출입 통제 시스템: PostgreSQL DB 스키마 정의서

본 문서는 **PostgreSQL HA 클러스터** 내의 통합 데이터베이스 스키마를 정의합니다.

1. 설계 원칙

- **중앙 집중식 HA:** `DB1`, `DB2` (Patroni + Streaming Replication)의 단일 HA 클러스터에 모든 데이터를 저장합니다.
- **논리적 분리 (Schema per Service):** 물리적 DB는 공유하지만, 각 마이크로서비스는 자신만의 테이블(또는 스키마)을 소유합니다.
- **API 우선 원칙:** 서비스 간 테이블 직접 접근은 금지되며, 반드시 `Spring Cloud OpenFeign`을 통한 API 호출로 데이터를 교환해야 합니다. (예: `Access Control Service`가 `User Service`의 API를 호출)
- **데이터 타입:** `UUID`를 기본 키(PK)로 사용하여 식별자의 고유성을 보장하고, `JSONB` 타입을 활용하여 유연한 메타데이터를 저장합니다.

2. User Service (출입자 및 관리자 계정)

`User Service`는 시스템의 모든 '개인(Identity)' 정보(출입자, 관리자)와 이들의 인증 매체, 그룹, 권한을 관리합니다.

2.1. `users` (출입자)

- **설명:** 일반 출입자(직원, 방문객 등)의 마스터 정보입니다.
- **캐시:** 이 테이블의 정보는 `Redis Cluster`에 캐시되어 `Access Control Service`의 0.1초 미만 판정에 사용됩니다.

컬럼명	데이터 타입	제약 조건	설명
`user_id`	UUID	PK (Primary Key)	사용자 고유 ID (논리적 키)
`name`	VARCHAR(100)	Not Null	출입자 이름
`department_id`	UUID	FK (departments.department_id), Not Null	소속 부서 ID

컬럼명	데이터 타입	제약 조건	설명
status	VARCHAR(20)	Not Null, Default: 'active'	계정 상태 ('active', 'suspended', 'visitor')
employee_id	VARCHAR(100)	Nullable, Unique	사번 (직원 ID)
title	VARCHAR(100)	Nullable	직급 (예: '선임', '팀장')
email	VARCHAR(255)	Nullable, Unique	이메일
phone_number	VARCHAR(50)	Nullable	연락처
photo_url	VARCHAR(512)	Nullable	MinIO에 저장된 사진 URL
created_at	TIMESTAMPTZ	Not Null	생성 일시
updated_at	TIMESTAMPTZ		수정 일시

2.2. credentials (인증 매체)

- **설명:** users 테이블에 1:N으로 매핑되는 실제 인증 수단입니다.

컬럼명	데이터 타입	제약 조건	설명
credential_id	UUID	PK	인증 매체 고유 ID
user_id	UUID	FK (users.user_id)	연결된 출입자 ID
type	VARCHAR(20)	Not Null	인증 방식 (card , nfc , fingerprint , qr)
value	VARCHAR(255)	Not Null, Unique	인증 값 (카드 번호, 지문 ID, NFC ID, QR ID)
status	VARCHAR(20)	Not Null, Default: 'active'	매체 상태 ('active', 'lost', 'expired')
expires_at	TIMESTAMPTZ		만료 일시 (주로 qr 타입 방문객용)

2.3. groups (출입자 그룹)

- **설명:** 정책 할당의 기준이 되는 출입자 그룹입니다.

컬럼명	데이터 타입	제약 조건	설명
group_id	UUID	PK	그룹 고유 ID
name	VARCHAR(100)	Not Null, Unique	그룹 이름 (예: '임원', '엔지니어', '방문객')

컬럼명	데이터 타입	제약 조건	설명
status	VARCHAR(20)	Not Null, Default: 'active'	그룹 상태 ('active', 'decommissioned')

2.4. user_groups (M:N 매핑)

- **설명:** 출입자와 그룹의 다대다(M:N) 관계 테이블.

컬럼명	데이터 타입	제약 조건	설명
user_id	UUID	PK, FK (users.user_id)	
group_id	UUID	PK, FK (groups.group_id)	

2.5. admin_users (시스템 관리자)

- **설명:** Admin UI에 로그인하는 관리자 계정. (출입자 users와 분리)

컬럼명	데이터 타입	제약 조건	설명
admin_user_id	UUID	PK	관리자 고유 ID
username	VARCHAR(100)	Not Null, Unique	로그인 ID
password_hash	VARCHAR(255)	Not Null	해시된 비밀번호
name	VARCHAR(100)	Not Null	관리자 이름
department_id	UUID	FK (departments.department_id), Not Null	관리자 소속 부서 ID
phone_number	VARCHAR(50)	Nullable	비상 연락처
status	VARCHAR(20)	Not Null, Default: 'active'	계정 상태 ('active', 'locked')
photo_url	VARCHAR(512)	Nullable	MinIO에 저장된 관리자 사진 URL

2.6. roles, permissions, role_permissions, admin_user_roles (RBAC 상세)

- **설명:** Admin UI의 RBAC(역할 기반 접근 제어)를 위한 표준 권한 관리 테이블.

roles (역할)

컬럼명	데이터 타입	제약 조건	설명
role_id	UUID	PK	역할 고유 ID

컬럼명	데이터 타입	제약 조건	설명
name	VARCHAR(100)	Not Null, Unique	역할 이름 (예: '최고 관리자', '정책 관리자')
description	TEXT		역할 설명
status	VARCHAR(20)	Not Null, Default: 'active'	역할 상태 ('active', 'decommissioned')

permissions (권한)

컬럼명	데이터 타입	제약 조건	설명
permission_id	UUID	PK	권한 고유 ID
name	VARCHAR(100)	Not Null, Unique	권한 이름 (예: USER_READ, POLICY_UPDATE)
description	TEXT		권한 설명 (예: '사용자 조회', '정책 수정')
status	VARCHAR(20)	Not Null, Default: 'active'	권한 상태 ('active', 'decommissioned')

role_permissions (역할-권한 M:N 매핑)

컬럼명	데이터 타입	제약 조건	설명
role_id	UUID	PK, FK (roles.role_id)	
permission_id	UUID	PK, FK (permissions.permission_id)	

admin_user_roles (관리자-역할 M:N 매핑)

컬럼명	데이터 타입	제약 조건	설명
admin_user_id	UUID	PK, FK (admin_users.admin_user_id)	
role_id	UUID	PK, FK (roles.role_id)	

2.7. departments (부서)

- **설명:** 관리자 및 출입자가 소속된 부서 마스터 테이블.

컬럼명	데이터 타입	제약 조건	설명
department_id	UUID	PK	부서 고유 ID

컬럼명	데이터 타입	제약 조건	설명
name	VARCHAR(100)	Not Null, Unique	부서 이름 (예: '엔지니어링팀', '경영지원팀')
description	TEXT		부서 설명
status	VARCHAR(20)	Not Null, Default: 'active'	부서 상태 ('active', 'decommissioned')

3. Policy Service (정책 및 장치)

Policy Service는 출입 규칙과 물리적 장치(구역)의 정보를 관리합니다. (이해를 돕기 위해 Device Service의 테이블도 여기에 포함합니다.)

3.1. zones (구역)

- **설명:** 물리적 공간의 논리적 단위. (예: '서버실', 'R&D 구역')

컬럼명	데이터 타입	제약 조건	설명
zone_id	UUID	PK	구역 고유 ID
name	VARCHAR(100)	Not Null	구역 이름
description	TEXT		설명
status	VARCHAR(20)	Not Null, Default: 'active'	구역 상태 ('active', 'decommissioned')

3.2. devices (단말기)

- **설명:** ACU 또는 IP 리더기 하드웨어 장치 마스터.

컬럼명	데이터 타입	제약 조건	설명
device_id	UUID	PK	장치 고유 ID
name	VARCHAR(100)	Not Null	장치 이름 (예: '서버실 정문 리더기')
type	VARCHAR(20)	Not Null	장치 타입 (sdac_reader , acu_controller , io_controller)
device_token_hash	VARCHAR(255)		SDAC 버전용 리더기 인증 비밀 키 (해시 저장)
ip_address	INET		장치 IP 주소
status	VARCHAR(20)	Not Null, Default: 'offline'	실시간 상태 ('online', 'offline', 'error', 'locked', 'decommissioned')

컬럼명	데이터 타입	제약 조건	설명
description	TEXT		상세 설명 (예: '서버실 입구, 지문/카드 겸용')
location	VARCHAR(255)		물리적 설치 위치 (예: 'R&D 센터 3층 서쪽')
serial_number	VARCHAR(255)	Nullable, Unique	하드웨어 시리얼 번호 (자산 관리용)
firmware_version	VARCHAR(50)		펌웨어 버전 (업데이트 관리용)
last_seen_at	TIMESTAMPTZ		마지막 Heartbeat 시간 (status 판별용)
metadata	JSONB		제조사, 모델명 등 기타 정보

3.3. doors (출입문)

- **설명:** zones 를 연결하는 물리적 문(개폐기) 정보.

컬럼명	데이터 타입	제약 조건	설명
door_id	UUID	PK	출입문 고유 ID
name	VARCHAR(100)	Not Null	출입문 이름 (예: '서버실 정문')
zone_id	UUID	FK (zones.zone_id)	이 문이 속한 구역
status	VARCHAR(20)	Not Null, Default: 'active'	문 상태 ('active', 'locked', 'decommissioned')
door_config	JSONB		relock_time: 5 , held_open_time: 30 등

3.4. door_devices (M:N 매핑)

- **설명:** 출입문(Door)과 장치(Device)의 다대다(M:N) 관계 테이블. (안티-패스백 지원)

컬럼명	데이터 타입	제약 조건	설명
door_id	UUID	PK, FK (doors.door_id)	
device_id	UUID	PK, FK (devices.device_id)	
direction	VARCHAR(10)	Not Null, Default: 'IN'	이 장치의 역할 (IN , OUT , IO)

3.5. time_schedules (시간표)

- **설명:** 재사용 가능한 시간표 템플릿.

컬럼명	데이터 타입	제약 조건	설명
schedule_id	UUID	PK	시간표 고유 ID
name	VARCHAR(100)	Not Null	시간표 이름 (예: '주간 근무 시간')
rules	JSONB	Not Null	{"mon": ["09:00-18:00"], "tue": ...}
status	VARCHAR(20)	Not Null, Default: 'active'	시간표 상태 ('active', 'decommissioned')

3.6. access_policies (접근 규칙)

- **설명:** [누가], [어디를], [언제] 접근할 수 있는지 정의하는 핵심 규칙 테이블.
- **캐시:** 이 테이블의 정보는 Redis Cluster에 캐시되어 Access Control Service의 0.1초 미만 판정에 사용됩니다.

컬럼명	데이터 타입	제약 조건	설명
policy_id	UUID	PK	정책 고유 ID
group_id	UUID	FK (groups.group_id)	[누가] 이 그룹이
zone_id	UUID	FK (zones.zone_id)	[어디를] 이 구역을
schedule_id	UUID	FK (time_schedules.schedule_id)	[언제] 이 시간표에
status	VARCHAR(20)	Not Null, Default: 'active'	정책 활성화 여부 ('active', 'inactive')

4. Log Service (로그 저장)

Log Service는 Kafka로부터 이벤트를 받아 이 테이블들에 저장합니다. **이 테이블들은 쓰기(Write)가 매우 빈번**하므로, PostgreSQL의 **파티셔닝(Partitioning)** 기능을 적용하는 것이 강력히 권장됩니다.

4.1. access_logs (출입 감사 로그)

- **설명:** 모든 출입 시도(성공/실패) 기록. (테이블 파티셔닝: timestamp 기준 월별)

컬럼명	데이터 타입	제약 조건	설명
log_id	BIGSERIAL	PK	로그 ID (대용량이므로 UUID 대신 BIGSERIAL)
timestamp	TIMESTAMPTZ	Not Null	이벤트 발생 시간

컬럼명	데이터 타입	제약 조건	설명
user_id	UUID	FK (users.user_id), Nullable	출입자 (알 수 없는 카드일 경우 Null)
device_id	UUID	FK (devices.device_id)	출입 시도 장치
door_id	UUID	FK (doors.door_id), Nullable	출입 시도 문 (장치와 문이 M:N이므로 Null 가능)
result	VARCHAR(20)	Not Null	판정 결과 (grant , deny)
deny_reason	VARCHAR(50)		거부 사유 (POLICY_TIME , INVALID_CARD 등)
raw_credential	VARCHAR(255)		사용된 실제 카드 값 (감사용)

4.2. admin_audit_logs (관리자 활동 로그)

- **설명:** Admin UI 에서 발생한 모든 중요 변경 이력(로그인, 정책 수정 등).

컬럼명	데이터 타입	제약 조건	설명
audit_log_id	BIGSERIAL	PK	
timestamp	TIMESTAMPTZ	Not Null	활동 시간
admin_user_id	UUID	FK (admin_users.admin_user_id)	[누가] 이 관리자가
source_ip	INET		[어디서] 요청이 발생한 클라이언트 IP
action_type	VARCHAR(50)	Not Null	[무엇을] (예: POLICY_UPDATE , USER_CREATE)
target_resource	VARCHAR(100)		[어떤 것을] (예: policy_id: ...)
details	JSONB		변경 전/후 상세 내역