### ロガーモデルの作成

新しいロガーモデルを追加します。この操作には管理者権限が必要です。

#### HTTPリクエスト

POST /api/sonar/logger-models

cURL例

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

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| guid | × | 文字列 | ロガーモデル識別子 | 36文字のGUID。未設定時は自動生成 |
| name | ○ | 文字列 | ロガーモデル名 | 最小1文字、最大50文字 |
| description | × | 文字列 | ロガーモデルの説明 | 最大2,000文字 |
| logger\_factory\_name | ○ | 文字列 | ロガータイプ識別子 |  |
| parser\_code | × | 文字列 | パーサ識別子 |  |
| rules | × | オブジェクト配列 | 正規化ルール一覧 | 下記参照 |

rules属性

* **guid**（文字列）：正規化ルール識別子。未設定時は自動生成されます。
* **name**（文字列）：正規化ルール名
* **log\_schema\_code**（文字列）：ログスキーマ識別子
* **stream\_query**（文字列）：ストリームクエリ文字列
* **stream\_interval**（32ビット整数）：ストリームクエリのリフレッシュインターバル

#### 正常レスポンス

{}

#### エラーレスポンス

必須パラメータが不足している場合

HTTPステータスコード 400 のレスポンス。

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

パラメータ値の長さが不正な場合

HTTPステータスコード 400 のレスポンス。

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

パーサが存在しない場合

HTTPステータスコード 500 のレスポンス。

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

ロガータイプが存在しない場合

HTTPステータスコード 500 のレスポンス。

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

ロガーモデル名が重複している場合

HTTPステータスコード 500 のレスポンス。

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

管理権限がない場合

HTTPステータスコード 500 のレスポンス。

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