로그프레소 소나 REST API 레퍼런스

## 쿼리 API

### 쿼리

로그프레소 쿼리를 실행하여 완료될 때까지 대기한 후 쿼리 결과를 조회합니다. 장시간 소요되는 쿼리의 경우 클라이언트 설정에 따라 타임아웃이 발생할 수 있으므로 [커서 생성](https://docs.logpresso.com/ko/sonar/4.0/api/create-cursor) API를 사용하는 것을 권장합니다. HTTP 연결을 끊는 경우 실행하던 쿼리는 즉시 취소됩니다.

#### HTTP 요청

GET /api/sonar/query

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/query?q=system+tables"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| q | O | 문자열 | 로그프레소 쿼리 문자열 |  |
| offset | X | 64비트 정수 | 건너뛸 갯수 | 최소 0. 기본값 0 |
| limit | X | 64비트 정수 | 최대 갯수 | 최소 0. 미지정 시 전체 조회 |
| fields | X | 문자열 | 출력 필드 이름 목록 | 쉼표(,)로 구분 |
| format | X | 문자열 | 출력 형식 | html, xml, csv, json 중 하나 |

#### 정상 응답

아래는 system tables | fields table 쿼리의 응답 예시입니다. Accept 헤더에 text/html이 주어진 경우에는 HTML 형식으로 출력하고, 그 외의 경우에는 개행으로 구분된 JSON 형식으로 출력합니다.

{"table":"sonar\_event\_00001"}{"table":"sonar\_raw\_event\_00001"}

#### 오류 응답

쿼리 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "q should be not null"}

쿼리가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-query", "error\_msg": "(10200) missing-json-quotation"}

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "offset should be long type."}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "offset should be non-negative integer."}

format 값이 잘못 지정된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be html, xml, csv, or json."}

### 쿼리 상태 조회

현재 세션의 계정에서 실행한 특정 포어그라운드 혹은 백그라운드 쿼리의 상태를 조회합니다.

#### HTTP 요청

GET /api/sonar/queries/:id

#### 정상 응답

{ "id": 60, "source": "adhoc", "login\_name": "xeraph", "remote\_ip": "0:0:0:0:0:0:0:1", "rows": 32, "elapsed": 21, "is\_finished": true, "is\_cancelled": false, "is\_scheduled\_query": false, "constants": {}, "query\_string": "system tables", "start\_time": 1663044689188, "finish\_time": 1663044689209, "last\_started": "2022-09-13 13:51:29+0900", "background": false, "commands": [ { "command": "system tables", "status": "End" "push\_count": 32, } ], "sub\_queries": [], "stamp": 5, "tags": {}}

* **id** (32비트 정수): 쿼리 ID
* **source** (문자열): 쿼리 실행 유형
* 사용자 임의 실행 (adhoc)
* CLI 콘솔 실행 (console)
* 예약된 쿼리 실행 (scheduled-query)
* REST API 클라이언트 (rest-api)
* 자바 클라이언트 (java-client)
* 파이썬 클라이언트 (python-client)
* 로그프레소 엔터프라이즈의 내부 실행 (system)
* 로그프레소 소나의 내부 실행 (sonar)
* 로그프레소 소나의 배치 탐지 시나리오 (batch-rule)
* **login\_name** (문자열): 로그인 계정 이름
* **remote\_ip** (문자열): 클라이언트 IP 주소. 로드밸런서를 거치는 경우에는 X-Forwarded-For 헤더 값이 사용됩니다.
* **rows** (64비트 정수): 쿼리 결과 건수. 쿼리가 완료되기 전까지는 단조 증가할 수 있습니다.
* **elapsed** (64비트 정수): 쿼리 실행 경과 시간 (밀리초 단위)
* **is\_finished** (불리언): 쿼리 완료 여부
* **is\_cancelled** (불리언): 쿼리 취소 요청 여부. 사용자가 명시적으로 취소 요청하거나, 명령어 내부 동작 중 실패(네트워크 오류 등)하여 쿼리가 취소될 수 있습니다. 쿼리 취소 요청 후 쿼리 완료까지 시간 차이가 있습니다.
* **is\_scheduled\_query** (불리언): 예약 쿼리 여부
* **constants** (맵): 상수 키-값 목록. 프로시저나 예약된 쿼리 실행 등 쿼리 매개변수를 전달할 때 사용됩니다.
* **query\_string** (문자열): 쿼리 문자열 원본 (최초 입력 형태 유지)
* **start\_time** (64비트 정수): 쿼리 시작 시각 (UNIX epoch)
* **finish\_time** (64비트 정수): 쿼리 완료 시각 (UNIX epoch)
* **last\_started** (문자열): 쿼리 시작 시각 (yyyy-MM-dd HH:mm:ssZ 형식)
* **background** (불리언): 백그라운드 실행 여부. 포어그라운드 쿼리는 세션 종료 시 즉시 취소되지만, 백그라운드 쿼리는 세션을 종료해도 쿼리를 계속 실행합니다.
* **commands** (배열): 쿼리를 구성하는 명령어 목록
* **command** (문자열): 정규화된 쿼리 명령어
* **status** (문자열): 명령어 실행 상태. 대기 (Waiting), 실행중 (Running), 완료중 (Finalizing), 완료 (End) 중 하나의 상태.
* **push\_count** (64비트 정수): 다음 명령어로 전달한 레코드의 수
* **sub\_queries** (배열): 서브 쿼리 목록
* **id** (32비트 정수): 쿼리 ID
* **commands** (배열): 명령어 목록
* **name** (32비트 정수): 명령어 이름
* **command** (문자열): 정규화된 명령어 구문
* **push\_count** (64비트 정수): 다음 명령어로 전달한 레코드 수
* **status** (문자열): 명령어 실행 상태. 대기 (Waiting), 실행중 (Running), 완료중 (Finalizing), 완료 (End) 중 하나의 상태.
* **stamp** (32비트 정수): 쿼리 상태 조회 버전. 클라이언트에서 동시에 2개 이상의 상태 조회 요청을 한 경우, 동일 쿼리 ID에 대한 최신 버전의 상태 응답을 구분하는 용도로 사용합니다.
* **tags** (맵): 태그 키-값 목록. 클라이언트가 로그프레소 서버의 쿼리 객체에 임의의 휘발성 사용자 정의 데이터를 보관하는 용도로 사용합니다. (예: 쿼리별 페이징 건수)

#### 오류 응답

쿼리가 존재하지 않는 경우

HTTP 상태 코드 403 응답. 쿼리가 존재하지 않거나 다른 계정에서 실행한 쿼리의 경우 쿼리 상태를 조회할 수 없습니다.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

쿼리 ID가 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

### 커서 생성

백그라운드 모드로 쿼리를 시작하고 서버 커서를 반환합니다.

커서 사용이 끝나면 반드시 커서를 삭제해야 합니다. 사용되지 않고 남아있는 커서는 로그프레소 서버의 힙 메모리를 불필요하게 점유합니다.

#### HTTP 요청

POST /api/sonar/cursors

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| q | O | 문자열 | 로그프레소 쿼리 문자열 |  |

#### 정상 응답

{ "id": 109 }

* **id** (32비트 정수): 백그라운드 모드로 생성된 쿼리 ID

#### 오류 응답

쿼리 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "q should be not null"}

쿼리가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-query", "error\_msg": "(10200) missing-json-quotation"}

### 커서 조회

지정한 쿼리 ID의 쿼리 결과를 조회합니다.

#### HTTP 요청

GET /api/sonar/cursors/:id

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/cursors/109?offset=0&limit=10"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| id | O | 32비트 정수 | 로그프레소 쿼리 ID |  |
| offset | X | 64비트 정수 | 건너뛸 갯수 | 최소 0. 기본값 0 |
| limit | X | 64비트 정수 | 최대 갯수 | 최소 0. 기본값 1000 |
| format | X | 문자열 | 출력 형식 | html, xml, csv, json 중 하나 |

#### 정상 응답

아래는 system tables | fields table 쿼리의 응답 예시입니다. format을 별도로 지정하지 않으면 개행으로 구분된 JSON 형식으로 출력합니다.

{"table":"sonar\_event\_00001"}{"table":"sonar\_raw\_event\_00001"}

쿼리 결과의 전체 건수와 같거나 그보다 큰 offset을 지정하면 아무 것도 조회되지 않으므로, [쿼리 상태 조회](https://docs.logpresso.com/ko/sonar/4.0/api/get-query-status)의 rows 건수 범위 내에서 조회해야 합니다.

#### 오류 응답

지정된 커서를 조회할 수 없는 경우

HTTP 상태 코드 403 응답. 쿼리가 존재하지 않거나 다른 계정에서 실행한 쿼리의 경우 쿼리 결과를 조회할 수 없습니다.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

쿼리 ID가 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "offset should be long type."}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "offset should be non-negative integer."}

format 값이 잘못 지정된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be html, xml, csv, or json."}

### 커서 삭제

지정한 쿼리 ID의 서버 커서를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/cursors/:id

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| id | O | 32비트 정수 | 로그프레소 쿼리 ID |  |

#### 정상 응답

{ "status": "ok"}

#### 오류 응답

쿼리가 존재하지 않는 경우

HTTP 상태 코드 403 응답. 커서가 존재하지 않거나 다른 계정에서 실행한 쿼리의 경우 커서를 삭제할 수 없습니다.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

쿼리 ID가 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

## 계정 API

### 암호 인증

로그인 계정과 암호를 검증합니다. 이 API는 테넌트 관리자 이상의 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/verify-password

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=xeraph \ -d password=PASSWORD \ -X POST \ https://HOSTNAME/api/sonar/verify-password

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| login | O | 문자열 | 로그인 계정 이름 | 최대 255자 |
| password | O | 문자열 | 암호 |  |

#### 정상 응답

{ "status": "ok"}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

계정이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "status": "error", "reason": "user-not-found"}

암호가 일치하지 않는 경우

HTTP 상태 코드 200 응답

{ "status": "error", "reason": "password-mismatch"}

인증 API 사용 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 계정 목록 조회

검색 조건과 일치하는 계정 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/users

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/users

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | login, name, title, dept, phone, mobile 대상으로 검색 |
| company\_guid | X | 문자열 | 회사 GUID | 클러스터 관리자 계정만 필터 적용됨 |
| guids | X | 문자열 목록 | 계정 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |

#### 정상 응답

{ "total\_count": 1, "users": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "login": "gildong", "name": "홍길동", "title": null, "dept": null, "phone": null, "mobile": null, "email": "gildong@example.com", "locale": "ko", "role\_id": 1, "role\_name": "클러스터 관리자", "home\_menu\_id": 18, "user\_group\_guids": [], "trust\_hosts": [], "idle\_behavior": "lock", "idle\_timeout": 3600, "password\_expiration": -1, "last\_pw\_change": "2022-09-11 21:08:39+0900", "login\_lock\_count": 5, "login\_lock\_interval": 10, "login\_lock\_until": null, "login\_fail\_count": 0, "auth\_mode": 0, "has\_api\_key": true, "preferences": {}, "created": "2022-09-01 00:31:13+0900", "updated": "2022-09-11 21:08:39+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 건수
* **users** (배열): 계정 목록
* **guid** (문자열): 계정 고유 식별자
* **company\_guid** (문자열): 회사 고유 식별자
* **login** (문자열): 로그인 계정 이름
* **name** (문자열): 사용자 성명
* **title** (문자열): 직함
* **dept** (문자열): 부서
* **phone** (문자열): 유선 전화번호
* **mobile** (문자열): 휴대 전화번호
* **email** (문자열): 이메일
* **locale** (문자열): 언어. en 혹은 ko
* **role\_id** (32비트 정수): 역할 ID. 게스트 (0), 클러스터 관리자 (1), 회사 관리자 (2), 사용자 (3)
* **role\_name** (문자열): 역할 이름
* **home\_menu\_id** (32비트 정수): 로그인 후 표시할 메뉴 ID
* **user\_group\_guids** (배열): 계정이 속한 계정 그룹 식별자 목록
* **trust\_hosts** (문자열): 신뢰하는 호스트 주소 목록. IP 주소가 설정된 경우 해당 IP 주소 이외의 로그인을 허용하지 않습니다.
* **idle\_behavior** (문자열): 세션 유휴 시 보호 동작. 화면 잠금 (lock), 자동 로그아웃 (logout)
* **idle\_timeout** (32비트 정수): 초 단위의 세션 유휴 기준 시각. 값은 0부터 최대 604800초의 범위이며, 0은 무제한을 의미합니다.
* **password\_expiration** (32비트 정수): 암호 만료 기준 일자 수. 시스템 기본값 적용 (-1), 무제한 (0), 최소 7일부터 최대 3650일 이하의 값을 사용합니다.
* **last\_pw\_change** (문자열): 마지막 암호 변경일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **login\_lock\_count** (32비트 정수): 로그인 잠금 기준 횟수. 최소 0부터 최대 5회의 값을 사용합니다. 0인 경우 인증 실패 시 즉시 로그인이 잠깁니다.
* **login\_lock\_interval** (32비트 정수): 로그인 잠금 유지 시간. 최소 1분부터 최대 100000000분 이하의 값을 사용합니다.
* **login\_lock\_until** (문자열): 계정 잠금 해제 일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **login\_fail\_count** (32비트 정수): 로그인 연속 실패 횟수
* **auth\_mode** (32비트 정수): 인증 모드. 모든 인증 방식 시도 (0), 외부 인증 전용 (1)
* **has\_api\_key** (불리언): API 키 존재 여부
* **preferences** (맵): 개인화 설정 목록
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### 계정 조회

지정된 식별자의 계정을 조회합니다.

#### HTTP 요청

GET /api/sonar/users/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/users/ffaf431b-653a-4329-8f83-913cbb00342d

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 계정 식별자 |  |

#### 정상 응답

{ "user": { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "login": "gildong", "name": "홍길동", "title": null, "dept": null, "phone": null, "mobile": null, "email": "gildong@example.com", "locale": null, "role\_id": 1, "role\_name": "클러스터 관리자", "home\_menu\_id": 18, "granted\_tables": [ { "type": "TABLE", "name": "weblog", "read\_only": true, "created": "2022-09-11 21:23:45+0900" } ], "user\_granted\_profiles": [ { "type": "PROFILE", "guid": "2011297e-6a3f-45de-92a3-8c187edb62d2", "name": "testdb (데이터베이스)", "read\_only": true, "created": "2022-09-11 21:23:45+0900" } ], "group\_granted\_profiles": [], "user\_group\_guids": ["28c1251b-2f7c-4c58-95a1-fc4a1ead877e"], "trust\_hosts": [], "idle\_behavior": "lock", "idle\_timeout": 3600, "password\_expiration": 7, "last\_pw\_change": "2022-09-11 21:08:39+0900", "login\_lock\_count": 5, "login\_lock\_interval": 10, "login\_lock\_until": null, "login\_fail\_count": 0, "auth\_mode": 0, "has\_api\_key": true, "preferences": {}, "created": "2022-09-01 00:31:13+0900", "updated": "2022-09-11 21:08:39+0900" }}

* **user** (맵): 계정
* **guid** (문자열): 계정 고유 식별자
* **company\_guid** (문자열): 회사 고유 식별자
* **login** (문자열): 로그인 계정 이름
* **name** (문자열): 사용자 성명
* **title** (문자열): 직함
* **dept** (문자열): 부서
* **phone** (문자열): 유선 전화번호
* **mobile** (문자열): 휴대 전화번호
* **email** (문자열): 이메일
* **locale** (문자열): 언어. en 혹은 ko
* **role\_id** (32비트 정수): 역할 ID. 게스트 (0), 클러스터 관리자 (1), 회사 관리자 (2), 사용자 (3)
* **role\_name** (문자열): 역할 이름
* **home\_menu\_id** (32비트 정수): 로그인 후 표시할 메뉴 ID
* (배열) granted\_tables
* **type** (문자열): TABLE 고정
* **name** (문자열): 테이블 이름
* **read\_only** (불리언): 읽기 전용 여부
* **생성일시 (yyyy-MM-dd HH** (문자열):mm:ssZ 형식)
* (배열) user\_granted\_profiles
* **type** (문자열): PROFILE 고정
* **guid** (문자열): 프로파일 식별자
* **name** (문자열): 테이블 이름
* **read\_only** (불리언): 읽기 전용 여부
* **생성일시 (yyyy-MM-dd HH** (문자열):mm:ssZ 형식)
* (배열) group\_granted\_profiles
* **type** (문자열): PROFILE 고정
* **guid** (문자열): 프로파일 식별자
* **name** (문자열): 테이블 이름
* **read\_only** (불리언): 읽기 전용 여부
* **생성일시 (yyyy-MM-dd HH** (문자열):mm:ssZ 형식)
* **user\_group\_guids** (배열): 계정이 속한 계정 그룹 식별자 목록
* **trust\_hosts** (문자열): 신뢰하는 호스트 주소 목록. IP 주소가 설정된 경우 해당 IP 주소 이외의 로그인을 허용하지 않습니다.
* **idle\_behavior** (문자열): 세션 유휴 시 보호 동작. 화면 잠금 (lock), 자동 로그아웃 (logout)
* **idle\_timeout** (32비트 정수): 초 단위의 세션 유휴 기준 시각. 값은 0부터 최대 604800초의 범위이며, 0은 무제한을 의미합니다.
* **password\_expiration** (32비트 정수): 암호 만료 기준 일자 수. 시스템 기본값 적용 (-1), 무제한 (0), 최소 7일부터 최대 3650일 이하의 값을 사용합니다.
* **last\_pw\_change** (문자열): 마지막 암호 변경일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **login\_lock\_count** (32비트 정수): 로그인 잠금 기준 횟수. 최소 0부터 최대 5회의 값을 사용합니다. 0인 경우 인증 실패 시 즉시 로그인이 잠깁니다.
* **login\_lock\_interval** (32비트 정수): 로그인 잠금 유지 시간. 최소 1분부터 최대 100000000분 이하의 값을 사용합니다.
* **login\_lock\_until** (문자열): 계정 잠금 해제 일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **login\_fail\_count** (32비트 정수): 로그인 연속 실패 횟수
* **auth\_mode** (32비트 정수): 인증 모드. 모든 인증 방식 시도 (0), 외부 인증 전용 (1)
* **has\_api\_key** (불리언): API 키 존재 여부
* **preferences** (맵): 개인화 설정 목록
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

계정 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

계정이 없거나 조회 권한이 없는 경우

HTTP 상태 코드 200 응답

{ "user": null}

### 계정 생성

새 계정을 생성합니다.

#### HTTP 요청

POST /api/sonar/users

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=jsmith \ -d role\_id=2 \ -d name="John Smith" \ -d email="john.smith@example.com" \ -d password="PASSWORD" \ -X POST \ https://HOSTNAME/api/sonar/users

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| login | O | 문자열 | 로그인 계정 이름 | 최대 255자 |
| role\_id | O | 32비트 정수 | 역할 ID | 1, 2, 3 중 하나. 하단 참조 |
| name | O | 문자열 | 사용자 성명 | 최소 1자, 최대 50자 |
| email | O | 문자열 | 이메일 주소 | 최소 1자, 최대 255자 |
| password | X | 문자열 | 암호 | 최소 9자, 암호 규칙 준수 |
| api\_key | X | 문자열 | API 키 | 36자 GUID |
| company\_guid | X | 문자열 | 회사 GUID | 36자 GUID |
| title | X | 문자열 | 직함 | 최대 20자 |
| dept | X | 문자열 | 부서 | 최대 50자 |
| phone | X | 문자열 | 내선번호 | 최대 50자 |
| mobile | X | 문자열 | 휴대번호 | 최대 50자 |
| locale | X | 문자열 | 언어 | en 혹은 ko |
| home\_menu\_id | X | 32비트 정수 | 첫페이지 메뉴 ID |  |
| ticket\_repos | X | 문자열 목록 | 티켓 분류 GUID 목록 | 여러 개의 티켓 분류 GUID는 쉼표(,)로 구분 |
| readable\_tables | X | 문자열 목록 | 읽기 허용 테이블 목록 | 여러 개의 테이블 이름은 쉼표(,)로 구분 |
| user\_group\_guids | X | 문자열 목록 | 계정 그룹 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |
| trust\_hosts | X | 문자열 목록 | 접속 허용 IP | 여러 개의 IP 주소는 쉼표(,)로 구분 |
| idle\_behavior | X | 문자열 | 세션 유휴 동작 | lock 또는 logout |
| idle\_timeout | X | 32비트 정수 | 세션 유휴 기준 시간 (초) | 최소 60, 최대 604800. 기본값 600 |
| password\_expiration | X | 32비트 정수 | 암호 만료 기준 일자 | 시스템 기본값 -1, 무제한 0, 최소 7, 최대 3650 |
| login\_lock\_count | X | 32비트 정수 | 로그인 잠금 기준 횟수 | 최소 0, 최대 5. 기본값 5 |
| login\_lock\_interval | X | 32비트 정수 | 로그인 잠금 유지 시간 (분) | 최소 1, 최대 100000000, 기본값 10 |
| auth\_mode | X | 32비트 정수 | 인증 모드 | 모든 인증 방식 시도 0, 외부 인증 전용 1. 기본값 0 |

**역할 ID**

* (1) 클러스터 관리자: 클러스터 설정을 포함한 모든 관리 권한 부여
* (2) 회사 관리자: 테넌트에 한정된 관리 권한 부여
* (3) 사용자: 대시보드, 위젯, 데이터셋, 티켓과 같은 사용자 객체 편집과 조회성 작업 권한

**암호 규칙**

* 최소 9자 이상
* 영문, 숫자, 특수문자 혼합
* 3자 이상 연속되는 동일 문자는 허용하지 않음

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'login' must be shorter than or equal to 255 characters."}

회사 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

로그인 계정 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicate-login"}

이메일 형식이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'email' parameter is not a valid email address: foo"}

암호 인증 모드에서 암호가 누락된 경우

HTTP 상태 코드 400 응답. auth\_mode를 지정하지 않았거나 0인 경우 암호를 지정해야 합니다.

{ "error\_code": "null-argument", "error\_msg": "password should be not null"}

암호 복잡도가 충분하지 않은 경우

HTTP 상태 코드 400 응답. 암호에 로그인 계정 이름을 포함

{ "error\_code": "invalid-argument", "error\_msg": "password contains login name"}

HTTP 상태 코드 400 응답. 암호가 영문자, 숫자, 특수문자의 조합으로 구성되지 않음

{ "error\_code": "invalid-argument", "error\_msg": "password should contain digits, alphabets, and special characters"}

HTTP 상태 코드 400 응답. 암호에 동일 문자가 3회 이상 연속됨

{ "error\_code": "invalid-argument", "error\_msg": "password should not repeat same characters"}

지원하지 않는 언어를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "unsupported locale: ru"}

존재하지 않는 역할 ID를 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "unknown role id: 5"}

존재하지 않는 메뉴 ID를 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "unknown menu id: 0"}

정의되지 않은 인증 모드를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "auth\_mode should be 0 or 1. input is 2."}

상위 권한의 계정 생성을 시도한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no permission: cannot create cluster admin by user"}

존재하지 않거나 접근 불가 그룹을 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "user group not found: 28c1251b-2f7c-4c58-95a1-fc4a1ead877e"}

### 계정 수정

지정한 계정의 정보를 수정합니다.

#### HTTP 요청

PUT /api/sonar/users/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=jsmith \ -d role\_id=2 \ -d name="John Smith" \ -d idle\_behavior=lock \ -d idle\_timeout=600 \ -d email="john.smith@example.com" \ -X PUT \ https://HOSTNAME/api/sonar/users/bfd00bb0-be99-4fd5-8380-166f544975fa

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 계정 식별자 | 36자 |
| login | O | 문자열 | 로그인 계정 이름 | 최대 255자 |
| role\_id | O | 32비트 정수 | 역할 ID | 1, 2, 3 중 하나. 하단 참조 |
| name | O | 문자열 | 사용자 성명 | 최소 1자, 최대 50자 |
| email | O | 문자열 | 이메일 주소 | 최소 1자, 최대 255자 |
| password | X | 문자열 | 암호 | 최소 9자, 암호 규칙 준수. 미지정 시 기존 암호 유지 |
| api\_key | X | 문자열 | API 키 | 36자 GUID. 미지정 시 기존 API 키 유지 |
| company\_guid | X | 문자열 | 회사 GUID | 36자 GUID. 미지정 시 기존 회사 유지 |
| title | X | 문자열 | 직함 | 최대 20자. 미지정 시 기존 값 삭제 |
| dept | X | 문자열 | 부서 | 최대 50자. 미지정 시 기존 값 삭제 |
| phone | X | 문자열 | 내선번호 | 최대 50자. 미지정 시 기존 값 삭제 |
| mobile | X | 문자열 | 휴대번호 | 최대 50자. 미지정 시 기존 값 삭제 |
| locale | X | 문자열 | 언어 | en 혹은 ko. 미지정 시 세션 로케일 적용 |
| home\_menu\_id | X | 32비트 정수 | 첫페이지 메뉴 ID | 미지정 시 기존 값 삭제 |
| ticket\_repos | X | 문자열 목록 | 티켓 분류 GUID 목록 | 쉼표(,)로 구분. 미지정 시 기존 값 삭제 |
| readable\_tables | X | 문자열 목록 | 읽기 허용 테이블 이름 목록 | 쉼표(,)로 구분. 미지정 시 기존 값 삭제 |
| user\_group\_guids | X | 문자열 목록 | 계정 그룹 식별자 목록 | 쉼표(,)로 구분. 미지정 시 기존 값 삭제 |
| trust\_hosts | X | 문자열 목록 | 접속 허용 IP | 쉼표(,)로 구분. 미지정 시 기존 값 삭제 |
| idle\_behavior | X | 문자열 | 세션 유휴 동작 | lock 또는 logout. 미지정 시 기존 값 삭제 |
| idle\_timeout | X | 32비트 정수 | 세션 유휴 기준 시간 (초) | 최소 60, 최대 604800. 기본값 600 |
| password\_expiration | X | 32비트 정수 | 암호 만료 기준 일자 | 시스템 기본값 -1, 무제한 0, 최소 7, 최대 3650 |
| login\_lock\_count | X | 32비트 정수 | 로그인 잠금 기준 횟수 | 최소 0, 최대 5. 기본값 5 |
| login\_lock\_interval | X | 32비트 정수 | 로그인 잠금 유지 시간 (분) | 최소 1, 최대 100000000, 기본값 10 |
| auth\_mode | X | 32비트 정수 | 인증 모드 | 모든 인증 방식 시도 0, 외부 인증 전용 1. 기본값 0 |

**역할 ID**

* (1) 클러스터 관리자: 클러스터 설정을 포함한 모든 관리 권한 부여
* (2) 회사 관리자: 테넌트에 한정된 관리 권한 부여
* (3) 사용자: 대시보드, 위젯, 데이터셋, 티켓과 같은 사용자 객체 편집과 조회성 작업 권한

**암호 규칙**

* 최소 9자 이상
* 영문, 숫자, 특수문자 혼합
* 3자 이상 연속되는 동일 문자는 허용하지 않음

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'login' must be shorter than or equal to 255 characters."}

계정 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

로그인 계정 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicate-login"}

이메일 형식이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'email' parameter is not a valid email address: foo"}

암호 인증 모드에서 암호가 누락된 경우

HTTP 상태 코드 400 응답. auth\_mode를 지정하지 않았거나 0인 경우 암호를 지정해야 합니다.

{ "error\_code": "null-argument", "error\_msg": "password should be not null"}

암호 복잡도가 충분하지 않은 경우

HTTP 상태 코드 400 응답. 암호에 로그인 계정 이름을 포함

{ "error\_code": "invalid-argument", "error\_msg": "password contains login name"}

HTTP 상태 코드 400 응답. 암호가 영문자, 숫자, 특수문자의 조합으로 구성되지 않음

{ "error\_code": "invalid-argument", "error\_msg": "password should contain digits, alphabets, and special characters"}

HTTP 상태 코드 400 응답. 암호에 동일 문자가 3회 이상 연속됨

{ "error\_code": "invalid-argument", "error\_msg": "password should not repeat same characters"}

지원하지 않는 언어를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "unsupported locale: ru"}

존재하지 않는 역할 ID를 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "unknown role id: 5"}

존재하지 않는 메뉴 ID를 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "unknown menu id: 0"}

정의되지 않은 인증 모드를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "auth\_mode should be 0 or 1. input is 2."}

상위 권한의 계정 변경을 시도한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

자기 자신의 역할을 변경 시도한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "cannot update role by yourself."}

존재하지 않거나 접근 불가 그룹을 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "user group not found: 28c1251b-2f7c-4c58-95a1-fc4a1ead877e"}

### 계정 일괄 삭제

지정한 계정을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/users

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/users?guids=6ba6031e-9d03-4a2b-8372-20ceee8f2a76"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 계정 식별자 목록 | 쉼표(,)로 구분된 계정 식별자 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

계정 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

상위 권한의 계정 삭제를 시도한 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "login": "xeraph" "name": "양봉열", "reason": "no-permission", } ]}

자기 자신을 삭제 시도한 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "login": "xeraph" "name": "양봉열", "reason": "cannnot-remove-yourself", } ]}

계정이 존재하지 않는 경우

HTTP 상태 코드 200 응답. 클러스터 관리자가 아닌 세션에서 다른 테넌트(회사)의 계정을 삭제하려고 시도한 경우에도 조회 실패로 처리합니다.

{ "failures": [ { "guid": "6ba6031e-9d03-4a2b-8372-20ceee8f2a75" "reason": "user-not-found", } ]}

## 계정 그룹 API

### 계정 그룹 목록 조회

검색 조건과 일치하는 계정 그룹 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/user-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/user-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | name, description 대상으로 검색 |
| company\_guid | X | 문자열 | 회사 GUID | 클러스터 관리자 계정만 필터 적용됨 |
| guids | X | 문자열 목록 | 계정 그룹 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |

#### 정상 응답

{ "total\_count": 1, "user\_groups": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "Cyber Security", "description": "", "owner\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "owner\_name": "Yang", "created": "2022-09-01 01:08:00+0900", "updated": "2022-09-01 01:08:00+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 건수
* **groups** (배열): 계정 그룹 목록
* **company\_guid** (문자열): 회사(테넌트)의 식별자
* **company\_name** (문자열): 회사(테넌트)의 이름
* **guid** (문자열): 계정 그룹의 식별자
* **name** (문자열): 계정 그룹의 이름
* **description** (문자열): 설명
* **owner\_guid** (문자열): 계정 그룹을 만든 계정의 식별자
* **owner\_name** (문자열): 계정 그룹을 만든 계정의 이름
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식.

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 계정 그룹 조회

지정된 계정 그룹을 조회합니다.

#### HTTP 요청

GET /api/sonar/user-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/user-groups/28c1251b-2f7c-4c58-95a1-fc4a1ead877e

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 계정 그룹 식별자 | 36자 GUID |

#### 정상 응답

{ "user\_group": { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "Cyber Security", "description": "", "owner\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "owner\_name": "Yang", "user\_guids": ["ffaf431b-653a-4329-8f83-913cbb00342d"], "created": "2022-09-01 01:08:00+0900", "updated": "2022-09-01 01:08:00+0900" }}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 건수
* **groups** (배열): 계정 그룹 목록
* **company\_guid** (문자열): 회사(테넌트)의 식별자
* **company\_name** (문자열): 회사(테넌트)의 이름
* **guid** (문자열): 계정 그룹의 식별자
* **name** (문자열): 계정 그룹의 이름
* **description** (문자열): 설명
* **owner\_guid** (문자열): 계정 그룹을 만든 계정의 식별자
* **owner\_name** (문자열): 계정 그룹을 만든 계정의 이름
* **user\_guids** (배열): 계정 그룹에 속한 계정 식별자 목록
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식.

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

계정 그룹을 조회할 수 없는 경우

HTTP 상태 코드 200 응답

{ "user\_group": null}

### 계정 그룹 생성

새 계정 그룹을 생성합니다.

#### HTTP 요청

POST /api/sonar/user-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Cyber Security" \ -X POST \ https://HOSTNAME/api/sonar/user-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| name | O | 문자열 | 계정 그룹 이름 | 최소 1자, 최대 200자 |
| guid | X | 문자열 | 계정 그룹 GUID | 36자 |
| company\_guid | X | 문자열 | 회사 GUID | 36자. 클러스터 관리자만 사용 가능 |
| description | X | 문자열 | 설명 | 최대 2,000자 |
| user\_guids | X | 배열 | 계정 식별자 목록 | 유효하지 않은 계정 식별자는 무시됨 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 200 characters."}

계정 식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "user\_guids should be guid type."}

### 계정 그룹 수정

지정한 계정 그룹의 정보를 수정합니다.

#### HTTP 요청

PUT /api/sonar/user-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Cyber Security" \ -d user\_guids=ffaf431b-653a-4329-8f83-913cbb00342d \ -X PUT \ https://HOSTNAME/api/sonar/user-groups/a2a42968-787f-45a3-bec9-b6b68db21c2f

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| name | O | 문자열 | 계정 그룹 이름 | 최소 1자, 최대 200자 |
| guid | X | 문자열 | 계정 그룹 GUID | 36자 |
| description | X | 문자열 | 설명 | 최대 2,000자 |
| user\_guids | X | 배열 | 계정 식별자 목록 | 유효하지 않은 계정 식별자는 무시됨 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 200 characters."}

계정 식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "user\_guids should be guid type."}

계정 그룹이 존재하지 않는 경우

클러스터 관리자가 아닌 세션에서 다른 테넌트(회사)의 계정 그룹을 수정하려고 시도한 경우에도 조회 실패로 처리합니다.

{ "error\_code": "illegal-state", "error\_msg": "user group not found: a2a42968-787f-45a3-bec9-b6b68db21c2d"}

### 계정 그룹 일괄 삭제

지정한 계정 그룹을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/user-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/user-groups?guids=a2a42968-787f-45a3-bec9-b6b68db21c2f"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 계정 그룹 식별자 목록 | 쉼표(,)로 구분된 계정 그룹 식별자 목록 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

그룹 관리 권한이 없는 경우

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 접속 프로파일 API

### 접속 프로파일 유형 목록 조회

사용 가능한 접속 프로파일 유형 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/connect-profile-types

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profile-types

#### 정상 응답

아래 예시는 기본 패키지에 내장된 접속 프로파일 유형이며 앱을 설치하면 동적으로 접속 프로파일 목록이 확장됩니다.

{ "profile\_factories": [ { "type": "ftp", "name": "FTP", "description": "FTP 접속 정보를 관리합니다." }, { "type": "ldap", "name": "LDAP", "description": "LDAP 접속 정보를 관리합니다." }, { "type": "ssh", "name": "SSH", "description": "SSH 접속 정보를 관리합니다." }, { "type": "taxii", "name": "TAXII", "description": "TAXII 2.0 프로토콜 접속을 관리합니다." }, { "type": "jdbc", "name": "데이터베이스", "description": "JDBC 드라이버 접속 정보를 관리합니다." }, { "type": "mongo", "name": "몽고DB", "description": "몽고DB 접속 정보를 관리합니다." } ]}

* **profile\_factories** (배열): 접속 프로파일 유형 목록
* **type** (문자열): 접속 프로파일 유형의 식별자
* **name** (문자열): 접속 프로파일 유형의 이름
* **description** (문자열): 접속 프로파일 유형에 대한 설명

### 접속 프로파일 설정 명세 조회

지정한 접속 프로파일 유형의 설정 명세를 조회합니다.

#### HTTP 요청

GET /api/sonar/connect-profile-types/:type/options

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profile-types/ssh/options

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| type | O | 문자열 | 접속 프로파일 유형 식별자 |  |

#### 정상 응답

{ "options": [ { "type": "string", "subtype": "connection-string", "name": "connection\_string", "required": true, "display\_name": "연결 문자열", "description": "연결 문자열", "default\_value": null, "protected": false }, { "type": "string", "subtype": null, "name": "user", "required": false, "display\_name": "계정", "description": "", "default\_value": null, "protected": false }, { "type": "string", "subtype": null, "name": "password", "required": false, "display\_name": "암호", "description": "", "default\_value": null, "protected": true }, { "type": "boolean", "subtype": null, "name": "read\_only", "required": false, "display\_name": "읽기 전용", "description": "읽기 전용", "default\_value": "false", "protected": false } ]}

* **options** (배열): 설정 명세 목록
* **type** (문자열): 데이터 타입. string, integer, boolean 중 하나.
* **subtype** (문자열): UI에서 인식하는 확장 컴포넌트 유형
* **name** (문자열): 설정 키
* **required** (불리언): 필수 설정 여부
* **display\_name** (문자열): 로케일이 적용된 화면 표시 이름
* **description** (문자열): 로케일이 적용된 화면 표시 설명
* **default\_value** (문자열): 화면에 표시할 설정 기본값
* **protected** (불리언): 보호 설정 여부. password 등 접속 프로파일 조회 시 노출되면 안 되는 설정 항목은 true로 지정합니다.

#### 오류 응답

프로파일 유형이 존재하지 않는 경우

{ "options": null}

### 접속 프로파일 목록 조회

사용 가능한 접속 프로파일 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/connect-profiles

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/connect-profiles?offset=0&limit=20"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 기본값 2147483647 |
| type | X | 문자열 | 접속 프로파일 유형 | 지정된 유형만 검색 |
| keywords | X | 문자열 | 검색 키워드 | code, name, description 대상으로 검색 |
| company\_guid | X | 문자열 | 회사 GUID | 클러스터 관리자의 경우 특정 회사로 결과 한정 |

#### 정상 응답

{ "total\_count": 1, "profiles": [ { "guid": "b7f00412-8720-4a8f-ac35-7d7f359f797e", "code": "build", "name": "빌드서버 SSH", "type": "ssh", "description": "", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "configs": { "password": "", "port": 22, "host": "build", "server\_alive\_interval": null, "user": "logpresso", "timeout": 30 }, "config\_description": "호스트: build, 포트: 22, 계정: xeraph, 인증 방식: 암호, 타임아웃: 30초", "factory\_display\_name": "SSH", "created": "2022-09-01 00:39:35+0900", "updated": "2022-09-01 00:39:35+0900", "grant\_users": [ { "type": "USER", "guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "name": "홍길동", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "grant\_groups": [ { "type": "USER", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "dev", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "protected\_keys": ["password"] } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 접속 프로파일 수
* **profiles** (배열): 검색 조건과 일치하는 접속 프로파일 목록
* **guid** (문자열): 접속 프로파일 고유 식별자
* **code** (문자열): 쿼리용 식별자. 동일 접속 프로파일 유형 중 유일한 이름
* **name** (문자열): 접속 프로파일 화면 표시 이름
* **type** (문자열): 접속 프로파일 유형
* **description** (문자열): 접속 프로파일 설명
* **company\_guid** (문자열): 접속 프로파일이 속한 회사의 고유 식별자
* **company\_name** (문자열): 접속 프로파일이 속한 회사의 이름
* **configs** (맵): 접속 프로파일의 키/값 쌍. password처럼 보호 대상 설정은 원본 값을 반환하지 않고, 빈 문자열을 이용하여 설정이 되어있다는 사실만 반환합니다.
* **config\_description** (문자열): 접속 프로파일 설정 요약 정보. 목록에서 특정 접속 프로파일을 구분할 수 있는 핵심 정보를 표시합니다.
* **factory\_display\_name** (문자열): 접속 프로파일 유형의 화면 표시 이름. 예를 들어 jdbc 유형은 한글로 데이터베이스를 반환합니다.
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **grant\_users** (배열): 접속 프로파일 사용 권한이 부여된 계정 목록
* **type** (문자열): 공유 객체 유형. 항상 USER로 응답
* **guid** (문자열): 계정의 고유 식별자
* **name** (문자열): 사용자 성명
* **read\_only** (불리언): 편집 가능 여부. 항상 false로 응답
* **created** (문자열): 권한 매핑 생성 일시
* **grant\_groups** (배열): 접속 프로파일 사용 권한이 부여된 계정 그룹 목록
* **type** (문자열): 공유 객체 유형. 항상 USER로 응답
* **guid** (문자열): 계정 그룹의 고유 식별자
* **name** (문자열): 계정 그룹의 이름
* **read\_only** (불리언): 편집 가능 여부. 항상 false로 응답
* **created** (문자열): 권한 매핑 생성 일시
* **protected\_keys** (배열): 보호되는 설정 키 이름의 목록. 예를 들어 password 설정은 조회 시 반환되지 않습니다.

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### 접속 프로파일 조회

지정한 접속 프로파일을 조회합니다.

#### HTTP 요청

GET /api/sonar/connect-profiles/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profiles/b7f00412-8720-4a8f-ac35-7d7f359f797e

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 접속 프로파일 식별자 |  |

#### 정상 응답

{ "profile": { "guid": "b7f00412-8720-4a8f-ac35-7d7f359f797e", "code": "build", "name": "빌드서버 SSH", "type": "ssh", "description": "", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "configs": { "password": "", "port": 22, "host": "build", "server\_alive\_interval": null, "user": "logpresso", "timeout": 30 }, "config\_description": "호스트: build, 포트: 22, 계정: xeraph, 인증 방식: 암호, 타임아웃: 30초", "factory\_display\_name": "SSH", "created": "2022-09-01 00:39:35+0900", "updated": "2022-09-01 00:39:35+0900", "grant\_users": [ { "type": "USER", "guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "name": "홍길동", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "grant\_groups": [ { "type": "USER", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "dev", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "protected\_keys": ["password"] }}

* **profile** (맵): 지정된 접속 프로파일
* **guid** (문자열): 접속 프로파일 고유 식별자
* **code** (문자열): 쿼리용 식별자. 동일 접속 프로파일 유형 중 유일한 이름
* **name** (문자열): 접속 프로파일 화면 표시 이름
* **type** (문자열): 접속 프로파일 유형
* **description** (문자열): 접속 프로파일 설명
* **company\_guid** (문자열): 접속 프로파일이 속한 회사의 고유 식별자
* **company\_name** (문자열): 접속 프로파일이 속한 회사의 이름
* **configs** (맵): 접속 프로파일의 키/값 쌍. password처럼 보호 대상 설정은 원본 값을 반환하지 않고, 빈 문자열을 이용하여 설정이 되어있다는 사실만 반환합니다.
* **config\_description** (문자열): 접속 프로파일 설정 요약 정보. 목록에서 특정 접속 프로파일을 구분할 수 있는 핵심 정보를 표시합니다.
* **factory\_display\_name** (문자열): 접속 프로파일 유형의 화면 표시 이름. 예를 들어 jdbc 유형은 한글로 데이터베이스를 반환합니다.
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **grant\_users** (배열): 접속 프로파일 사용 권한이 부여된 계정 목록
* **type** (문자열): 공유 객체 유형. 항상 USER로 응답
* **guid** (문자열): 계정의 고유 식별자
* **name** (문자열): 사용자 성명
* **read\_only** (불리언): 편집 가능 여부. 항상 false로 응답
* **created** (문자열): 권한 매핑 생성 일시
* **grant\_groups** (배열): 접속 프로파일 사용 권한이 부여된 계정 그룹 목록
* **type** (문자열): 공유 객체 유형. 항상 USER로 응답
* **guid** (문자열): 계정 그룹의 고유 식별자
* **name** (문자열): 계정 그룹의 이름
* **read\_only** (불리언): 편집 가능 여부. 항상 false로 응답
* **created** (문자열): 권한 매핑 생성 일시
* **protected\_keys** (배열): 보호되는 설정 키 이름의 목록. 예를 들어 password 설정은 조회 시 반환되지 않습니다.

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-argument", "error\_msg": "Invalid UUID string: invalid"}

접속 프로파일이 존재하지 않는 경우

{ "profile": null}

### 접속 프로파일 생성

새 접속 프로파일을 생성합니다.

#### HTTP 요청

POST /api/sonar/connect-profiles

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d company\_guid=6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311 \ -d code=testdb \ -d type=jdbc \ -d name="Hyper SQL" \ -d description="Embedded file database" \ -d configs="{""connection\_string"":""jdbc:hsqldb:file:testdb"", ""user"":""SA"", ""password"":null, ""read\_only"":false}" \ -X POST \ https://HOSTNAME/api/sonar/connect-profiles

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| company\_guid | X | 문자열 | 회사 GUID | 36자. 기본값은 현재 세션의 회사 |
| guid | X | 문자열 | 접속 프로파일 GUID | 36자. 기본값은 무작위 생성 |
| code | O | 문자열 | 접속 프로파일 이름 | 최소 1자, 최대 50자 |
| type | O | 문자열 | 접속 프로파일 유형 | 예: jdbc |
| name | O | 문자열 | 접속 프로파일 화면 표시 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 접속 프로파일 설명 | 최대 2,000자 |
| grant\_users | X | 문자열 | 권한 부여된 계정 GUID 목록 | 여러 개의 항목은 쉼표(,)로 구분 |
| grant\_groups | X | 문자열 | 권한 부여된 계정 그룹 GUID 목록 | 여러 개의 항목은 쉼표(,)로 구분 |
| configs | O | 문자열 키/값 | 설정 값 | JSON 형식 문자열 |

접속 프로파일 이름(code)은 parse 명령어 등 쿼리에서 참조하는 이름으로 사용됩니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

필수 설정 값이 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "config option must be not null: connection\_string"}

접속 프로파일 유형이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "unknown-profile-type", "error\_msg": null}

접속 프로파일 식별자가 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicate-code: testdb"}

회사 GUID가 유효하지 않은 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "invalid-company-guid: 1fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311"}

관리 권한이 없는 회사를 지정한 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 접속 프로파일 수정

지정한 접속 프로파일을 수정합니다.

#### HTTP 요청

PUT /api/sonar/connect-profiles/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Hyper SQL" \ -d description="Embedded file database" \ -d configs="{""connection\_string"":""jdbc:hsqldb:file:testdb"", ""user"":""SA"", ""password"":""NEW\_PASSWORD"", ""read\_only"":false, ""update\_keys"": [""password""]}" \ -X PUT \ https://HOSTNAME/api/sonar/connect-profiles/b7f00412-8720-4a8f-ac35-7d7f359f797e

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 접속 프로파일 식별자 | 36자 |
| name | O | 문자열 | 접속 프로파일 화면 표시 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 접속 프로파일 설명 | 최대 2,000자 |
| grant\_users | X | 문자열 | 권한 부여된 계정 GUID 목록 | 여러 개의 항목은 쉼표(,)로 구분 |
| grant\_groups | X | 문자열 | 권한 부여된 계정 그룹 GUID 목록 | 여러 개의 항목은 쉼표(,)로 구분 |
| configs | O | 문자열 키/값 | 설정 값. 하단 설명 참조 | JSON 형식 문자열 |

접속 프로파일 수정 요청 시 보호되는 설정 키를 configs 매개변수에 포함하지 않으면, 이전의 설정 값을 그대로 유지합니다. 보호되는 설정 키를 새 값으로 수정하려면, configs 매개변수의 키/값 쌍에 update\_keys 키와 보호 키 이름의 목록을 포함하여 전송해야 합니다.

update\_keys 지시가 없으면 기존 설정 값을 유지하려고 null을 전송한 것인지 기존 설정 값을 삭제하려고 null을 전송한 것인지 구분할 수 없기 때문입니다.

#### 정상 응답

{}

#### 오류 응답

접속 프로파일이 존재하지 않는 경우

{ "error\_code": "profile-not-found", "error\_msg": null}

필수 매개변수가 누락된 경우

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

필수 설정 값이 누락된 경우

{ "error\_code": "invalid-argument", "error\_msg": "config option must be not null: connection\_string"}

관리 권한이 없는 회사를 지정한 경우

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 접속 프로파일 일괄 삭제

지정한 여러 개의 접속 프로파일을 삭제합니다. GUID와 일치하는 접속 프로파일이 존재하지 않거나, 해당 접속 프로파일에 대한 관리 권한이 없는 경우 삭제 요청을 무시합니다.

#### HTTP 요청

DELETE /api/sonar/connect-profiles

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/connect-profiles?guids=b7f00412-8720-4a8f-ac35-7d7f359f797e,77e0aa85-14d3-43a9-ab23-4dc97dfc185e"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 접속 프로파일 식별자 | 쉼표(,)로 구분된 식별자 목록 |

#### 정상 응답

{}

#### 오류 응답

GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### SSH 공개 키 조회

로그프레소의 SSH 공개 키를 조회합니다. 로그프레소의 SSH 공개 키를 다른 시스템의 authorized\_keys 파일에 등록하고 SSH 키 기반 인증을 수행할 수 있습니다.

#### HTTP 요청

GET /api/sonar/ssh-public-key

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/ssh-public-key

#### 정상 응답

{ "public\_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC9w0vWHeB/HFXPXM4lTwXALyiatCGtSAoenfyJsrl63uZGU7Xji9Iz/pJJ6t5tWYz7mm2Frg9JjGq2p42xW525FgjRtIhyiPiT7/ZT80GG79Fi1wUE+BlIzXKwmfNxHxaBoW7UcPp1gMSmEycIVU/4b79JM1jfCpfPr+mq9XYzYw== "}

* **public\_key** (문자열): SSH 공개 키

### SSH 공개 키 재생성

로그프레소의 기존 SSH 공개 키를 파기하고 다시 생성합니다. 기존에 접속하던 모든 시스템에서 로그프레소 SSH 키 기반 인증이 무효화되므로 공개 키를 다시 등록해야 합니다. 이 작업은 되돌릴 수 없으니 주의하세요. 이 API를 실행하려면 클러스터 관리자 권한이 필요합니다.

#### HTTP 요청

POST /api/sonar/renew-ssh-public-key

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/renew-ssh-public-key

#### 정상 응답

{ "public\_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCjU/Fx6gogfQDS+egS2ym1c0yill9UkVxZuxpRBqSvh6/xPV24aXaFEywkYCJ0ZJkRyvyJl2FDnyO0ghu9cTRdkNWo+nlHD+LiIbAmglVLOde0I85BLVclXu2HqT8Fd4TIWmUUiIYa1adA96B8qprqKKMCLQwZSqDSNzyRG0/AvQ== "}

* **public\_key** (문자열): 새로 생성된 SSH 공개 키

#### 오류 응답

클러스터 관리자 권한이 없는 경우

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 파서 API

### 파서 유형 목록 조회

파서 유형 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/parser-factories

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parser-factories

#### 정상 응답

아래는 파서 유형 목록의 예시입니다. 앱 설치에 따라 사용 가능한 파서 유형이 동적으로 확장됩니다.

{ "groups": ["시스로그", "범용", "스크립트", "SNMP", "파일"], "factories": [ { "name": "cef", "display\_name": "CEF", "display\_group": "범용", "description": "CEF (Common Event Format) 형식의 로그를 파싱합니다.", "options": [], "deprecated": false }, { "name": "csv", "display\_name": "CSV", "display\_group": "범용", "description": "CSV 형식으로 구분된 각 토큰에 대하여 설정된 필드 이름들을 순서대로 적용하여 파싱합니다.", "options": [ { "type": "string", "subtype": null, "name": "use\_tab", "required": false, "display\_name": "탭문자 사용 여부", "description": "구분자로 탭문자를 사용할지 결정합니다. true 혹은 false", "default\_value": null }, { "type": "string", "subtype": null, "name": "use\_double\_quote", "required": false, "display\_name": "큰 따옴표 이스케이프", "description": "특수문자를 구분하기 위한 이스케이프 문자를 큰 따옴표로 사용합니다. true 혹은 false", "default\_value": null }, { "type": "string", "subtype": null, "name": "column\_headers", "required": false, "display\_name": "필드 이름 목록", "description": "파싱된 결과 필드 이름들", "default\_value": null }, { "type": "string", "subtype": null, "name": "target\_field", "required": false, "display\_name": "대상 필드", "description": "파싱할 대상 필드 이름", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_target", "required": false, "display\_name": "원본 값 포함 여부", "description": "CSV로 파싱된 결과 외에 원본 필드 값도 포함할지 설정합니다. true 혹은 false", "default\_value": null } ], "deprecated": false }, { "name": "json", "display\_name": "JSON", "display\_group": "범용", "description": "JSON 형식의 문자열을 파싱합니다.", "options": [ { "type": "string", "subtype": null, "name": "target\_field", "required": false, "display\_name": "대상 필드", "description": "파싱할 대상 필드 이름", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_target", "required": false, "display\_name": "원본 값 포함 여부", "description": "JSON 형식으로 파싱된 결과 외에 원본 필드 값도 포함할지 설정합니다. true 혹은 false", "default\_value": null } ], "deprecated": false }, { "name": "leef", "display\_name": "LEEF", "display\_group": "시스로그", "description": "LEEF 로그를 파싱합니다.", "options": [], "deprecated": false }, { "name": "welf", "display\_name": "WELF 포맷", "display\_group": "범용", "description": "웹트렌드 로그 포맷", "options": [], "deprecated": false }, { "name": "delimiter", "display\_name": "구분자", "display\_group": "범용", "description": "구분자로 구분된 각 토큰에 대 하여 설정된 필드 이름들을 순서대로 적용하여 파싱합니다.", "options": [ { "type": "string", "subtype": null, "name": "delimiter", "required": true, "display\_name": "구분자", "description": "하나의 아스키 구분자 혹은 4자리 유니코드 이스케이프 시퀀스 (예: \u0007)", "default\_value": null }, { "type": "string", "subtype": null, "name": "column\_headers", "required": false, "display\_name": "필드 이름 목록", "description": "쉼표(,)로 구분된 필드 이름들", "default\_value": null }, { "type": "string", "subtype": null, "name": "delimiter\_target", "required": false, "display\_name": "대상 필드", "description": "구분자로 파싱할 대상 필드 이름", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_delimiter\_target", "required": false, "display\_name": "원본 값 포함 여부", "description": "구분자로 파싱된 결과 외에 원본 필드 값도 포함할지 설정합니다. true 혹은 false", "default\_value": null } ], "deprecated": false }, { "name": "groovy", "display\_name": "그루비", "display\_group": "스크립트", "description": "그루비 파서 스크립트", "options": [ { "type": "string", "subtype": null, "name": "script\_name", "required": true, "display\_name": "스크립트 이름", "description": ".groovy 확장자를 제외한 스크립트 파일 이름", "default\_value": null } ], "deprecated": false }, { "name": "regex", "display\_name": "정규표현식", "display\_group": "범용", "description": "정규표현식을 이용하여 로그를 파싱합니다.", "options": [ { "type": "string", "subtype": null, "name": "regex", "required": true, "display\_name": "정규표현식", "description": "필드 이름이 포함된 정규표현식", "default\_value": null }, { "type": "string", "subtype": null, "name": "field", "required": false, "display\_name": "대상 필드", "description": "정규표현식을 적용할 필드, 미설정 시 기본값은 line", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_original\_field", "required": false, "display\_name": "원본 필드 포함", "description": "정규표현식으로 파싱된 결과 외에 원본 필드 값도 포함할지 설정합니다. true 혹은 false", "default\_value": null } ], "deprecated": false }, { "name": "query", "display\_name": "쿼리 기반 파서", "display\_group": "범용", "description": "쿼리를 이용하여 파싱을 수행합니다.", "options": [ { "type": "string", "subtype": null, "name": "query", "required": true, "display\_name": "쿼리", "description": "로그 파싱에 사용할 쿼리", "default\_value": null } ], "deprecated": false } ]}

* **groups** (배열): 파서 그룹 이름 목록
* **factories** (배열): 파서 유형 목록
* **name** (문자열): 파서 유형 식별자
* **display\_name** (문자열): 파서 유형의 화면 표시 이름
* **display\_group** (문자열): 파서 유형의 화면 표시 그룹
* **description** (문자열): 파서 유형에 대한 설명
* **options** (배열): 설정 명세 목록
* **type** (문자열): 데이터 타입. string, integer, boolean 중 하나.
* **subtype** (문자열): UI에서 인식하는 확장 컴포넌트 유형
* **name** (문자열): 설정 키 이름
* **required** (불리언): 필수 여부
* **display\_name** (문자열): 로케일이 적용된 화면 표시 이름
* **description** (문자열): 로케일이 적용된 화면 표시 설명
* **default\_value** (문자열): 화면에 표시할 설정 기본값
* **deprecated** (불리언): 기능 제거 예정 여부. 이전 버전에서 설정된 경우 호환성을 지원하지만 UI에서 새로운 설정은 불가능하도록 처리합니다.

### 파서 유형 조회

지정한 파서 유형을 조회합니다.

#### HTTP 요청

GET /api/sonar/parser-factories/:name

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/parser-factories/regex?locale=ko"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| name | O | 문자열 | 파서 유형 식별자 |  |
| locale | X | 문자열 | 로케일 | en 또는 ko |

#### 정상 응답

아래는 정규표현식 파서 유형에 대한 조회 결과입니다.

{ "factory": { "name": "regex", "display\_name": "정규표현식", "display\_group": "범용", "description": "정규표현식을 이용하여 로그 를 파싱합니다.", "deprecated": false, "options": [ { "type": "string", "subtype": null, "name": "regex", "required": true, "display\_name": "정규표현식", "description": "필드 이름이 포함된 정규표현식", "default\_value": null }, { "type": "string", "subtype": null, "name": "field", "required": false, "display\_name": "대상 필드", "description": "정규표현식을 적용할 필드, 미설정 시 기본값은 line", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_original\_field", "required": false, "display\_name": "원본 필드 포함", "description": "정규표현식으로 파싱된 결과 외에 원본 필드 값도 포함할지 설정합니다. true 혹은 false", "default\_value": null } ] }}

* **groups** (배열): 파서 그룹 이름 목록
* **factories** (배열): 파서 유형 목록
* **name** (문자열): 파서 유형 식별자
* **display\_name** (문자열): 파서 유형의 화면 표시 이름
* **display\_group** (문자열): 파서 유형의 화면 표시 그룹
* **description** (문자열): 파서 유형에 대한 설명
* **options** (배열): 설정 명세 목록
* **type** (문자열): 데이터 타입. string, integer, boolean 중 하나.
* **subtype** (문자열): UI에서 인식하는 확장 컴포넌트 유형
* **name** (문자열): 설정 키 이름
* **required** (불리언): 필수 여부
* **display\_name** (문자열): 로케일이 적용된 화면 표시 이름
* **description** (문자열): 로케일이 적용된 화면 표시 설명
* **default\_value** (문자열): 화면에 표시할 설정 기본값
* **deprecated** (불리언): 기능 제거 예정 여부. 이전 버전에서 설정된 경우 호환성을 지원하지만 UI에서 새로운 설정은 불가능하도록 처리합니다.

### 파서 목록 조회

검색 조건과 일치하는 파서 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/parsers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parsers

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 |  |
| type | X | 문자열 | 파서 유형 | parser 혹은 normalizer |
| keywords | X | 문자열 | 검색 키워드 | code, name 대상으로 검색 |

#### 정상 응답

{ "total\_count": 27, "parsers": [ { "code": "fortigate", "name": "포티게이트", "description": "WELF 형식으로 된 포티게이트 로그를 파싱합니다.", "factory\_name": "fortigate", "factory\_display\_name": "포티게이트", "builtin": true, "configs": { "ver": "2" }, "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 건수
* **parsers** (배열): 파서 목록
* **code** (문자열): 파서 식별자. [parse 명령어](https://docs.logpresso.com/ko/sonar/4.0/api/ko/query/parse-command)에서 파서 호출 시 참조됨.
* **name** (문자열): 파서 화면 표시 이름
* **description** (문자열): 파서에 대한 설명
* **factory\_name** (문자열): [파서 유형 식별자](https://docs.logpresso.com/ko/sonar/4.0/api/get-parser-factories)
* **factory\_display\_name** (문자열): 파서 유형 화면 표시 이름
* **builtin** (불리언): 패키지 내장 파서 여부
* **schema\_code** (문자열): 정규화 스키마의 이름. 정규화 파서의 경우에만 출력됨.
* **schema\_name** (문자열): 정규화 스키마의 화면 표시 이름. 정규화 파서의 경우에만 출력됨.
* **configs** (맵): [파서 유형별 설정 명세](https://docs.logpresso.com/ko/sonar/4.0/api/get-parser-factory)에 정의된 설정 키/값 목록
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식.

#### 오류 응답

잘못된 파서 유형을 지정한 경우

{ "error\_code": "invalid-argument", "error\_msg": "type should be 'parser' or 'normalizer': unknown"}

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 파서 조회

지정한 파서 설정을 조회합니다.

#### HTTP 요청

GET /api/sonar/parsers/:code

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parsers/fortigate

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 파서 식별자 |  |

#### 정상 응답

{ "parser": { "code": "fortigate", "name": "포티게이트", "description": "WELF 형식으로 된 포티게이트 로그를 파싱합니다.", "factory\_name": "fortigate", "factory\_display\_name": "포티게이트", "builtin": true, "configs": { "ver": "2" }, "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **parser** (맵): 파서 정보
* **code** (문자열): 파서 식별자. [parse 명령어](https://docs.logpresso.com/ko/sonar/4.0/api/ko/query/parse-command)에서 파서 호출 시 참조됨.
* **name** (문자열): 파서 화면 표시 이름
* **description** (문자열): 파서에 대한 설명
* **factory\_name** (문자열): [파서 유형 식별자](https://docs.logpresso.com/ko/sonar/4.0/api/get-parser-factories)
* **factory\_display\_name** (문자열): 파서 유형 화면 표시 이름
* **builtin** (불리언): 패키지 내장 파서 여부
* **schema\_code** (문자열): 정규화 스키마의 이름. 정규화 파서의 경우에만 출력됨.
* **schema\_name** (문자열): 정규화 스키마의 화면 표시 이름. 정규화 파서의 경우에만 출력됨.
* **configs** (맵): [파서 유형별 설정 명세](https://docs.logpresso.com/ko/sonar/4.0/api/get-parser-factory)에 정의된 설정 키/값 목록
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식.

#### 오류 응답

HTTP 상태 코드 200 응답

파서가 존재하지 않는 경우

{ "parser": null}

### 파서 생성

새 파서를 생성합니다. 이 작업은 클러스터 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/parsers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d code=test \ -d name=테스트 \ -d factory\_name=fortigate \ -d configs="{""ver"":""2""}" \ -X POST \ https://HOSTNAME/api/sonar/parsers

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 파서 식별자 | 최소 1자, 최대 50자 |
| name | O | 문자열 | 파서 화면 표시 이름 | 최소 1자, 최대 50자 |
| factory\_name | O | 문자열 | 파서 유형 식별자 |  |
| description | X | 문자열 | 파서 설명 | 최대 2,000자 |
| schema\_code | X | 문자열 | 정규화 스키마 식별자 |  |
| configs | X | 문자열 키/값 | 설정 목록 | JSON 형식 문자열 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

파서 식별자 혹은 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated parser: foo"}

파서 유형이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "parser factory not found: unknown"}

스키마가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

설정이 설정 명세와 맞지 않는 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "parser config [query] should be not null"}

### 파서 수정

기존 파서를 수정합니다. 이 작업은 클러스터 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/parsers/:code

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=테스트 \ -d factory\_name=fortigate \ -d configs="{""ver"":""1""}" \ -X PUT \ https://HOSTNAME/api/sonar/parsers/test

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 파서 식별자 | 최소 1자, 최대 50자 |
| name | O | 문자열 | 파서 화면 표시 이름 | 최소 1자, 최대 50자 |
| factory\_name | O | 문자열 | 파서 유형 식별자 |  |
| description | X | 문자열 | 파서 설명 | 최대 2,000자 |
| schema\_code | X | 문자열 | 정규화 스키마 식별자 |  |
| configs | X | 문자열 키/값 | 설정 목록 | JSON 형식 문자열 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

파서가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "parser not found: unknown"}

파서 유형이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "parser factory not found: unknown"}

스키마가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

설정이 설정 명세와 맞지 않는 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "parser config [query] should be not null"}

### 파서 일괄 삭제

지정한 파서를 삭제합니다. 이 작업은 클러스터 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/parsers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/parsers?codes=test"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| codes | O | 문자열 | 파서 식별자 목록 | 쉼표(,)로 구분된 파서 식별자 목록 |

#### 정상 응답

{ "failures": {}}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "codes should be not null"}

파서 삭제에 실패한 경우

HTTP 상태 코드 200 응답

{ "failures": { "unknown": ["not-exist"] }}

* **failures** (맵): 삭제 실패한 파서 목록. 키는 파서 식별자, 값은 삭제 실패 사유의 배열
* not-exist: 파서가 존재하지 않음
* referenced-by-logger-model: 수집 모델에서 참조됨
* referenced-by-extractor-model: 추출 모델에서 참조됨

### 파서 테스트

#### HTTP 요청

POST /api/sonar/parsers/:code/test

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d line="<36>[SNIPER-2000] [Attack\_Name=(0023)UDP Check Sum Error], [Time=2013/05/14 14:32:05], [Hacker=130.1.254.133], [Victim=130.1.213.10], [Protocol=udp/514], [Risk=Medium], [Handling=Alarm], [Information=], [SrcPort=514]" \ -X POST \ https://HOSTNAME/api/sonar/parsers/sniper/test

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 파서 식별자 |  |
| line | O | 문자열 | 테스트 대상 문자열 |  |

#### 정상 응답

아래는 cURL 예시의 스나이퍼 IPS 로그를 파싱한 결과입니다.

{ "rows": [ { "time": "2013-05-14 14:32:05+0900", "risk": "MEDIUM", "category": null, "host\_name": "SNIPER-2000", "src\_ip": "130.1.254.133", "src\_port": 514, "dst\_ip": "130.1.213.10" "dst\_port": 514, "protocol": "UDP", "hack\_code": "0023", "signature": "(0023)UDP Check Sum Error", "action": "DETECT", } ]}

* **rows** (배열): 파싱 결과 레코드 목록. 파서 설정에 따라 필드 및 값의 구성은 모두 다름.

#### 오류 응답

파서가 존재하지 않는 경우

{ "error\_code": "illegal-state", "error\_msg": "parser profile not found: unknown"}

파싱에 실패한 경우

파싱에 실패한 경우 원본 데이터를 line 필드에 그대로 반환합니다.

{ "rows": [ { "line": "Hello world," } ]}

### 로그 스키마 목록 조회

검색 조건과 일치하는 로그 스키마 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/log-schemas

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | code, name, description 대상으로 검색 |

#### 정상 응답

아래는 session으로 검색한 경우의 예시입니다.

{ "total\_count": 1, "schemas": [ { "code": "session", "name": "세션", "description": "방화벽 세션 및 네트워크 플로우", "created": "2022-09-01 00:31:13+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 스키마의 갯수
* **schemas** (배열): 로그 스키마 목록
* **code** (문자열): 코드 (최대 50자). 정규화된 로그의 \_schema 필드에 기록되는 식별자.
* **name** (문자열): 이름 (최대 50자)
* **description** (문자열): 설명 (최대 255자)
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 로그 스키마 조회

지정한 로그 스키마의 필드 구성 정보를 조회합니다.

#### HTTP 요청

GET /api/sonar/log-schemas/:code

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas/session

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 로그 스키마 코드 |  |

#### 정상 응답

아래는 session 로그 스키마에 대한 조회 예시입니다.

{ "schema": { "code": "session", "name": "세션", "description": "방화벽 세션 및 네트워크 플로우", "created": "2022-09-01 00:31:13+0900", "fields": [ { "name": "\_time", "display\_name": "시각", "type": "DATE", "ordinal": 1 }, { "name": "src\_ip", "display\_name": "출발지IP", "type": "IP", "ordinal": 2 }, { "name": "src\_port", "display\_name": "출발지포트", "type": "PORT", "ordinal": 3 }, { "name": "dst\_ip", "display\_name": "목적지IP", "type": "IP", "ordinal": 4 }, { "name": "dst\_port", "display\_name": "목적지포트", "type": "PORT", "ordinal": 5 }, { "name": "protocol", "display\_name": "프로토콜", "type": "STRING", "ordinal": 6 }, { "name": "app", "display\_name": "응용", "type": "STRING", "ordinal": 7 }, { "name": "action", "display\_name": "대응", "type": "STRING", "ordinal": 8 }, { "name": "nat\_src\_ip", "display\_name": "NAT출발지IP", "type": "IP", "ordinal": 9 }, { "name": "nat\_src\_port", "display\_name": "NAT출발지포트", "type": "PORT", "ordinal": 10 }, { "name": "nat\_dst\_ip", "display\_name": "NAT목적지IP", "type": "IP", "ordinal": 11 }, { "name": "nat\_dst\_port", "display\_name": "NAT목적지포트", "type": "PORT", "ordinal": 12 }, { "name": "policy", "display\_name": "정책", "type": "STRING", "ordinal": 13 }, { "name": "duration", "display\_name": "접속시간", "type": "LONG", "ordinal": 14 }, { "name": "total\_bytes", "display\_name": "바이트", "type": "STRING", "ordinal": 15 }, { "name": "total\_pkts", "display\_name": "패킷", "type": "STRING", "ordinal": 16 }, { "name": "sent\_pkts", "display\_name": "송신패킷", "type": "LONG", "ordinal": 17 }, { "name": "rcvd\_pkts", "display\_name": "수신패킷", "type": "LONG", "ordinal": 18 }, { "name": "sent\_bytes", "display\_name": "송신바이트", "type": "LONG", "ordinal": 19 }, { "name": "rcvd\_bytes", "display\_name": "수신바이트", "type": "LONG", "ordinal": 20 }, { "name": "src\_country", "display\_name": "출발지국가", "type": "COUNTRY", "ordinal": 21 }, { "name": "dst\_country", "display\_name": "목적지국가", "type": "COUNTRY", "ordinal": 22 } ] }}

* **schema** (맵): 로그 스키마 정의
* **code** (문자열): 코드
* **name** (문자열): 이름
* **description** (문자열): 설명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **fields** (배열): 정규화된 필드 정의 목록
* **name** (문자열): 필드 이름
* **display\_name** (문자열): 화면 표시 이름
* **type** (문자열): 유형. DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL 중 하나.
* **ordinal** (32비트 정수): 필드 표시 순서

#### 오류 응답

로그 스키마가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "schema": null}

### 로그 스키마 생성

새 로그 스키마를 생성합니다.

#### HTTP 요청

POST /api/sonar/log-schemas

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d code="ping" \ -d name="핑" \ -d fields="[{""name"":""\_time"", ""type"":""DATE"", ""display\_name"":""시각"", ""ordinal"":1}, {""name"":""dst\_ip"", ""type"":""IP"", ""display\_name"":""목적지IP"", ""ordinal"":2}, {""name"":""rtt"", ""type"":""INT"", ""display\_name"":""왕복시간"", ""ordinal"":2}]" \ -X POST \ https://HOSTNAME/api/sonar/log-schemas

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 정규화 스키마 코드 | 최소 1자, 최대 50자 |
| name | O | 문자열 | 정규화 스키마 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 정규화 스키마 설명 | 최대 255자 |
| fields | X | 문자열 | 필드 정의 목록 | JSON 배열 |

fields는 JSON 배열 형식의 문자열이며 아래의 속성을 포함합니다:

* **type** (문자열): 필드 유형
* DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL 중 하나.
* **name** (문자열): 필드 이름 (최대 50자)
* **display\_name** (문자열): 화면 표시 이름 (최대 50자)
* **ordinal** (32비트 정수): 필드 순서

#### 정상 응답

{}

#### 오류 응답

로그 스키마 생성 권한이 없는 경우

HTTP 상태 코드 500 응답. 로그 스키마는 시스템 전체에 적용되므로 클러스터 관리자 권한이 필요합니다.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

로그 스키마 코드가 중복된 경우

{ "error\_code": "illegal-state", "error\_msg": "duplicated log schema code: ping"}

### 로그 스키마 수정

기존 로그 스키마를 수정합니다.

#### HTTP 요청

PUT /api/sonar/log-schemas/:code

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="핑" \ -d fields="[{""name"":""\_time"", ""type"":""DATE"", ""display\_name"":""시각"", ""ordinal"":1}, {""name"":""src\_ip"", ""type"":""IP"", ""display\_name"":""출발지IP"", ""ordinal"":2}, {""name"":""dst\_ip"", ""type"":""IP"", ""display\_name"":""목적지IP"", ""ordinal"":3},{""name"":""rtt"", ""type"":""INT"", ""display\_name"":""왕복시간"", ""ordinal"":4}]" \ -X PUT \ https://HOSTNAME/api/sonar/log-schemas/ping

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| code | O | 문자열 | 정규화 스키마 코드 | 최소 1자, 최대 50자 |
| name | O | 문자열 | 정규화 스키마 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 정규화 스키마 설명 | 최대 255자 |
| fields | X | 문자열 | 필드 정의 목록 | JSON 배열 |

fields는 JSON 배열 형식의 문자열이며 아래의 속성을 포함합니다:

* **type** (문자열): 필드 유형
* DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL 중 하나.
* **name** (문자열): 필드 이름 (최대 50자)
* **display\_name** (문자열): 화면 표시 이름 (최대 50자)
* **ordinal** (32비트 정수): 필드 순서

#### 정상 응답

{}

#### 오류 응답

로그 스키마 생성 권한이 없는 경우

HTTP 상태 코드 500 응답. 로그 스키마는 시스템 전체에 적용되므로 클러스터 관리자 권한이 필요합니다.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

로그 스키마가 존재하지 않는 경우

{ "error\_code": "illegal-state", "error\_msg": "log schema not found: test"}

### 로그 스키마 일괄 삭제

지정한 로그 스키마를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/log-schemas

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE "https://HOSTNAME/api/sonar/log-schemas?codes=ping"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| codes | O | 문자열 | 정규화 스키마 코드 목록 | 쉼표(,)로 구분된 정규화 스키마 코드 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "codes should be not null"}

로그 스키마 삭제에 실패한 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "session", "reason": "referenced-by-object" }, { "id": "ping2", "reason": "table-schema-not-found" } ]}

* **failures** (배열): 삭제 실패 목록
* **id** (문자열): 로그 스키마 코드
* **reason** (문자열): 삭제 실패 사유
* 로그 스키마가 존재하지 않음 (log-schema-not-found)
* 추출 모델 등 다른 객체에 의해 참조된 상태 (referenced-by-object)

## 수집 유형 API

### 수집 유형 목록 조회

전체 클러스터 또는 지정된 서버에서 수집 유형 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-factories

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| node\_pair\_guid | X | 문자열 | 서버 쌍 GUID | 36자. 지정한 서버 쌍에 등록된 수집 유형만 조회 |

#### 정상 응답

API 키와 연결된 계정의 로케일 설정에 따라 수집 유형의 이름과 설명을 반환합니다. 표시 이름(display\_name) 기준으로 오름차순 정렬하여 출력합니다.

{ "logger\_factories": [ { "name": "cepevent", "display\_name": "CEP 이벤트", "description": "CEP 컨텍스트 이벤트를 수집합니다." }, { "name": "tap-dns", "display\_name": "DNS 스니퍼", "description": "네트워크를 미러링하여 DNS 패킷을 기록합니다." }, { "name": "ftp-dirwatch", "display\_name": "FTP 디렉터리 와처", "description": "지정된 FTP 서버 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "ftp-rotation", "display\_name": "FTP 로테이션 로그 파일", "description": "FTP를 통해 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "ftp-daily-rolling-dirwatch", "display\_name": "FTP 일자별 디렉터리", "description": "FTP를 이용하여 일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "gzip-dirwatch", "display\_name": "GZIP 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 gzip 파일을 수집합니다." }, { "name": "http-post", "display\_name": "HTTP POST", "description": "HTTP POST를 통해 로그를 수신합니다." }, { "name": "http-monitor", "display\_name": "HTTP 모니터", "description": "웹 서비스 응답 코드와 통계 정보를 수집합니다." }, { "name": "tap-http", "display\_name": "HTTP 스니퍼", "description": "네트워크를 미러링하여 HTTP 패킷을 기록합니다." }, { "name": "jdbc", "display\_name": "JDBC 수집기", "description": "JDBC를 통해 데이터베이스에서 데이터를 수집합니다." }, { "name": "netflow", "display\_name": "NetFlow", "description": "UDP를 통해 넷플로우 v5와 v9 패킷을 수신합니다." }, { "name": "pcap-dirwatch", "display\_name": "PCAP 디렉터리 와처", "description": "디렉터리에서 PCAP 파일을 수집합니다." }, { "name": "pcap", "display\_name": "PCAP 패킷", "description": "PCAP 스트림을 통해 패킷를 수집합니다." }, { "name": "rss", "display\_name": "RSS 수집기", "description": "RSS 통해 로그를 수신합니다." }, { "name": "sftp-wtmp", "display\_name": "SFTP WTMP 파일", "description": "SFTP 서버를 통해 wtmp 로그 파일을 수집합니다." }, { "name": "sftp-dirwatch", "display\_name": "SFTP 디렉터리 와처", "description": "원격 SFTP 서버에 접속하여 텍스트 로그 파일을 수집합니다." }, { "name": "sftp-rotation", "display\_name": "SFTP 로테이션 로그 파일", "description": "SFTP를 통해 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "sftp-multi-rotation", "display\_name": "SFTP 멀티 로테이션 로그 파일", "description": "원격 SFTP 서버에 접속하여 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일들을 수집합니다." }, { "name": "sftp-daily-rolling-dirwatch", "display\_name": "SFTP 일자별 디렉터리", "description": "SFTP를 이용하여 일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "snmpget", "display\_name": "SNMP GET", "description": "SNMP GET 호출을 이용하여 OID 값을 수집합니다." }, { "name": "snmpmon", "display\_name": "SNMP 인터페이스 통계", "description": "SNMP 쿼리를 통해 인터페이스별 트래픽 통계를 수집합니다." }, { "name": "snmptrap", "display\_name": "SNMP 트랩 수신기", "description": "UDP로 SNMP 트랩 패킷을 수신합니다." }, { "name": "snmpv3get", "display\_name": "SNMPv3 GET", "description": "SNMPv3 GET 호출을 이용하여 OID 값을 수집합니다." }, { "name": "snmpmonv3", "display\_name": "SNMPv3 인터페이스 통계", "description": "SNMPv3 쿼리를 통해 인터페이스별 트래픽 통계를 수집합니다." }, { "name": "ssh-exec", "display\_name": "SSH 실행", "description": "SSH 쉘의 표준 출력을 로그로 수집합니다." }, { "name": "port-check", "display\_name": "TCP 포트 상태 수집기", "description": "TCP 포트의 개방 여부를 확인합니다." }, { "name": "wtmp", "display\_name": "WTMP", "description": "터미널 로그인, 로그아웃 기록을 수집합니다." }, { "name": "sflow", "display\_name": "sFlow", "description": "UDP를 통해 에스플로우 v5 패킷을 수신합니다." }, { "name": "dirwatch", "display\_name": "디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "disk-usage", "display\_name": "디스크 사용량", "description": "디스크 사용량을 주기적으로 모니터링합니다." }, { "name": "rotation", "display\_name": "로테이션 로그 파일", "description": "일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "linux-account-watch", "display\_name": "리눅스 계정 이벤트 탐지", "description": "계정이 추가/삭제될 때마다 로그를 발생합니다." }, { "name": "gzip-recursive-dirwatch", "display\_name": "리커시브 GZIP 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 GZIP 로그 파일을 수집합니다." }, { "name": "recursive-dirwatch", "display\_name": "리커시브 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "multi-rotation", "display\_name": "멀티 로테이션 로그 파일", "description": "일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일들을 수집합니다." }, { "name": "config-watch", "display\_name": "설정 파일 변경 탐지", "description": "설정 파일이 변경될 때마다 로그를 발생합니다." }, { "name": "sentry-perf", "display\_name": "센트리 성능 로그", "description": "로그프레소 센트리 성능 로그를 일괄 수집합니다." }, { "name": "stream", "display\_name": "스트림 쿼리 출력", "description": "스트림 쿼리의 출력을 수집합니다." }, { "name": "syslog", "display\_name": "시스로그 수집기", "description": "시스로그(TCP/UDP) 포트를 통해 시스로그를 수신합니다." }, { "name": "exec", "display\_name": "외부프로그램", "description": "외부 프로그램의 표준 출력을 로그로 수집합니다." }, { "name": "daily-dirwatch", "display\_name": "일자별 디렉터리", "description": "일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." } ]}

* **logger\_factories** (배열): 수집 유형 목록
* **name** (문자열): 식별자
* **display\_name** (문자열): 표시 이름
* **description** (문자열): 설명

### 수집 유형 조회

지정한 수집 유형을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-factories/:node\_pair\_guid/:namespace/:name

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories/27102ae5-3698-44d4-aad5-4f2def80f275/local/syslog

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| node\_pair\_guid | O | 문자열 | 서버 쌍 GUID | 36자 |
| namespace | O | 문자열 | 이름 공간 | local 또는 센트리 식별자 |
| name | O | 문자열 | 식별자 | 예: syslog, dirwatch |

#### 정상 응답

{ "logger\_factory": { "full\_name": "local\\syslog", "display\_group": "시스로그", "group": "Syslog", "display\_name": "시스로그 수집기", "namespace": "local", "name": "syslog", "description": "시스로그(TCP/UDP) 포트를 통해 시스로그를 수신합니다." }}

* **logger\_factory** (맵): 수집 유형
* **full\_name** (문자열): 이름공간\식별자 형식의 전체 이름
* **name** (문자열): 식별자
* **display\_group** (문자열): 로케일에 따라 표시되는 그룹 이름
* **group** (문자열): 그룹 식별자
* **display\_name** (문자열): 로케일에 따라 표시되는 이름
* **namespace** (문자열): 이름 공간. local 또는 센트리 식별자
* **description** (문자열): 설명

### 수집 유형 설정 명세 조회

지정한 수집 유형의 설정 명세를 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-factories/:node\_pair\_guid/:namespace/:name/options

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories/27102ae5-3698-44d4-aad5-4f2def80f275/local/syslog/options

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| node\_pair\_guid | O | 문자열 | 서버 쌍 GUID | 36자 |
| namespace | O | 문자열 | 이름 공간 | local 또는 센트리 식별자 |
| name | O | 문자열 | 식별자 | 예: syslog, dirwatch |

#### 정상 응답

{ "options": [ { "type": "string", "subtype": "ip-range", "name": "remote\_ip", "required": false, "display\_name": "원격지 IP", "description": "원격지 IP 주소 또는 범위, 예를 들면 IP 또는 IP1-IP2 또는 IP/CIDR", "default\_value": null }, { "type": "string", "subtype": "port", "name": "dst\_port", "required": false, "display\_name": "포트", "description": "수신 포트 필터(설정하지 않은 경우 모든 포트에 대하여 수신합니다.)", "default\_value": null }, { "type": "string", "subtype": null, "name": "facility", "required": false, "display\_name": "시스로그 설비 목록", "description": "쉼표(`,`)로 구분된 시스로그 설비 번호", "default\_value": null }, { "type": "string", "subtype": "regex", "name": "date\_pattern", "required": false, "display\_name": "날짜 정규표현식", "description": "날짜 및 시각을 추출하는데 사용할 정규표현식", "default\_value": null }, { "type": "string", "subtype": "date-format", "name": "date\_format", "required": false, "display\_name": "날짜 포맷", "description": "날짜 및 시각 문자열을 파싱하는데 사용할 포맷. 예) yyyy-MM-dd HH:mm:ss", "default\_value": null }, { "type": "string", "subtype": "date-locale", "name": "date\_locale", "required": false, "display\_name": "날짜 로케일", "description": "날짜 로케일, 예를 들면 ko", "default\_value": null }, { "type": "string", "subtype": "timezone", "name": "timezone", "required": false, "display\_name": "시간대", "description": "시간대, 예를 들면 KST 또는 Asia/Seoul", "default\_value": null }, { "type": "string", "subtype": "regex", "name": "regex", "required": false, "display\_name": "정규식 필터", "description": "추출할 데이터를 선별할 정규식 패턴", "default\_value": null } ]}

* **options** (배열): 설정 명세 목록
* **type** (문자열): 값 유형. string, integer, boolean 중 하나
* **subtype** (문자열): UI 컴포넌트 세부 유형. date-format, date-locale, ip-range, port, regex, timezone 중 하나
* **name** (문자열): 변수 이름
* **required** (불리언): 필수 입력 여부
* **display\_name** (문자열): 화면 표시 이름
* **description** (문자열): 화면 표시 설명
* **default\_value** (문자열): 수집기 생성 시 제안할 기본값

## 수집 모델 API

### 수집 모델 목록 조회

수집 모델 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-models

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-models?offset=0&limit=10

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값: 0 |
| limit | X | 32비트 정수 | 최대 갯수 |  |
| keywords | X | 문자열 | 수집 모델 이름(name)에서 검색할 단어 |  |

#### 정상 응답

{ "total\_count": 2, "logger\_models": [ { "guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "description": null, "logger\_factory\_name": "wtmp", "logger\_factory\_display\_name": "WTMP", "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" }, { "guid": "cd09b2b7-fbc3-11ed-9320-02d178f999a6", "name": "윈도우 XML 이벤트 로그", "description": null, "logger\_factory\_name": "windows-evtx", "logger\_factory\_display\_name": null, "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 모든 수집 모델 개수
* **logger\_models** (배열): 수집 모델 목록
* **guid** (문자열): 수집 모델 식별자
* **name** (문자열): 수집 모델 이름
* **description** (문자열): 수집 모델 설명
* **logger\_factory\_name** (문자열): 수집 유형 식별자
* **logger\_factory\_display\_name** (문자열): 수집 유형 표시 이름
* **parser\_code** (문자열): 파서 식별자
* **parser\_name** (문자열): 파서 이름
* **app\_code** (문자열): 앱 식별자
* **app\_built\_in** (불리언): 앱 내장 객체 여부
* **rule\_count** (32비트 정수): 정규화 규칙 수
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 수집 모델 조회

지정한 수집 모델을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-models/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-models/cd09ae6f-fbc3-11ed-9320-02d178f999a6

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집 모델 식별자 | 36자 GUID |

#### 정상 응답

{ "logger\_model": { "guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "description": null, "logger\_factory\_name": "wtmp", "logger\_factory\_display\_name": "WTMP", "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "rules": [ { "guid": "cd0cdd74-fbc3-11ed-9320-02d178f999a6", "name": "WTMP - 인증", "log\_schema\_code": "auth", "log\_schema\_name": "인증", "parser\_code": null, "parser\_name": null, "stream\_query": "eval action = case(type == \"UserProcess\", \"LOGIN\", type == \"DeadProcess\", \"LOGOUT\"), src\_ip = ip(host), user = if(len(user) == 0, null, user)", "stream\_interval": 60, "app\_code": null, "app\_built\_in": null } ], "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" }}

* **logger\_model** (맵): 수집 모델
* **guid** (문자열): 수집 모델 식별자
* **name** (문자열): 수집 모델 이름
* **description** (문자열): 수집 모델 설명
* **logger\_factory\_name** (문자열): 수집 유형 식별자
* **logger\_factory\_display\_name** (문자열): 수집 유형 표시 이름
* **parser\_code** (문자열): 파서 식별자
* **parser\_name** (문자열): 파서 이름
* **app\_code** (문자열): 앱 식별자
* **app\_built\_in** (불리언): 앱 내장 객체 여부
* **rule\_count** (32비트 정수): 정규화 규칙 수
* **rules** (배열): 정규화 규칙 목록
* **guid** (문자열): 정규화 규칙 식별자
* **name** (문자열): 정규화 규칙 이름
* **log\_schema\_code** (문자열): 로그 스키마 식별자
* **log\_schema\_name** (문자열): 로그 스키마 이름
* **parser\_code** (문자열): 파서 식별자
* **parser\_name** (문자열): 파서 이름
* **stream\_query** (문자열): 스트림 쿼리
* **stream\_interval** (32비트 정수): 스트림 새로고침 주기
* **app\_code** (문자열): 앱 식별자
* **app\_built\_in** (불리언): 앱 내장 객체 여부
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

수집 모델이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "logger\_model": null}

### 수집 모델 생성

새 수집 모델을 추가합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/logger-models

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="NGINX" \ -d logger\_factory\_name="dirwatch" \ -d 'rules=[{"name": "Web log", "log\_schema\_code": "web", "stream\_query": "rex field=line \"(?<src\_ip>\\S+) \\S+ \\S+ \\[(?<event\_time>\\S+ \\S+)\\] \\\"\\S+ \\S+ \\S+\\\" (?<status>\\d+) (?<sc\_bytes>\\d+) \\S+ \\\"(?<user\_agent>[^\\\"]+)\" | eval event\_time = date(event\_time, \"dd/MMM/yyyy:HH:mm:ss Z\"), src\_ip = ip(src\_ip), sc\_bytes = long(sc\_bytes)", "stream\_interval": 0}]' \ -X POST https://HOSTNAME/api/sonar/logger-models

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 수집 모델 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 수집 모델 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집 모델 설명 | 최대 2,000자 |
| logger\_factory\_name | O | 문자열 | 수집 유형 식별자 |  |
| parser\_code | X | 문자열 | 파서 식별자 |  |
| rules | X | 객체 배열 | 정규화 규칙 목록 | 하단 참조 |

rules 속성

* **guid** (문자열): 정규화 규칙 식별자. 미설정 시 무작위 식별자 부여.
* **name** (문자열): 정규화 규칙 이름
* **log\_schema\_code** (문자열): 로그 스키마 식별자
* **stream\_query** (문자열): 스트림 쿼리 문자열
* **stream\_interval** (32비트 정수): 스트림 쿼리 새로고침 주기

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

파서가 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "parser not found: nginx"}

수집 유형이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "logger factory not found: unknown"}

수집 모델 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated logger model name: NGINX"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집 모델 수정

지정한 수집 모델을 수정합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/logger-models/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="NGINX" \ -d description="Demo" \ -d 'rules=[{"name": "Web log", "log\_schema\_code": "web", "stream\_query": "rex field=line \"(?<src\_ip>\\S+) \\S+ \\S+ \\[(?<event\_time>\\S+ \\S+)\\] \\\"\\S+ \\S+ \\S+\\\" (?<status>\\d+) (?<sc\_bytes>\\d+) \\S+ \\\"(?<user\_agent>[^\\\"]+)\" | eval event\_time = date(event\_time, \"dd/MMM/yyyy:HH:mm:ss Z\"), src\_ip = ip(src\_ip), sc\_bytes = long(sc\_bytes)", "stream\_interval": 0}]' \ -X PUT https://HOSTNAME/api/sonar/logger-models

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 수집 모델 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 수집 모델 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집 모델 설명 | 최대 2,000자 |
| parser\_code | X | 문자열 | 파서 식별자 |  |
| rules | X | 객체 배열 | 정규화 규칙 목록 | 하단 참조 |

rules 속성

* **guid** (문자열): 정규화 규칙 식별자. 미설정 시 무작위 GUID 부여.
* **name** (문자열): 정규화 규칙 이름
* **log\_schema\_code** (문자열): 로그 스키마 식별자
* **stream\_query** (문자열): 스트림 쿼리 문자열
* **stream\_interval** (32비트 정수): 스트림 쿼리 새로고침 주기

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

파서가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "parser not found: nginx"}

수집 모델 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated logger model name: NGINX"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집 모델 일괄 삭제

지정한 수집 모델을 삭제합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/logger-models

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/logger-models

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 수집 모델 식별자 목록 | 쉼표(,)를 구분자로 하는 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

수집 모델이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-model-not-found" } ]}

수집 모델을 사용 중인 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "reason": "referenced-by-loggers" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 수집기 그룹 API

### 수집기 그룹 목록 조회

수집기 그룹 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-groups?offset=0&limit=10

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 개수 | 기본값: 0 |
| limit | X | 32비트 정수 | 최대 개수 | 기본값: 무제한 |

#### 정상 응답

{ "total\_count": 1, "logger\_groups": [ { "guid": "0565a218-a78d-43ff-89b6-a9899adcf8c5", "name": "Firewall", "description": null, "parent\_guid": null, "created": "2023-10-01 22:20:44+0900", "updated": "2023-10-01 22:20:44+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 모든 수집기 그룹 개수
* **logger\_groups** (배열): 수집기 그룹 목록
* **guid** (문자열): 수집기 그룹 식별자
* **name** (문자열): 수집기 그룹 이름
* **description** (문자열): 수집기 그룹 설명
* **parent\_guid** (문자열): 부모 수집기 그룹 식별자
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 수집기 그룹 조회

지정한 수집기 그룹을 조회합니다.

#### HTTP 요청

GET /api/sonar/logger-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-groups/0565a218-a78d-43ff-89b6-a9899adcf8c5

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 그룹 식별자 | 36자 GUID |

#### 정상 응답

{ "logger\_group": { "guid": "0565a218-a78d-43ff-89b6-a9899adcf8c5", "name": "Firewall", "description": null, "parent\_guid": null, "created": "2023-10-01 22:20:44+0900", "updated": "2023-10-01 22:20:44+0900" }}

* **logger\_group** (맵): 수집기 그룹
* **guid** (문자열): 수집기 그룹 식별자
* **name** (문자열): 수집기 그룹 이름
* **description** (문자열): 수집기 그룹 설명
* **parent\_guid** (문자열): 부모 수집기 그룹 식별자
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

수집기 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "logger\_group": null}

### 수집기 그룹 생성

새 수집기 그룹을 생성합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/logger-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Firewall" \ -X POST https://HOSTNAME/api/sonar/logger-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 수집기 그룹 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 수집기 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집기 그룹 설명 | 최대 2,000자 |
| parent\_guid | X | 문자열 | 부모 수집기 그룹 식별자 | 36자 GUID |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 그룹 수정

지정한 수집기 그룹을 수정합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/logger-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Firewall" \ -d parent\_guid="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X PUT https://HOSTNAME/api/sonar/logger-groups/0565a218-a78d-43ff-89b6-a9899adcf8c5

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 그룹 식별자 | 36자 GUID |
| name | O | 문자열 | 수집기 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집기 그룹 설명 | 최대 2,000자 |
| parent\_guid | X | 문자열 | 부모 수집기 그룹 식별자 | 36자 GUID |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 그룹 일괄 삭제

지정한 수집기 그룹을 삭제합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/logger-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/logger-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 수집기 그룹 식별자 목록 | 쉼표(,)를 구분자로 하는 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

수집기 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-group-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 수집기 API

### 수집기 목록 조회

수집기 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/loggers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/loggers?offset=0&limit=10

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값: 0 |
| limit | X | 32비트 정수 | 최대 갯수 |  |
| keywords | X | 문자열 | 검색 키워드 | 수집기 이름(name)에서 검색할 단어 |
| schema\_code | X | 문자열 | 로그 스키마 식별자 | 실시간 탐지 시나리오의 수집기 목록 지원용 필터 |

#### 정상 응답

{ "total\_count": 1, "loggers": [ { "id": 1, "guid": "b90ea540-4f47-4bcf-b708-af610a649c50", "name": "WTMP", "description": "", "table\_name": "WTMP", "interval": 5000, "cron\_schedule": null, "enabled": true, "status": "running", "failure": null, "is\_passive": false, "model\_guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "model\_name": "WTMP", "group\_guid": null, "group\_name": null, "node\_pair\_guid": "27102ae5-3698-44d4-aad5-4f2def80f275", "node\_pair\_name": "control", "sentry\_guid": null, "asset\_guid": null, "asset\_ip": null, "hostname": null, "log\_count": 892, "log\_volume": 97531, "drop\_count": 0, "drop\_volume": 0, "configs": { "path": "/var/log/wtmp", "server": null, "regex\_filter\_target\_field": null, "regex\_filter\_pattern": null, "regex\_filter\_negate": "false", "dst\_ip": null }, "created": "2023-10-01 23:59:22+0900", "updated": "2023-10-01 23:59:39+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 모든 수집기 개수
* **loggers** (배열): 수집기 목록
* **id** (32비트 정수): 수집기 번호
* **guid** (문자열): 수집기 식별자
* **name** (문자열): 수집기 이름
* **description** (문자열): 수집기 설명
* **table\_name** (문자열): 수집된 로그를 저장할 테이블 이름
* **interval** (32비트 정수): 수집 간격(단위: 밀리초)
* **cron\_schedule** (문자열): CRON 문법으로 작성된 수집 일정. 예를 들어 매일 새벽 4시 수집은 0 4 \* \* \*
* **enabled** (불리언): 활성화 여부
* **status** (문자열): 동작 상태. running, stopped 중 하나. 활성화하더라도 수집기 오류로 인해 중지될 수 있음.
* **failure** (문자열): 마지막 발생한 오류 내용. 예를 들어 SFTP 수집기는 Auth fail이 발생할 수 있음.
* **is\_passive** (불리언): 수집 간격이나 일정 설정과 무관하게 동작하는 수집기 여부
* **model\_guid** (문자열): 수집 모델 식별자
* **model\_name** (문자열): 수집 모델 이름
* **site\_guid** (문자열): 사이트 식별자
* **site\_name** (문자열): 사이트 이름
* **node\_pair\_guid** (문자열): 서버 쌍 식별자
* **node\_pair\_name** (문자열): 서버 쌍 이름
* **sentry\_guid** (문자열): 센트리 식별자
* **asset\_guid** (문자열): 자산 IP 식별자
* **asset\_ip** (문자열): 자산 IP 주소
* **hostname** (문자열): 자산 호스트명
* **log\_count** (64비트 정수): 수집된 로그의 건수. 수집 후 정규식 필터로 버린 로그는 포함하지 않음
* **log\_volume** (64비트 정수): 수집된 로그의 바이트 단위 용량. 수집 후 정규식 필터로 버린 로그는 포함하지 않음
* **drop\_count** (64비트 정수): 정규식 필터로 버린 로그의 건수
* **drop\_volume** (64비트 정수): 정규식 필터로 버린 로그의 용량 (단위: 바이트)
* **configs** (맵): 설정 키/값 쌍. 수집 모델의 수집 유형에 따라 다른 설정을 요구함.
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 수집기 조회

지정한 수집기를 조회합니다.

#### HTTP 요청

GET /api/sonar/loggers/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 식별자 | 36자 GUID |

#### 정상 응답

{ "logger": { "id": 1, "guid": "b90ea540-4f47-4bcf-b708-af610a649c50", "name": "WTMP", "description": "", "table\_name": "WTMP", "interval": 5000, "cron\_schedule": null, "enabled": true, "status": "running", "failure": null, "is\_passive": false, "model\_guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "model\_name": "WTMP", "group\_guid": null, "group\_name": null, "node\_pair\_guid": "27102ae5-3698-44d4-aad5-4f2def80f275", "node\_pair\_name": "control", "sentry\_guid": null, "asset\_guid": null, "asset\_ip": null, "hostname": null, "log\_count": 892, "log\_volume": 97531, "drop\_count": 0, "drop\_volume": 0, "configs": { "path": "/var/log/wtmp", "server": null, "regex\_filter\_target\_field": null, "regex\_filter\_pattern": null, "regex\_filter\_negate": "false", "dst\_ip": null }, "created": "2023-10-01 23:59:22+0900", "updated": "2023-10-01 23:59:39+0900" }}

* **logger** (맵): 수집기
* **id** (32비트 정수): 수집기 번호
* **guid** (문자열): 수집기 식별자
* **name** (문자열): 수집기 이름
* **description** (문자열): 수집기 설명
* **table\_name** (문자열): 수집된 로그를 저장할 테이블 이름
* **interval** (32비트 정수): 수집 간격(단위: 밀리초)
* **cron\_schedule** (문자열): CRON 문법으로 작성된 수집 일정. 예를 들어 매일 새벽 4시 수집은 0 4 \* \* \*
* **enabled** (불리언): 활성화 여부
* **status** (문자열): 동작 상태. running, stopped 중 하나. 활성화 설정하더라도 수집기 오류로 인해 정지할 수 있음.
* **failure** (문자열): 마지막 발생한 오류 내용. 예를 들어 SFTP 수집기는 Auth fail이 발생할 수 있음.
* **is\_passive** (불리언): 수집 간격이나 일정 설정과 무관하게 동작하는 수집기 여부
* **model\_guid** (문자열): 수집 모델 식별자
* **model\_name** (문자열): 수집 모델 이름
* **site\_guid** (문자열): 사이트 식별자
* **site\_name** (문자열): 사이트 이름
* **node\_pair\_guid** (문자열): 서버 쌍 식별자
* **node\_pair\_name** (문자열): 서버 쌍 이름
* **sentry\_guid** (문자열): 센트리 식별자
* **asset\_guid** (문자열): 자산 IP 식별자
* **asset\_ip** (문자열): 자산 IP 주소
* **hostname** (문자열): 자산 호스트명
* **log\_count** (64비트 정수): 수집된 로그의 건수. 수집 후 정규식 필터로 버린 로그는 포함하지 않음
* **log\_volume** (64비트 정수): 수집된 로그의 바이트 단위 용량. 수집 후 정규식 필터로 버린 로그는 포함하지 않음
* **drop\_count** (64비트 정수): 정규식 필터로 버린 로그의 건수
* **drop\_volume** (64비트 정수): 정규식 필터로 버린 로그의 바이트 단위 용량
* **configs** (맵): 설정 키/값 쌍. 수집 모델의 수집 유형에 따라 다른 설정을 요구함.
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 수집기 생성

새 수집기를 생성합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/loggers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d model\_guid="cd09ae6f-fbc3-11ed-9320-02d178f999a6" \ -d name="WTMP" \ -d node\_pair\_guid="27102ae5-3698-44d4-aad5-4f2def80f275" \ -d table\_name="WTMP" \ -d interval=5000 \ -d 'configs={"path": "/var/log/wtmp"}' \ -X POST https://HOSTNAME/api/sonar/loggers

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 수집기 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| model\_guid | O | 문자열 | 수집 모델 식별자 | 36자 GUID |
| name | O | 문자열 | 수집기 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집기 설명 | 최대 2,000자 |
| node\_pair\_guid | O | 문자열 | 서버 쌍 식별자 | 36자 |
| table\_name | O | 문자열 | 테이블 이름 |  |
| sentry\_guid | X | 문자열 | 센트리 식별자 |  |
| interval | X | 32비트 정수 | 수집 간격 | 최소 1000 (단위: 밀리초) |
| cron\_schedule | X | 문자열 | 수집 주기 | CRON 문법에 따라 작성된 일정 |
| asset\_guid | X | 문자열 | 자산 식별자 | 자산 IP 주소의 GUID |
| configs | X | 문자열 키/값 | 설정 | [수집 유형별 설정 명세](https://docs.logpresso.com/ko/sonar/4.0/api/get-logger-factory-options) 확인 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "asset\_guid should be guid type."}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

수집 일정 문법이 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "wrong cron expression format: \* \* \* \*"}

수집 모델이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "logger model not found: bd09ae6f-fbc3-11ed-9320-02d178f999a6"}

서버 쌍이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "node pair not found: 37102ae5-3698-44d4-aad5-4f2def80f275"}

센트리가 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "sentry not found: test"}

자산이 존재하지 않는 경우

{ "error\_code": "illegal-state", "error\_msg": "asset not found: cd09ae6f-fbc3-11ed-9320-02d178f999a6"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 수정

지정한 수집기를 수정합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/loggers/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="WTMP" \ -d description="demo" \ -d interval=10000 \ -d 'configs={"path": "/var/log/wtmp"}' \ -X PUT https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 식별자 | 36자 GUID |
| name | O | 문자열 | 수집기 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 수집기 설명 | 최대 2,000자 |
| interval | X | 32비트 정수 | 수집 간격 | 최소 1000 (단위: 밀리초) |
| cron\_schedule | X | 문자열 | 수집 주기 |  |
| asset\_guid | X | 문자열 | 자산 식별자 | 자산 IP 및 사이트 연결 |
| configs | X | 문자열 키/값 | 설정 | [수집 유형별 설정 명세](https://docs.logpresso.com/ko/sonar/4.0/api/get-logger-factory-options) 확인 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "asset\_guid should be guid type."}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

수집 일정 문법이 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "wrong cron expression format: \* \* \* \*"}

자산이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "asset not found: cd09ae6f-fbc3-11ed-9320-02d178f999a6"}

수집기가 존재하지 않는 경우

{ "error\_code": "illegal-state", "error\_msg": "logger not found: c90ea540-4f47-4bcf-b708-af610a649c50"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 삭제

지정한 수집기를 삭제합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/loggers/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 식별자 | 36자 GUID |
| drop\_table | X | 불리언 | 테이블 삭제 여부 | 기본값: false |

#### 정상 응답

{}

수집기 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 일괄 삭제

지정한 수집기 목록을 삭제합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/loggers

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/loggers

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 수집기 식별자 목록 | 쉼표(,)를 구분자로 하는 GUID 목록 |
| drop\_table | X | 불리언 | 테이블 삭제 여부 | 기본값: false |

#### 정상 응답

{ "failures": []}

#### 오류 응답

삭제 대상 테이블을 다른 수집기에서 사용하는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "3a2e6570-3a5e-4b2f-982f-037eff266139", "name": "WTMP2", "reason": "table is referenced by other loggers: WTMP" } ]}

수집기 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 활성화

지정한 수집기를 활성화합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/loggers/:guid/enable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50/enable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 식별자 | 36자 GUID |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

수집기가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "logger not found: 05efb651-9644-4518-950f-dbd648c973a7"}

수집기 활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 비활성화

지정한 수집기를 비활성화합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/loggers/:guid/disable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50/disable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 수집기 식별자 | 36자 GUID |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

수집기가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "logger not found: 05efb651-9644-4518-950f-dbd648c973a7"}

수집기 비활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 수집기 상태 일괄 초기화

지정한 수집기의 상태를 초기화합니다. 수집기의 상태가 초기화되면 처음부터 다시 수집합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/loggers/states

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/loggers/states

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 수집기 식별자 목록 | 쉼표(,)를 구분자로 하는 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

수집기가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 주소 그룹 API

### 주소 그룹 목록 조회

사용 가능한 주소 그룹 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/address-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/address-groups?offset=0&limit=20"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 기본값 2147483647 |
| keywords | X | 문자열 | 검색 키워드 | name, description 대상으로 검색 |

#### 정상 응답

{ "total\_count": 1, "address\_groups": [ { "guid": "4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "name": "방화벽 차단 IP", "description": "차단 연동용 IP 블랙리스트", "count": 1, "version": 7, "created": "2022-10-05 15:34:59+0900", "updated": "2022-10-06 00:46:35+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 주소 그룹 수
* **address\_groups** (배열): 검색 조건과 일치하는 페이징된 주소 그룹 목록
* **guid** (문자열): 주소 그룹 고유 식별자
* **company\_guid** (문자열): 주소 그룹이 속한 회사의 고유 식별자
* **company\_name** (문자열): 주소 그룹이 속한 회사의 이름
* **name** (문자열): 주소 그룹 이름
* **description** (문자열): 주소 그룹 설명
* **count** (32비트 정수): 주소 그룹에 속한 주소 갯수
* **version** (32비트 정수): 단조 증가하는 버전
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 주소 그룹 조회

지정한 주소 그룹을 조회합니다.

#### HTTP 요청

GET /api/sonar/address-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 주소 그룹 식별자 | 36자 GUID |

#### 정상 응답

{ "address\_group": { "guid": "4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "name": "방화벽 차단 IP", "description": "차단 연동용 IP 블랙리스트", "count": 1, "version": 7, "created": "2022-10-05 15:34:59+0900", "updated": "2022-10-06 00:46:35+0900" }}

* **address\_group** (맵): 지정된 주소 그룹
* **guid** (문자열): 주소 그룹 고유 식별자
* **company\_guid** (문자열): 주소 그룹이 속한 회사의 고유 식별자
* **company\_name** (문자열): 주소 그룹이 속한 회사의 이름
* **name** (문자열): 주소 그룹 이름
* **description** (문자열): 주소 그룹 설명
* **count** (32비트 정수): 주소 그룹에 속한 주소 갯수
* **version** (32비트 정수): 단조 증가하는 버전
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

지정한 주소 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "address\_group": null}

식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### 주소 그룹 생성

새 주소 그룹을 생성합니다.

#### HTTP 요청

POST /api/sonar/address-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=Exceptions \ -X POST \ https://HOSTNAME/api/sonar/address-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| name | O | 문자열 | 주소 그룹 이름 | 최소 1자, 최대 50자 |
| guid | X | 문자열 | 주소 그룹 GUID | 36자. 기본값은 무작위 생성 |
| company\_guid | X | 문자열 | 회사 GUID | 36자. 기본값은 현재 세션의 회사 |
| description | X | 문자열 | 주소 그룹 설명 | 최대 2,000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 50 characters."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

회사가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "company not found: 1245cbbc-681c-4c52-a01b-f4b496d95d50"}

### 주소 그룹 수정

지정한 주소 그룹을 수정합니다.

#### HTTP 요청

PUT /api/sonar/address-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=Exceptions \ -d description="Service assets" \ -X PUT \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 주소 그룹 GUID | 36자. 기본값은 무작위 생성 |
| name | O | 문자열 | 주소 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 주소 그룹 설명 | 최대 2,000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 50 characters."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

주소 그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "address group not found: 81e7ff9e-457e-4f65-8f8e-bb9b3a0021c8"}

주소 그룹 수정 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 주소 그룹 일괄 삭제

지정한 여러 개의 주소 그룹을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/address-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/address-groups?guids=4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 주소 그룹 식별자 | 쉼표(,)로 구분된 식별자 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

주소 그룹 삭제에 실패한 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "55e6d809-96c8-4d7a-9e20-98e2b34b6cec", "reason": "address-group-not-found" } ]}

삭제 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 주소 객체 목록 조회

지정한 주소 그룹에 속한 주소 객체 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/address-groups/:guid/addresses

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/address-groups/8df64276-a16e-4bae-93cd-c207c8155159/addresses

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 주소 그룹 GUID | 36자 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 50건 |
| keywords | X | 문자열 | 검색 키워드 | ip, description 대상으로 검색 |

#### 정상 응답

{ "total\_count": 1, "addresses": [ { "guid": "d4915ba2-763f-4ec0-a875-38b292a99a24", "ip": "20.214.237.145", "country": "US", "count": 1, "description": "Web app attack", "created": "2022-11-07 01:30:40+0900", "updated": "2022-11-07 01:30:40+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 주소 수
* **addresses** (배열): 주소 목록
* **guid** (문자열): 주소 고유 식별자
* **ip** (문자열): IP 주소
* **country** (문자열): IP 주소 할당 국가 (ISO 2자리 국가 코드)
* **count** (32비트 정수): 등록 건수
* **description** (문자열): 설명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 주소 객체 생성

지정한 주소 그룹에 새 주소 객체를 생성합니다.

#### HTTP 요청

POST /api/sonar/address-groups/:guid/addresses

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d address=1.1.1.1 \ -d description="Public DNS" \ -X POST \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2/addresses

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 주소 그룹 GUID | 36자 |
| address | O | 문자열 | IP 주소 |  |
| description | X | 문자열 | 설명 | 최대 255자 |
| period | X | 32비트 정수 | 유지 기간 (분 단위) | 최소 1, 최대 52560000 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "address should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'description' must be shorter than or equal to 255 characters."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

유효한 IP 주소가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "address should be valid IPv4 address: 256.255.255.255"}

유지 기간의 값이 1보다 작은 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be greater than or equal to 1."}

유지 기간의 값이 52560000보다 큰 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be less than or equal to 52560000."}

주소 그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "address group not found: ede06992-dd57-4b79-8c54-a295f33d8613"}

주소 그룹 관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 주소 객체 일괄 삭제

지정한 주소 그룹에서 여러 개의 주소 객체를 삭제합니다. 존재하지 않는 IP 주소에 대한 삭제 요청은 무시합니다.

#### HTTP 요청

DELETE /api/sonar/address-groups/:guid/addresses

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2/addresses?addresses=1.1.1.1"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 주소 그룹 GUID | 36자 |
| addresses | O | 문자열 | IP 주소 목록 | 쉼표(,)로 구분된 IP 주소 목록 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "addresses should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

유효한 IP 주소가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "addresses should contain only valid IP addresses. input is 256.255.255.255"}

주소 그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "address group not found: ede06992-dd57-4b79-8c54-a295f33d8613"}

주소 그룹 관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 네트워크 대역 그룹 API

### 네트워크 대역 그룹 목록 조회

검색 조건과 일치하는 네트워크 대역 그룹 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/subnet-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명 대상으로 검색 |

#### 정상 응답

{ "total\_count": 1, "subnet\_groups": [ { "guid": "bb994ca4-1471-4b91-89f2-99a61bd529b5", "name": "내부망 대역", "description": null, "subnet\_count": 3, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 모든 네트워크 대역 그룹 수
* **subnet\_groups** (배열): 페이징된 네트워크 대역 그룹 목록
* **guid** (문자열): 네트워크 대역 그룹 식별자
* **name** (문자열): 네트워크 대역 그룹 이름
* **description** (문자열): 네트워크 대역 그룹 설명
* **subnet\_count** (32비트 정수): 그룹에 속한 네트워크 대역 갯수
* **company\_guid** (문자열): 그룹이 속한 회사 (테넌트) 식별자
* **company\_name** (문자열): 그룹이 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 네트워크 대역 그룹을 생성한 계정의 GUID
* **user\_name** (문자열): 네트워크 대역 그룹을 생성한 계정의 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 네트워크 대역 그룹 조회

지정한 네트워크 대역 그룹을 조회합니다.

#### HTTP 요청

GET /api/sonar/subnet-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups/bb994ca4-1471-4b91-89f2-99a61bd529b5

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 식별자 | 36자 GUID |

#### 정상 응답

{ "subnet\_group": { "guid": "bb994ca4-1471-4b91-89f2-99a61bd529b5", "name": "내부망 대역", "description": null, "subnet\_count": 3, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **subnet\_group** (맵): 네트워크 대역 그룹
* **guid** (문자열): 네트워크 대역 그룹 식별자
* **name** (문자열): 네트워크 대역 그룹 이름
* **description** (문자열): 네트워크 대역 그룹 설명
* **subnet\_count** (32비트 정수): 그룹에 속한 네트워크 대역 갯수
* **company\_guid** (문자열): 그룹이 속한 회사 (테넌트) 식별자
* **company\_name** (문자열): 그룹이 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 네트워크 대역 그룹을 생성한 계정의 GUID
* **user\_name** (문자열): 네트워크 대역 그룹을 생성한 계정의 성명

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

네트워크 대역 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "subnet\_group": null}

### 네트워크 대역 그룹 생성

새 네트워크 대역 그룹을 생성합니다.

#### HTTP 요청

POST /api/sonar/subnet-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="OA" \ -d description="Office zone" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 네트워크 대역 그룹 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 네트워크 대역 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 네트워크 대역 그룹 설명 | 최대 50자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

그룹 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated subnet group name: OA"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 네트워크 대역 그룹 수정

지정한 네트워크 대역 그룹을 수정합니다.

#### HTTP 요청

PUT /api/sonar/subnet-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="OA" \ -d description="Office zone network" \ -X PUT \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 그룹 GUID | 36자 |
| name | O | 문자열 | 네트워크 대역 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 네트워크 대역 그룹 설명 | 최대 50자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "subnet group not found: c1dfe306-abba-4ed8-862b-0e98e2effcb5"}

그룹 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated subnet group name: OA"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 네트워크 대역 그룹 일괄 삭제

지정한 네트워크 대역 그룹을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/subnet-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/subnet-groups?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 네트워크 대역 그룹 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

네트워크 대역 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "subnet-group-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 네트워크 대역 목록 조회

지정한 네트워크 대역 그룹에 속한 네트워크 대역 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/subnet-groups/:guid/subnets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups/bb994ca4-1471-4b91-89f2-99a61bd529b5/subnets

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 그룹 GUID | 36자 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 20건 |
| keywords | X | 문자열 | 검색 키워드 | 설명 대상으로 검색 |

#### 정상 응답

{ "total\_count": 3, "subnets": [ { "id": 1, "start\_ip": "10.0.0.0", "end\_ip": "10.255.255.255", "cidr": 0, "description": "A 클래스" }, { "id": 2, "start\_ip": "172.16.0.0", "end\_ip": "172.31.255.255", "cidr": 0, "description": null }, { "id": 3, "start\_ip": "192.168.0.0", "end\_ip": "192.168.255.255", "cidr": 0, "description": null } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 네트워크 대역의 갯수
* **subnets** (배열): 페이징된 네트워크 대역 목록
* **id** (32비트 정수): 네트워크 대역 ID
* **start\_ip** (문자열): 범위 시작 IP 주소
* **end\_ip** (문자열): 범위 끝 IP 주소
* **cidr** (32비트 정수): CIDR 서브넷 마스크 값
* **description** (문자열): 설명

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 네트워크 대역 생성

지정한 네트워크 대역 그룹에 새 네트워크 대역을 추가합니다.

#### HTTP 요청

POST /api/sonar/subnet-groups/:guid/subnets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d start\_ip="192.168.253.1" \ -d end\_ip="192.168.253.255" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8/subnets

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 그룹 GUID | 36자 |
| start\_ip | O | 문자열 | 시작 IP 주소 | 최소 7자, 최대 15자 |
| end\_ip | X | 문자열 | 끝 IP 주소 | 최소 7자, 최대 15자 |
| cidr | X | 32비트 정수 | CIDR | 최소 0, 최대 32 |
| description | X | 문자열 | 네트워크 대역 설명 | 최대 255자 |

end\_ip와 cidr 매개변수 중 하나는 반드시 지정해야 합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "start\_ip should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'start\_ip' must be less than or equal to 15 characters."}

cidr이 정수가 아닌 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'cidr' parameter should be int type"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 네트워크 대역 수정

지정한 네트워크 대역 그룹의 네트워크 대역 정보를 수정합니다.

#### HTTP 요청

PUT /api/sonar/subnet-groups/:guid/subnets/:id

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d start\_ip="192.168.253.1" \ -d end\_ip="192.168.253.2" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8/subnets/10

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 그룹 GUID | 36자 |
| id | O | 32비트 정수 | 네트워크 대역 ID |  |
| start\_ip | O | 문자열 | 시작 IP 주소 | 최소 7자, 최대 15자 |
| end\_ip | X | 문자열 | 끝 IP 주소 | 최소 7자, 최대 15자 |
| cidr | X | 32비트 정수 | CIDR | 최소 0, 최대 32 |
| description | X | 문자열 | 네트워크 대역 설명 | 최대 255자 |

end\_ip와 cidr 매개변수 중 하나는 반드시 지정해야 합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "start\_ip should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'start\_ip' must be less than or equal to 15 characters."}

cidr이 정수가 아닌 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'cidr' parameter should be int type"}

네트워크 대역 그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "subnet group not found: 0c74771b-568e-4696-80ed-6dd4d8b71a12"}

네트워크 대역이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "subnet not found: 100"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 네트워크 대역 일괄 삭제

지정한 네트워크 대역을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/subnet-groups/:guid/subnets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/subnet-groups/638cfeb2-e259-46af-961a-1eeb65ea35f0/subnets?ids=10"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 네트워크 대역 그룹 GUID | 36자 |
| ids | O | 32비트 정수 목록 | 네트워크 대역 ID 목록 | 쉼표(,)로 구분된 ID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

네트워크 대역 그룹 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

네트워크 대역 식별자가 32비트 정수 목록이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'ids' parameter should be int\_list type"}

네트워크 대역이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "6", "reason": "subnet-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 패턴 그룹 API

### 패턴 그룹 목록 조회

검색 조건과 일치하는 패턴 그룹 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/pattern-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 |  |
| keywords | X | 문자열 | 검색 키워드 | name, description 대상으로 검색 |

#### 정상 응답

{ "total\_count": 23, "pattern\_groups": [ { "guid": "28ad21b2-585c-4b68-9fad-b78711078496", "name": "IPS WAS 취약점 공격 경보", "description": "알려진 WAS의 취약점을 이용하여 원격코드 실행하거나 서비스 거부 등을 일으키는 공격 탐지", "pattern\_count": 15, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 건수
* **pattern\_groups** (배열): 패턴 그룹 목록
* **guid** (문자열): 패턴 그룹 GUID
* **name** (문자열): 패턴 그룹 이름
* **description** (문자열): 패턴 그룹 설명
* **pattern\_count** (32비트 정수): 패턴 건수
* **company\_guid** (문자열): 그룹이 속한 회사(테넌트) 식별자
* **company\_name** (문자열): 그룹이 속한 회사(테넌트) 이름
* **user\_guid** (문자열): 패턴 그룹을 생성한 계정의 GUID
* **user\_name** (문자열): 패턴 그룹을 생성한 계정의 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 패턴 그룹 조회

지정한 패턴 그룹을 조회합니다.

#### HTTP 요청

GET /api/sonar/pattern-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups/28ad21b2-585c-4b68-9fad-b78711078496

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 식별자 | 36자 GUID |

#### 정상 응답

{ "pattern\_group": { "guid": "28ad21b2-585c-4b68-9fad-b78711078496", "name": "IPS WAS 취약점 공격 경보", "description": "알려진 WAS의 취약점을 이용하여 원격코드 실행하거나 서비스 거부 등을 일으키는 공격 탐지", "pattern\_count": 15, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **pattern\_group** (맵): 패턴 그룹
* **guid** (문자열): 패턴 그룹 GUID
* **name** (문자열): 패턴 그룹 이름
* **description** (문자열): 패턴 그룹 설명
* **pattern\_count** (32비트 정수): 패턴 건수
* **company\_guid** (문자열): 그룹이 속한 회사(테넌트) 식별자
* **company\_name** (문자열): 그룹이 속한 회사(테넌트) 이름
* **user\_guid** (문자열): 패턴 그룹을 생성한 계정의 GUID
* **user\_name** (문자열): 패턴 그룹을 생성한 계정의 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

패턴 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "pattern\_group": null}

### 패턴 그룹 생성

새 패턴 그룹을 생성합니다.

#### HTTP 요청

POST /api/sonar/pattern-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Webshell" \ -X POST \ https://HOSTNAME/api/sonar/pattern-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 패턴 그룹 식별자 | 36자 GUID. 미설정 시 무작위 생성 |
| name | O | 문자열 | 패턴 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 패턴 그룹 설명 | 최대 50자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

그룹 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated pattern group name: Webshell"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 패턴 그룹 수정

지정한 패턴 그룹을 수정합니다.

#### HTTP 요청

PUT /api/sonar/pattern-groups/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Webshell" \ -d description="Webshell patterns" \ -X PUT \ https://HOSTNAME/api/sonar/pattern-groups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 GUID | 36자 |
| name | O | 문자열 | 패턴 그룹 이름 | 최소 1자, 최대 50자 |
| description | X | 문자열 | 패턴 그룹 설명 | 최대 50자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

그룹이 존재하지 않는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "pattern group not found: c1dfe306-abba-4ed8-862b-0e98e2effcb5"}

그룹 이름이 중복된 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "duplicated pattern group name: Webshell"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 패턴 그룹 일괄 삭제

지정한 패턴 그룹을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/pattern-groups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/pattern-groups?guids=75c80aad-45d5-483a-b771-35bc4609dedc

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 패턴 그룹 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

패턴 그룹이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "pattern-group-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 패턴 목록 조회

지정한 패턴 그룹에 속한 패턴 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/pattern-groups/:guid/patterns

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups/8df64276-a16e-4bae-93cd-c207c8155159/patterns

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 GUID | 36자 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 20건 |
| keywords | X | 문자열 | 검색 키워드 | rule, expr, expr2 대상으로 검색 |

#### 정상 응답

{ "total\_count": 2, "patterns": [ { "id": 112, "expr": "\"passwd\"", "expr2": "path == \"\*passwd\"", "rule": "/etc/passwd", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }, { "id": 113, "expr": "\"authorized\_keys\"", "expr2": "path == \"\*authorized\_keys\"", "rule": "/.ssh/authorized\_keys", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]]

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 패턴 수
* **patterns** (배열): 패턴 목록
* **id** (32비트 정수): 패턴 ID
* **expr** (문자열): 키워드 불린 표현식
* **expr2** (문자열): 검증식. 키워드 매치된 결과에 대하여 필터링 수행
* **rule** (문자열): 패턴명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 패턴 생성

지정한 패턴 그룹에 새 패턴을 추가합니다.

#### HTTP 요청

POST /api/sonar/pattern-groups/:guid/patterns

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d expr="""/.git/HEAD""" \ -d rule="/.git/HEAD file scan" \ -X POST \ https://HOSTNAME/api/sonar/pattern-groups/e93dafa7-6215-4e98-8bfc-1e0a67171bf1/patterns

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 GUID | 36자 |
| expr | O | 문자열 | 키워드 불린 표현식 | 최소 3자, 최대 1000자 |
| expr2 | X | 문자열 | 검증식 | 최대 1000자 |
| rule | O | 문자열 | 패턴명 | 최대 1000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "expr should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'expr' must be less than or equal to 1000 characters."}

키워드 표현식 문법이 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "expr syntax error: not-quoted"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 패턴 수정

지정한 패턴 그룹의 패턴 정보를 수정합니다.

#### HTTP 요청

PUT /api/sonar/pattern-groups/:guid/patterns/:id

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d expr=""/.git/HEAD"" \ -d expr2="path == ""\*/.git/HEAD""" \ -d rule="/.git/HEAD file scan" \ -X PUT \ https://HOSTNAME/api/sonar/pattern-groups/e93dafa7-6215-4e98-8bfc-1e0a67171bf1/patterns/

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 GUID | 36자 |
| expr | O | 문자열 | 키워드 불린 표현식 | 최소 3자, 최대 1000자 |
| expr2 | X | 문자열 | 검증식 | 최대 1000자 |
| rule | O | 문자열 | 패턴명 | 최대 1000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "null-argument", "error\_msg": "expr should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "'expr' must be less than or equal to 1000 characters."}

키워드 표현식 문법이 잘못된 경우

HTTP 상태 코드 400 응답.

{ "error\_code": "invalid-argument", "error\_msg": "expr syntax error: not-quoted"}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 패턴 일괄 삭제

지정한 패턴을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/pattern-groups/:guid/patterns

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/pattern-groups/638cfeb2-e259-46af-961a-1eeb65ea35f0/pattern?ids=10"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 패턴 그룹 GUID | 36자 |
| ids | O | 32비트 정수 목록 | 패턴 ID 목록 | 쉼표(,)로 구분된 ID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

패턴 그룹 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

패턴 식별자가 32비트 정수 목록이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'ids' parameter should be int\_list type"}

패턴이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "6", "reason": "pattern-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 테이블 API

### 테이블 목록 조회

검색 조건과 일치하는 로그프레소 소나의 테이블 목록을 조회합니다.

동일 인스턴스라도 로그프레소 엔터프라이즈에서 생성한 테이블은 로그프레소 소나에 구성 정보가 없으므로 표시되지 않습니다.

#### HTTP 요청

GET /api/sonar/tables

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tables

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 기본값 2147483647 |
| keywords | X | 문자열 | 검색 키워드 | table\_name 대상으로 검색 |
| company\_guid | X | 문자열 | 회사 GUID | 클러스터 관리자의 경우 특정 회사로 결과 한정 |

#### 정상 응답

{ "total\_count": 1, "tables": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "table\_name": "evtx\_system", "layout": "columnar", "compression": "snappy", "retention": 180, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900", "table\_size": 7195337, "index\_size": 0, "ratio": 100 } ]}

* **total\_count** (32비트 정수): 검색 결과와 일치하는 전체 건수
* **tables** (배열): 테이블 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **table\_name** (문자열): 테이블 이름
* **layout** (문자열): 블록 레이아웃
* **compression** (문자열): 압축 알고리즘
* **crypto\_profile\_guid** (문자열): 암호화 프로파일 식별자
* **crypto\_profile\_name** (문자열): 암호화 프로파일 이름
* **min\_day** (문자열): 저장된 최소 로그 날짜 (\_time 필드 기준)
* **max\_day** (문자열): 저장된 최대 로그 날짜 (\_time 필드 기준)
* **table\_size** (64비트 정수): 테이블 데이터 크기 (바이트 단위)
* **index\_size** (64비트 정수): 인덱스 데이터 크기 (바이트 단위)
* **retention** (32비트 정수): 일 단위 데이터 보관 기간
* **ratio** (64비트 실수): 스토리지 사용 비율

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### 테이블 조회

지정한 테이블의 설정 및 상태를 조회합니다.

동일 인스턴스라도 로그프레소 엔터프라이즈에서 생성한 테이블은 로그프레소 소나에 구성 정보가 없으므로 표시되지 않습니다.

#### HTTP 요청

GET /api/sonar/tables/:table

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tables/demo

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| table | O | 문자열 | 테이블 이름 | 대소문자 구분됨. 최소 1자, 최대 50자 |

테이블 이름은 숫자, 영문 대소문자, 밑줄만 사용 가능합니다.

#### 정상 응답

{ "table": { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "table\_name": "evtx\_system", "layout": "columnar", "compression": "snappy", "retention": 180, "table\_size": 7731856, "index\_size": 10645038, "ratio": 100, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900", "shared\_users": [ { "type": "USER", "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "name": "양봉열", "read\_only": true, "created": "2022-09-11 21:57:20+0900" } ], "shared\_groups": [], "node\_stats": [ { "node\_pair\_name": "control", "table\_size": 7731856, "index\_size": 10645038, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900" } ] }}

* **table** (맵): 테이블 구성 정보
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **table\_name** (문자열): 테이블 이름
* **layout** (문자열): 블록 레이아웃
* **compression** (문자열): 압축 알고리즘
* **retention** (32비트 정수): 데이터 보관 일자 수
* **crypto\_profile\_guid** (문자열): 암호화 프로파일 식별자
* **crypto\_profile\_name** (문자열): 암호화 프로파일 이름
* **table\_size** (64비트 정수): 테이블 데이터 크기 (바이트 단위)
* **index\_size** (64비트 정수): 인덱스 데이터 크기 (바이트 단위)
* **ratio** (64비트 실수): 전체 테이블 중 디스크 사용량 비중 (0-1)
* **min\_day** (문자열): 저장된 최소 로그 날짜 (\_time 필드 기준)
* **max\_day** (문자열): 저장된 최대 로그 날짜 (\_time 필드 기준)
* **shared\_users** (배열): 권한 부여된 계정 목록
* **type** (문자열): USER 고정
* **guid** (문자열):
* **shared\_groups** (배열): 권한 부여된 계정 그룹 목록
* **node\_stats** (배열): 노드별 테이블 통계 정보
* **node\_pair\_name** (문자열): 노드 페어 이름
* **table\_size** (64비트 정수): 테이블 데이터 크기
* **index\_size** (64비트 정수): 인덱스 데이터 크기
* **min\_day** (문자열): 저장된 최소 로그 날짜 (\_time 필드 기준)
* **max\_day** (문자열): 저장된 최대 로그 날짜 (\_time 필드 기준)

#### 오류 응답

테이블이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "table": null}

### 테이블 생성

새로운 로그프레소 소나 테이블을 생성합니다. 이 작업은 회사 (테넌트) 관리자 이상의 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/tables

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d table=demo \ -d company\_guid=6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311 \ -X POST \ https://HOSTNAME/api/sonar/tables

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| table | O | 문자열 | 테이블 이름 | 대소문자 구분됨. 최소 1자, 최대 50자 |
| company\_guid | O | 문자열 | 회사 식별자 | 36자 |
| compression | X | 문자열 | 압축 알고리즘 | 기본값 snappy |
| layout | X | 문자열 | 블록 레이아웃 | 기본값 columnar |
| crypto\_profile\_guid | X | 문자열 | 암호화 프로파일 식별자 | 36자 GUID |
| retention | X | 32비트 정수 | 일 단위 보관 주기 | 최소 0 (무제한), 최대 36500. 기본값 0 |

테이블 이름은 숫자, 영문 대소문자, 밑줄만 사용 가능합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "table should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'table' must be shorter than or equal to 50 characters."}

테이블 이름이 규칙을 벗어난 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

압축 알고리즘을 잘못 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'compression' should be one of deflate or snappy."}

블록 레이아웃을 잘못 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'layout' should be one of row or columnar."}

보관기간의 유효 범위를 벗어난 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'retention' must be less than or equal to 36500."}

테이블 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

테이블 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated table name: demo"}

회사가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "company not found: 6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa312"}

암호화 프로파일이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "crypto profile not found: 6f238ab0-7c11-4dc3-9543-ebb3d1cdde12"}

### 테이블 삭제

지정한 테이블을 삭제합니다. 이 작업은 회사 (테넌트) 관리자 이상의 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/tables/:table

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/tables/demo

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| table | O | 문자열 | 테이블 이름 | 대소문자 구분됨. 최소 1자, 최대 50자 |

테이블 이름은 숫자, 영문 대소문자, 밑줄만 사용 가능합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "table should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'table' must be shorter than or equal to 50 characters."}

테이블 이름이 규칙을 벗어난 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

테이블 삭제 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

테이블이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### 테이블 파티션 삭제

지정한 날짜 구간의 테이블 데이터를 삭제합니다. 이 작업은 회사 (테넌트) 관리자 이상의 권한을 요구합니다.

#### HTTP 요청

DELETE /api/sonar/tables/:table/partitions

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE "https://HOSTNAME/api/sonar/tables/demo/partitions?start=2022-01-01&end=2022-12-31"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| table | O | 문자열 | 테이블 이름 | 대소문자 구분됨. 최소 1자, 최대 50자 |
| start | O | 문자열 | 시작 날짜 | yyyy-MM-dd 형식 |
| end | O | 문자열 | 끝 날짜 | 마지막 날짜 포함하여 삭제. yyyy-MM-dd 형식 |

테이블 이름은 숫자, 영문 대소문자, 밑줄만 사용 가능합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "start should be not null"}

날짜 형식이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'end' should be yyyy-MM-dd format."}

시작 날짜가 끝 날짜보다 큰 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "date range is unacceptable."}

테이블 이름이 규칙을 벗어난 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

테이블 파티션 삭제 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

테이블이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### 테이블 보관주기 설정

#### HTTP 요청

PUT /api/sonar/tables/:table/retention

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X PUT \ "https://HOSTNAME/api/sonar/tables/demo/retention?period=180"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| table | O | 문자열 | 테이블 이름 | 대소문자 구분됨. 최소 1자, 최대 50자 |
| period | O | 32비트 정수 | 보관 일수 | 최소 0 (무제한), 최대 36500 |

테이블 이름은 숫자, 영문 대소문자, 밑줄만 사용 가능합니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "period should be not null"}

보관 일수 범위를 벗어난 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be less than or equal to 36500."}

테이블이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### 프로시저 목록

검색 조건과 일치하는 프로시저 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/procedures

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/procedures

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 개수 | 기본값: 0 |
| limit | X | 32비트 정수 | 최대 조회 개수 | 기본값: 모든 프로시저 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명 대상으로 검색 |

#### 정상 응답

{ "total\_count": 1, "procedures": [ { "guid": "5ad13151-dbc1-41c0-92a7-dfeb5f534f4c", "name": "test", "description": null, "parameters": [ { "name": "테이블", "description": "검색 대상 테이블 이름", "type": "string", "key": "table" } ], "query": "system tables | search table == $(\"table\")", "owner\_guid": "13437402-81ed-4b6c-8a6f-7893c7c958b1", "owner\_name": "데모", "owner\_login\_name": "demo", "company\_public": false, "created": "2023-10-03 12:38:13+0900", "updated": "2023-10-03 22:14:28+0900" } ]}

프로시저 목록 조회는 계정 및 그룹 권한 부여 상태를 반환하지 않습니다.

* **total\_count** (32비트 정수): 검색 조건과 일치하는 프로시저 개수
* **procedures** (배열): 프로시저 목록
* **guid** (문자열): 프로시저 식별자
* **name** (문자열): 프로시저 이름
* **description** (문자열): 프로시저 설명
* **parameters** (배열): 매개변수 목록
* **name** (문자열): 매개변수 화면 표시 이름
* **description** (문자열): 매개변수 설명
* **type** (문자열): 매개변수 타입. string, int, double, bool, datetime, date, ip 중 하나.
* **key** (문자열): 매개변수 이름
* **query** (문자열): 쿼리 문자열
* **owner\_guid** (문자열): 소유자 식별자
* **owner\_name** (문자열): 소유자 성명
* **owner\_login\_name** (문자열): 소유자 로그인 계정
* **company\_public** (불리언): 전체 공유 여부
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 프로시저 조회

지정한 프로시저를 조회합니다.

#### HTTP 요청

GET /api/sonar/procedures/:guid

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/procedures/5ad13151-dbc1-41c0-92a7-dfeb5f534f4c

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 프로시저 식별자 | 36자 |

#### 정상 응답

{ "procedure": { "guid": "5ad13151-dbc1-41c0-92a7-dfeb5f534f4c", "name": "test", "description": null, "parameters": [ { "name": "테이블", "description": "검색 대상 테이블 이름", "type": "string", "key": "table" } ], "query": "system tables | search table == $(\"table\")", "owner\_guid": "13437402-81ed-4b6c-8a6f-7893c7c958b1", "owner\_name": "데모", "owner\_login\_name": "demo", "company\_public": false, "granted\_users": [ { "guid": "b5bc3133-b53e-4b61-96b5-8857015ade0d", "name": "demo2", } ], "granted\_groups": [], "created": "2023-10-03 12:38:13+0900", "updated": "2023-10-03 22:15:28+0900" }}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 프로시저 개수
* **procedures** (배열): 프로시저 목록
* **guid** (문자열): 프로시저 식별자
* **name** (문자열): 프로시저 이름
* **description** (문자열): 프로시저 설명
* **parameters** (배열): 매개변수 목록
* **name** (문자열): 매개변수 화면 표시 이름
* **description** (문자열): 매개변수 설명
* **type** (문자열): 매개변수 타입. string, int, double, bool, datetime, date, ip 중 하나.
* **key** (문자열): 매개변수 이름
* **query** (문자열): 쿼리 문자열
* **owner\_guid** (문자열): 소유자 식별자
* **owner\_name** (문자열): 소유자 성명
* **owner\_login\_name** (문자열): 소유자 로그인 계정
* **company\_public** (불리언): 전체 공유 여부
* **granted\_users** (배열):
* **guid** (문자열): 계정 식별자
* **name** (문자열): 계정 이름
* **granted\_groups** (배열):
* **guid** (문자열): 계정 식별자
* **name** (문자열): 계정 이름
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

### 프로시저 생성

새 프로시저를 추가합니다.

#### HTTP 요청

POST /api/sonar/procedures

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d 'query=system tables | search table == $("table")' \ -d 'parameters=[{"type": "string", "name": "테이블", "key": "table"}]' \ -d granted\_user\_guids=b5bc3133-b53e-4b61-96b5-8857015ade0d \ -X POST https://HOSTNAME/api/sonar/procedures

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 프로시저 식별자 | 36자. 미설정 시 무작위 생성 |
| name | O | 문자열 | 프로시저 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 프로시저 설명 | 최대 2,000자 |
| query | O | 문자열 | 쿼리 문자열 |  |
| parameters | X | 객체 배열 | 매개변수 목록 | 객체 배열에 type, key, name, description 포함 |
| company\_public | X | 불리언 | 전체 공유 여부 |  |
| granted\_user\_guids | X | 문자열 배열 | 공유 계정 목록 | 쉼표(,)를 구분자로 하는 계정 GUID 목록 |
| granted\_group\_guids | X | 문자열 배열 | 공유 계정 그룹 목록 | 쉼표(,)를 구분자로 하는 계정 그룹 GUID 목록 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

계정 및 그룹 식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "granted\_user\_guids should be guid type."}

### 프로시저 수정

지정한 프로시저를 수정합니다.

#### HTTP 요청

PUT /api/sonar/procedures/:guid

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d 'query=system tables | search table == $("table")' \ -d 'parameters=[{"type": "string", "name": "테이블", "key": "table"}]' \ -d granted\_user\_guids=b5bc3133-b53e-4b61-96b5-8857015ade0d \ -X PUT https://HOSTNAME/api/sonar/procedures/5ad13151-dbc1-41c0-92a7-dfeb5f534f4c

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 프로시저 식별자 | 36자 |
| name | O | 문자열 | 프로시저 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 프로시저 설명 | 최대 2,000자 |
| query | O | 문자열 | 쿼리 문자열 |  |
| parameters | X | 객체 배열 | 매개변수 목록 | 객체 배열에 type, key, name, description 포함 |
| company\_public | X | 불리언 | 전체 공유 여부 | 기본값: false |
| granted\_user\_guids | X | 문자열 배열 | 공유 계정 목록 | 쉼표(,)를 구분자로 하는 계정 GUID 목록 |
| granted\_group\_guids | X | 문자열 배열 | 공유 계정 그룹 목록 | 쉼표(,)를 구분자로 하는 계정 그룹 GUID 목록 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

계정 및 그룹 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "granted\_user\_guids should be guid type."}

### 프로시저 일괄 삭제

지정한 프로시저를 모두 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/procedures

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids=5ad13151-dbc1-41c0-92a7-dfeb5f534f4c \ -X DELETE https://HOSTNAME/api/sonar/procedures

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 프로시저 식별자 목록 | 쉼표(,)로 구분된 식별자 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

프로시저가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "procedure-not-found" } ]}

관리 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 실시간 탐지 시나리오 API

### 실시간 탐지 시나리오 목록 조회

검색 조건과 일치하는 실시간 탐지 시나리오 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/stream-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명, 쿼리 대상으로 검색 |

#### 정상 응답

아래는 실시간 탐지 시나리오 목록 중 일부입니다.

{ "total\_count": 52, "rules": [ { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "윈도우 방화벽 비활성화", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "윈도우 방화벽 비활성화: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "보안 우회", "schema\_code": "edr-process", "schema\_name": "EDR 프로세스", "logger\_guids": [], "commands": [ { "template\_id": 1, "field\_name": "", "args": {}, "query": "search (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*advfirewall\*\" and lower(cmd\_line) == \"\*off\*\") or (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*firewall\*\" and lower(cmd\_line) == \"\*disable\*\")", "invert": false, "ordinal": 0 } ], "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "cmd\_line, image", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 실시간 탐지 시나리오 갯수
* **rules** (배열): 페이징된 실시간 탐지 시나리오 목록
* **priority** (문자열): LOW, MEDIUM, HIGH 중 하나.
* **guid** (문자열): 실시간 탐지 시나리오 GUID
* **name** (문자열): 실시간 탐지 시나리오 이름
* **description** (문자열): 실시간 탐지 시나리오 설명
* **msg** (문자열): 메시지 템플릿. $field 형식의 매크로를 사용하여 필드 값을 메시지에 반영할 수 있음.
* **enabled** (불리언): 탐지 활성화 여부
* **category\_guid** (문자열): 탐지 시나리오 분류 GUID
* **category\_name** (문자열): 탐지 시나리오 분류 이름
* **schema\_code** (문자열): 정규화 스키마 식별자
* **schema\_name** (문자열): 정규화 스키마 이름
* **logger\_guids** (배열): 수집기 GUID 목록
* **commands** (배열): 실시간 탐지 시나리오 명령어 목록
* **template\_id** (32비트 정수): 실시간 탐지 시나리오 명령어 템플릿 ID
* **field\_name** (문자열): 대상 필드 이름
* **args** (맵): 인자 키/값 쌍
* **query** (문자열): 인자가 반영된 쿼리 문자열
* **invert** (불리언): true인 경우 NOT 조건
* **ordinal** (32비트 정수): 순서
* **address\_group\_guid** (문자열): 주소 그룹 GUID
* **address\_field** (문자열): 주소 그룹에 등록할 대상 필드
* **ticket\_repo\_guid** (문자열): 티켓 분류 GUID
* **ticket\_assignee\_guid** (문자열): 티켓 할당자 GUID
* **ticket\_assignee\_name** (문자열): 티켓 할당자 성명
* **ticket\_suppress\_interval** (32비트 정수): 중복 티켓 축약 기간 (초 단위)
* **event\_suppress\_interval** (32비트 정수): 중복 이벤트 제거 기간 (초 단위)
* **suppress\_key** (문자열): 중복 기준 필드. $field 형식으로 지정된 매크로를 해당 필드 값으로 대체하여 이벤트 컨텍스트 키로 사용함.
* **keep\_alive** (불리언): true인 경우 축약 타이머 유지. false인 경우 축약 타이머 초기화.
* 축약 타이머 유지 시 티켓을 완료 처리하더라도 만료 시간에 도달할 때까지 이벤트가 기존 티켓에 병합됩니다.
* **audit\_category\_guid** (문자열): 소명 분류 GUID
* **audit\_category\_name** (문자열): 소명 분류 이름
* **auditor\_guid** (문자열): 소명 확인 계정의 GUID. 미지정 시 부서장 전결.
* **auditor\_name** (문자열): 소명 확인 계정의 성명. 미지정 시 부서장 전결.
* **audit\_days** (32비트 정수): 소명 제출 마감 시한 (일 단위)
* **employee\_key\_field** (문자열): 사번 필드 이름. 통상 정규화된 필드인 emp\_key를 사용함.
* **alarm\_group\_guid** (문자열): 알람 그룹 GUID
* **alarm\_group\_name** (문자열): 알람 그룹 이름
* **field\_order** (문자열): 근거 자료 출력 시 필드 순서. 쉼표로 구분된 필드 이름 목록.
* **company\_guid** (문자열): 시나리오가 속한 회사 (테넌트) GUID
* **company\_name** (문자열): 시나리오가 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 시나리오를 생성한 사용자 GUID
* **user\_name** (문자열): 시나리오를 생성한 사용자 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 실시간 탐지 시나리오 조회

지정한 실시간 탐지 시나리오를 조회합니다.

#### HTTP 요청

GET /api/sonar/stream-rules/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rules/3b05608f-8dd0-4218-9d6d-391515b6280d

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |

#### 정상 응답

{ "rule": { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "윈도우 방화벽 비활성화", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "윈도우 방화벽 비활성화: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "보안 우회", "schema\_code": "edr-process", "schema\_name": "EDR 프로세스", "logger\_guids": [], "commands": [ { "template\_id": 1, "field\_name": "", "args": {}, "query": "search (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*advfirewall\*\" and lower(cmd\_line) == \"\*off\*\") or (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*firewall\*\" and lower(cmd\_line) == \"\*disable\*\")", "invert": false, "ordinal": 0 } ], "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "cmd\_line, image", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" }}

* **rule** (맵): 실시간 탐지 시나리오
* **priority** (문자열): LOW, MEDIUM, HIGH 중 하나.
* **guid** (문자열): 실시간 탐지 시나리오 GUID
* **name** (문자열): 실시간 탐지 시나리오 이름
* **description** (문자열): 실시간 탐지 시나리오 설명
* **msg** (문자열): 메시지 템플릿. $field 형식의 매크로를 사용하여 필드 값을 메시지에 반영할 수 있음.
* **enabled** (불리언): 탐지 활성화 여부
* **category\_guid** (문자열): 탐지 시나리오 분류 GUID
* **category\_name** (문자열): 탐지 시나리오 분류 이름
* **schema\_code** (문자열): 정규화 스키마 식별자
* **schema\_name** (문자열): 정규화 스키마 이름
* **logger\_guids** (배열): 수집기 GUID 목록
* **commands** (배열): 실시간 탐지 시나리오 명령어 목록
* **template\_id** (32비트 정수): 실시간 탐지 시나리오 명령어 템플릿 ID
* **field\_name** (문자열): 대상 필드 이름
* **args** (맵): 인자 키/값 쌍
* **query** (문자열): 인자가 반영된 쿼리 문자열
* **invert** (불리언): true인 경우 NOT 조건
* **ordinal** (32비트 정수): 순서
* **address\_group\_guid** (문자열): 주소 그룹 GUID
* **address\_field** (문자열): 주소 그룹에 등록할 대상 필드
* **ticket\_repo\_guid** (문자열): 티켓 분류 GUID
* **ticket\_assignee\_guid** (문자열): 티켓 할당자 GUID
* **ticket\_assignee\_name** (문자열): 티켓 할당자 성명
* **ticket\_suppress\_interval** (32비트 정수): 중복 티켓 축약 기간 (초 단위)
* **event\_suppress\_interval** (32비트 정수): 중복 이벤트 제거 기간 (초 단위)
* **suppress\_key** (문자열): 중복 기준 필드. $field 형식으로 지정된 매크로를 해당 필드 값으로 대체하여 이벤트 컨텍스트 키로 사용함.
* **keep\_alive** (불리언): true인 경우 축약 타이머 유지. false인 경우 축약 타이머 초기화.
* 축약 타이머 유지 시 티켓을 완료 처리하더라도 만료 시간에 도달할 때까지 이벤트가 기존 티켓에 병합됩니다.
* **audit\_category\_guid** (문자열): 소명 분류 GUID
* **audit\_category\_name** (문자열): 소명 분류 이름
* **auditor\_guid** (문자열): 소명 확인 계정의 GUID. 미지정 시 부서장 전결.
* **auditor\_name** (문자열): 소명 확인 계정의 성명. 미지정 시 부서장 전결.
* **audit\_days** (32비트 정수): 소명 제출 마감 시한 (일 단위)
* **employee\_key\_field** (문자열): 사번 필드 이름. 통상 정규화된 필드인 emp\_key를 사용함.
* **alarm\_group\_guid** (문자열): 알람 그룹 GUID
* **alarm\_group\_name** (문자열): 알람 그룹 이름
* **field\_order** (문자열): 근거 자료 출력 시 필드 순서. 쉼표로 구분된 필드 이름 목록.
* **company\_guid** (문자열): 시나리오가 속한 회사 (테넌트) GUID
* **company\_name** (문자열): 시나리오가 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 시나리오를 생성한 사용자 GUID
* **user\_name** (문자열): 시나리오를 생성한 사용자 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

지정한 시나리오가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "rule": null}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### 실시간 탐지 시나리오 생성

새 실시간 탐지 시나리오를 생성합니다.

#### HTTP 요청

POST /api/sonar/stream-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="HIGH" \ -d name="알려진 봇넷 대역 접속" \ -d msg="알려진 봇넷 대역 접속: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나 |
| guid | X | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |
| name | O | 문자열 | 실시간 탐지 시나리오 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 실시간 탐지 시나리오 설명 | 최대 2,000자 |
| msg | O | 문자열 | 메시지 템플릿 | 최소 1자, 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | true 혹은 false |
| category\_guid | X | 문자열 | 시나리오 분류 GUID | 36자 |
| schema\_code | O | 문자열 | 정규화 스키마 식별자 | 최소 1자, 최대 50자 |
| logger\_guids | O | 배열 | 수집기 GUID 목록 |  |
| commands | O | 배열 | 실시간 탐지 명령어 목록 | 1개 이상의 명령어 필요. 하단 설명 참조 |
| address\_group\_guid | X | 문자열 | 주소 그룹 GUID | 36자 |
| address\_field | X | 문자열 | 주소 필드 | 주소 그룹에 등록할 필드 이름. 최대 50자 |
| ticket\_repo\_guid | X | 문자열 | 티켓 분류 GUID | 미설정 시 티켓 발생하지 않음. 36자 |
| ticket\_assignee\_guid | X | 문자열 | 티켓 할당자 GUID | 지정 시 담당자 자동 할당 |
| ticket\_suppress\_interval | X | 32비트 정수 | 중복 티켓 축약 기간 | 초 단위. 0 또는 미설정 시 동일 티켓을 병합하지 않음 |
| event\_suppress\_interval | X | 32비트 정수 | 중복 이벤트 제거 기간 | 초 단위. 0 또는 미설정 시 중복 이벤트를 제거하지 않음 |
| suppress\_key | X | 문자열 | 중복 기준 필드 | $field 형식으로 매크로 사용 가능. 최대 2,000자 |
| keep\_alive | X | 불리언 | 축약 타이머 유지 여부 | 축약 타이머 유지 시 true, 초기화 시 false |
| audit\_category\_guid | X | 문자열 | 소명 분류 GUID | 미설정 시 자동 소명 요청이 비활성화됨. 36자 |
| auditor\_guid | X | 문자열 | 소명 확인 계정 GUID | 미설정 시 부서장 전결. 36자 |
| audit\_days | X | 32비트 정수 | 소명 제출 마감 시한 | 최소 1일, 최대 365일 |
| employee\_key\_field | X | 문자열 | 사번 필드 이름 | 미설정 시 자동 소명 요청이 비활성화됨. 최대 50자 |
| alarm\_group\_guid | X | 문자열 | 알람 그룹 GUID | 36자 |
| field\_order | X | 문자열 | 근거 자료 필드 출력 순서 | 최대 2,000자 |

commands의 각 배열 요소는 아래와 같이 정의합니다:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| template\_id | O | 32비트 정수 | 실시간 탐지 명령어 템플릿 ID |  |
| query | O | 문자열 | 부분 쿼리 문자열 |  |
| field\_name | X | 문자열 | 대상 필드 이름 |  |
| args | X | 맵 | 인자 키/값 |  |
| invert | X | 불리언 | 반전 여부 |  |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

잘못된 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

실시간 탐지 명령어 목록이 유효한 JSON 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

정규화 스키마가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

시나리오 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 실시간 탐지 시나리오 수정

지정한 실시간 탐지 시나리오를 수정합니다.

#### HTTP 요청

PUT /api/sonar/stream-rules/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="MEDIUM" \ -d name="알려진 봇넷 대역 접속" \ -d msg="알려진 봇넷 대역 접속: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" -X PUT \ https://HOSTNAME/api/sonar/stream-rules/5a6b63f0-87d5-49c4-a5a1-94da4141b2f5

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나 |
| guid | O | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |
| name | O | 문자열 | 실시간 탐지 시나리오 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 실시간 탐지 시나리오 설명 | 최대 2,000자 |
| msg | O | 문자열 | 메시지 템플릿 | 최소 1자, 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | true 혹은 false |
| category\_guid | X | 문자열 | 시나리오 분류 GUID | 36자 |
| schema\_code | O | 문자열 | 정규화 스키마 식별자 | 최소 1자, 최대 50자 |
| logger\_guids | O | 배열 | 수집기 GUID 목록 |  |
| commands | O | 배열 | 실시간 탐지 명령어 목록 | 1개 이상의 명령어 필요. 하단 설명 참조 |
| address\_group\_guid | X | 문자열 | 주소 그룹 GUID | 36자 |
| address\_field | X | 문자열 | 주소 필드 | 주소 그룹에 등록할 필드 이름. 최대 50자 |
| ticket\_repo\_guid | X | 문자열 | 티켓 분류 GUID | 미설정 시 티켓 발생하지 않음. 36자 |
| ticket\_assignee\_guid | X | 문자열 | 티켓 할당자 GUID | 지정 시 담당자 자동 할당 |
| ticket\_suppress\_interval | X | 32비트 정수 | 중복 티켓 축약 기간 | 초 단위. 0 또는 미설정 시 동일 티켓을 병합하지 않음 |
| event\_suppress\_interval | X | 32비트 정수 | 중복 이벤트 제거 기간 | 초 단위. 0 또는 미설정 시 중복 이벤트를 제거하지 않음 |
| suppress\_key | X | 문자열 | 중복 기준 필드 | $field 형식으로 매크로 사용 가능. 최대 2,000자 |
| keep\_alive | X | 불리언 | 축약 타이머 유지 여부 | 축약 타이머 유지 시 true, 초기화 시 false |
| audit\_category\_guid | X | 문자열 | 소명 분류 GUID | 미설정 시 자동 소명 요청이 비활성화됨. 36자 |
| auditor\_guid | X | 문자열 | 소명 확인 계정 GUID | 미설정 시 부서장 전결. 36자 |
| audit\_days | X | 32비트 정수 | 소명 제출 마감 시한 | 최소 1일, 최대 365일 |
| employee\_key\_field | X | 문자열 | 사번 필드 이름 | 미설정 시 자동 소명 요청이 비활성화됨. 최대 50자 |
| alarm\_group\_guid | X | 문자열 | 알람 그룹 GUID | 36자 |
| field\_order | X | 문자열 | 근거 자료 필드 출력 순서 | 최대 2,000자 |

commands의 각 배열 요소는 아래와 같이 정의합니다:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| template\_id | O | 32비트 정수 | 실시간 탐지 명령어 템플릿 ID |  |
| query | O | 문자열 | 부분 쿼리 문자열 |  |
| field\_name | X | 문자열 | 대상 필드 이름 |  |
| args | X | 맵 | 인자 키/값 |  |
| invert | X | 불리언 | 반전 여부 |  |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

잘못된 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

실시간 탐지 명령어 목록이 유효한 JSON 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 9071a6fe-6b91-4448-9761-7123381cb026"}

정규화 스키마가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

시나리오 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 실시간 탐지 시나리오 일괄 삭제

지정한 실시간 탐지 시나리오를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/stream-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/stream-rules?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 실시간 탐지 시나리오 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

시나리오가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "stream-rule-not-found" } ]}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### 실시간 탐지 시나리오 활성화

지정한 실시간 탐지 시나리오를 활성화합니다.

#### HTTP 요청

POST /api/sonar/stream-rules/:guid/enable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules/4f2fe6ea-7c96-4529-88db-2ddf09ce1fa2/enable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

이미 시나리오가 활성화된 상태인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "stream rule is already enabled: 64bf7657-6f0c-4c14-b0b2-d455263d9205"}

시나리오 활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 실시간 탐지 시나리오 비활성화

지정한 실시간 탐지 시나리오를 비활성화합니다.

#### HTTP 요청

POST /api/sonar/stream-rules/:guid/disable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules/4f2fe6ea-7c96-4529-88db-2ddf09ce1fa2/disable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 실시간 탐지 시나리오 GUID | 36자 |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

이미 시나리오가 비활성화된 상태인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "stream rule is already disabled: 64bf7657-6f0c-4c14-b0b2-d455263d9205"}

시나리오 비활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 실시간 탐지 명령어 템플릿 목록 조회

모든 실시간 탐지 명령어 템플릿 목록을 조회합니다.

실시간 탐지 명령어 템플릿은 GUI 방식의 실시간 탐지 시나리오 편집을 지원하는 용도로 사용합니다.

#### HTTP 요청

GET /api/sonar/stream-rule-command-templates

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rule-command-templates

#### 정상 응답

아래는 전체 실시간 탐지 명령어 템플릿 목록 중 일부입니다.

{ "templates": [ { "id": 2, "name": "IP 주소 일치", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "ip", "type": "string", "subtype": "ip", "display\_name": "비교 IP", "description": "비교 대상 IP를 입력합니다." } ], "query": "search $field$ == ip($ip$)", "query2": "search $field$ != ip($ip$)" }, { "id": 3, "name": "IP 주소가 네트워크 대역에 포함", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "subnet", "type": "string", "subtype": "subnet", "display\_name": "비교 네트워크 대역", "description": "비교 대상 네트워크 그룹을 선택합니다." } ], "query": "matchnet field=$field$ guid=$subnet$ verify=f", "query2": "matchnet invert=t field=$field$ guid=$subnet$ verify=f" } ]}

* **templates** (배열): 모든 실시간 탐지 명령어 템플릿 목록
* **id** (32비트 정수): 템플릿 고유 식별자
* **name** (문자열): 템플릿 이름
* **field\_type** (문자열): 적용 대상 필드 유형. DATE, IP, PORT, STRING, SHORT, INT, LONG, MD5, URL 중 하나.
* **description** (문자열): 템플릿 설명
* **config\_specs** (배열): 템플릿 변수 명세 목록
* **name** (문자열): 변수 이름
* **type** (문자열): 변수 타입. string, number, array
* **subtype** (문자열): UI 렌더링 힌트. ip, date, country, port\_group 등 자동완성 및 유효성 검사를 지원하는 컴포넌트 선택을 지원하는 용도.
* **display\_name** (문자열): 로케일 적용된 변수 이름
* **description** (문자열): 로케일 적용된 변수 설명
* **query** (문자열): AND 조건에서 적용할 쿼리 문자열
* **query2** (문자열): NOT 조건에서 적용할 쿼리 문자열

### 실시간 탐지 명령어 템플릿 조회

지정한 실시간 탐지 명령어 템플릿을 조회합니다.

실시간 탐지 명령어 템플릿은 GUI 방식의 실시간 탐지 시나리오 편집을 지원하는 용도로 사용합니다.

#### HTTP 요청

GET /api/sonar/stream-rule-command-templates/:id

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rule-command-templates/2

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| id | O | 32비트 정수 | 템플릿 ID |  |

#### 정상 응답

{ "template": { "id": 2, "name": "IP 주소 일치", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "ip", "type": "string", "subtype": "ip", "display\_name": "비교 IP", "description": "비교 대상 IP를 입력합니다." } ], "query": "search $field$ == ip($ip$)", "query2": "search $field$ != ip($ip$)" }}

* **template** (맵): 시간 탐지 명령어 템플릿
* **id** (32비트 정수): 템플릿 고유 식별자
* **name** (문자열): 템플릿 이름
* **field\_type** (문자열): 적용 대상 필드 유형. DATE, IP, PORT, STRING, SHORT, INT, LONG, MD5, URL 중 하나.
* **description** (문자열): 템플릿 설명
* **config\_specs** (배열): 템플릿 변수 명세 목록
* **name** (문자열): 변수 이름
* **type** (문자열): 변수 타입. string, number, array
* **subtype** (문자열): UI 렌더링 힌트. ip, date, country, port\_group 등 자동완성 및 유효성 검사를 지원하는 컴포넌트 선택을 지원하는 용도.
* **display\_name** (문자열): 로케일 적용된 변수 이름
* **description** (문자열): 로케일 적용된 변수 설명
* **query** (문자열): AND 조건에서 적용할 쿼리 문자열
* **query2** (문자열): NOT 조건에서 적용할 쿼리 문자열

#### 오류 응답

id가 정수가 아닌 경우

{ "error\_code": "invalid-argument", "error\_msg": "'id' parameter should be int type"}

## 배치 탐지 시나리오 API

### 배치 탐지 시나리오 목록 조회

검색 조건과 일치하는 배치 탐지 시나리오 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/batch-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명, 쿼리 대상으로 검색 |

#### 정상 응답

아래는 배치 탐지 시나리오 목록 중 일부입니다.

{ "total\_count": 1, "rules": [ { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": null, "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 배치 탐지 시나리오 갯수
* **rules** (배열): 페이징된 배치 탐지 시나리오 목록
* **priority** (문자열): LOW, MEDIUM, HIGH 중 하나.
* **guid** (문자열): 배치 탐지 시나리오 GUID
* **name** (문자열): 배치 탐지 시나리오 이름
* **description** (문자열): 배치 탐지 시나리오 설명
* **msg** (문자열): 메시지 템플릿. $field 형식의 매크로를 사용하여 필드 값을 메시지에 반영할 수 있음.
* **enabled** (불리언): 탐지 활성화 여부
* **category\_guid** (문자열): 탐지 시나리오 분류 GUID
* **category\_name** (문자열): 탐지 시나리오 분류 이름
* **schedule** (문자열): 실행 주기. CRON 일정 문법 사용
* **duration** (32비트 정수): 분석 대상 기간 (초). 설정 값은 쿼리의 from, to 매개변수로 전달됩니다.
* **datetrunc** (32비트 정수): 시간 절사 단위 (초). from, to 쿼리 매개변수의 시간 절사.
* **dataset\_guid** (문자열): 데이터셋 GUID
* **dataset\_name** (문자열): 데이터셋 이름
* **address\_group\_guid** (문자열): 주소 그룹 GUID
* **address\_field** (문자열): 주소 그룹에 등록할 대상 필드
* **ticket\_repo\_guid** (문자열): 티켓 분류 GUID
* **ticket\_assignee\_guid** (문자열): 티켓 할당자 GUID
* **ticket\_assignee\_name** (문자열): 티켓 할당자 성명
* **ticket\_suppress\_interval** (32비트 정수): 중복 티켓 축약 기간 (초 단위)
* **event\_suppress\_interval** (32비트 정수): 중복 이벤트 제거 기간 (초 단위)
* **suppress\_key** (문자열): 중복 기준 필드. $field 형식으로 지정된 매크로를 해당 필드 값으로 대체하여 이벤트 컨텍스트 키로 사용함.
* **keep\_alive** (불리언): true인 경우 축약 타이머 유지. false인 경우 축약 타이머 초기화.
* 축약 타이머 유지 시 티켓을 완료 처리하더라도 만료 시간에 도달할 때까지 이벤트가 기존 티켓에 병합됩니다.
* **audit\_category\_guid** (문자열): 소명 분류 GUID
* **audit\_category\_name** (문자열): 소명 분류 이름
* **auditor\_guid** (문자열): 소명 확인 계정의 GUID. 미지정 시 부서장 전결.
* **auditor\_name** (문자열): 소명 확인 계정의 성명. 미지정 시 부서장 전결.
* **audit\_days** (32비트 정수): 소명 제출 마감 시한 (일 단위)
* **employee\_key\_field** (문자열): 사번 필드 이름. 통상 정규화된 필드인 emp\_key를 사용함.
* **alarm\_group\_guid** (문자열): 알람 그룹 GUID
* **alarm\_group\_name** (문자열): 알람 그룹 이름
* **field\_order** (문자열): 근거 자료 출력 시 필드 순서. 쉼표로 구분된 필드 이름 목록.
* **company\_guid** (문자열): 시나리오가 속한 회사 (테넌트) GUID
* **company\_name** (문자열): 시나리오가 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 시나리오를 생성한 사용자 GUID
* **user\_name** (문자열): 시나리오를 생성한 사용자 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### 배치 탐지 시나리오 조회

지정한 배치 탐지 시나리오를 조회합니다.

#### HTTP 요청

GET /api/sonar/batch-rules/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules/f4ca02c8-0679-49e7-8c10-76667c26b595

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 배치 탐지 시나리오 GUID | 36자 |

#### 정상 응답

아래는 배치 탐지 시나리오 목록 중 일부입니다.

{ "rule": { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" }}

* **rule** (맵): 배치 탐지 시나리오
* **priority** (문자열): LOW, MEDIUM, HIGH 중 하나.
* **guid** (문자열): 배치 탐지 시나리오 GUID
* **name** (문자열): 배치 탐지 시나리오 이름
* **description** (문자열): 배치 탐지 시나리오 설명
* **msg** (문자열): 메시지 템플릿. $field 형식의 매크로를 사용하여 필드 값을 메시지에 반영할 수 있음.
* **enabled** (불리언): 탐지 활성화 여부
* **category\_guid** (문자열): 탐지 시나리오 분류 GUID
* **category\_name** (문자열): 탐지 시나리오 분류 이름
* **schedule** (문자열): 실행 주기. CRON 일정 문법 사용
* **duration** (32비트 정수): 분석 대상 기간 (초). 설정 값은 쿼리의 from, to 매개변수로 전달됩니다.
* **datetrunc** (32비트 정수): 시간 절사 단위 (초). from, to 쿼리 매개변수의 시간 절사.
* **dataset\_guid** (문자열): 데이터셋 GUID
* **dataset\_name** (문자열): 데이터셋 이름
* **address\_group\_guid** (문자열): 주소 그룹 GUID
* **address\_field** (문자열): 주소 그룹에 등록할 대상 필드
* **ticket\_repo\_guid** (문자열): 티켓 분류 GUID
* **ticket\_assignee\_guid** (문자열): 티켓 할당자 GUID
* **ticket\_assignee\_name** (문자열): 티켓 할당자 성명
* **ticket\_suppress\_interval** (32비트 정수): 중복 티켓 축약 기간 (초 단위)
* **event\_suppress\_interval** (32비트 정수): 중복 이벤트 제거 기간 (초 단위)
* **suppress\_key** (문자열): 중복 기준 필드. $field 형식으로 지정된 매크로를 해당 필드 값으로 대체하여 이벤트 컨텍스트 키로 사용함.
* **keep\_alive** (불리언): true인 경우 축약 타이머 유지. false인 경우 축약 타이머 초기화.
* 축약 타이머 유지 시 티켓을 완료 처리하더라도 만료 시간에 도달할 때까지 이벤트가 기존 티켓에 병합됩니다.
* **audit\_category\_guid** (문자열): 소명 분류 GUID
* **audit\_category\_name** (문자열): 소명 분류 이름
* **auditor\_guid** (문자열): 소명 확인 계정의 GUID. 미지정 시 부서장 전결.
* **auditor\_name** (문자열): 소명 확인 계정의 성명. 미지정 시 부서장 전결.
* **audit\_days** (32비트 정수): 소명 제출 마감 시한 (일 단위)
* **employee\_key\_field** (문자열): 사번 필드 이름. 통상 정규화된 필드인 emp\_key를 사용함.
* **alarm\_group\_guid** (문자열): 알람 그룹 GUID
* **alarm\_group\_name** (문자열): 알람 그룹 이름
* **field\_order** (문자열): 근거 자료 출력 시 필드 순서. 쉼표로 구분된 필드 이름 목록.
* **company\_guid** (문자열): 시나리오가 속한 회사 (테넌트) GUID
* **company\_name** (문자열): 시나리오가 속한 회사 (테넌트) 이름
* **user\_guid** (문자열): 시나리오를 생성한 사용자 GUID
* **user\_name** (문자열): 시나리오를 생성한 사용자 성명
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

지정한 시나리오가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "rule": null}

식별자가 GUID 형식이 아닌 경우

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### 배치 탐지 시나리오 생성

새 배치 탐지 시나리오를 생성합니다.

#### HTTP 요청

POST /api/sonar/batch-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="웹 취약점 스캔" \ -d schedule="\*/30 \* \* \* \*" -d msg="웹 취약점 스캔: $dst\_ip" \ -d query="table duration=30m weblog | search status >= 400 | stats count as error\_count, dc(path) as page\_count, values(concat(method, " ", path)) as request by src\_ip | eval request = strjoin("\n", request) | lof eps=0.1 error\_count, page\_count | search \_lof > 1.5 | sort -\_lof" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나 |
| guid | X | 문자열 | 배치 탐지 시나리오 GUID | 36자 |
| name | O | 문자열 | 배치 탐지 시나리오 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 배치 탐지 시나리오 설명 | 최대 2,000자 |
| msg | O | 문자열 | 메시지 템플릿 | 최소 1자, 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | true 혹은 false |
| category\_guid | X | 문자열 | 시나리오 분류 GUID | 36자 |
| schedule | O | 문자열 | 실행 주기 | CRON 일정 문법 사용 |
| duration | X | 32비트 정수 | 분석 대상 기간 | 초 단위로 지정. 최대 31536000초 (365일) |
| datetrunc | X | 32비트 정수 | 시간 절사 | 1, 60, 3600, 86400 중 하나 (초 단위) |
| dataset\_guid | X | 문자열 | 데이터셋 GUID | dataset\_guid와 query 중 하나는 필수 입력. 36자 |
| query | X | 문자열 | 탐지 쿼리 | dataset\_guid와 query 중 하나는 필수 입력. 최대 65535자 |
| address\_group\_guid | X | 문자열 | 주소 그룹 GUID | 36자 |
| address\_field | X | 문자열 | 주소 필드 | 주소 그룹에 등록할 필드 이름. 최대 50자 |
| ticket\_repo\_guid | X | 문자열 | 티켓 분류 GUID | 미설정 시 티켓 발생하지 않음. 36자 |
| ticket\_assignee\_guid | X | 문자열 | 티켓 할당자 GUID | 지정 시 담당자 자동 할당 |
| ticket\_suppress\_interval | X | 32비트 정수 | 중복 티켓 축약 기간 | 초 단위. 0 또는 미설정 시 동일 티켓을 병합하지 않음 |
| event\_suppress\_interval | X | 32비트 정수 | 중복 이벤트 제거 기간 | 초 단위. 0 또는 미설정 시 중복 이벤트를 제거하지 않음 |
| suppress\_key | X | 문자열 | 중복 기준 필드 | $field 형식으로 매크로 사용 가능. 최대 2,000자 |
| keep\_alive | X | 불리언 | 축약 타이머 유지 여부 | 축약 타이머 유지 시 true, 초기화 시 false |
| audit\_category\_guid | X | 문자열 | 소명 분류 GUID | 미설정 시 자동 소명 요청이 비활성화됨. 36자 |
| auditor\_guid | X | 문자열 | 소명 확인 계정 GUID | 미설정 시 부서장 전결. 36자 |
| audit\_days | X | 32비트 정수 | 소명 제출 마감 시한 | 최소 1일, 최대 365일 |
| employee\_key\_field | X | 문자열 | 사번 필드 이름 | 미설정 시 자동 소명 요청이 비활성화됨. 최대 50자 |
| alarm\_group\_guid | X | 문자열 | 알람 그룹 GUID | 36자 |
| field\_order | X | 문자열 | 근거 자료 필드 출력 순서 | 최대 2,000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "schedule should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'address\_field' must be shorter than or equal to 50 characters."}

잘못된 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

일정 CRON 문법이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "schedule has wrong cron expression format: \* \* \* \* \* \*"}

데이터셋과 쿼리 모두 지정하지 않은 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "query should be not null"}

시간 절사 값이 유효하지 않은 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "datetrunc should be one of 1 (1 second), 60 (1 minute), 3600 (1 hour), 86400 (1 day)."}

시나리오 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 배치 탐지 시나리오 수정

지정한 배치 탐지 시나리오를 수정합니다.

#### HTTP 요청

PUT /api/sonar/batch-rules/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="웹 취약점 스캔" \ -d schedule="\*/10 \* \* \* \*" -d msg="웹 취약점 스캔: $dst\_ip" \ -d query="table duration=30m weblog | search status >= 400 | stats count as error\_count, dc(path) as page\_count, values(concat(method, " ", path)) as request by src\_ip | eval request = strjoin("\n", request) | lof eps=0.1 error\_count, page\_count | search \_lof > 1.5 | sort -\_lof" \ -X PUT \ https://HOSTNAME/api/sonar/batch-rules/410fe6af-b2f8-4674-af70-8d5b12ddc3fe

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나 |
| guid | O | 문자열 | 배치 탐지 시나리오 GUID | 36자 |
| name | O | 문자열 | 배치 탐지 시나리오 이름 | 최소 1자, 최대 255자 |
| description | X | 문자열 | 배치 탐지 시나리오 설명 | 최대 2,000자 |
| msg | O | 문자열 | 메시지 템플릿 | 최소 1자, 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | true 혹은 false |
| category\_guid | X | 문자열 | 시나리오 분류 GUID | 36자 |
| schedule | O | 문자열 | 실행 주기 | CRON 일정 문법 사용 |
| duration | X | 32비트 정수 | 분석 대상 기간 | 초 단위로 지정. 최대 31536000초 (365일) |
| datetrunc | X | 32비트 정수 | 시간 절사 | 1, 60, 3600, 86400 중 하나 (초 단위) |
| dataset\_guid | X | 문자열 | 데이터셋 GUID | dataset\_guid와 query 중 하나는 필수 입력. 36자 |
| query | X | 문자열 | 탐지 쿼리 | dataset\_guid와 query 중 하나는 필수 입력. 최대 65535자 |
| address\_group\_guid | X | 문자열 | 주소 그룹 GUID | 36자 |
| address\_field | X | 문자열 | 주소 필드 | 주소 그룹에 등록할 필드 이름. 최대 50자 |
| ticket\_repo\_guid | X | 문자열 | 티켓 분류 GUID | 미설정 시 티켓 발생하지 않음. 36자 |
| ticket\_assignee\_guid | X | 문자열 | 티켓 할당자 GUID | 지정 시 담당자 자동 할당 |
| ticket\_suppress\_interval | X | 32비트 정수 | 중복 티켓 축약 기간 | 초 단위. 0 또는 미설정 시 동일 티켓을 병합하지 않음 |
| event\_suppress\_interval | X | 32비트 정수 | 중복 이벤트 제거 기간 | 초 단위. 0 또는 미설정 시 중복 이벤트를 제거하지 않음 |
| suppress\_key | X | 문자열 | 중복 기준 필드 | $field 형식으로 매크로 사용 가능. 최대 2,000자 |
| keep\_alive | X | 불리언 | 축약 타이머 유지 여부 | 축약 타이머 유지 시 true, 초기화 시 false |
| audit\_category\_guid | X | 문자열 | 소명 분류 GUID | 미설정 시 자동 소명 요청이 비활성화됨. 36자 |
| auditor\_guid | X | 문자열 | 소명 확인 계정 GUID | 미설정 시 부서장 전결. 36자 |
| audit\_days | X | 32비트 정수 | 소명 제출 마감 시한 | 최소 1일, 최대 365일 |
| employee\_key\_field | X | 문자열 | 사번 필드 이름 | 미설정 시 자동 소명 요청이 비활성화됨. 최대 50자 |
| alarm\_group\_guid | X | 문자열 | 알람 그룹 GUID | 36자 |
| field\_order | X | 문자열 | 근거 자료 필드 출력 순서 | 최대 2,000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "schedule should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'address\_field' must be shorter than or equal to 50 characters."}

잘못된 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

일정 CRON 문법이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "schedule has wrong cron expression format: \* \* \* \* \* \*"}

데이터셋과 쿼리 모두 지정하지 않은 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "query should be not null"}

시간 절사 값이 유효하지 않은 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "datetrunc should be one of 1 (1 second), 60 (1 minute), 3600 (1 hour), 86400 (1 day)."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 9071a6fe-6b91-4448-9761-7123381cb026"}

시나리오 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 배치 탐지 시나리오 일괄 삭제

지정한 배치 탐지 시나리오를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/batch-rules

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/batch-rules?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 배치 탐지 시나리오 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

시나리오가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "batch-rule-not-found" } ]}

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### 배치 탐지 시나리오 실행

지정한 배치 탐지 시나리오를 즉시 실행합니다. 시스템은 배치 탐지 시나리오 쿼리를 비동기적으로 실행하므로 쿼리 완료를 대기하지 않고 응답합니다. 아래의 경우에는 실행하더라도 이벤트나 티켓이 발생하지 않습니다:

* 배치 시나리오가 비활성화된 경우
* 쿼리 실행 중에 배치 시나리오가 삭제된 경우

#### HTTP 요청

POST /api/sonar/batch-rules/:guid/run

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/run

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 배치 탐지 시나리오 GUID | 36자 |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

### 배치 탐지 시나리오 활성화

지정한 배치 탐지 시나리오를 활성화합니다.

#### HTTP 요청

POST /api/sonar/batch-rules/:guid/enable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/enable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 배치 탐지 시나리오 GUID | 36자 |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

이미 시나리오가 활성화된 상태인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule is already enabled: c4ca4744-f310-4480-baa8-0548067abfb3""}

시나리오 활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 배치 탐지 시나리오 비활성화

지정한 배치 탐지 시나리오를 비활성화합니다.

#### HTTP 요청

POST /api/sonar/batch-rules/:guid/disable

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/disable

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 배치 탐지 시나리오 GUID | 36자 |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

시나리오가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

이미 시나리오가 비활성화된 상태인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "batch rule is already disabled: c4ca4744-f310-4480-baa8-0548067abfb3""}

시나리오 활성화 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 티켓 API

### 티켓 목록 조회

검색 조건과 일치하는 티켓 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/tickets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 최소 0, 최대 1000. 미지정 시 1000 |
| from | X | 날짜 | 시작 일시 | yyyy-MM-dd HH:mm:ssZ 형식. 범위에 시작 일시 포함 |
| to | X | 날짜 | 끝 일시 | yyyy-MM-dd HH:mm:ssZ 형식. 범위에 끝 일시 포함 |
| statuses | X | 문자열 목록 | 상태 | 쉼표(,)로 구분. 하단 상태 코드 참조 |
| keywords | X | 문자열 | 검색 키워드 |  |
| priorities | X | 32비트 정수 목록 | 중요도 목록 | 상 (3), 중 (2), 하 (1). 다중 선택 시 쉼표(,)로 구분 |
| assignees | X | 문자열 목록 | 할당자 목록 | 쉼표(,)로 구분된 계정 GUID 목록 |
| approvers | X | 문자열 목록 | 결재자 목록 | 쉼표(,)로 구분된 계정 GUID 목록 |
| sort\_type | X | 문자열 | 정렬 유형 | ASC, DESC 중 하나 |
| sort\_column | X | 문자열 | 정렬 기준 | id, created\_at, updated\_at, closed\_at 중 하나 |

**티켓 상태 코드**

* 신규 (NEW)
* 할당 (ASSIGNED)
* 처리중 (IN\_PROGRESS)
* 결재중 (SUBMITTED)
* 승인 (APPROVED)
* 반려 (REJECTED)
* 완료 (CLOSED)

#### 정상 응답

{ "total": 15, "tickets": [ { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "위협분석", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "웹 서버 설정 수집 시도: 20.0.31.172", "priority": "LOW", "status": "ASSIGNED", "format": "JSON", "count": 7, "attack": true, "incident": false, "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "구동언", "task\_type": "ASSIGNEE", "task\_status": "ASSIGNED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "approvers": [], "created": "2022-09-14 17:34:19+0900", "updated": "2022-09-14 23:55:29+0900", "closed": null, "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* (32비트 정수) total
* (배열) tickets
* **id** (32비트 정수): 티켓 ID
* **repo\_guid** (문자열): 티켓 유형 식별자
* **repo\_name** (문자열): 티켓 유형 이름
* **site\_guid** (문자열): 사이트 식별자
* **site\_name** (문자열): 사이트 이름
* **guid** (문자열): 티켓 식별자
* **title** (문자열): 제목
* **priority** (문자열): 중요도. 상 (HIGH), 중 (MEDIUM), 하 (LOW) 중 하나.
* **status** (문자열): 상태. 신규 (NEW), 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 결재중 (SUBMITTED), 승인 (APPROVED), 반려 (REJECTED), 완료 (CLOSED) 중 하나.
* **format** (문자열): 티켓 형식. JSON, MARKDOWN, PLAIN 중 하나. 위협 탐지 티켓은 JSON 형식으로 정보 기록.
* **count** (32비트 정수): 중복 축약 건수.
* **attack** (불리언): 분석 후 기록한 정탐 여부. 탐지 자체가 정확하다면 true로 기록함.
* **incident** (불리언): 분석 후 기록한 사고 발생 여부. 엔드포인트 감염 발생 등 즉각적 대응이 필요한 상황인 경우 true로 기록함.
* **assignees** (배열): 티켓 할당자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 할당자 계정 식별자
* **user\_name** (문자열): 할당자 성명
* **task\_type** (문자열): ASSIGNEE 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 완료 (CLOSED) 중 하나.
* **x\_login** (문자열): 할당자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 할당자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 할당자 계정 삭제 시 기록되는 부서 이름
* **approvers** (배열): 티켓 결재자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 결재자 계정 식별자
* **user\_name** (문자열): 결재자 성명
* **task\_type** (문자열): APPROVER 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 승인 (ASSIGNED), 반려 (REJECTED) 중 하나.
* **x\_login** (문자열): 결재자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 결재자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 결재자 계정 삭제 시 기록되는 부서 이름
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식
* **closed** (문자열): 완료일시. yyyy-MM-dd HH:mm:ssZ 형식
* **x\_login** (문자열): 티켓 작성 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 티켓 작성 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 티켓 작성 계정 삭제 시 기록되는 부서 이름
* **x\_site** (문자열): 사이트 삭제 시 기록되는 사이트 이름

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

from, to 날짜 포맷이 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'from' parameter should be date format (yyyy-MM-dd HH:mm:ss+0000)"}

정의되지 않은 상태 코드를 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'statuses' should contain elements that is one of NEW, ASSIGNED, IN\_PROGRESS, SUBMITTED, APPROVED, REJECTED, CLOSED."}

정의되지 않은 중요도 값을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "element of priorities should be one of 1 (LOW), 2 (MEDIUM), 3 (HIGH). input is 4"}

정의되지 않은 정렬 유형을 사용한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "sort\_type should be one of ASC or DESC. input is NONE"}

허용되지 않은 정렬 컬럼을 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "sort\_column should be one of id, created\_at, updated\_at, closed\_at."}

assignees, approvers 목록의 값이 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "assignees should contains only guid values."}

### 티켓 조회

지정한 티켓을 조회합니다.

#### HTTP 요청

GET /api/sonar/tickets/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/49272877-75f2-4c2f-9301-d21c4f9a106d

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{ "ticket": { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "위협분석", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "웹 서버 설정 수집 시도: 20.0.31.172", "priority": "LOW", "status": "APPROVED", "format": "JSON", "rule\_guid": "ad4b9871-d5f0-4a8b-a341-8ac0afcdcddf", "rule\_type": "STREAM", "rule\_name": "웹 서버 설정 수집 시도", "count": 7, "content": "{\"first\_seen\":\"2022-09-14 17:34:19+0900\",\"last\_seen\":\"2022-09-14 23:55:29+0900\",\"priority\":\"LOW\",\"rule\_type\":\"STREAM\",\"rule\_id\":27,\"src\_ip\":\"20.0.31.172\",\"src\_port\":null,\"dst\_ip\":null,\"dst\_port\":null,\"protocol\":null,\"action\":null,\"count\":1,\"msg\":\"웹 서버 설정 수집 시도: 20.0.31.172\",\"user\":null,\"host\_ip\":null,\"mail\_from\":null,\"mail\_to\":null,\"mail\_cc\":null,\"logger\_id\":28,\"logger\_name\":\"ko.logpresso.com \",\"field\_order\":\"\_time, src\_ip, src\_port, dst\_ip, dst\_port, status, method, path, query, user\_agent\",\"url\":null,\"md5\":null,\"src\_asn\":\"AS8075 Microsoft Corporation\",\"src\_country\":\"US\",\"src\_city\":null,\"src\_lat\":37.750999450683594,\"src\_lng\":-97.8219985961914}", "attack": true, "incident": false, "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "구동언", "task\_type": "ASSIGNEE", "task\_status": "CLOSED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "approvers": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "task\_type": "APPROVER", "task\_status": "APPROVED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "attachments": [ { "guid": "d4390b7a-7d64-4a24-bd3e-af74b4f3c204", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "ticket\_guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "file\_name": "3bc31b3d-bc25-4be5-8dae-d3cb1831da02.png", "file\_size": 124118 } ], "created": "2022-09-14 17:34:19+0900", "updated": "2022-09-14 23:55:29+0900", "closed": null, "x\_login": null, "x\_user": null, "x\_dept": null, "comments": [ { "guid": "b66a31b5-db94-478b-8751-194b5ee5f358", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "type": "TEXT", "format": "MARKDOWN", "content": "\* 방화벽에서 IP 차단함", "created": "2022-09-14 23:57:34+0900", "updated": "2022-09-14 23:57:34+0900", "x\_login": null, "x\_user": null, "x\_dept": null } ] }}

* (맵) ticket
* **id** (32비트 정수): 티켓 ID
* **repo\_guid** (문자열): 티켓 유형 식별자
* **repo\_name** (문자열): 티켓 유형 이름
* **site\_guid** (문자열): 사이트 식별자
* **site\_name** (문자열): 사이트 이름
* **guid** (문자열): 티켓 식별자
* **title** (문자열): 제목
* **priority** (문자열): 중요도. 상 (HIGH), 중 (MEDIUM), 하 (LOW) 중 하나.
* **status** (문자열): 상태. 신규 (NEW), 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 결재중 (SUBMITTED), 승인 (APPROVED), 반려 (REJECTED), 완료 (CLOSED) 중 하나.
* **format** (문자열): 티켓 형식. JSON, MARKDOWN, PLAIN 중 하나. 위협 탐지 티켓은 JSON 형식으로 정보 기록.
* **rule\_guid** (문자열): 탐지 시나리오 식별자
* **rule\_type** (문자열): 탐지 시나리오 유형. STREAM, BATCH 중 하나.
* **rule\_name** (문자열): 탐지 시나리오 이름
* **count** (32비트 정수): 중복 축약 건수.
* **content** (문자열): 티켓 데이터. 위협 탐지 티켓은 이벤트 필드가 JSON 형식으로 기록됨.
* **attack** (불리언): 분석 후 기록한 정탐 여부. 탐지 자체가 정확하다면 true로 기록함.
* **incident** (불리언): 분석 후 기록한 사고 발생 여부. 엔드포인트 감염 발생 등 즉각적 대응이 필요한 상황인 경우 true로 기록함.
* **assignees** (배열): 티켓 할당자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 할당자 계정 식별자
* **user\_name** (문자열): 할당자 성명
* **task\_type** (문자열): ASSIGNEE 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 완료 (CLOSED) 중 하나.
* **x\_login** (문자열): 할당자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 할당자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 할당자 계정 삭제 시 기록되는 부서 이름
* **approvers** (배열): 티켓 결재자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 결재자 계정 식별자
* **user\_name** (문자열): 결재자 성명
* **task\_type** (문자열): APPROVER 고정.
* **task\_status** (문자열): 할당 (ASSIGNED), 승인 (ASSIGNED), 반려 (REJECTED) 중 하나.
* **x\_login** (문자열): 결재자 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 결재자 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 결재자 계정 삭제 시 기록되는 부서 이름
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식
* **closed** (문자열): 완료일시. yyyy-MM-dd HH:mm:ssZ 형식
* **x\_login** (문자열): 티켓 작성 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 티켓 작성 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 티켓 작성 계정 삭제 시 기록되는 부서 이름
* **x\_site** (문자열): 사이트 삭제 시 기록되는 사이트 이름
* **comments** (배열): 티켓 메모 목록
* **guid** (문자열): 티켓 메모 식별자
* **user\_guid** (문자열): 티켓 작성자 식별자
* **user\_name** (문자열): 티켓 작성자 성명
* **type** (문자열): TEXT 고정.
* **format** (문자열): 마크다운 (MARKDOWN), 일반 텍스트 (PLAIN) 중 하나.
* **content** (문자열): 메모 내용
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식
* **x\_login** (문자열): 메모 작성 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 메모 작성 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 메모 작성 계정 삭제 시 기록되는 부서 이름

#### 오류 응답

티켓이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "ticket": null}

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### 티켓 생성

새 티켓을 생성합니다.

#### HTTP 요청

POST /api/sonar/tickets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d repo\_guid=5f0ba741-7551-400d-8bd6-1f14a6e8536d \ -d guid=638cfeb2-e259-46af-961a-1eeb65ea35f0 \ -d priority=LOW \ -d title="웹 서버 설정 수집 시도" \ -d format=JSON \ --data-urlencode content="{""first\_seen"":""2022-09-20 14:55:54+0900"",""last\_seen"":""2022-09-20 14:55:54+0900"",""priority"":""LOW"",""src\_ip"":""3.83.23.230"",""dst\_ip"":""13.125.82.152"",""dst\_port"":443}" \ -X POST \ https://HOSTNAME/api/sonar/tickets

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| repo\_guid | O | 문자열 | 티켓 분류 GUID | 36자 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나. |
| title | O | 문자열 | 제목 | 최소 1자, 최대 255자 |
| format | O | 문자열 | 내용 형식 | JSON, MARKDOWN, PLAIN 중 하나. |
| content | O | 문자열 | 내용 | 최소 1자, 최대 100000자 |
| assignees | X | 문자열 목록 | 담당자 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |
| approvers | X | 문자열 목록 | 결재자 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |
| attachments | X | 문자열 목록 | 첨부파일 GUID 목록 | 여러 개의 GUID는 쉼표(,)로 구분 |

첨부파일은 이미 업로드 된 파일 객체를 참조하므로 티켓이 생성되기 전에 존재할 수 있습니다. 참조되지 않는 티켓 파일 객체는 매일 자정에 자동으로 파기됩니다.

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "repo\_guid should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

유효하지 않은 중요도를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

유효하지 않은 형식을 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of 'JSON', 'MARKDOWN', 'PLAIN'."}

내용이 JSON 형식이 아닌 경우

내용 형식(format)을 JSON으로 지정한 경우, 내용(content)이 JSON 형식이 아니면 오류가 발생합니다.

{ "error\_code": "invalid-argument", "error\_msg": "content should be JSON format - Expected a ',' or '}' at character 146"}

담당자, 결재자 목록이 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "assignees should be guid type."}

티켓 GUID가 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated ticket guid: 638cfeb2-e259-46af-961a-1eeb65ea35f0"}

담당자, 결재자가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "assignee not found: fae7fa2b-756e-4d3d-b314-e631daf70c7a"}

첨부 파일이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "attachment not found: 8e904789-b9b9-443a-b1a1-86a36119c74c"}

### 티켓 수정

지정한 티켓을 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority=HIGH \ -d title="웹 서버 설정 수집 시도" \ -d format=JSON \ --data-urlencode content="{""first\_seen"":""2022-09-20 14:55:54+0900"",""last\_seen"":""2022-09-20 19:44:24+0900"",""priority"":""HIGH"",""src\_ip"":""3.83.23.230"",""dst\_ip"":""13.125.82.152"",""dst\_port"":443}" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/638cfeb2-e259-46af-961a-1eeb65ea35f0

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나. |
| title | O | 문자열 | 제목 | 최소 1자, 최대 255자 |
| format | O | 문자열 | 내용 형식 | JSON, MARKDOWN, PLAIN 중 하나. |
| content | O | 문자열 | 내용 | 최소 1자, 최대 100000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "title should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

유효하지 않은 중요도를 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

유효하지 않은 형식을 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of 'JSON', 'MARKDOWN', 'PLAIN'."}

내용이 JSON 형식이 아닌 경우

내용 형식(format)을 JSON으로 지정한 경우, 내용(content)이 JSON 형식이 아니면 오류가 발생합니다.

{ "error\_code": "invalid-argument", "error\_msg": "content should be JSON format - Expected a ',' or '}' at character 146"}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 638cfeb2-e259-46af-961a-1eeb65ea35f1"}

시스템이 생성한 티켓을 수정하는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "cannot update system ticket: 638cfeb2-e259-46af-961a-1eeb65ea35f1"}

### 티켓 일괄 삭제

지정한 티켓을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/tickets

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/tickets?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 목록 | 티켓 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

티켓이 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "ticket-not-found" } ]}

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### 티켓 중요도 수정

지정한 티켓의 중요도를 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/priority

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority=HIGH \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/priority

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| priority | O | 문자열 | 중요도 | LOW, MEDIUM, HIGH 중 하나. |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "priority should be not null"}

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 제목 수정

지정한 티켓의 제목을 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/title

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d title="Updated title" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/title

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| title | O | 문자열 | 제목 | 최소 1자, 최대 255자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "title should be not null"}

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 정오탐 수정

지정한 티켓의 정오탐 여부를 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/attack

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d attack=true \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/attack

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| attack | X | 불리언 | 정오탐 여부 | 미지정 시 null |

#### 정상 응답

{}

#### 오류 응답

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 사고 여부 수정

지정한 티켓의 사고 여부를 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/incident

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d incident=true \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/incident

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| incident | X | 불리언 | 사고 여부 | 미지정 시 null |

#### 정상 응답

{}

#### 오류 응답

티켓 식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 태그 수정

지정한 티켓의 태그를 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/tags

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority=HIGH \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/priority

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| tags | O | 문자열 목록 | 태그 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{}

### 티켓 담당자 할당

특정 티켓의 처리나 결재를 지정한 사용자에게 할당합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/assign

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d type=ASSIGNEE \ -d assignees=fae7fa2b-756e-4d3d-b314-e631daf70c7d \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/assign

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 GUID |
| type | O | 문자열 | 할당 유형 | ASSIGNEE, APPROVER 중 하나 |
| assignees | O | 문자열 목록 | 계정 GUID 목록 | 쉼표(,)로 구분된 GUID 목록 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 담당자 목록 조회

특정 티켓에 할당된 담당자 또는 결재자 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/tickets/:guid/assignees

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/tickets/c63ff706-85bc-44e3-9acd-24a0628da1fb/assignees?type=APPROVER"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| type | O | 문자열 | 할당 유형 | ASSIGNEE, APPROVER 중 하나 |

#### 정상 응답

{ "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "task\_type": "APPROVER", "task\_status": "APPROVED", "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* **assignees** (배열): 담당자 혹은 결재자 목록
* **company\_guid** (문자열): 회사 (테넌트) 식별자
* **company\_name** (문자열): 회사 (테넌트) 이름
* **user\_guid** (문자열): 담당자 혹은 결재자 식별자
* **user\_name** (문자열): 담당자 혹은 결재자 성명
* **task\_type** (문자열): ASSIGNEE 또는 APPROVER
* **task\_status** (문자열): 티켓 작업 처리 상태
* 담당자인 경우 할당 (ASSIGNED), 처리중 (IN\_PROGRESS), 완료 (CLOSED) 중 하나.
* 결재자인 경우 할당 (ASSIGNED), 승인 (ASSIGNED), 반려 (REJECTED) 중 하나.
* **x\_login** (문자열): 계정 삭제 시 기록되는 로그인 계정 이름
* **x\_user** (문자열): 계정 삭제 시 기록되는 사용자 성명
* **x\_dept** (문자열): 계정 삭제 시 기록되는 부서 이름

### 티켓 담당자 상태 변경

처리 혹은 결재를 할당받은 티켓에 대해 현재 작업 상태를 변경합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:guid/assignee-status

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d type=ASSIGNEE \ -d status=IN\_PROGRESS \ -X PUT \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/assignee-status

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |
| type | O | 문자열 | 할당 유형 | ASSIGNEE, APPROVER 중 하나 |
| status | O | 문자열 | 작업 상태 | 담당자는 ASSIGNED, IN\_PROGRESS, CLOSED. 결재자는 APPROVED, REJECTED 중 하나. |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

유효하지 않은 담당자 상태의 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "assignee status should be one of ASSIGNED, IN\_PROGRESS, CLOSED."}

유효하지 않은 결재자 상태의 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "approver status should be one of APPROVED, REJECTED."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

티켓을 할당받지 않은 경우

{ "error\_code": "illegal-state", "error\_msg": "not assigned"}

결재 요청되지 않은 티켓을 승인, 반려한 경우

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: 511ce7fe-36bd-45d8-a868-99a5349c3575"}

### 티켓 완료 처리

지정한 티켓을 완료 상태로 전환합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/close

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/close

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 다시 열기

지정한 티켓을 신규 또는 할당 상태로 다시 전환합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/reopen

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/reopen

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 결재 요청

작업이 완료된 티켓에 대해 승인을 요청합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/submit

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/submit

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답. 일반 계정은 티켓 분류에 대한 접근 권한을 부여받지 않으면 할당받은 상태라도 티켓을 조회할 수 없습니다.

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

결재자가 지정되지 않은 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-approvers"}

티켓 담당자가 아닌 경우

HTTP 상태 코드 500 응답. 할당된 담당자의 세션에서만 작업 완료 후 승인을 요청할 수 있습니다.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

작업이 완료되지 않은 경우

HTTP 상태 코드 500 응답. 할당된 모든 담당자의 작업이 완료 상태로 전환되어야 승인을 요청할 수 있습니다.

{ "error\_code": "illegal-state", "error\_msg": "not-completed"}

### 티켓 결재 승인

결재 요청을 받은 티켓을 승인합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/approve

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/approve

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

결재자로 지정되지 않은 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

결재 요청되지 않은 티켓인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: c63ff706-85bc-44e3-9acd-24a0628da1fb"}

### 티켓 결재 반려

결재 요청을 받은 티켓을 반려합니다.

#### HTTP 요청

POST /api/sonar/tickets/:guid/reject

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/reject

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

결재자로 지정되지 않은 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

결재 요청되지 않은 티켓인 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: c63ff706-85bc-44e3-9acd-24a0628da1fb"}

### 티켓 첨부 파일 목록 조회

#### HTTP 요청

GET /api/sonar/tickets/:guid/attachments

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/8de3c683-a793-4bde-bf41-657396d17ef5/attachments

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 GUID | 36자 |

#### 정상 응답

{ "attachments": [ { "guid": "75624e2d-dc78-4a21-974b-78c2281dc089", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "ticket\_guid": "8de3c683-a793-4bde-bf41-657396d17ef5", "file\_name": "66c7e112-edc9-4b11-b332-5a0581a24211.png", "file\_size": 124109 } ]}

* **attachments** (배열): 첨부 파일 목록
* **guid** (문자열): 첨부 파일 식별자
* **user\_guid** (문자열): 계정 식별자
* **ticket\_guid** (문자열): 티켓 식별자
* **file\_name** (문자열): 파일 이름
* **file\_size** (64비트 정수): 파일 크기

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

### 티켓 첨부 파일 삭제

지정한 티켓 첨부 파일을 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/tickets/:ticket\_guid/attachments/:file\_guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/tickets/8de3c683-a793-4bde-bf41-657396d17ef5/attachments/75624e2d-dc78-4a21-974b-78c2281dc089

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| ticket\_guid | O | 문자열 | 티켓 GUID | 36자 |
| file\_guid | O | 문자열 | 파일 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "ticket\_guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

첨부 파일이 존재하지 않는 경우

{ "error\_code": "illegal-state", "error\_msg": "ticket attachment not found: 75624e2d-dc78-4a21-974b-78c2281dc089"}

### 티켓 메모 목록 조회

지정한 티켓의 메모 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/tickets/:guid/comments

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/49272877-75f2-4c2f-9301-d21c4f9a106c/comments

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 티켓 식별자 | 36자 |
| output\_html | X | 불리언 | HTML 출력 여부 | 미지정 시 텍스트 원문 |

#### 정상 응답

{ "comments": [ { "guid": "b66a31b5-db94-478b-8751-194b5ee5f358", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "양봉열", "type": "TEXT", "format": "MARKDOWN", "content": "\* 방화벽에서 IP 차단함", "created": "2022-09-14 17:52:20+0900", "updated": "2022-09-14 17:52:20+0900", "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* (배열) comments
* **guid** (문자열): 티켓 메모 식별자
* **user\_guid** (문자열): 작성자 식별자
* **user\_name** (문자열): 작성자 성명
* **type** (문자열): TEXT 고정. 메모 유형 확장 시 사용됩니다.
* **format** (문자열): PLAIN, MARKDOWN 중 하나. JSON은 예약된 값입니다.
* **content** (문자열): 메모 내용. output\_html 옵션을 true로 설정한 경우 마크다운 텍스트를 HTML 형식으로 변환하여 출력합니다.
* **created** (문자열): 생성일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **updated** (문자열): 수정일시. yyyy-MM-dd HH:mm:ssZ 형식.
* **x\_login** (문자열): 로그인 계정 이름. 작성자 계정 삭제 시 기록됩니다.
* **x\_user** (문자열): 사용자 성명. 작성자 계정 삭제 시 기록됩니다.
* **x\_dept** (문자열): 부서 이름. 작성자 계정이 삭제 시 기록됩니다.

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

### 티켓 메모 추가

지정한 티켓에 메모를 추가합니다.

#### HTTP 요청

POST /api/sonar/tickets/:ticket\_guid/comments

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d format=MARKDOWN \ -d content="\* 방화벽에서 IP 차단 완료" \ -X POST \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| ticket\_guid | O | 문자열 | 티켓 GUID | 36자 |
| guid | X | 문자열 | 메모 GUID | 36자 |
| format | O | 문자열 | 내용 형식 | JSON, MARKDOWN, PLAIN 중 하나. |
| content | O | 문자열 | 내용 |  |

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

유효하지 않은 형식을 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of PLAIN, MARKDOWN, JSON."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 티켓 메모 수정

지정한 티켓의 메모를 수정합니다.

#### HTTP 요청

PUT /api/sonar/tickets/:ticket\_guid/comments/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d format=MARKDOWN \ -d content="\* DDoS에서 IP 차단 완료" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments/08ee89f1-630f-4b24-b6b2-e0c88c5f3003

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| ticket\_guid | O | 문자열 | 티켓 GUID | 36자 |
| guid | O | 문자열 | 메모 GUID | 36자 |
| format | O | 문자열 | 내용 형식 | JSON, MARKDOWN, PLAIN 중 하나. |
| content | O | 문자열 | 내용 |  |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

유효하지 않은 형식을 지정한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of PLAIN, MARKDOWN, JSON."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

메모가 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket comment not found: 08ee89f1-630f-4b24-b6b2-e0c88c5f3002"}

### 티켓 메모 삭제

지정한 티켓의 메모를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/tickets/:ticket\_guid/comments/:guid

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments/08ee89f1-630f-4b24-b6b2-e0c88c5f3003

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| ticket\_guid | O | 문자열 | 티켓 GUID | 36자 |
| guid | O | 문자열 | 메모 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

티켓이 존재하지 않는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### 소명 템플릿 목록 조회

현재 세션이 속한 테넌트의 모든 소명 템플릿 설정을 조회합니다.

#### HTTP 요청

GET /api/sonar/push-templates

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/push-templates

#### 정상 응답

{ "templates": { "sms\_explain\_req\_msg": "$category 건에 대한 소명 요청이 메일로 발송되었습니다. 기한: $expire\_date", "sms\_explain\_review\_req\_msg": "$emp\_name $emp\_title 소명 검토 요청이 메일로 발송되었습니다. 기한: $expire\_date" }}

* **templates** (맵): 템플릿 설정 키/값 쌍

|  |  |
| --- | --- |
| 설정 키 | 설명 |
| explanation\_domain | 소명 제출 도메인. https://DOMAIN 형태 |
| mail\_explain\_req\_subject | 소명 요청 메일의 제목 |
| mail\_explain\_req\_body | 소명 요청 메일의 본문 |
| mail\_explain\_review\_req\_subject | 소명 검토 요청 메일의 제목 |
| mail\_explain\_review\_req\_body | 소명 검토 요청 메일의 본문 |
| sms\_explain\_req\_msg | 소명 요청 알림 SMS |
| sms\_explain\_review\_req\_msg | 소명 검토 요청 SMS |

* 각 템플릿에는 아래의 매크로를 사용할 수 있습니다:

|  |  |
| --- | --- |
| 매크로 | 설명 |
| $category | 분류 |
| $emp\_key | 소명자 사번 |
| $emp\_name | 소명자 성명 |
| $emp\_title | 소명자 직급 |
| $url | 소명 제출 URL |
| $expire\_date | 소명 제출 마감일 (yyyy-MM-dd) |
| $expire\_time | 소명 제출 마감시각 (HH:mm:ss) |
| $user\_note | 수동 소명 요청 시 설명 |

### 소명 템플릿 조회

현재 세션이 속한 테넌트의 특정 소명 템플릿 설정을 조회합니다.

#### HTTP 요청

GET /api/sonar/push-templates/:type

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/push-templates/sms\_explain\_req\_msg

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| type | O | 문자열 | 템플릿 유형 | 하단 표 참조 |

템플릿 유형은 아래의 키를 사용할 수 있습니다:

|  |  |
| --- | --- |
| 템플릿 유형 | 설명 |
| explanation\_domain | 소명 제출 도메인. https://DOMAIN 형태 |
| mail\_explain\_req\_subject | 소명 요청 메일의 제목 |
| mail\_explain\_req\_body | 소명 요청 메일의 본문 |
| mail\_explain\_review\_req\_subject | 소명 검토 요청 메일의 제목 |
| mail\_explain\_review\_req\_body | 소명 검토 요청 메일의 본문 |
| sms\_explain\_req\_msg | 소명 요청 알림 SMS |
| sms\_explain\_review\_req\_msg | 소명 검토 요청 SMS |

#### 정상 응답

{ "template": "$category 건에 대한 소명 요청이 메일로 발송되었습니다. 기한: $expire\_date"}

* **template** (문자열): 템플릿 내용
* 템플릿 내용에는 아래의 매크로를 사용할 수 있습니다:

|  |  |
| --- | --- |
| 매크로 | 설명 |
| $category | 분류 |
| $emp\_key | 소명자 사번 |
| $emp\_name | 소명자 성명 |
| $emp\_title | 소명자 직급 |
| $url | 소명 제출 URL |
| $expire\_date | 소명 제출 마감일 (yyyy-MM-dd) |
| $expire\_time | 소명 제출 마감시각 (HH:mm:ss) |
| $user\_note | 수동 소명 요청 시 설명 |

#### 오류 응답

지원하지 않는 템플릿 유형인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "type should be one of explanation\_domain, mail\_explain\_req\_subject, mail\_explain\_req\_body, mail\_explain\_review\_req\_subject, mail\_explain\_review\_req\_body, sms\_explain\_req\_msg, sms\_explain\_review\_req\_msg."}

### 소명 템플릿 설정

현재 세션이 속한 테넌트의 특정 소명 템플릿을 설정합니다.

#### HTTP 요청

POST /api/sonar/push-templates/:type

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d template="$emp\_name $emp\_title님, 메일함에서 소명 요청을 확인해주세요." \ -X POST \ https://HOSTNAME/api/sonar/push-templates/sms\_explain\_req\_msg

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| type | O | 문자열 | 템플릿 유형 | 하단 표 참조 |
| template | X | 문자열 | 템플릿 내용 | 최대 16MB, 미지정 시 null 초기화 |

템플릿 유형은 아래의 키를 사용할 수 있습니다:

|  |  |
| --- | --- |
| 템플릿 유형 | 설명 |
| explanation\_domain | 소명 제출 도메인. https://DOMAIN 형태 |
| mail\_explain\_req\_subject | 소명 요청 메일의 제목 |
| mail\_explain\_req\_body | 소명 요청 메일의 본문 |
| mail\_explain\_review\_req\_subject | 소명 검토 요청 메일의 제목 |
| mail\_explain\_review\_req\_body | 소명 검토 요청 메일의 본문 |
| sms\_explain\_req\_msg | 소명 요청 알림 SMS |
| sms\_explain\_review\_req\_msg | 소명 검토 요청 SMS |

템플릿 내용에는 아래의 매크로를 사용할 수 있습니다:

|  |  |
| --- | --- |
| 매크로 | 설명 |
| $category | 분류 |
| $emp\_key | 소명자 사번 |
| $emp\_name | 소명자 성명 |
| $emp\_title | 소명자 직급 |
| $url | 소명 제출 URL |
| $expire\_date | 소명 제출 마감일 (yyyy-MM-dd) |
| $expire\_time | 소명 제출 마감시각 (HH:mm:ss) |
| $user\_note | 수동 소명 요청 시 설명 |

#### 정상 응답

{}

#### 오류 응답

지원하지 않는 템플릿 유형인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "type should be one of explanation\_domain, mail\_explain\_req\_subject, mail\_explain\_req\_body, mail\_explain\_review\_req\_subject, mail\_explain\_review\_req\_body, sms\_explain\_req\_msg, sms\_explain\_review\_req\_msg."}

설정 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 예약된 쿼리 API

### 예약된 쿼리 목록 조회

검색 조건과 일치하는 예약된 쿼리 목록을 조회합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

GET /api/sonar/scheduled-queries

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/scheduled-queries

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너 뛸 갯수 | 기본값: 0 |
| limit | X | 32비트 정수 | 최대 조회 갯수 | 기본값: 모든 예약된 쿼리 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명, 쿼리 스트링 대상으로 검색 |

#### 정상 응답

아래는 예약된 쿼리 목록 중 일부입니다.

{ "total\_count": 15, "scheduled\_queries": [ { "guid": "95e17283-1d08-44f0-bac7-b734813d2dcd", "name": "test", "description": "", "enabled": false, "node\_types": null, "query": "json \"{}\"", "output\_parameter": false, "trigger\_type": "cron", "cron\_schedule": "\* \* \* \* \*", "preceding\_guid": null, "preceding\_name": null, "preceding\_action": null, "running\_state": null, "result\_state": null, "elapsed\_time": null, "last\_run\_time": null, "last\_failure\_time": null, "last\_failure\_reason": null, "created": "2023-09-18 16:12:44+0900", "updated": "2023-09-18 16:12:44+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 예약된 쿼리의 갯수
* **scheduled\_queries** (배열): 페이징된 예약된 쿼리 목록
* **guid** (문자열): 예약된 쿼리의 GUID
* **name** (문자열): 이름
* **description** (문자열): 설명
* **enabled** (불리언): 활성화 여부
* **node\_types** (배열): 실행 위치(control: 분석 서버, data: 수집 서버)
* **query** (문자열): 쿼리문
* **output\_parameter** (불리언): 쿼리 매개변수 출력 제어 여부
* **trigger\_type** (문자열): 실행 방식(cron: 예약 실행, workflow: 다른 쿼리의 결과에 따라 실행)
* **cron\_schedule** (문자열): (trigger\_type이 cron일 때) CRON 문법으로 작성된 실행 일정
* **preceding\_guid** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 GUID
* **preceding\_name** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 이름
* **preceding\_action** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 실행 결과(succeeded: 성공, failed: 실패, finished: 실행 완료)
* **elapsed\_time** (32비트 정수): 실행 시간(단위: 밀리초)
* **running\_state** (문자열): 실행 상태(running: 실행 중, stopping: 중지하는 중, finished: 완료, canceled: 취소됨)
* **result\_state** (문자열): 실행 결과(succeeded: 성공, failed: 실패, , canceled: 취소)
* **last\_run\_time** (문자열): 최근 실행 시각 (yyyy-MM-dd HH:mm:ssZ 형식)
* **last\_failure\_time** (문자열): 최근 실패 시각 (yyyy-MM-dd HH:mm:ssZ 형식)
* **last\_failure\_reason** (문자열): 쿼리 실행에 실패한 원인
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 조회

지정한 예약된 쿼리를 조회합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

GET /api/sonar/scheduled-queries/:guid

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/scheduled-queries/95e17283-1d08-44f0-bac7-b734813d2dcd

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 예약된 쿼리 GUID |  |

#### 정상 응답

{ "scheduled\_query": { "guid": "95e17283-1d08-44f0-bac7-b734813d2dcd", "name": "test", "description": "", "enabled": false, "node\_types": ["control", "data"], "query": "json \"{}\"", "output\_parameter": false, "trigger\_type": "cron", "cron\_schedule": "\* \* \* \* \*", "preceding\_guid": null, "preceding\_name": null, "preceding\_action": null, "running\_state": null, "result\_state": null, "elapsed\_time": null, "last\_run\_time": null, "last\_failure\_time": null, "last\_failure\_reason": null, "created": "2023-09-18 16:12:44+0900", "updated": "2023-09-18 16:12:44+0900" }}

* **scheduled\_query** (맵): 예약된 쿼리
* **guid** (문자열): 예약된 쿼리의 GUID
* **name** (문자열): 이름
* **description** (문자열): 설명
* **enabled** (불리언): 활성화 여부
* **node\_types** (배열): 실행 위치(control: 분석 서버, data: 수집 서버)
* **query** (문자열): 쿼리문
* **output\_parameter** (불리언): 쿼리 매개변수 출력 제어 여부
* **trigger\_type** (문자열): 실행 방식(cron: 예약 실행, workflow: 다른 쿼리의 결과에 따라 실행)
* **cron\_schedule** (문자열): (trigger\_type이 cron일 때) CRON 문법으로 작성된 실행 일정
* **preceding\_guid** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 GUID
* **preceding\_name** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 이름
* **preceding\_action** (문자열): (trigger\_type이 workflow일 때) 선행 예약된 쿼리의 실행 결과(succeeded: 성공, failed: 실패, finished: 실행 완료)
* **elapsed\_time** (32비트 정수): 실행 시간(단위: 밀리초)
* **running\_state** (문자열): 실행 상태(running: 실행 중, stopping: 중지하는 중, finished: 완료, canceled: 취소됨)
* **result\_state** (문자열): 실행 결과(succeeded: 성공, failed: 실패, , canceled: 취소)
* **last\_run\_time** (문자열): 최근 실행 시각 (yyyy-MM-dd HH:mm:ssZ 형식)
* **last\_failure\_time** (문자열): 최근 실패 시각 (yyyy-MM-dd HH:mm:ssZ 형식)
* **last\_failure\_reason** (문자열): 쿼리 실행에 실패한 원인
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

지정한 예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "result": false, "error\_msg": "scheduled query not found : 0fb16aa8-dbc1-458a-9769-342de5cf9211"}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 생성

새 예약된 쿼리를 생성합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d query="table duration=1m sonar\_cpu\_logs | search idle <= 10" \ -d type="cron" \ -d cron\_schedule="\* \* \* \* \*" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| name | O | 문자열 | 이름 | 최대 255자 |
| description | X | 문자열 | 설명 | 최대 2000자 |
| enabled | X | 불리언 | 활성화 여부 | 기본값: false |
| query | O | 문자열 | 쿼리문 |  |
| trigger\_type | O | 문자열 | 실행 방식 | cron(예약 실행)과 workflow(다른 쿼리의 결과에 따라 실행) 중 선택 |
| cron\_schedule | O | 문자열 | 실행 조건 | trigger\_type이 cron일 때 필수 |
| preceding\_guid | X | 문자열 | 선행 예약된 쿼리의 GUID | trigger\_type이 workflow일 때 필수 |
| preceding\_action | X | 문자열 | 선행 예약된 쿼리의 실행 상태 | trigger\_type이 workflow일 때 succeeded, failed, finished 중 하나 지정 |
| node\_types | X | 문자열 목록 | 실행 위치 | control(분석 서버) 또는 data(수집 서버)를 쉼표로 구분하여 기입 |
| output\_parameter | X | 불리언 | 매개변수 출력 제어 | 기본값: false |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값 길이가 긴 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 255 characters."}

같은 이름의 예약된 쿼리가 있는 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated name: test"}

trigger\_type이 cron일 때, cron\_schedule에 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "cron\_schedule should be not null"}

trigger\_type이 workflow일 때, preceding\_action에 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "preceding\_action should be not null"}

trigger\_type이 workflow일 때, preceding\_action에 허용되지 않은 값이 입력된 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "preceding\_action value must be one of 'finished', 'succeeded', 'failed'."}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 수정

기존 예약된 쿼리를 수정합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/scheduled-queries/:guid

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d query="table duration=1m sonar\_cpu\_logs | search idle <= 10" \ -d type="cron" \ -d cron\_schedule="\* \* \* \* \*" \ -X PUT https://HOSTNAME/api/sonar/scheduled-queries/95e17283-1d08-44f0-bac7-b734813d2dcd

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 예약된 쿼리 GUID |  |
| name | O | 문자열 | 이름 | 최대 255자 |
| description | X | 문자열 | 설명 | 최대 2,000자 |
| enabled | X | 불리언 | 활성화 여부 | 기본값: false |
| query | O | 문자열 | 쿼리문 |  |
| trigger\_type | O | 문자열 | 실행 방식 | cron(예약 실행)과 workflow(다른 쿼리의 결과에 따라 실행) 중 선택 |
| cron\_schedule | O | 문자열 | 실행 조건 | trigger\_type이 cron일 때 필수 |
| preceding\_guid | X | 문자열 | 선행 예약된 쿼리의 GUID | trigger\_type이 workflow일 때 필수 |
| preceding\_action | X | 문자열 | 선행 예약된 쿼리의 실행 상태 | trigger\_type이 workflow일 때 succeeded, failed, finished 중 하나 지정 |
| node\_types | X | 문자열 목록 | 실행 위치 | control(분석 서버) 또는 data(수집 서버)를 쉼표(,)로 구분하여 기입 |
| output\_parameter | X | 불리언 | 매개변수 출력 제어 | 기본값: false |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값 길이가 긴 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 255 characters."}

같은 이름의 예약 쿼리가 있는 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated name: test"}

trigger\_type이 cron일 때, cron\_schedule에 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "cron\_schedule should be not null"}

trigger\_type이 workflow일 때, preceding\_action에 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "preceding\_action should be not null"}

trigger\_type이 workflow일 때, preceding\_action에 허용되지 않은 값이 입력 된 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "preceding\_action value must be one of 'finished', 'succeeded', 'failed'."}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 삭제

지정된 여러 개의 예약된 쿼리를 삭제합니다. 이 작업은 관리자 권한을 요구합니다. 일부 목록에 대한 동작 실패를 허용하며, 삭제 실패 시 failures 매개변수에 객체의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

DELETE /api/sonar/scheduled-queries

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -d policy="skip" -X DELETE https://HOSTNAME/api/sonar/scheduled-queries

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 예약된 쿼리 GUID 목록 | 쉼표(,)로 구분된 예약된 쿼리 GUID 목록 |
| policy | X | 문자열 | 삭제 시 옵션 | skip, force 중 선택, 미지정 시 skip |

* skip: 예약된 쿼리가 실행 중인 경우 삭제하지 않습니다.
* force: 예약된 쿼리가 실행 중이라도 중지하고 삭제합니다.

#### 정상 응답

모두 성공

{ "succeeded": 1, "failures": []}

* **succeeded** (32비트 정수): 삭제한 예약된 쿼리의 갯수, policy가 skip이면 실행 중인 예약 쿼리를 삭제하지 않으므로 삭제한 예약된 쿼리의 갯수에 집계하지 않습니다.
* **failures** (배열): 삭제 실패한 예약된 쿼리 목록
* **id** (문자열): 예약된 쿼리의 GUID
* **reason** (문자열): 오류 내용

일부 성공

실행 예시

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X DELETE https://HOSTNAME/api/sonar/scheduled-query

응답 예시

{ "succeed": 1, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### 오류 응답

GUID 매개변수 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "succeed": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 활성화

지정된 예약된 쿼리를 활성화합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/:guid/enable

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/:guid/enable

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 예약된 쿼리 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

존재하지 않는 GUID인 경우

HTTP 상태코드 200 응답

{ "result": false, "error\_msg": "scheduled query not found : 0fb16aff-dbc1-458a-9769-342de5cf9219"}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 비활성화

지정된 예약된 쿼리를 비활성화합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/:guid/disable

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/:guid/disable

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 예약된 쿼리 GUID | 36자 |

#### 정상 응답

{}

#### 오류 응답

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guid should be not null"}

존재하지 않는 GUID인 경우

HTTP 상태코드 200 응답

{ "result": false, "error\_msg": "scheduled query not found: 0fb16aff-dbc1-458a-9769-342de5cf9219"}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 일괄 활성화

지정된 여러 개의 예약된 쿼리를 활성화합니다. 이 작업은 관리자 권한을 요구합니다. 이 작업은 일부 동작 실패를 허용합니다. 활성화하지 못한 예약된 쿼리가 있으면 failures 매개변수에 해당 예약된 쿼리의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/enable

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/enable

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 예약된 쿼리 GUID 목록 | 쉼표(,)를 구분자로 하는 예약된 쿼리 GUID 목록 |

#### 정상 응답

모두 성공

{ "succeeded": 1, "failures": []}

* **succeeded** (32비트 정수): 활성화에 성공한 예약된 쿼리의 갯수, 이미 활성화 상태인 예약된 쿼리는 포함되지 않습니다.
* **failures** (배열): 활성화에 실패한 예약된 쿼리의 오류
* **id** (문자열): 예약된 쿼리의 GUID
* **reason** (문자열): 오류 내용

일부 성공

실행 예시

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/enable

응답 예시

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### 오류 응답

필수 매개변수가 존재하지 않는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 일괄 비활성화

지정된 여러개의 예약된 쿼리를 비활성화합니다. 이 작업은 관리자 권한을 요구합니다. 이 작업은 일부 동작 실패를 허용합니다. 비활성화하지 못한 예약된 쿼리가 있으면 failures 매개변수에 해당 예약된 쿼리의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/disable

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -X POST https://HOSTNAME/api/sonar/scheduled-queries/disable

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 예약된 쿼리 GUID 목록 | 쉼표(,)를 구분자로 하는 예약된 쿼리 GUID 목록 |

#### 정상 응답

모두 성공

{ "succeeded": 1, "failures": []}

* **succeeded** (32비트 정수): 비활성화에 성공한 예약된 쿼리의 갯수, 이미 비활성화 성태인 예약된 쿼리는 포함되지 않습니다.
* **failures** (배열): 비활성화에 실패한 예약된 쿼리의 오류
* **id** (문자열): 예약된 쿼리의 GUID
* **reason** (문자열): 오류 내용

일부 성공

실행 예시

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/disable

응답 예시

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### 오류 응답

필수 매개변수가 존재하지 않는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 일괄 실행

지정된 여러 개의 예약된 쿼리를 실행합니다. 이 작업은 관리자 권한을 요구합니다. 이 작업은 일부 동작 실패를 허용합니다. 실행하지 못한 예약된 쿼리가 있으면 failures 매개변수에 해당 예약된 쿼리의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/run

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/run

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 예약된 쿼리 GUID 목록 | 쉼표(,)를 구분자로 하는 예약된 쿼리 GUID 목록 |
| policy | X | 문자열 | 실행 중인 예약 쿼리가 있는 경우 처리 옵션 | skip, restart 중 선택, 미지정 시 skip |

* skip: 실행 중인 예약 쿼리가 있으면 실행하지 않습니다.
* restart: 실행 중인 예약 쿼리를 중지시키고 다시 실행합니다.

#### 정상 응답

모두 성공

{ "succeeded": 1, "failures": []}

* **succeeded** (32비트 정수): 실행에 성공한 예약된 쿼리의 갯수, 이미 실행 되어있는 예약된 쿼리중 policy가 skip이어서 실행하지 않는 경우에는 포함되지 않습니다.
* **failures** (배열): 실행에 실패 한 예약된 쿼리의 오류
* **id** (문자열): 예약된 쿼리의 GUID
* **reason** (문자열): 오류 내용

일부 성공

실행 예시

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/run

응답 예시

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### 오류 응답

필수 매개변수가 존재하지 않는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 예약된 쿼리 일괄 중지

지정된 여러 개의 예약된 쿼리의 실행을 중지합니다. 이 작업은 관리자 권한을 요구합니다. 이 작업은 일부 동작 실패를 허용합니다. 중지하지 못한 예약된 쿼리가 있으면 failures 매개변수에 해당 예약된 쿼리의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

POST /api/sonar/scheduled-queries/stop

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -X POST https://HOSTNAME/api/sonar/scheduled-queries/stop

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 예약된 쿼리 GUID 목록 | 쉼표(,)를 구분자로 하는 예약된 쿼리 GUID 목록 |

#### 정상 응답

모두 성공

{ "succeeded": 1, "failures": []}

* **succeeded** (32비트 정수): 중지에 성공한 예약된 쿼리의 갯수, 이미 중지된 경우에는 포함되지 않습니다.
* **failures** (배열): 중지에 실패한 예약된 쿼리의 오류
* **id** (문자열): 예약된 쿼리의 GUID
* **reason** (문자열): 오류 내용

일부 성공

실행 예시

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/stop

응답 예시

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### 오류 응답

필수 매개변수가 존재하지 않는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

예약된 쿼리가 존재하지 않는 경우

HTTP 상태코드 200 응답

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## 룩업 API

### 룩업 목록 조회

검색 조건과 일치하는 룩업 목록을 조회합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

GET /api/sonar/lookups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/lookups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| offset | X | 32비트 정수 | 건너 뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 전체 조회 |
| keywords | X | 문자열 | 검색 키워드 | 이름, 설명, 쿼리 대상으로 검색 |

#### 정상 응답

{ "total\_count": 17, "lookups": [ { "guid": "76b8699d-91a1-4576-a908-7db753570a0a", "name": "country\_code", "description": "국가코드 한글 이름 매핑", "record\_count": 236, "fields": [ { "field\_name": "country", "len": 2, "use\_null": false }, { "field\_name": "name", "len": 255, "use\_null": false } ], "created": "2023-09-23 17:13:15+0900", "updated": "2023-09-23 17:13:15+0900" } ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 룩업 갯수
* **lookups** (배열): 페이징된 룩업 목록
* **guid** (문자열): 룩업 GUID
* **name** (문자열): 룩업 이름
* **description** (문자열): 룩업 설명
* **record\_count** (32비트 정수): 룩업에 포함된 레코드 갯수
* **fields** (배열): 필드 정의 목록
* **field\_name** (문자열): 필드 이름
* **len** (32비트 정수): 값 최대 길이
* **use\_null** (불리언): 빈 값 허용 여부
* **created** (문자열): 생성일시 (yyyy-MM-dd HH:mm:ssZ 형식)
* **updated** (문자열): 수정일시 (yyyy-MM-dd HH:mm:ssZ 형식)

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

룩업 조회 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 생성

새 룩업을 생성합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

POST /api/sonar/lookups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=country\_code \ -d description="국가코드 한글 이름 매핑" \ -d fields="[{""field\_name"":"country\_code",""len"":2,""use\_null"":false},{""field\_name"":""name"",""len"":255,""use\_null"":false}]" -X POST https://HOSTNAME/api/sonar/lookups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | X | 문자열 | 룩업 GUID | 36자. 기본값은 랜덤 생성 |
| name | O | 문자열 | 룩업 이름 | 최소 1자, 최대 255자. 영문, 숫자, 밑줄만 사용 |
| description | X | 문자열 | 룩업 설명 | 최대 2000자 |
| fields | O | 객체 배열 | 필드 정의 목록 | field\_name, len, use\_null 키를 포함한 객체의 배열 |

fields 배열 요소 구성

* **field\_name** (문자열): 필드 이름
* **len** (32비트 정수): 값의 최대 길이
* **use\_null** (불리언): 빈 값 허용 여부

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

룩업 이름에 허용되지 않는 문자를 포함한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "illegal-state", "error\_msg": "lookup name must be alphanumeric and underscore characters only: hello-world"}

룩업 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated lookup name: country\_code"}

룩업 생성 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 수정

기존 룩업 정보를 수정합니다. 이 작업은 관리자 권한을 요구합니다.

#### HTTP 요청

PUT /api/sonar/lookups

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guid=76b8699d-91a1-4576-a908-7db753570a0a \ -d name=country\_code2 \ -d description="국가코드 한글 이름 매핑" \ -X PUT https://HOSTNAME/api/sonar/lookups

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 룩업 GUID | 36자 |
| name | O | 문자열 | 룩업 이름 | 최소 1자, 최대 255자. 영문, 숫자, 밑줄만 사용 |
| description | X | 문자열 | 룩업 설명 | 최대 2000자 |

#### 정상 응답

{}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

매개변수 값의 길이가 잘못된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

룩업 이름에 허용되지 않는 문자를 포함한 경우

HTTP 상태 코드 400 응답

{ "error\_code": "illegal-state", "error\_msg": "lookup name must be alphanumeric and underscore characters only: hello-world"}

룩업 이름이 중복된 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "duplicated lookup name: country\_code2"}

룩업 수정 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 일괄 삭제

지정된 여러 개의 룩업을 삭제합니다. 이 작업은 관리자 권한을 요구합니다. 일부 목록에 대한 동작 실패를 허용하며, 삭제 실패 시 failures 매개변수에 객체의 식별자와 실패 원인을 반환합니다.

#### HTTP 요청

DELETE /api/sonar/lookups

#### cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -X DELETE https://HOSTNAME/api/sonar/lookups

#### 요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guids | O | 문자열 | 룩업 GUID 목록 | 쉼표로 구분된 룩업 GUID 목록 |

#### 정상 응답

모두 성공

{ "failures": []}

일부 성공

{ "failures": [ { "id":"7062774f-dbff-4d6f-aa68-c618eb9f6a41", "reason":"lookup-not-found" } ]}

#### 오류 응답

GUID 매개변수 값이 없는 경우

HTTP 상태코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

식별자가 GUID 형식이 아닌 경우

HTTP 상태코드 400 응답

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

관리자 권한이 아닌 경우

HTTP 상태코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 레코드 조회

지정한 룩업에 속한 레코드 목록을 조회합니다.

#### HTTP 요청

GET /api/sonar/lookups/:guid/records

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 룩업 GUID | 36자 |
| offset | X | 32비트 정수 | 건너 뛸 갯수 | 기본값 0 |
| limit | X | 32비트 정수 | 최대 갯수 | 미지정 시 20건 |
| keywords | X | 문자열 | 검색 키워드 | 레코드 전체를 대상으로 검색 |

#### 정상 응답

{ "total\_count": 236, "fields": [ "country", "name" ], "records": [ ["AE", "아랍에미리트 연합국"], ["AF", "아프카니스탄"], ["AG", "안티가 부다"], ["AI", "안굴라"], ["AL", "알바니아"], ["AM", "아르메니아"], ["AN", "안틸레스"], ["AO", "앙골라"], ["AQ", "남극지역"], ["AR", "아르엔티나"], ["AS", "미국령 사모아"], ["AT", "오스트리아"], ["AU", "호주"], ["AW", "아루바"], ["AZ", "아제르바이잔"], ["BA", "보스니아-헤르체고비아"], ["BB", "바베이도스"], ["BD", "방글라데시"], ["BE", "벨기에"], ["BF", "부르키나파소"] ]}

* **total\_count** (32비트 정수): 검색 조건과 일치하는 전체 룩업 레코드 수
* **fields** (배열): 필드 이름 목록
* **records** (배열): 레코드 목록

#### 오류 응답

offset, limit 값이 정수가 아닌 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset, limit 값이 음수인 경우

HTTP 상태 코드 400 응답

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

룩업 레코드 조회 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 레코드 일괄 추가

지정한 룩업에 여러 개의 레코드를 일괄 추가합니다.

#### HTTP 요청

POST /api/sonar/lookups/:guid/records

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d records="[[""KR"",""대한민국""],["VN",""베트남""]]" \ -X POST https://HOSTNAME/api/sonar/lookups/76b8699d-91a1-4576-a908-7db753570a0a/records

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 룩업 GUID | 36자 |
| records | O | 객체 배열 | 레코드 목록 | 값 배열의 배열 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

레코드 키가 중복된 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "KR", "reason": "duplicated-key" } ], "result": false, "error\_msg": "invalid-records"}

레코드 값 갯수가 잘못된 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "VN", "reason": "invalid-record-size" } ], "result": false, "error\_msg": "invalid-records"}

레코드 추가 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 레코드 수정

지정한 룩업의 특정 레코드를 수정합니다.

#### HTTP 요청

PUT /api/sonar/lookups/:guid/records/:key

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d record="KR,한국" \ -X PUT https://HOSTNAME/api/sonar/lookups/76b8699d-91a1-4576-a908-7db753570a0a/records/KR

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 룩업 GUID | 36자 |
| record | O | 문자열 배열 | 레코드 | 값 배열 |

#### 정상 응답

{ "failure": {}}

#### 오류 응답

레코드가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failure": { "id": "FF", "reason": "record-not-found" }, "result": false, "error\_msg": "invalid-record"}

레코드 값 갯수가 잘못된 경우

HTTP 상태 코드 200 응답

{ "failure": { "id": "KR", "reason": "invalid-record-size" }, "result": false, "error\_msg": "invalid-record"}

레코드 수정 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### 룩업 레코드 일괄 삭제

지정한 룩업 레코드를 삭제합니다.

#### HTTP 요청

DELETE /api/sonar/lookups/:guid/records

cURL 예시

curl -H "Authorization: Bearer <API\_KEY>" \ -d keys="KR" \ -X DELETE "https://HOSTNAME/api/sonar/lookups/76b8699d-91a1-4576-a908-7db753570a0a/records"

요청 매개변수

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 키 | 필수 | 타입 | 설명 | 비고 |
| guid | O | 문자열 | 룩업 GUID | 36자 |
| keys | O | 문자열 | 레코드 키 목록 | 쉼표로 구분된 삭제 대상 레코드 키 목록 |

#### 정상 응답

{ "failures": []}

#### 오류 응답

필수 매개변수가 누락된 경우

HTTP 상태 코드 400 응답

{ "error\_code": "null-argument", "error\_msg": "keys should be not null"}

레코드가 존재하지 않는 경우

HTTP 상태 코드 200 응답

{ "failures": [ { "id": "FF", "reason": "record-not-found" } ], "result": false, "error\_msg": "invalid-records"}

레코드 삭제 권한이 없는 경우

HTTP 상태 코드 500 응답

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}