

[문서 번호: SOP-INFRA-2025-001]

[시행 일자: 2025. 12. 10]

## [인프라] 서버/클라우드 장애 조치 매뉴얼 (SOP)

: 장애 현상별 초동 조치 및 복구 절차 (Standard Operating Procedure)

### 1. 개요 (General Info)

#### 1.1 목적

본 매뉴얼은 서버(On-Premise/Cloud) 운영 중 발생하는 주요 장애 상황(접속 불가, 속도 저하, 자원 부족 등)에 대해 시스템 엔지니어가 수행해야 할 표준 조치 절차를 정의합니다. 이를 통해 장애 복구 시간(MTTR)을 단축하고 서비스 연속성을 보장합니다.

#### 1.2 RAG 매핑 가이드 (AI 학습용)

- 사용자 질문 키워드:** "서버 다운", "접속 안 됨", "503 에러", "502 에러", "사이트 느림", "디스크 꽉 참", "데몬 죽음".
- AI 응답 전략:** 질문의 '현상'을 파악하여 아래 해당 섹션의 [진단] → [조치] 단계를 순서대로 안내하십시오.

### 2. 유형별 조치 절차 (Scenario & Action)

#### 시나리오 A. 서비스 접속 불가 (Service Down)

[현상] 웹 브라우저에서 사이트 접속 시 502 Bad Gateway, 503 Service Unavailable 에러 발생 또는 "사이트에 연결할 수 없음" 메시지 출력.

#### [진단 및 조치 순서]

##### 1. 프로세스(데몬) 생존 확인

- 명령어:** ps -ef | grep [프로세스명] 또는 systemctl status [서비스명]
- 판단:** 프로세스가 존재하지 않거나 상태가 inactive/dead인 경우.
- 조치:** 서비스 재기동 수행.
  - systemctl restart [서비스명] (예: systemctl restart nginx)
  - 재기동 실패 시 로그 확인 (/var/log/messages 또는 애플리케이션

로그).

## 2. L4 스위치(로드밸런서) 상태 확인

- **체크:** L4 스위치 관리 콘솔에서 해당 리얼 서버(Real Server)의 상태가 Active인지 확인.
- **판단:** Health Check 실패로 인해 Inactive 상태로 제외된 경우.
- **조치:** 서버 상의 Health Check 페이지(예: /health.jsp)가 정상 호출되는지 curl 명령어로 로컬 테스트.
  - curl -v http://localhost/health

## 3. 포트 리스닝(Listen) 확인

- **명령어:** netstat -anp | grep LISTEN | grep [포트번호]
- **조치:** 프로세스는 떠 있으나 포트가 열리지 않은 경우, WAS 설정 파일 (server.xml 등) 오류 점검.

---

## 시나리오 B. 시스템 속도 저하 (High Latency)

[현상] 접속은 되으나 페이지 로딩이 5초 이상 걸리거나, 간헐적으로 504 Gateway Timeout 발생.

### [진단 및 조치 순서]

#### 1. 시스템 리소스 사용량 점검 (CPU/Memory)

- **명령어:** top 또는 htop
- **판단:**
  - **CPU:** us(User)가 90% 이상 지속 시 → 특정 프로세스 로직 루프 의심.
  - **Memory:** Swap 사용량이 급증 시 → 메모리 누수(Leak) 의심.
  - **Load Average:** CPU 코어 수 대비 Load가 2배 이상 높을 때.
- **조치:** 자원을 과점유하는 프로세스 PID 확인 후, 불필요한 경우 kill -9 [PID]로 강제 종료 또는 개발팀에 스택 트레이스 분석 요청.

#### 2. DB 연결 상태 확인 (Connection Pool)

- **명령어:** netstat -an | grep [DB포트] | wc -l
- **판단:** ESTABLISHED 또는 TIME\_WAIT 상태의 연결이 임계치(예: 2,000개)를 초과하여 더 이상 연결할 수 없는 상태.
- **조치:** WAS 재기동으로 커넥션 풀 초기화 후, DB 락(Lock) 발생 여부 DBA에게 확인 요청.

### 3. I/O Wait 확인

- **명령어:** iostat -x 1
  - **판단:** %util이 90% 이상이거나 await 수치가 비정상적으로 높음.
  - **조치:** 디스크 I/O를 유발하는 배치 작업(백업, 로그 압축 등) 일시 중지.
- 

## 시나리오 C. 디스크 용량 부족 (Disk Full)

[현상] 애플리케이션 로그에 No space left on device 에러 발생, 파일 업로드 실패, 서비스 기동 불가.

### [진단 및 조치 순서]

#### 1. 파티션 사용량 확인

- **명령어:** df -h
- **판단:** Use%가 95%~100%인 파운트 지점 확인 (보통 / 또는 /var, /home).

#### 2. 대용량 파일 식별

- **명령어:** du -sh \* | sort -hr | head -n 10 (루트 디렉토리부터 하위로 탐색)
- **타겟:** 주로 텍스트 로그 파일(\*.log), 덤프 파일(\*.hprof, core), 임시 파일.

#### 3. 공간 확보 (삭제 및 압축)

- **조치 1 (로그 정리):** 30일 지난 로그 삭제.
  - find /var/log/app -name "\*.log" -mtime +30 -delete
- **조치 2 (압축):** 당장 삭제가 어려운 경우 압축.
  - gzip large\_access.log
- **조치 3 (Nullify):** 서비스 중단 없이 로그 파일 비우기 (파일 삭제 시 프로

세스가 잡고 있을 수 있음).

- cat /dev/null > /var/log/nginx/access.log
- 

## 시나리오 D. 서비스 데몬 중지 (Daemon Crash)

[현상] 프로세스 모니터링 알림 수신 ("Process Down"), ps 명령어로 조회되지 않음.

### [진단 및 조치 순서]

#### 1. 재기동 시도

- 조치: systemctl start [서비스명] 또는 시작 스크립트(.start.sh) 실행.

#### 2. 원인 분석 (재발 방지)

- 로그 확인: /var/log/syslog 또는 dmesg 명령어 실행.
- OOM Killer 확인: 메모리 부족으로 OS가 강제로 죽였는지 확인.
  - grep -i "Out of memory" /var/log/messages
- 조치: OOM(Out Of Memory) 발생 시, 서버 메모리 증설(Scale-up) 또는 JVM Heap Size 조정 검토.

### 3. 비상 연락망 (Escalation Path)

자체 조치로 해결되지 않거나 원인 파악이 불가능한 경우, 즉시 아래 담당자에게 에스컬레이션 하십시오.

역할	담당 부서	연락처	에스컬레이션 기준
인프라 담당	시스템운영 팀	010-XXXX-XXXX	OS 부팅 불가, 하드웨어 장애, L4/L3 장애
DB 담당	데이터관리 팀	010-XXXX-XXXX	DB 접속 불가, 쿼리 타임아웃 지속
개발 담당	서비스개발	010-XXXX-	소스 코드 오류(500 에러), 배포 후

역할	담당 부서	연락처	에스컬레이션 기준
	팀	XXXX	장애
보안 담당	정보보호팀	010-XXXX-XXXX	DDoS 공격 의심, 웹 해킹 시도 감지