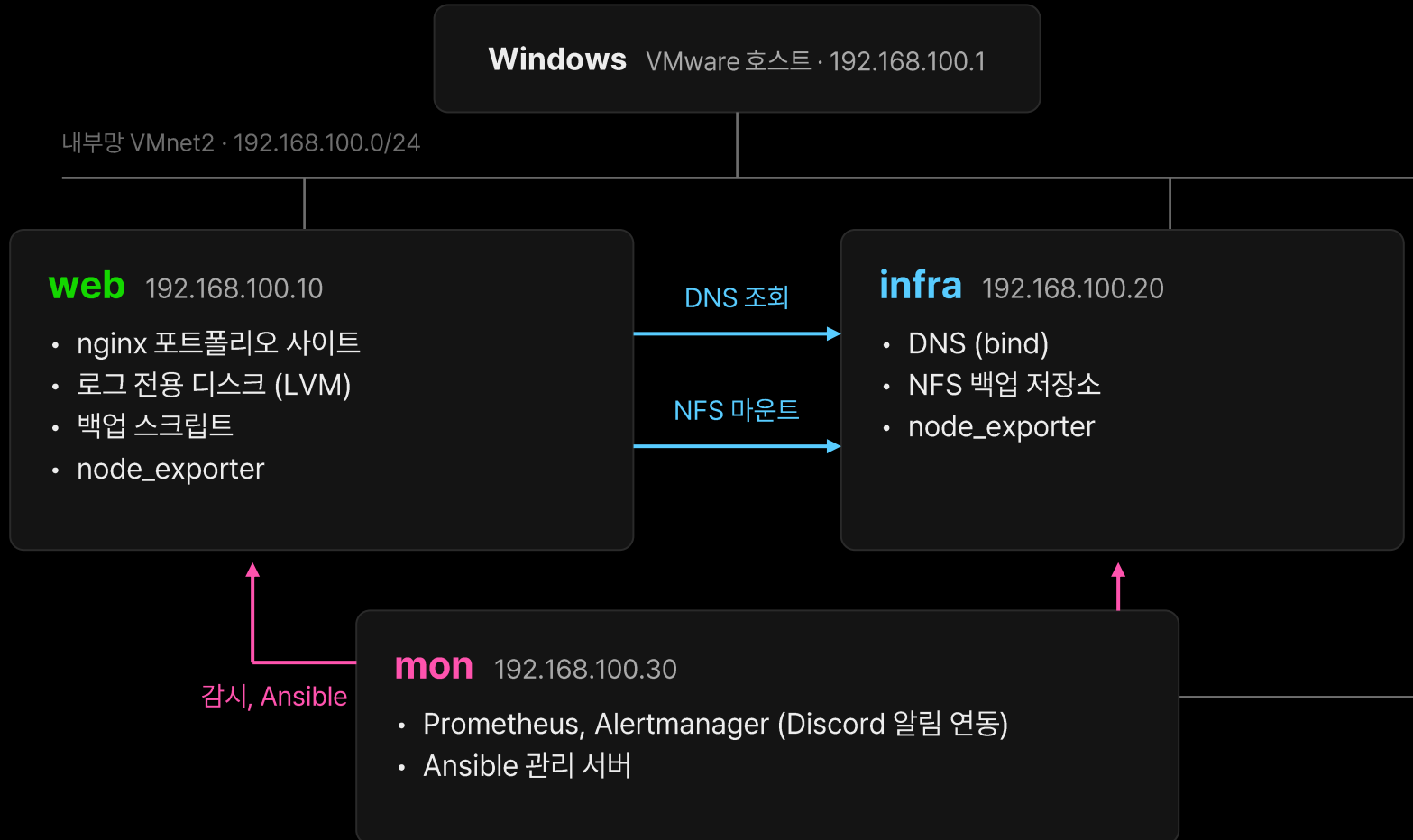
Ansible

git

Discord

서버 구성도

web은 infra의 DNS와 NFS를 사용하고, mon이 두 서버를 감시



접근 제한

SSH

SSH 키 접속만 허용, root 접속 차단

9100 (node_exporter)

mon에서만 접속 허용

9090, 9093 (모니터링 화면)

Windows에서만 접속 허용

ansible 계정

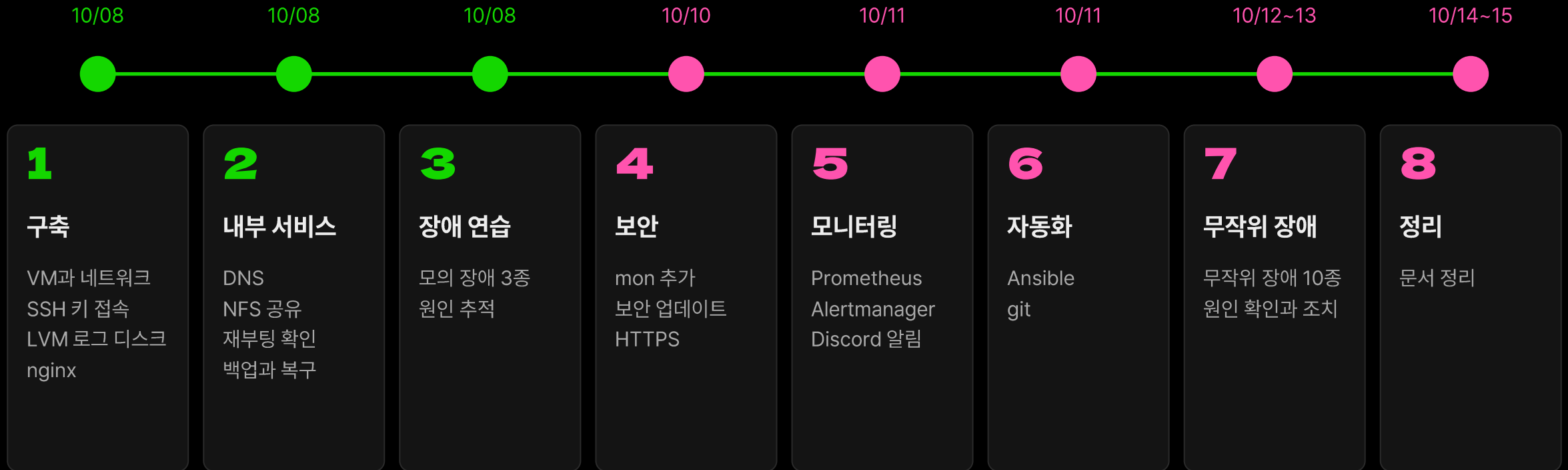
mon에서 오는 접속만 허용

NFS

web에만 공유

진행 단계

web·infra 2대로 시작, 4단계에서 mon 추가



구축과 운영

서버 구축, 내부 DNS와 NFS, 백업, 보안 업데이트 진행

서버 구축

- 인터넷용(NAT)과 서버 간 통신용(내부망) 네트워크 카드를 분리
- 로그 전용 디스크(LVM)로 로그가 가득 차도 OS 디스크 영향 방지
- SELinux는 끄지 않고 라벨 지정 → 403 오류 방지

내부 DNS와 NFS 공유

- web은 infra만 DNS로 사용하도록 변경
- web의 root가 만든 파일은 infra에서 nobody 소유로 저장되는 것 확인 (root_squash)
- 종료는 web → infra
시작은 infra → web
(infra를 먼저 끄면 web 종료 지연)

```
[15:23:16 hyunsu@web ~]$ curl -I http://localhost
HTTP/1.1 200 OK
Server: nginx/1.26.3
Date: Thu, 08 Oct 2026 06:23:19 GMT
Content-Type: text/html
Content-Length: 53808
Last-Modified: Thu, 08 Oct 2026 06:16:19 GMT
Connection: keep-alive
ETag: "6ac73533-d230"
Accept-Ranges: bytes
```

```
[15:23:19 hyunsu@web ~]$ getenforce
Enforcing
[15:23:24 hyunsu@web ~]$
```

웹 응답 200, SELinux Enforcing

백업과 복구 테스트

- 백업 위치를 infra(NFS)로 두어 web이 고장 나도 백업 보존
- 백업(tar)이 실패하면 스크립트가 바로 멈추도록 set -e 사용.
새 백업이 없는데 오래된 백업까지 지우는 일 방지
- index.html 삭제(복구 시험) → 403, 백업에서 복구 → 200

보안 업데이트와 HTTPS

- 보안 공지 129건 적용, 재부팅은 mon → web → infra 순서
- 자체 서명 인증서로 HTTPS 적용, http로 접속하면 https로 이동(301)

장애 대응 연습

모의 장애로 증상에서 원인까지 추적하는 순서 연습

장애	증상	원인을 찾은 과정	조치
DNS 중단	web에서 NFS 마운트 실패 (infra.lab 이름을 찾지 못함)	ping은 됨 → DNS 조회는 거부됨 → infra의 named 서비스 중지	infra에서 named 시작
NFS 방화벽 차단	web에서 마운트가 멈춤	이름 조회와 ping은 정상 → NFS 포트(2049)만 연결 안 됨	infra 방화벽 복구
SELinux 라벨 오류	브라우저에서 403	파일 권한은 정상 → SELinux 라벨이 바뀌어 있음 → 감사 로그에서 거부 기록 확인	restorecon으로 라벨 복원

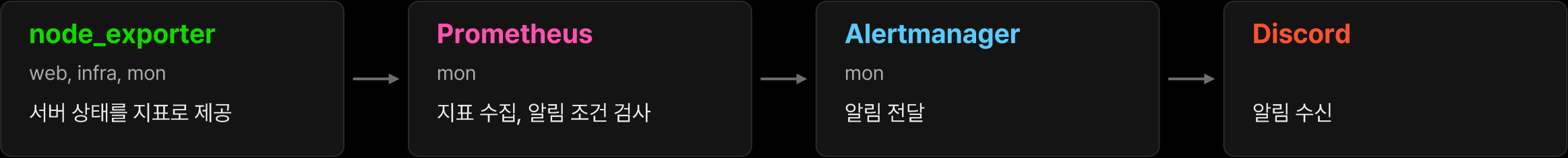
```
[18:20:19 hyunsu@web ~]$ ls -l /srv/portfolio/index.html
-rw-r--r--. 1 root root 53808 Oct  8 15:16 /srv/portfolio/index.html
[18:21:27 hyunsu@web ~]$ sudo tail -n 3 /var/log/nginx/error.log
2026/10/08 18:20:17 [error] 1329#1329: *2 open() "/srv/portfolio/assets/rhel-lab.png" failed (13: Permission denied), client: 192.168.100.1, server: _, request: "GET /assets/rhel-lab.png HTTP/1.1", host: "192.168.100.10", referer: "http://192.168.100.10/"
2026/10/08 18:20:17 [error] 1330#1330: *1 open() "/srv/portfolio/assets/rhel-lab.png" failed (13: Permission denied), client: 192.168.100.1, server: _, request: "GET /assets/rhel-lab.png HTTP/1.1", host: "192.168.100.10", referer: "http://192.168.100.10/"
2026/10/08 18:20:22 [error] 1330#1330: *1 open() "/srv/portfolio/index.html" failed (13: Permission denied), client: 192.168.100.1, server: _, request: "GET / HTTP/1.1", host: "192.168.100.10"
[18:21:51 hyunsu@web ~]$ ls -Z /srv/portfolio/index.html
unconfined_u:object_r:user_home_t:s0 /srv/portfolio/index.html
[18:22:04 hyunsu@web ~]$ sudo ausearch -m AVC -ts recent
----
time->Thu Oct  8 18:20:22 2026
type=PROCTITLE msg=audit(1791451222.171:191): proctitle=6E67696E783A20776F726865722070726F63657373
type=SYSCALL msg=audit(1791451222.171:191): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=55c1e83fe593 a2=800 a3=0 items=0 ppid=1326 pid=1330
  auid=4294967295 uid=992 gid=992 suid=992 fsuid=992 egid=992 sgid=992 fsgid=992 tty=(none) ses=4294967295 comm="nginx" exe="/usr/sbin/nginx" subj=system_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1791451222.171:191): avc: denied { read } for pid=1330 comm="nginx" name="index.html" dev="dm-0" ino=17312658 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_t:s0 tclass=file permissive=0
```

SELinux 원인 확인 화면

- 파일 권한은 -rw-r--r--로 정상
- 라벨이 user_home_t로 되어 있어 nginx가 읽지 못함
- ausearch로 거부 기록(AVC denied) 확인

모니터링과 알림

서버나 서비스에 문제가 생기면 Discord로 알림이 오도록 구성



알림 규칙	조건
InstanceDown	서버 또는 node_exporter 응답 없음
DiskUsageHigh	디스크 사용률 80% 초과
ServiceDown	nginx, named 등 필요한 서비스 중지
NFSMountProblem	web의 NFS 마운트 이상
BackupStale	3시간 넘게 백업 성공 기록 없음
BackupMetricMissing	백업 기록 없음
CertExpiringSoon	인증서 만료 30일 이내

알림 시험

서비스 중지, 백업 실패, 백업 오래됨, 알림 전달 4건 모두 알림 발생 확인

시험 중 발견한 문제

원래 꺼져 있는 서비스에도 알림 발생

web은 NFS 서버(nfs-server)를 쓰지 않는데 ServiceDown 알림 발생.
규칙이 모든 서버에서 같은 서비스를 감시한 것이 원인

서버마다 감시할 서비스를 나눠 규칙 재작성

수정한 규칙 검사 성공 (7개 규칙)

Ansible과 git으로 설정 관리

수동으로 구성한 web의 설정을 플레이북(web.yml)으로 자동화하고, 바뀐 설정의 복구 확인

Ansible 전용 계정

- SSH 키로만 접속
- mon에서 오는 접속만 허용
- Windows 접속 거부 확인

git 변경 이력

- 변경 순서: 수정 → git diff → 미리보기
→ 적용 → 커밋
- 사이트에 섞인 내부 파일 2개 발견
(README.txt 등)
- 배포 원본에서 빼도 서버 파일은 남음
→ 플레이북에 "없어야 함"(state: absent) 추가
- 조치 전 200 → 조치 후 404

바뀐 설정 되돌리기

- **플레이북 실행** changed=0. 플레이북과 web의 실제 상태가 일치
- **web 설정 2곳 임의 변경** https 방화벽 제거
http → https 자동 이동 설정 해제
- **미리보기 (--check --diff)** 바뀐 2곳만 변경 예정으로 표시
- **플레이북 적용** 2곳만 원래대로 복구
- **한 번 더 실행** changed=0. 추가 변경 없음
- **접속 확인** https 200, http 301. 원래 상태와 동일

infra DNS의 외부 이름 조회 실패

외부 다운로드가 처음엔 실패하고 다시 하면 성공하는 문제가 반복되어 원인을 찾음

증상

web과 mon에서 Prometheus 설치 파일, Ansible 컬렉션, 보안 업데이트를 받을 때 이름을 찾지 못해 실패하나 재시도 시 성공

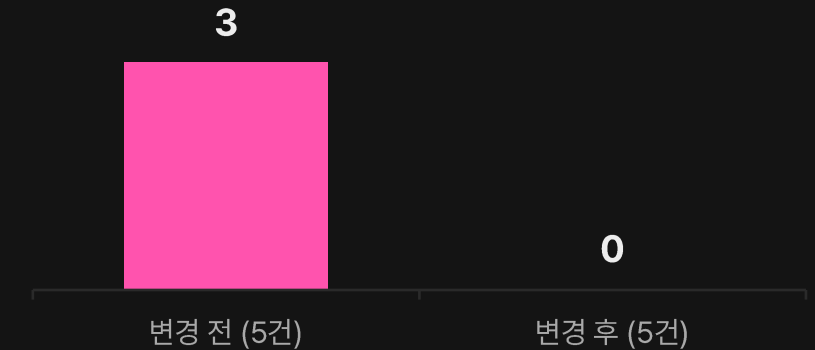
원인을 찾는 과정

- 1 infra의 DNS(bind) 로그**
실패한 시각에 web의 질의를 실패(SERVFAIL)로 응답한 기록 확인
- 2 같은 이름을 다른 DNS로 조회**
VMware 기본 DNS는 성공, infra의 bind만 실패 → 인터넷 연결 문제가 아님
- 3 bind 로그를 다시 확인**
외부 DNS 서버의 IPv6 주소로 질의하다 실패한 기록이 많음 (IPv6 경로가 없는 환경)

조치

bind를 IPv4만 쓰도록 설정 (실행 옵션 -4)

결과: 캐시를 비우고 처음 조회한 이름 5개 중 실패 수



Alertmanager 화면 접속 불가

Windows에서 Prometheus(9090)는 접속되나 Alertmanager(9093)만 접속 불가

원인을 찾는 과정

- 1 서비스 상태**
두 서비스 실행 중, 각 포트 대기(LISTEN) 확인
- 2 Windows에서 포트 확인**
9090은 연결됨, 9093은 연결 안 됨 → 방화벽 문제로 좁힘
- 3 방화벽 설정 확인**
9090, 9093 허용 규칙 모두 없음 → 9090이 열리는 이유 불명
- 4 실제 적용된 규칙 확인**
출처 불명의 9090 허용 규칙 발견
- 5 방화벽 서비스 목록 확인**
방화벽에 등록된 cockpit(서버 관리 도구) 서비스가 9090 개방

원인

- 9093: 허용 규칙 없음
(모니터링 구성 때 넣은 규칙의 영구 저장 누락으로 추정)
- 9090: cockpit 서비스가 열어 두어 문제가 가려짐

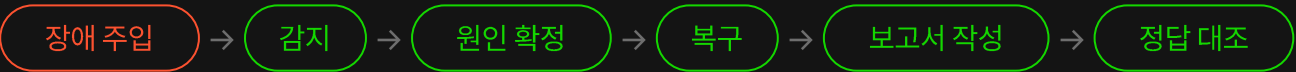
조치

- 9090, 9093을 Windows만 허용하는 규칙으로 영구 저장
- 필요 없는 cockpit 서비스를 방화벽에서 제거
- 확인: 두 포트 모두 Windows만 허용된 상태

무작위 장애 대응

장애 종류를 알 수 없는 상태에서 감지부터 정답 대조까지 9회 수행

진행 방식



9회차에 걸쳐 10종의 장애에 대응

회차	장애	원인 서버	감지 방법
1	nginx 중지	web	알림(ServiceDown)
2	index.html SELinux 라벨 user_home_t → 403	web	사이트 접속(알림 없음)
3	node_exporter 중지 → 알림 3개 연쇄	web	알림(InstanceDown 외)
4	DNS에 등록된 web 주소 변경 (.10 → .99)	infra	정상 확인표 대조(알림 없음)
5	인증서 이동 → nginx 시작 실패	web	알림(ServiceDown)
6	crond 중지	web	알림(ServiceDown)
7	named 중지	infra	알림(ServiceDown)
8	nfs-server 중지 + 방화벽 런타임 nfs 제거	infra	알림(ServiceDown, NFSMountProblem)
9	로그 디스크 100%(fill.tmp)	web	알림(DiskUsageHigh)

DNS가 잘못된 IP로 응답한 장애

알림 없이 감지 · 증상은 web·mon, 원인은 infra

원인을 찾는 과정

- 1 정상 확인표 대조**
web getent에서 web.lab이 192.168.100.99 (정상은 .10) → 이름 조회 이상
- 2 범위 나누기**
mon에서도 .99 → 공통으로 쓰는 DNS
- 3 출처 가르기**
hosts 파일을 보지 않는 dig도 .99 → DNS 서버가 틀린 답
- 4 DNS 서버 확인 (infra)**
존 파일 10번째 줄이 .99, named-checkzone은 OK → 문법이 아니라 값
- 5 언제·누가**
파일 수정 시각 → 같은 시각 저널에서 주체·명령 확인 → 변경 주체 확인

원인

존 파일의 web 주소가 .99로 바뀌고, DNS 서버(named)가 이를 다시 읽어 틀린 값으로 응답

조치 (infra)

- 1 존 파일 백업
- 2 10번째 줄 수정, serial 올림
- 3 named-checkzone으로 검사
- 4 rndc reload로 DNS에 반영
- 5 dig · getent · curl로 확인

원인 확정 전에는 아무것도 바꾸지 않음

알림이 놓친 장애 3가지와 개선 방향

서비스 상태를 보는 알림으로는 보이지 않았던 장애 정리

웹 응답 403

2회차

알림이 없던 이유

nginx는 켜져 있어 서비스 알림이 뜨지 않음

감지

사이트 접속 시 발견

DNS가 틀린 답

4회차

알림이 없던 이유

DNS 서버는 정상 동작, 답이 맞는지 확인하는 감시 없음

감지

정상 확인표 대조로 발견

방화벽 런타임 규칙 누락

8회차

알림이 없던 이유

6회차에 주입됐으나 이미 맺어진 NFS 연결은 유지되어 증상 없음

감지

8회차 NFS 서버 재시작 후 새 연결이 막히며 드러남

공통점

세 경우 모두 서비스는 정상이라 서비스 상태 알림으로는 감지 불가

개선 방향

- 이름으로 새 연결을 맺어 응답을 확인하는 감시 (blackbox_exporter 등)
- 런타임 방화벽 규칙과 영구 규칙을 비교하는 점검

검토

회고

배운 점

- 재시도로 성공한 오류도 원인 확인 필요.
DNS 문제는 세 번 넘긴 뒤에야 원인 파악
- 증상이 나온 서버만 보지 않고
그 서버가 의존하는 서버(DNS·NFS)까지 확인
- 서비스가 켜져 있는지뿐 아니라
결과값(응답 코드, DNS 답)이 맞는지도 확인해야 함

부족한 점

- infra 한 대가 DNS와 NFS를 모두 맡고 있어,
nfra가 멈추면 web도 영향을 받는 구조
- 자체 서명 인증서라 브라우저 경고가 남음
- IPv6 중복 주소 경고는 원인 미확인, IPv6를 꺼서 우회
- 7단계 1~3회차에서 원인 확정 전에 설정을 바꿈