

출입 통제 시스템: 실행 플랫폼 상세 가이드 (Docker Swarm)

본 문서는 [sdac-final-architecture.md](#) 의 모든 애플리케이션 및 지원 서비스가 실행되는 **인프라 계층(실행 플랫폼)**을 상세히 정의합니다. 이 플랫폼은 **Docker Swarm**을 기반으로 고가 용성(HA)과 자동화된 운영을 보장합니다.

1. 플랫폼 개요

본 시스템의 실행 플랫폼은 K8s(쿠버네티스)의 복잡성을 피하고 폐쇄망 환경에 최적화된 **Docker Swarm**을 선택합니다. Docker Swarm은 [API Gateway](#), [Access Control Service](#) 등 모든 서비스 컨테이너를 관리하는 "클러스터 운영체제" 역할을 수행합니다.

2. 고가용성(HA) 클러스터 구성

플랫폼의 안정성은 **최소 3대의 노드**로 구성된 HA 클러스터에서 나옵니다.

구성 요소	수량	역할	HA 보장 원리 (필수 조건)
Swarm Node	최소 3대 (Node 1 , 2, 3)	모든 노드가 Docker Swarm 매니저 역할을 겸합니다.	과반수(Quorum) 유지: 1개 노드 (Node 1)가 다운되어도, 남은 2개 노드(Node 2, 3)가 2/3로 과반수를 만족하여 클러스터 마비 없이 즉시 리더를 재선출하고 운영을 지속합니다. (2-노드 구성 시 1대 다운되면 과반수 봉고로 전체 중단됨)
자원 관리	Active/Active 모델	3대의 노드 모두 평상시(예: 60%) 작업을 분담합니다.	예비 공간(Headroom) 확보: Node 1 장애 시, Node 1 이 하던 일을 Node 2, 3 의 남은 40% 예비 공간에서 즉시 이어받아 처리합니다. (자원 낭비 없음)

3. 플랫폼의 4대 핵심 기능 (자동화)

Docker Swarm은 [systemd](#), [Eureka](#) 등 복잡한 솔루션 없이 4가지 핵심 기능을 플랫폼 레벨에서 자동으로 제공합니다.

A. 자동 장애 복구 (Automatic Failover & Self-Healing)

관리자 개입 없이 시스템 연속성을 보장하는 가장 중요한 기능입니다.

- 컨테이너 다운 (자가 치유):** `User Service` 컨테이너(프로세스)가 버그로 종료되면, Swarm은 즉시 감지하고 같은 노드에 자동으로 재시작시킵니다.
- 노드 다운 (Failover):** `Node 1` 서버 자체가 다운되면, Swarm 매니저들은 이를 감지하고 `Node 2` 나 `Node 3`에 `Node 1`에서 실행 중이던 모든 서비스 컨테이너를 즉시 새로 실행시킵니다.

B. 서비스 발견 및 로드 밸런싱 (Built-in DNS)

`Spring Cloud Eureka` 같은 별도의 서비스 레지스트리가 필요 없습니다.

- 서비스 발견:** Swarm의 내장 DNS가 '주소록' 역할을 수행합니다.
- 연결 방식:** `API Gateway` 는 `http://user-service`처럼 서비스 이름으로만 요청을 보냅니다. Swarm이 이 이름을 `User Service` 컨테이너의 실제 IP로 자동 변환하여 연결합니다.
- 로드 밸런싱:** `User Service` 가 3개(`replicas=3`) 실행 중이면, Swarm은 `http://user-service`로 오는 요청을 3대의 컨테이너에 자동으로 분산(Load Balancing)시킵니다.

C. 수평 확장 (Horizontal Scaling)

`sdac-right-sizing-guide.md`에서 정의한 '소프트웨어 확장' 기능입니다.

- 기능:** 출입문 증가로 `Access Control Service`의 부하가 증가하면, `docker service scale access-control-service=5` (예: 2개 -> 5개) 명령어 하나로 복제본(컨테이너) 수를 늘릴 수 있습니다.
- 효과:** Swarm이 5개의 컨테이너를 `Node 1, 2, 3`에 자동으로 분산시켜 늘어난 트래픽을 처리합니다.

D. 무중단 업데이트 (Rolling Updates)

서비스 재배포 시에도 시스템 중단이 없습니다.

- 작동 방식:** `User Service` v1.1 배포 시, Swarm은 `v1.1` 컨테이너 1개를 먼저 띄워 정상 작동을 확인한 후, `v1.0` 컨테이너 1개를 내립니다. 이 과정을 순차적으로 반복하여 서비스 중단 없이 업데이트를 완료합니다.

4. 플랫폼 지원 인프라

안정적인 플랫폼 운영을 위해 Swarm 클러스터는 다음 인프라를 전제로 합니다.

- 네트워크 이중화 (HA Network):** `Node 1, 2, 3`는 **2개 이상의 NIC(네트워크 포트)**를 **2대 이상의 물리적 스위치**에 나누어 연결하고, OS 레벨에서 **NIC 본딩(Bonding)**으로 구성하여 네트워크 단일 장애 지점(SPOF)을 제거합니다.

- **사설 Docker Registry:** 폐쇄망 운영을 위해, `Node 1` 등에 `registry:2` 컨테이너를 실행하여 모든 서비스 이미지를 저장/공유하는 **중앙 이미지 저장소** 역할을 합니다.
- **HTTPS/SSL Termination (Ingress):** `API Gateway` 앞단에 `Traefik` 또는 `Nginx` 를 배치하여, 외부 HTTPS 트래픽을 전담 처리하고 `API Gateway` 의 부담을 줄여줍니다.