

一 kong 部署

1.1 部署 kong 的依赖数据库 postgres

```
docker run -d --name kong-database --net=host -v /data/kong-database/data:/var/lib/postgresql/data -e "POSTGRES_USER=kong" -e "POSTGRES_DB=kong" postgres:9.5
```

1.2 初始化 kong 数据库

```
docker run --rm \
  --link kong-database:kong-database \
  -e "KONG_DATABASE=postgres" \
  -e "KONG_PG_HOST=kong-database" \
  -e "KONG_CASSANDRA_CONTACT_POINTS=kong-database" \
  172.16.59.153/aiaas/aikong:1.0.3 kong migrations up
```

1.3 启动 kong

```
docker run -d --name kong --net=host \
  -e "KONG_PG_HOST=10.1.87.70" \
  -e "KONG_PLUGINS=bundled,xfyun-hmac-ws" \
  -e "KONG_LOG_LEVEL=error" \
  -e "KONG_ADMIN_LISTEN=127.0.0.1:8001" \
  -e "KONG_ADMIN_LISTEN_SSL=127.0.0.1:8444" \
  -e "KONG_PROXY_LISTEN=0.0.0.0:80" \
  -e "KONG_PROXY_LISTEN_SSL=0.0.0.0:443" \
  172.16.59.153/aiaas/aikong:1.0.3
```

1.4 部署 kong 管理控制台 konga

```
docker run -d --net=host -e "TOKEN_SECRET=123456" -e "NODE_ENV=production" --name konga pantsel/konga:0.13.0
```

二 kong 配置 (使用 konga 控制台)

准备工作: CONNECTIONS->NEW CONNECTION 将 kong 的 admin api 地址添加进来 (http:127.0.0.1:8001)

2.1 创建 service

SERVICES->ADD NEW SERVICE

Services

Service entities, as the name implies, are abstractions of each of your own upstream services. Example

+ ADD NEW SERVICE

必填配置：

CREATE SERVICE ×

Name (optional)	webgate-ws-iat The service name.
Description (optional)	iat web api service An optional service description.
Tags (optional)	Optionaly add tags to the service
Url (shorthand-attribute)	Shorthand attribute to set protocol , host , port and path at once. This attribute is write-only (the Admin API never "returns" the url).
Protocol (semi-optional)	http The protocol used to communicate with the upstream. It can be one of http or https .
Host (semi-optional)	upstream-webgate-ws-iat The host of the upstream server.
Port (semi-optional)	8082 The upstream server port. Defaults to 80 .
Path (optional)	/ The path to be used in requests to the upstream server. Empty by default.
Retries (optional)	5 The number of retries to execute upon failure to proxy. The default is 5 .
Connect timeout (optional)	60000 The timeout in milliseconds for establishing a connection to your upstream server. Defaults to 60000 .
Write timeout (optional)	60000 The timeout in milliseconds between two successive write operations for transmitting a request to the upstream server. Defaults to 60000 .
Read timeout (optional)	60000 The timeout in milliseconds between two successive read operations for transmitting a request to the upstream server. Defaults to 60000 .

Host: 上游服务地址，可以是具体的 IP 地址，也可以是个 upstream-name

Port: 上游服务端口号

2.2 创建 Routes

Service webgate-ws-iat

services / show

Service Details

Routes

Plugins

Eligible consumers

beta

Routes

+ ADD ROUTE

search routes...

HostsPathsProtocolsMethodsRegex priorityCreated

no data found

ADD ROUTE TO WEBGATE-WS-IAT

* For hosts, paths, methods and protocols, press enter to apply every value you type

Hosts
(semi-optional)

ws-api.xfyun.cn x 10.1.87.70 x

A list of domain names that match this Route. For example: example.com. At least one of hosts, paths, or methods must be set.

Paths
(semi-optional)

/v2/iat x

A list of paths that match this Route. For example: /my-path. At least one of hosts, paths, or methods must be set.

Methods
(semi-optional)

GET x

A list of HTTP methods that match this Route. At least one of hosts, paths, or methods must be set.

Strip Path
(optional)

☐ NO

When matching a Route via one of the paths, strip the matching prefix from the upstream request URL.

Preserve Host
(optional)

☐ NO

When matching a Route via one of the hosts domain names, use the request Host header in the upstream request headers. By default set to false, and the upstream Host header will be that of the Service's host

Protocols
(semi-optional)

http x https x

A list of the protocols this Route should allow. By default it is ["http", "https"], which means that the Route accepts both. When set to ["https"], HTTP requests are answered with a request to upgrade to HTTPS.

✓ SUBMIT ROUTE

2.3 配置鉴权插件

Websocket 接口使用 xfyun-hmac-ws 插件，http 接口使用 hmac-auth 插件

Service webgate-ws-iat

[services](#) / [show](#)

Service Details

Routes

Plugins

Eligible consumers

beta

Assigned plugins

Name	Consumer	Created
------	----------	---------

+ ADD PLUGIN

Authentication

Security

Traffic Control

Serverless

Analytics & Monitoring

Transformations

Logging

Custom

CUSTOM

Custom Plugins

Xfyun Hmac Ws



no description available...

ADD PLUGIN

ADD XFYUN HMAC WS

Configure the Plugin.

clock skew

300

enforce headers

host x

date x

requets-line x

Tip: Press **Enter** to accept a value.

algorithms

hmac-sha256 x

Tip: Press **Enter** to accept a value.

anonymous

hide credentials

NO

✓ ADD PLUGIN

2.4 创建 upstream ， upstream name 和 第一步创建 service 中填的 Host 中的值保持一致，

Upstreams

The upstream object represents a virtual hostname and can be used to loadbalance incoming requests over multiple services (targets). So for example an upstream named `service.v1.xyz` with an API object created with an `upstream_url=https://service.v1.xyz/some/path`. Requests for this API would be proxied to the targets defined within the upstream.

+ CREATE UPSTREAM

search_Results: 25

CREATE UPSTREAM

Name

upstream-webgate-ws-iat

(required)

This is a hostname like name that can be referenced in an `upstream_url` field of an `api` or the `host` of a service.

Slots

1000

(optional)

The number of slots in the loadbalancer algorithm (`10-65536`, defaults to `1000`).

Hash on

none

(optional)

What to use as hashing input: `none`, `consumer`, `ip`, or `header` (defaults to `none` resulting in a weighted-round-robin scheme).

Hash fallback

none

(optional)

What to use as hashing input if the primary `hash_on` does not return a hash (eg. header is missing, or no consumer identified)

Active health checks

Passive health checks

✓ SUBMIT UPSTREAM

Name:upstream name
Slots: 哈希算法中哈希槽的数量
Hash on:用于计算 hash 的字段
Hash fallback: 当没有取到 hash 字段时用于计算 hash 的字段

经过以上四步，一个基本可用的服务即可配置出来

三 kong 服务发现配置，使上游服务启动时能够自动注册 upstream。

3.1 创建 service kong-service-find

Name: kong-service-find

Host: 127.0.0.1 # kong admin api 监听地址

Port: 8001 #kong admin api 监听端口

Service 的创建方法参考 2.1

3.2 为 kong-service-find 创建路由

ADD ROUTE TO KONG-SERVICE-FIND

×

* For hosts, paths, methods and protocols, press enter to apply every value you type

Hosts
(semi-optional)

10.1.87.70 ×

A list of domain names that match this Route. For example: example.com. At least one of hosts, paths, or methods must be set.

Paths
(semi-optional)

/kong-service-find ×

A list of paths that match this Route. For example: /my-path. At least one of **hosts**, **paths**, or **methods** must be set.

Methods
(semi-optional)

GET × POST × DELETE × PATCH ×

A list of HTTP methods that match this Route. At least one of **hosts**, **paths**, or **methods** must be set.

Strip Path
(optional)

YES

When matching a Route via one of the **paths**, strip the matching prefix from the upstream request URL.

Preserve Host
(optional)

NO

When matching a Route via one of the **hosts** domain names, use the request **Host** header in the upstream request headers. By default set to **false**, and the upstream Host header will be that of the Service's **host**.

Protocols
(semi-optional)

A list of the protocols this Route should allow. By default it is **["http", "https"]**, which means that the Route accepts both. When set to **["https"]**, HTTP requests are answered with a request to upgrade to HTTPS.

✓ SUBMIT ROUTE

需要开启 strip path，如上，开启后上游服务可用通过 curl -X POST <http://10.1.87.70:8000/kong-service-find/upstreams/upstream-webgate-ws-iat/targets> -d "target=10.1.87.70:8082" 向 kong 注册服务。

3.3 服务发现路由放在 kong 上相当于暴露在公网上，需要添加 hmac-auth 插件并且添加 acl 控制。让只有指定的用户可以访问该接口

ADD PLUGIN



Authentication

Security

Traffic Control

Serverless

Analytics & Monitoring

Transformations

Logging

Custom

🔒 AUTHENTICATION

Protect your services with an authentication layer

Basic Auth



Add Basic Authentication...

ADD PLUGIN

Key Auth



Add a key authentication...

ADD PLUGIN

OAuth2



Add an OAuth 2.0...

ADD PLUGIN

Hmac Auth



Add HMAC Authentication...

ADD PLUGIN

Jwt



Verify and authenticate...

ADD PLUGIN

Ldap Auth



Integrate Kong with a LDAP...

ADD PLUGIN

EDIT HMAC AUTH



Add HMAC Signature Authentication to your APIs to establish the identity of the consumer. The plugin will check for valid signature in the **Proxy-Authorization** and **Authorization** header (in this order). This plugin implementation follows the [draft-cavage-http-signatures-00](#) draft with slightly changed signature scheme.

ENABLED

clock skew 300

Clock Skew in seconds to prevent replay attacks

validate request body

NO

enforce headers

host x

date x

request-line x

Tip: Press **Enter** to accept a value.

algorithms

hmac-sha256 x

Tip: Press **Enter** to accept a value.

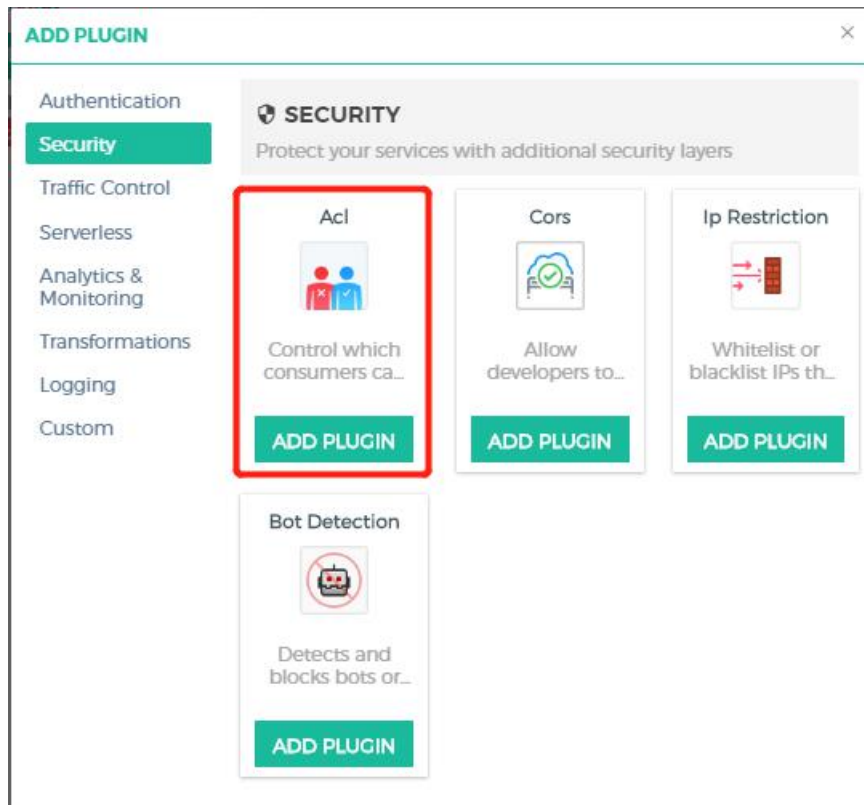
anonymous

hide credentials

NO

An optional boolean value telling the plugin to hide the credential to the upstream API server. It will be removed by Kong before proxying the request

✓ SUBMIT CHANGES



ADD ACL

Restrict access to an API by whitelisting or blacklisting consumers using arbitrary ACL group names. This plugin requires an authentication plugin to have been already enabled on the API.

hide groups header ☐ NO

blacklist

Tip: Press **Enter** to accept a value.

Comma separated list of arbitrary group names that are not allowed to consume the API. At least one between whitelist or blacklist must be specified.

whitelist

acl-service-find x

Tip: Press **Enter** to accept a value.

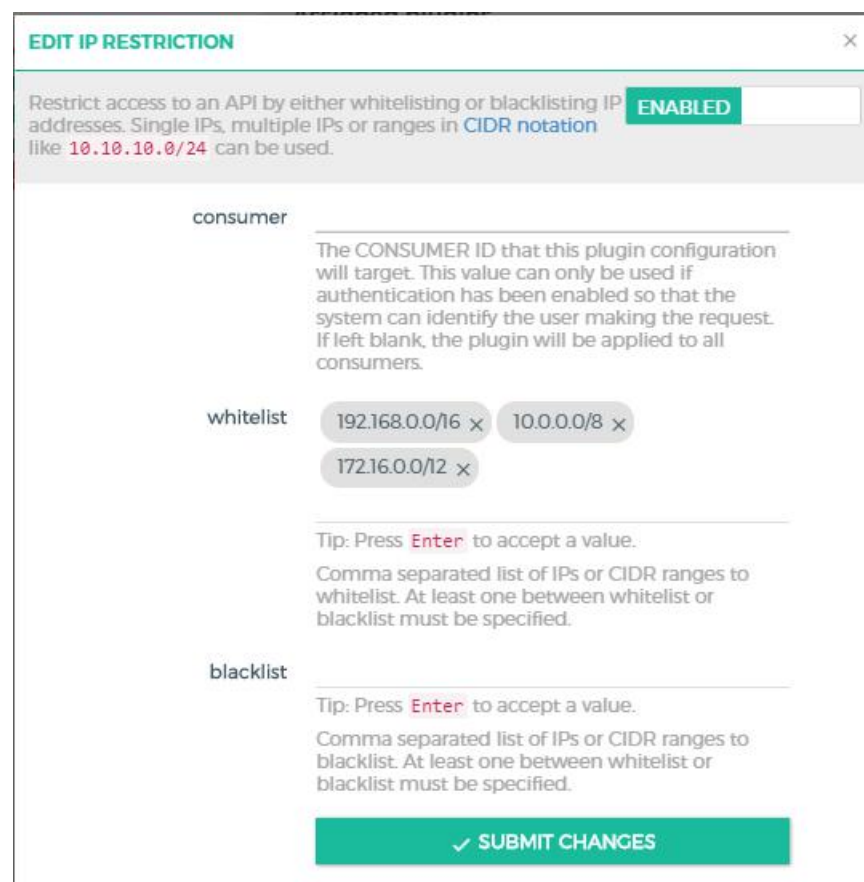
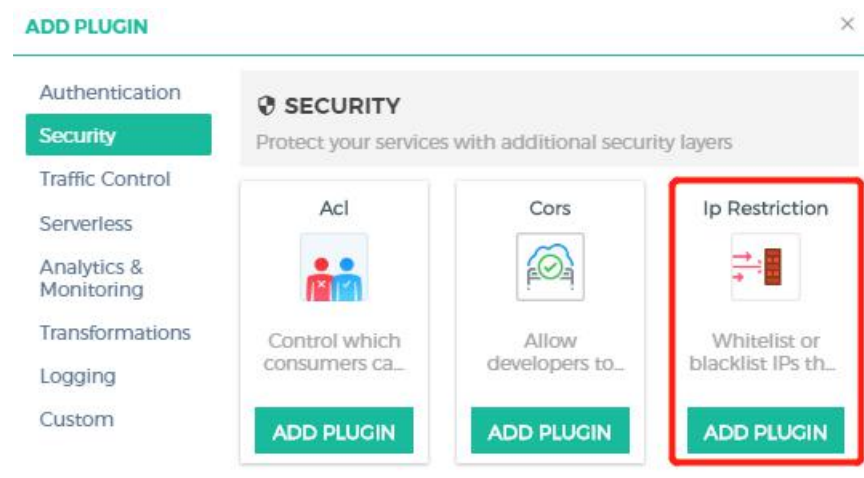
Comma separated list of arbitrary group names that are allowed to consume the API. At least one between whitelist or blacklist must be specified.

✓ ADD PLUGIN

添加了 hmac-auth 后上游服务需要认证登录才能访问该服务，（后面涉及到用户的插件都需要开启这个插件或者 xfyun-hamc-ws 插件才能生效）

添加了 acl whitelist 后只有隶属于改 whitelist 组的用户才有权限访问该服务。用户和用户组的添加参考下一节

为了更加安全起见，还可以为服务配置 ip 白名单，使该接口只能通过内网访问



四 用户的创建

4.1 创建用户(App_id)

CONSUMERS-> CREATE CONSUMER

Consumers

The Consumer object represents a consumer - or a user - of an API. You can either rely on Kong as the primary datastore, or you can map the consumer list with your database to keep consistency between Kong and your existing primary datastore.

+ CREATE CONSUMER

search_Results: 25

CREATE CONSUMER

username12345678
(semi-optional)
The username of the consumer. You must send either this field or `custom_id` with the request.

custom_id
(semi-optional)
Field for storing an existing ID for the consumer, useful for mapping Kong with users in your existing database. You must send either this field or `username` with the request.

✓ SUBMIT CONSUMER

Username: 用户名，即 appid
Custom_id: 用来关联外部的用户 id，可以为空

4.2 创建 api_key 和 secret

api_key 和 apisecret 用于鉴权，配置了鉴权插件（hmac-auth，xfyun-hmac-auth）的服务需要带上 api_key 和 apisecret 构建鉴权的参数才能访问服务。

CONSUMER: 12345678

consumers / edit consumer

Details

Groups

Credentials

Accessible APIs

Accessible Services

Accessible Routes

Plugins

BASIC

API KEYS

HMAC

OAuth2

JWT

<> HMAC Auth

+ CREATE CREDENTIALS

You have not created any HMAC credentials for this consumer yet

HMAC AUTH

Create HMAC credentials for **12345678**

username
(required) a6be919ece4be37083cdde67079
The username to use in the HMAC Signature verification

secret
(optional) kmkSqZwJARY5S7eMOLvQ2IElp
The secret to use in the HMAC Signature verification

✓ SUBMIT

Username: 即 api_key
Secret: 即 api_secret

4.3 添加用户到 acl 组

对于添加了 **acl** 插件的服务，只有在 **acl** 组中的用户才能访问到改服务，如第三章的服务发现服务，为用户添加到 **acl** 组后，该用户就有了访问对应的 **acl** 插件控制的服务的权限。

CONSUMER: 12345678
consumers / edit consumer

Details Groups Credentials Accessible APIs Accessible Services Accessible Routes Plugins

+ Add a group

ADD GROUP

Add a group to this consumer

Group name
(required) acl-service-find
The name of the ACL group

✓ SUBMIT GROUP

如上图所示，用户 **12345678** 添加进了服务发现 **acl** 组，使用 **12345678** 这个用户的 **apikey** 和 **apisecret** 就可以访问到服务发现服务了。