本文是GOKU网关的快速入门教程，通过讲解如何使用网关快速访问接口，还有提供插件的使用示例，来快速展示网关的使用方法。

## **理解概念**

通过网关访问接口，需要为该接口分配一个策略，策略相当于是网关给予的用户凭证。

如果不使用任何插件，AGW的使用流程大致是四个步骤：  
（1）新建API  
（2）新建策略；  
（3）为策略绑定API；  
（4）用户通过策略ID访问API

如果需要用到流量控制、鉴权、IP黑白名单等插件，可以对该策略 **设置策略插件** ；  
如果需要用到数据缓存、额外参数、参数校验、熔断等插件，可以对该策略的API **设置API插件** 。

#### **策略详解**

策略主要是用来限制用户的访问权限的，并且在策略上面可以设置一些插件，例如说鉴权插件、流量控制插件、IP黑白名单插件等等。  
常见的分策略方式是按照应用（调用方）分，就是我们实际对接上去网关调用API的调用方，多少个调用方就是多少个策略。  
网关支持匿名策略和非匿名策略。

（1）匿名策略，即 **开放策略** ，访问该策略下的API，无需带策略ID，相当于对用户采用放行访问，可不做任何身份校验；  
（2）非匿名策略，可以当作一家公司、一个部门或者一个用户，访问该策略下的API，需要带策略ID（策略ID作为header参数、body参数（form-data）、query参数）；  
（3）匿名策略仅有一个，非匿名策略可以无限新增；  
（4）匿名策略的插件使用方法与非匿名策略一致，包括流控和各类鉴权插件；  
（5）匿名策略与非匿名策略均支持 **启用** 和 **停用**，停用后，该策略下的接口将不能被使用该策略的用户访问。

###### **例子：**

*若是根据API的QPS进行限流，例如某API的QPS是5000（每秒最多支持5000次访问），这种情况下应该使用****匿名策略****，开放策略同样支持所有的鉴权插件。*

*若是需要对每个用户进行限流，并且不同用户的限流次数不同，这种情况应该使用****非匿名策略****，为每个用户分配一个具体的策略ID，再在各策略下进行限流操作。*

## **实际操作**

#### **操作准备**

（1）通过网关来访问网关的教程页面：<https://help.eolinker.com/agw> ，  
（2）该API无需请求参数，并且采用普通策略，对该策略进行鉴权与限流操作。

#### **操作步骤**

##### **1. 进入AGW控制台，选择一级导航的[接口管理]，新增API项目，新增API“示例接口\_教程页面”，录入该API的文档：**



##### **[映射时去除匹配网关请求路径] 选项说明：**

*例如，网关请求路径为/user\_login，映射路径为/login。  
此时，用户的完整请求地址为：节点IP:端口/user\_login（网关请求路径即为用户访问时的路径）*

* 勾选“映射时去除匹配网关请求路径”，则用户访问路径为：/user\_login，网关转发路径为：/login
* 不勾选“映射时去除匹配网关请求路径”，则用户访问路径为：/user\_login，网关转发路径为：/login/user\_login

#### **注：转发规则**

假设配置了三个API，下面的均是网关请求路径：  
（1）/abc  
（2）/abc/xyz  
（3）/abc/xyz/123

* 若用户访问/abc/xxx，网关会先匹配到/abc路径，再拼接/xxx。也就是转发的时候走（1）的配置。
* 若用户访问/abc/xyz/xxx，网关会先匹配到/abc/xyz路径，再拼接/xxx。也就是转发的时候走（2）的配置。
* 若用户访问的是/abc/xyz/123/xxx，网关会先匹配到/abc/xyz/123路径，再拼接/xxx。也就是转发的时候走（3）的配置。

通过优先匹配最完整路径，可以快速实现API的部署。

##### **2. 新增一个非匿名策略，名叫“示例策略”，得到策略ID，用于用户通过网关访问示例接口：**



##### **3. 我们为示例策略绑定“示例接口\_教程页面”API：**

注：可为不同用户绑定不同API，也可以绑定相同API，根据具体需求而定



##### **4. 访问接口：**

注意事项：

网关通过节点来转发请求，所以需要填写具体的 **节点IP** 或 **节点域名** 来访问请求。

策略ID支持作为header参数、body参数、url参数，参数字段均为：Strategy-Id

###### **此处通过EOLINKER AMS接口管理系统来演示测试访问：**



可以看到，点击 **测试** 按钮后，我们已经能通过网关正确访问接口，用户无需关注网关后面的真实接口地址。

## **插件演示**

#### **一. 鉴权：Apikey鉴权插件**

一般我们都需要为开放的接口加入鉴权，AGW支持动态token鉴权（OAuth2、JWT）和静态token鉴权（Apikey、Basic）。

在这里，我们为刚刚的示例接口添加一个Apikey鉴权。

##### **1. 确保插件在 插件管理 页面是已安装的状态：**



##### **2. 进入策略内页，在 插件设置 > 策略插件 页面，添加Apikey插件：**

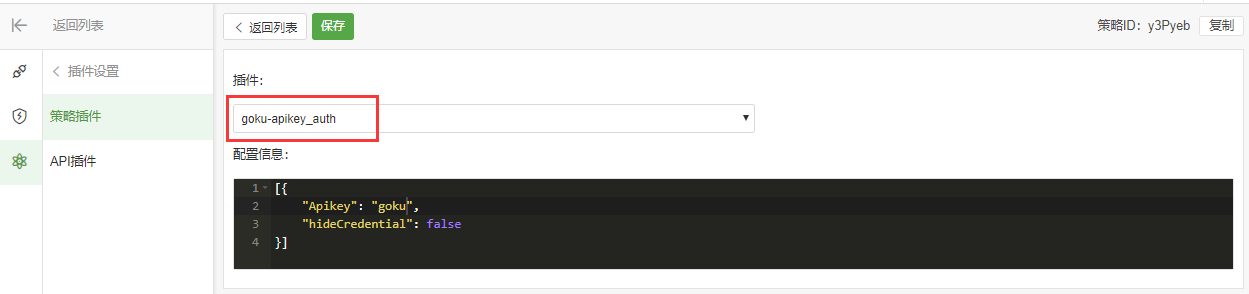
配置信息：

[{

"Apikey": "goku",

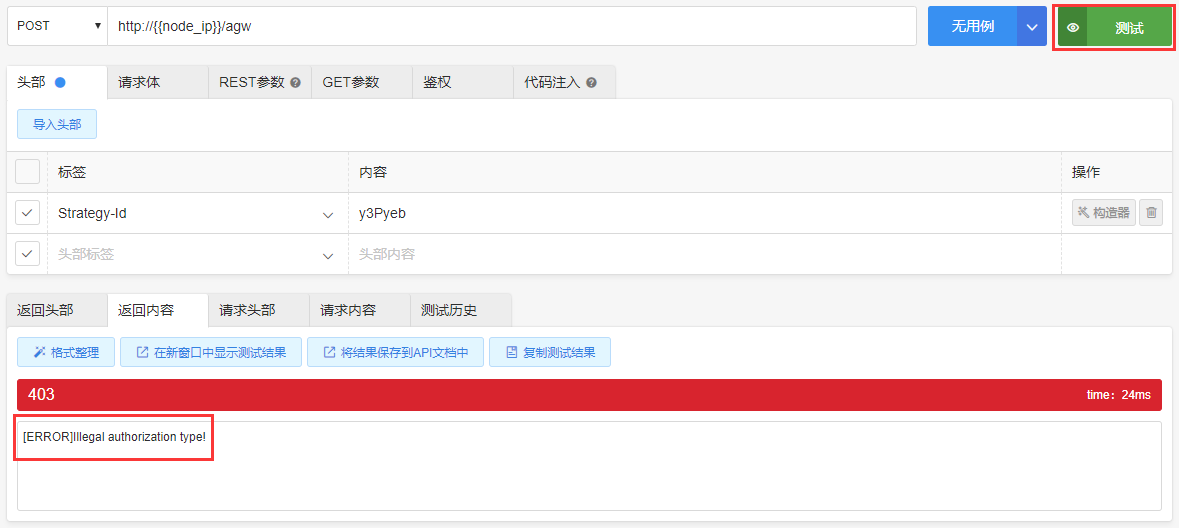
"hideCredential": false

}]



##### **3. 测试访问：**

* 若访问时不加鉴权信息，此时会提示非法的鉴权类型：



* 若填写正确的鉴权信息，则访问成功



*具体的鉴权注意事项请查看教程《快速入门》>>《鉴权规范》*

#### **二. 流量控制插件**

在加入鉴权插件后，我们再为示例策略加入一个流量控制插件，流控插件的支持单位为：时、分、秒、天。在这里，我们限制示例策略每分钟最多访问5次。

##### **1. 确保插件在 插件管理 页面是开启的状态：**

IMG_264

##### **2. 进入策略内页，在 插件设置 > 策略插件 页面，添加流量控制插件：**

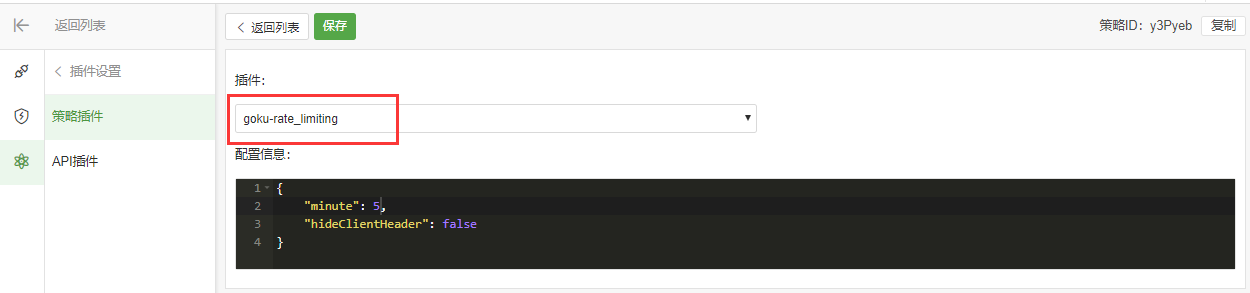
配置信息：

[{

"minute": 5,

"hideClientHeader": false

}]

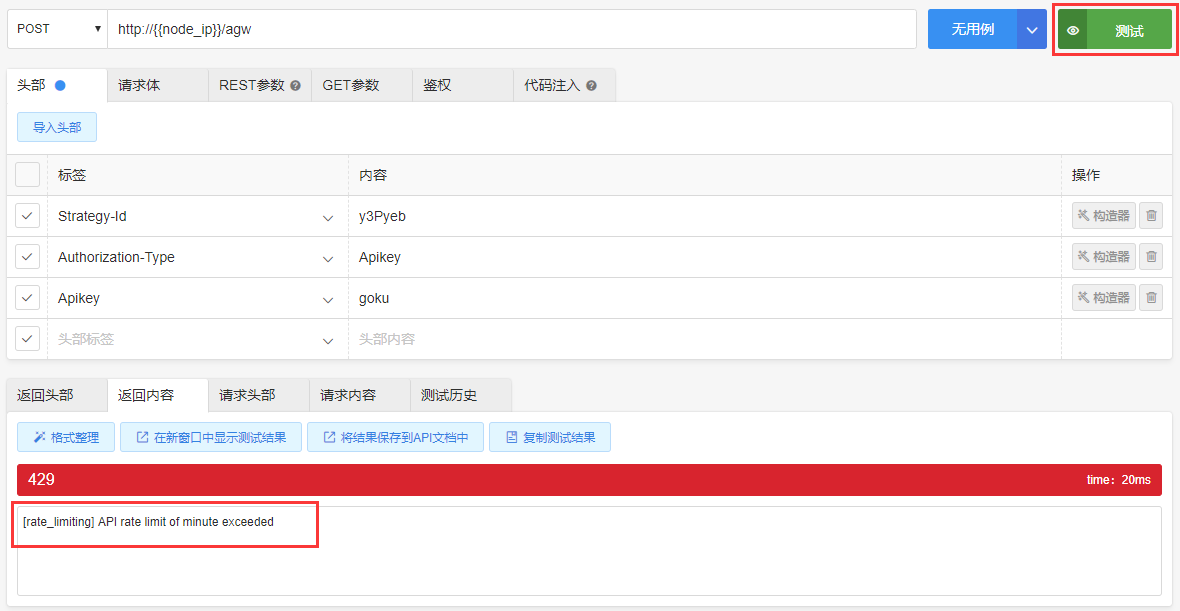


##### **3.现在我们的示例接口需要鉴权访问，并且限制了访问次数，测试访问：**

由于我们配置时：hideClientHeader:false ，所以我们可以在接口的返回头部看到接口剩余次数：

IMG_266

我们访问了5次后，可以看到接口返回超出限制：



**基本术语**

最近更新时间：2019-06-16 03:29:47

### **一. 节点与控制台**

一套完整的网关由一个控制台和若干个网关节点组成。建议控制台与节点分别部署在不同的服务器上，一般一台服务器部署一个网关节点。若服务器上部署了多台虚拟机，则建议控制台、各节点分别部署在不同的虚拟机上。

节点通过IP地址注册在控制台中，控制台内的配置项会对所有节点生效，并且节点会通过主动/被动的更新方式获取控制台上的最新配置信息。

### **二. 网关集群**

网关集群是一个开箱即用的集群，仅需将部署好的网关节点注册到现有的负载均衡器、F5、CDN等即可。网络请求经过上述负载均衡之后会到达网关节点，再通过网关节点转发到目标后端服务。

虽然每一个网关节点也支持负载均衡，但是该负载仅限于对真实后端服务器的负载均衡，而非受控端的负载均衡。

### **三. 负载后端**

负载后端是一组用于负载均衡的真实后端（Target/Upstream）的集合，真实后端可以是IP地址:端口或域名。

一个负载后端对应多个真实后端，每个真实后端可以设置不同权重（weight），网关按权重几率访问实际后端，最终实现负载均衡。

### **四. 策略**

网关分开 **开放策略** 与非开放的 **普通策略**：

* 开放策略，访问该策略下的API，无需带策略ID，相当于对用户采用放行访问，可不做任何身份校验；
* 普通策略，可以当作一家公司、一个部门或者一个用户，访问该策略下的API，需要带策略ID（策略ID作为header参数、body参数（form-data）、query参数）；
* 开放策略仅有一个，普通策略可以无限新增；
* 开放策略的插件使用方法与普通策略一致，包括流控和各类鉴权插件；
* 开放策略与普通策略均支持 **启用** 和 **停用**，停用后，该策略下的接口将不能被使用该策略的用户访问。

*某API的10分钟内最多支持5000次访问，这种情况下可以使用****开放策略****对API进行限流操作，开放策略同样支持所有的鉴权插件。  
如果是需要对每个用户进行限流，此时应该采取****普通策略****，为每个用户分配一个具体的策略ID，再对每个策略进行限流操作。*

### **五. 接口管理**

GoKu支持管理多个API项目，每个项目最多支持三级API分组。

每个API下可绑定多个插件，包括：参数映射插件、额外参数插件、请求大小限制插件、参数校验插件、数据缓存插件、熔断插件等。

### **六.权限管理**

##### **角色：**

网关支持权限角色控制，分为系统管理员、管理员、普通成员。

* 系统管理员：拥有最高级操作权限，可以新建管理员和普通成员，自定义普通成员的权限。
* 管理员：拥有最高级操作权限，可以新建普通成员，自定义普通成员的权限。
* 普通成员：根据赋予的权限，拥有相应模块的操作权限。

##### **功能模块：**

网关在控制台分为八大功能模块，分别是：

* 监控管理
* 接口管理
* 负载后端
* 策略管理
* 节点管理
* 插件管理
* 网关设置
* 告警管理
* 权限管理：此模块不在分配权限范围内

### **七. 插件**

##### **官方插件**

GOKU的插件分为：网关插件、策略插件、API插件。  
（1）网关插件，指针对整个GoKu节点来配置的插件，如日志。  
（2）策略插件，针对策略组来配置的插件，主要是鉴权、流控类插件，如流量控制、APIKey鉴权等。  
（3）API插件，仅可针对API来配置的插件，主要是请求处理类插件，如参数映射、参数校验等。

##### **自定义插件**

GOKU支持通过GO语言开发插件，插件类型依旧分为：网关插件、策略插件、API插件。

### **八. 插件的开启与禁用**

受控端网关服务根路径下拥有plugin文件夹，将需要开启的GoKu插件（.so后缀）文件以及相应的配置信息解压后放置于plugin文件夹内，通过控制台启用插件并且重启网关使得插件生效。

### **九. 插件状态**

插件状态分为：开启/关闭；启用/停用  
（1）**开启/关闭** 是针对控制台的状态，**启用/停用** 是针对配置对象（网关/策略/API）的状态。  
（2）插件启用后方可进行配置。  
（3）启用后，插件的使用状态默认为开启，可以选择关闭插件。  
（4）关闭，插件在控制台的状态仍为启用，但是对于配置对象而言，插件的状态为关闭。

**插件系统**

最近更新时间：2019-04-23 10:13:50

GoKu EE 的插件分为三类：**网关插件** 、**策略组插件** 和 **API插件**：

* 网关插件，指针对整个GoKu节点来配置的插件，如HTTP日志。
* 策略组插件，针对策略组来配置的插件，主要是鉴权、流控类插件，如流量控制、APIKey鉴权、OAuth2.0等。
* API插件，仅可针对API来配置的插件，主要是请求处理类插件，如参数映射、参数校验等。

插件优先级指的是插件当前的执行顺序，优先级高的先执行。  
注：不支持修改官方插件的信息，包括优先级、名称等。

| **插件名称** | **字段名** | **插件类型** | **作用范围** | **优先级** |
| --- | --- | --- | --- | --- |
| JWT鉴权 | goku-jwt\_auth | 策略 | 转发前 | 1005 |
| OAuth2鉴权 | goku-oauth2\_auth | 策略 | 转发前 | 1004 |
| APIKey鉴权 | goku-apikey\_auth | 策略 | 转发前 | 1003 |
| Basic鉴权 | goku-basic\_auth | 策略 | 转发前 | 1001 |
| IP黑白名单 | goku-ip\_restriction | 策略 | 转发前 | 990 |
| 流量控制 | goku-rate\_limiting | 策略 | 转发前 | 989 |
| 防重放攻击 | goku-replay\_attack\_defender | 策略 | 转发前 | 989 |
| 跨域 | goku-cors | 策略 | 转发前 | 985 |
| 默认返回 | goku-default\_response | 策略 | 转发前 | 960 |
| 请求大小限制 | goku-request\_size\_limiting | API | 转发前 | 951 |
| 返回头部 | goku-response\_headers | 策略 | 获取回复后 | 945 |
| 熔断 | goku-circuit\_breaker | API | 转发前、获取回复后 | 931 |
| 服务降级 | goku-service\_downgrade | API | 转发前、获取回复后 | 930 |
| 数据缓存 | goku-proxy\_caching | API | 转发前 | 915 |
| 参数校验 | goku-params\_check | API | 转发前 | 910 |
| 格式转换 | goku-data\_format\_transformer | API | 转发前 | 850 |
| 参数映射 | goku-params\_transformer | API | 转发前 | 801 |
| 额外参数 | goku-extra\_params | API | 转发前 | 800 |
| HTTP日志 | goku-http\_log |  |  |  |

**鉴权规范**

最近更新时间：2019-06-15 16:43:23

鉴权的对象为 **策略** (Strategy) ，策略可表示为一个公司、一个业务部门或一个用户。  
网关支持五种鉴权方式：Public、Basic、Apikey、OAuth2、JWT。

* 如果不开启这四种鉴权（Basic、Apikey、OAuth2、JWT）的任意一种，网关视为 **Public** 鉴权，此时网关不会对访问者进行身份校验。
* 同一策略支持同时开启多种鉴权，根据头部的Authorization-Type字段判定具体是何种鉴权。
* Apikey、OAuth2、JWT这三种鉴权默认支持三个地方传参：**header/body/query** 。
* 以下是四种鉴权的 **参数位置** 、**参数名** 以及 **Authorization-Type** 的值：

| **鉴权方式** | **header** | **body** | **query** | **Authorization-Type** |
| --- | --- | --- | --- | --- |
| Basic | Authorization |  |  | Basic |
| Apikey | Authorization:”Apikey” | Apikey | Apikey | Apikey |
| OAuth2 | Authorization:”bearer token值 或 token值” | access\_token | access\_token | Oauth2 |
| JWT | Authorization:”bearer token值 或 token值” |  |  |  |