FLOW DATA API

1. Mô hình tổng thể



1. Mô hình chi tiết



1. Mô tả chi tiết
   1. Kiểm tra Black List

* Mục đích của kiểm tra Black list:
  + Không cho phép 1 IP hoặc một dải IP được quyền truy cập vào hệ thống.
  + Không cho phép truy cập vào 1 hoặc nhiều API của hệ thống.
  + Không cho phép truy cập vào 1 hoặc nhiều Application của hệ thống.
* Các điều kiện kiểm tra Black list được lưu trong bảng AM\_BLOCK\_CONDITION.
* Điêu kiện kiểm tra Black list gồm 3 kiểu: IP, API, Application.
* Ý nghĩa các trường trong bảng AM\_BLOCK\_CONDITION
  + AM\_BLOCK\_ID: Trường ID khóa chính của bảng, trường tự tăng.
  + BLOCK\_NAME: Trường dữ liệu lưu text tương ứng với 3 kiểu: IP, API,Application.
  + BLOCK\_VALUE: Giá trị dữ liệu block.
  + BLOCK\_STATUS: Trạng thái: 0: unblock; 1: Block
* Kiểm tra với điều kiện IP:
  + Hệ thống lấy IP\_request gọi lên.
  + Kiểm tra IP\_ request đó có nằm trong danh sách Black List hay không? Kiểm tra IP\_request đó với giá trị Ip trong trường BLOCK\_VALUE = IP\_request , BLOCK\_NAME = IP, BLOCK\_STATUS=1. Nếu tồn tại thì hệ thống sẽ gửi ngay kết quả trả về cho Client với thông báo: IP hiện tại đang bị block và không xử lý tiếp. Nếu không tồn tại chuyển sang giai đoạn kiểm tra tiếp theo
  + Cách lưu IP trong trường BLOCK\_VALUE:
    - Kiểu tuyệt đối: 172.19.0.17- Hệ thống sẽ chặn đúng IP với giá trị 172.19.0.17
    - Kiểu chặn theo dải: 172.19.0.\*- Hệ thống sẽ chặn toàn bộ các Ip nằm trong dải: 172.19.0.1 🡪 172,19.0.255.
* Kiểm tra với điều kiện API:
  + Hệ thống lấy: {Context/version} trong URI gọi lên.
  + Kiểm tra giá trị {Context/version} gọi lên này với giá trị lưu trong BLOCK\_VALUE={ Context/version}, BLOCK\_NAME = API, BLOCK\_STATUS=1. Nếu tồn tại thì hệ thống sẽ gửi ngay kết quả trả về cho Client với thông báo: API hiện tại đang bị block và không xử lý tiếp. Nếu không tồn tại chuyển sang giai đoạn kiểm tra tiếp theo
  + Cách lưu API trong trường BLOCK\_VALUE: Context/version. Ví dụ: weather/1.0.
* Kiểm tra với điều kiện Application:
  + Hệ thống lấy: Token gọi lên.
  + Từ token sẽ kiểm tra xem được request đang yêu cầu lên là yêu cầu của Application nào. Ta sẽ lấy được tên Application\_Name
  + Kiểm tra giá trị Application\_Name sau khi lấy được theo Token gửi lên này với giá trị lưu trong BLOCK\_VALUE Application\_Name, BLOCK\_NAME = Application, BLOCK\_STATUS=1. Nếu tồn tại thì hệ thống sẽ gửi ngay kết quả trả về cho Client với thông báo: Application hiện tại đang bị block và không xử lý tiếp. Nếu không tồn tại chuyển sang giai đoạn kiểm tra tiếp theo
  + Cách lưu Application trong trường BLOCK\_VALUE là lưu tên của Application.
  1. Kiểm tra điều kiện mức System
* Sau khi kiểm tra IP, API, Application của API request lên không nằm trong danh sách Black list hệ thống tiếp tục kiểm tra điều kiện Mức System.
* Mục đich của điều kiện mức System, điều kiện này được đặt ra cho toàn bộ hệ thống:
  + Check số lượng request vào hệ thống.
  + Check số lượng Bandwidth request vào hệ thống.
* Điều kiện kiểm tra mức system được lưu trong bảng AP\_POLICY với Policy\_type = 1.
* Ý nghĩa các trường trong bảng AP\_POLICY
  + AM\_POLICY\_ID: Id của bảng, là khóa chính.
  + NAME: Tên của Policy.
  + DISPLAY\_NAME: Tên hiển thị của Policy
  + POLICY\_TYPE: Mức áp dụng: 1-System,2-Api,3-Application,4-Subscription
  + QUOTA\_TYPE: Kiểu policy: 1-Request Bandwidth; 2-Request Count
  + QUOTA: giá trị điều kiện. Ứng với Request Bandwidth: giá trị tính theo đơn vị KB. Request Count: giá trị là số lượng truy cập.
  + UNIT\_TIME: Thời gian áp đặt cho điều kiện có hiệu lực. Giá trị tính toán theo PHÚT.
  + DESCRIPTION: Mô tả
  + IS\_DEPLOYED: Giá trị default là 1- Active ; 0-Unactive
* Kiểm tra điều kiện Request Bandwidth:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán dung lượng request (a)gửi lên cộng với tổng số dung lượng request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 1, POLICY\_TYPE = 1 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng dung lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán dung lượng request gọi vào hệ thống và sẽ cộng dồn các dung lượng lại.
* Kiểm tra điều kiện Request Count:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán request (a)gửi lên cộng với tổng số request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 2, POLICY\_TYPE = 1 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán request gọi vào hệ thống và sẽ cộng dồn các request lại.
  1. Kiểm tra điều kiện mức API:
* Sau khi kiểm tra và pass qua mức System hệ thống kiểm tra mức API.
* Mục đich của điều kiện mức API:
  + Kiểm tra xem URL của Api request lên có tồn tại hay không.
  + Kiểm tra xem API trạng thái có đươc Published hay không.
  + Check số lượng request vào API có nằm trong ngưỡng điều kiện hay không.
  + Check số lượng Bandwidth request vào API có nằm trong ngưỡng điều kiện hay không.
  + Kiểm tra xem API này có thuộc nhóm điều kiện nào hay không. Nếu có thì các nhóm điều kiện này có giá trị như thế nào.
* Điều kiện kiểm tra mức API được lưu trong bảng AP\_POLICY với Policy\_type = 2. Nhóm điều kiện được lưu trong bảng AM\_GROUP\_CONDITION, AM\_IP\_CONDITION, AM\_HEADER\_FIELD\_CONDITION
* Ý nghĩa các trường trong bảng AP\_POLICY
  + AM\_POLICY\_ID: Id của bảng, là khóa chính.
  + NAME: Tên của Policy.
  + DISPLAY\_NAME: Tên hiển thị của Policy
  + POLICY\_TYPE: Mức áp dụng: 1-System,2-Api,3-Application,4-Subscription
  + QUOTA\_TYPE: Kiểu policy: 1-Request Bandwidth; 2-Request Count
  + QUOTA: giá trị điều kiện. Ứng với Request Bandwidth: giá trị tính theo đơn vị KB. Request Count: giá trị là số lượng truy cập.
  + UNIT\_TIME: Thời gian áp đặt cho điều kiện có hiệu lực. Giá trị tính toán theo PHÚT.
  + DESCRIPTION: Mô tả
  + IS\_DEPLOYED: Giá trị default là 1- Active ; 0-Unactive
* **Kiểm tra URL**: hệ thống sẽ đọc URL để lấy thông tin: {context},{version},{parttern} có trong bảng API version hay không? Nếu có chuyển sang kiểm tra điều kiện tiếp theo, nếu không có dừng lại và trả kết quả về cho Client với nội dung URI không tồn tại.
* **Kiểm tra xem API có ở trạng thái Published**: hệ thống sẽ đọc URI để lấy thông tin: {context},{version} có trong bảng API version để lấy trạng thái CURRENT\_STATE = 1. Nếu đúng hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Nếu không đúng hệ thống dừng lại và trả kết quả về cho Client nội dung API hiện đang không được Public.
* **Kiểm tra điều kiện Request Bandwidth**:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán dung lượng request (a)gửi lên cộng với tổng số dung lượng request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 1, POLICY\_TYPE = 2 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng dung lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán dung lượng request gọi vào hệ thống và sẽ cộng dồn các dung lượng lại.
* **Kiểm tra điều kiện Request Count**:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán request (a)gửi lên cộng với tổng số request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 2, POLICY\_TYPE = 2 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán request gọi vào hệ thống và sẽ cộng dồn các request lại.
* Kiểm tra xem API đó có thuộc nhóm điều kiện nào hay không? Kiểm tra xem Policy\_Id được gán cho Api có nằm trong bảng AM\_GROUP\_CONDITION. Policy\_id. Nếu không thuộc nhóm điều kiện nào thì chuyển sang kiểm tra điều kiện tiếp theo cho Applicaton, nếu thuộc nhóm điều kiện nào thì sẽ kiểm tra các điều kiện của nhóm điều kiện đấy như sau:
  + Kiểm tra IP có nằm trong phần Ip bị chặn không cho phép gọi API này hay không?
    - Dữ liệu kiểm tra được lưu trong bảng AM\_IP\_CONDITION.
    - Kiểm tra IP gọi vào hệ thống với giá trị SPECIFIC\_IP, hoặc IP thuộc khoảng [STARTING\_IP , ENDING\_IP]
    - Nếu đúng thì hệ thống dừng lại và thực hiện trả về cho client biết là IP của client không được phép truy cập vào API này. Nếu IP không nằm trong danh sách chặn thì sẽ chuyển sang kiểm tra điều kiện tiếp theo.
  + Kiểm tra giá trị tham số truyền trên Hearder có nằm trong danh sách bị chặn không
    - Dữ liệu kiểm tra được lưu trong bảng AM\_HEADER\_FIELD\_CONDITION.
    - Kiểm tra Header\_name và Header\_value truyền lên với HEADER\_FIELD\_NAME và HEADER\_FIELD\_VALUE
    - Nếu đúng thì hệ thống dừng lại và thực hiện trả về cho client biết là giá trị header của client truyền lên không được phép truy cập vào API này. Nếu không nằm trong danh sách chặn thì sẽ chuyển sang kiểm tra điều kiện tiếp theo.
  1. Kiểm tra điều kiện mức Application
* Sau khi pass qua các điều kiện API hệ thống chuyển sang mức kiểm tra Application.
* Mục đich của điều kiện mức Application:
  + Check xem token Client gửi lên có đúng hay không.
  + Check số lượng request .
  + Check số lượng Bandwidth request.
* Điều kiện kiểm tra mức Application được lưu trong bảng AP\_POLICY với Policy\_type = 3.
* Ý nghĩa các trường trong bảng AP\_POLICY
  + AM\_POLICY\_ID: Id của bảng, là khóa chính.
  + NAME: Tên của Policy.
  + DISPLAY\_NAME: Tên hiển thị của Policy
  + POLICY\_TYPE: Mức áp dụng: 1-System,2-Api,3-Application,4-Subscription
  + QUOTA\_TYPE: Kiểu policy: 1-Request Bandwidth; 2-Request Count
  + QUOTA: giá trị điều kiện. Ứng với Request Bandwidth: giá trị tính theo đơn vị KB. Request Count: giá trị là số lượng truy cập.
  + UNIT\_TIME: Thời gian áp đặt cho điều kiện có hiệu lực. Giá trị tính toán theo PHÚT.
  + DESCRIPTION: Mô tả
  + IS\_DEPLOYED: Giá trị default là 1- Active ; 0-Unactive
* Kiểm tra xem token có đúng hay không:
  + Hệ thống kiểm tra xem có giá trị token từ Client gửi lên hay không? Nếu có chuyển sang kiểm tra điều kiện tiếp theo. Nếu không có hệ thống dừng lại và thông báo cho Client biết là Client chưa truyền token lên.
  + Hệ thống nhận Token\_request từ client gửi lên. Kiểm tra token\_request với giá trị Token trong bảng AM\_APPLICATION\_TOKEN.TOKEN\_KEY = token\_request, START\_DATE<= ngày request =< END\_DATE. Nếu đúng hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Nếu không đúng hệ thống dừng lại và thông báo cho Client biết Token hết hiệu lực
* Kiểm tra điều kiện Request Bandwidth:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán dung lượng request (a)gửi lên cộng với tổng số dung lượng request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 1, POLICY\_TYPE = 3 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng dung lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán dung lượng request gọi vào hệ thống và sẽ cộng dồn các dung lượng lại.
* Kiểm tra điều kiện Request Count:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán request (a)gửi lên cộng với tổng số request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 2, POLICY\_TYPE = 3 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán request gọi vào hệ thống và sẽ cộng dồn các request lại.
  1. Kiểm tra điều kiện mức Subscription
* Sau khi pass qua các điều kiện Application hệ thống chuyển sang mức kiểm tra Subscription.
* Mục đich của điều kiện mức Subscription:
  + Check xem API này có đúng là được gán cho Application với Token truyền lên hay không.
  + Check API được gán cho Application được lưu trong bảng Subscription có Unlocked hay không.
  + Check số lượng Bandwidth request.
  + Check số lượng request count
* Điều kiện kiểm tra mức Subscription được lưu trong bảng AP\_POLICY với Policy\_type = 4.
* Ý nghĩa các trường trong bảng AP\_POLICY
  + AM\_POLICY\_ID: Id của bảng, là khóa chính.
  + NAME: Tên của Policy.
  + DISPLAY\_NAME: Tên hiển thị của Policy
  + POLICY\_TYPE: Mức áp dụng: 1-System,2-Api,3-Application,4-Subscription
  + QUOTA\_TYPE: Kiểu policy: 1-Request Bandwidth; 2-Request Count
  + QUOTA: giá trị điều kiện. Ứng với Request Bandwidth: giá trị tính theo đơn vị KB. Request Count: giá trị là số lượng truy cập.
  + UNIT\_TIME: Thời gian áp đặt cho điều kiện có hiệu lực. Giá trị tính toán theo PHÚT.
  + DESCRIPTION: Mô tả
  + IS\_DEPLOYED: Giá trị default là 1- Active ; 0-Unactive
* Check xem API này có đúng là được gán cho Application với Token truyền lên hay không:
  + Hệ thống nhận Token\_request từ client gửi lên. Kiểm tra token\_request với giá trị Token trong bảng AM\_APPLICATION\_TOKEN.TOKEN\_KEY = token\_request, để lấy thông tin Application. Với thông tin Application lấy được từ token\_request kiểm tra xem API này có được gán cho Applcation này hay không? Nếu có sẽ chuyển sang kiểm tra điều kiện tiếp theo, nếu không hệ thống dừng lại và thông báo cho client Api này chưa được gán cho Application tương ứng với Token.
* Check API được gán cho Application được lưu trong bảng Subscription có Unlocked hay không. Với API được gán cho Applictiong trong phần Subscription, hệ thống kiểm tra trạng thái việc gán này có được Unlocked hay không? Nếu có sẽ chuyển sang kiểm tra điều kiện tiếp theo, nếu không hệ thống dừng lại và thông báo cho client Api đang tạm khóa.
* Kiểm tra điều kiện Request Bandwidth:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán dung lượng request (a)gửi lên cộng với tổng số dung lượng request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 1, POLICY\_TYPE = 4 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng dung lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán dung lượng request gọi vào hệ thống và sẽ cộng dồn các dung lượng lại.
* Kiểm tra điều kiện Request Count:
  + Khi 1 request được gọi vào hệ thống, hệ thống sẽ tính toán request (a)gửi lên cộng với tổng số request đã thực hiện gọi lên thành công trước đó(b). Nếu số (a+b) <= QUOTA, QUOTA\_TYPE = 2, POLICY\_TYPE = 4 thì hệ thống chuyển sang kiểm tra điều kiện tiếp theo. Ngược lại hệ thống sẽ dừng lại không tính toán mà gửi lại cho Client thông báo: Số lượng request vượt quá ngưỡng giới hạn.
  + Sau mỗi lần request lên hệ thống thành công, hệ thống sẽ tính toán request gọi vào hệ thống và sẽ cộng dồn các request lại.
  1. Kiểm tra với End-Point
* Sau khi pass qua các điều kiện Subcription hệ thống chuyển sang mức kiểm tra End-Point,
* Mục đích: Kiểm tra thực hiện lấy dữ liệu từ End-Point.
* Request sẽ được gửi sang End-Point, Nếu End-Point lỗi hệ thống trả dừng lại và trả về kết quả cho client là End-point hiện đang bị lỗi. Nếu việc gọi sang End-Point không bị lỗi hệ thống trả về cho client các kết quả nhận được từ End-point.