Apusic 金蝶天燕

生成时间：2026-05-19

用户手册

金蝶Apusic负载均衡器v2.0

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

Apusic是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

1 用户手册

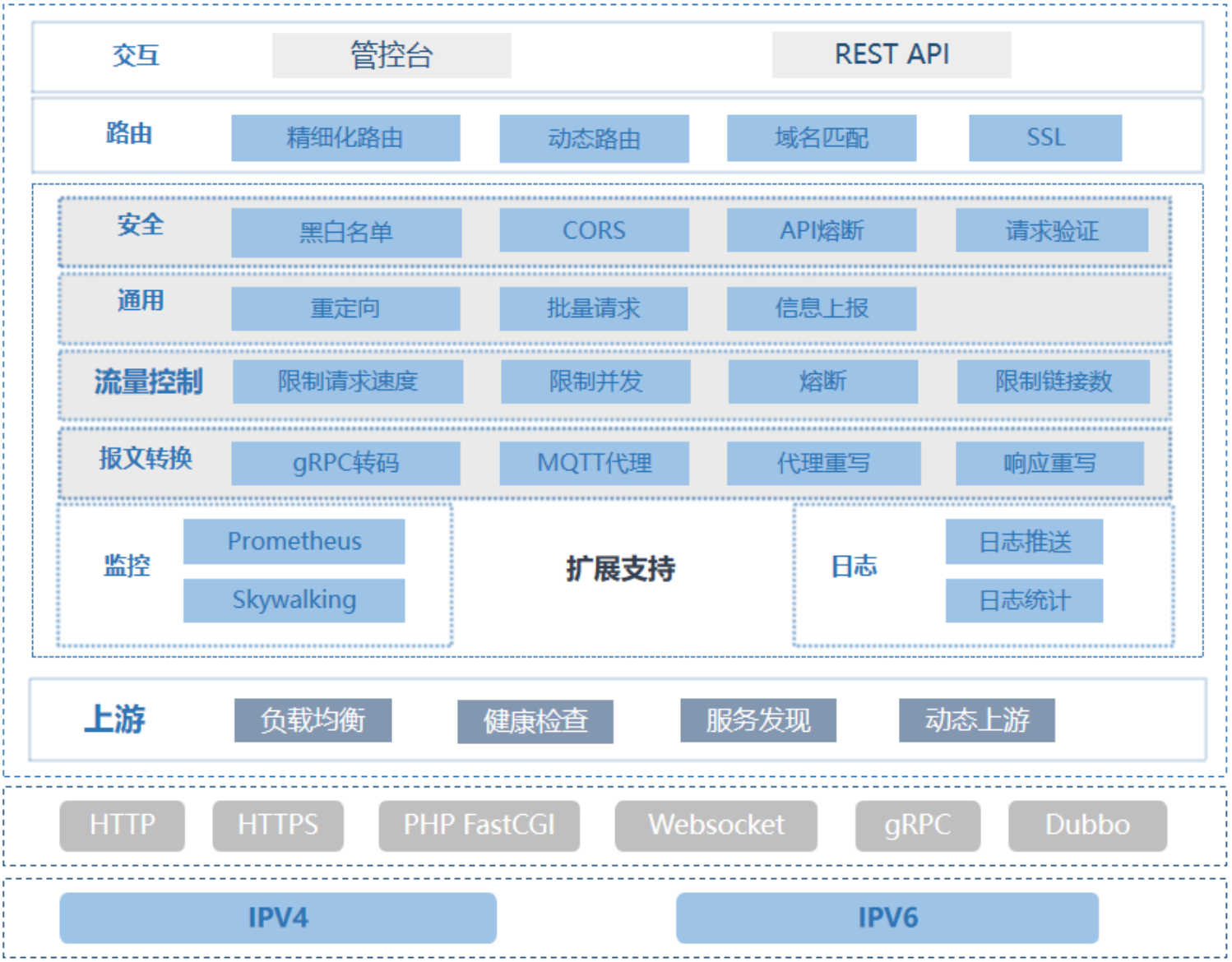
本用户手册指南介绍了金蝶Apusic负载均衡软件v2.0产品的安装、快速入门和产品功能介绍等内容。

1.1 基本介绍

金蝶Apusic负载均衡软件（Apusic Load Balance，ALB）是一款具备高性能、高可用性和可扩展性的流量治理软件。ALB能够应对大规模的集群、云平台在面向客户端提供服务时，对客户端访问请求和流量管理的需求，实现访问请求的验证、处理、转换和分发等操作，从而隔离客户端访问对提供服务的应用系统、平台以及资源的直接影响，达到对服务集群访问流量控制、访问管理和负载均衡的目的。

1.2 产品功能架构

ALB标准版的功能如下图所示：



2 产品安装

2.1 安装说明

相关资源

针对不同的操作系统及CPU架构平台，金蝶Apusic负载均衡软件提供不同的安装包。更多产品介质相关信息，可以访问金蝶天燕官方网站http://www.apusic.com获取。

基本概念

在正确使用应用服务器来部署、管理应用之前，需要先理解以下几个基本概念：

ALB：Apusic Load Balance，金蝶Apusic负载均衡软件。

- 安装与使用
- 安装前准备
- 获取安装包

> *从http://www.apusic.com/下载金蝶Apusic负载均衡软件v2.0安装包，或从金蝶Apusic负载均衡软件产品光盘中获得相应的安装包文件。*

支持的环境

平台类型	系统类型
芯片类型	鲲鹏、飞腾、兆芯等通用x86或arm架构cpu
国产操作系统	OpenEuler、统信UOS、银河麒麟系列、深度等
其他Linux系列	RedHat系列、CentOS、Suse Linux系列等

2.2 产品安装

下面以ARM架构下Kylin系统上安装ALB为例，下载好安装文件alb-standard-2.0-arm.tar.gz后，其安装步骤有：

1. 解压安装包
2. 导入license
3. 启动ALB

2.2.1 解压安装包到指定目录

1. 上传alb安装包至安装服务器的任意安装目录，（推荐/opt目录）。
2. 解压安装包：`tar -zvxf alb-standard-2.0-arm.tar.gz` 获得alb-standard-2.0文件夹。

3. 进入解压后的文件夹: `cd alb-standard-2.0-arm` 。

备注：下面演示的安装路径为/opt/目录（支持安装在任意目录）。

2.2.2 导入license

1. 将金蝶KBC授权或本地授权，把**授权文件放置在 `安装目录/alb-standard` 文件夹**下，

2.2.3 启动、停止、重新加载

- 启动： `./bin/start-alb.sh`
- 停止： `./bin/stop-alb.sh`
- 重新加载： `./bin/reload-alb.sh`

2.3 产品License配置说明

ALB标准版支持金蝶天燕认证、金蝶KBC认证、金蝶统一授权三种模式，默认授权类型为**金蝶KBC授权**。

金蝶KBC授权和本地授权，请把**授权文件放置在 `安装目录/alb-standard` 文件夹**下，

1. 授权类型配置

alb授权类型的配置文件为： **安装目录**`/alb-standard/conf/alb_license.conf`

```
license kbc license.lic;  # 使用KBC授权模式，授权文件为license.lic
```

如果如果授权文件名字不是license.lic, 需要在配置文件中将license.lic替换成实际的授权文件名即可。

2. 授权类型配置格式

语句格式规范： `license [授权类型] [授权文件或地址];`

3. 不同授权类型及其配置说明

- local: 表示金蝶天燕本地授权，后面需要紧跟授权文件。
  - 如： `license local license.xml;` ，
  - 把本地授权文件license.xml放置在 **安装目录**`/alb-standard` 文件夹下。
- kbc: 表示金蝶KBC授权，后面需要紧跟授权文件。如： `license kbc license.lic;` ，
  - KBC特征码获取：1、直接启动，2、授权配置文件写： `license kbc;`
  - 执行ALB启动 `./bin/start-alb.sh` 脚本，获取授权码: `KBC auth: Auth Code is: SZTY2500879438` 。
  - 授权码为SZTY开头的内容,如上为： `SZTY2500879438`
  - 使用授权码在KBC系统中申请授权文件。

- 获取授权文件后，放入 **安装目录**`/alb-standard`，并确认授权文件名和alb_license.conf配置一致（如上为license.lic文件），重启ALB即可。
- **注**：在多网卡多ip环境中，可以通过-ac参数指定网卡或ip，如 `license kbc license-file.lic -ac eth0`

- center: 表示金蝶天燕统一授权中心，后面需要跟授权服务器地址(IP:端口)、租户名称和命名空间。如：`license center 172.21.33.33:6789 tenant namespace;`
  - 如果租户名称不确定，可以填写为public。

4. 通过环境变量设置统一授权配置 alb支持环境变量中设置统一授权的配置，如下为使用export设置对应的环境变量：

```
export apusic_acls_enable=true                  # 开启变量统一授权
export apusic_acls_authUrls=172.24.3.116:6869   # 统一授权中心地址
export apusic_acls_ns=后付费                     # 命名空间
export apusic_acls_tenant=user_env中文           # 租户名称
```

3 产品快速入门

本快速入门指南介绍了金蝶Apusic负载均衡软件v2.0产品的功能和使用，为用户快速使用本产品提供指导。

3.1 登录管理控制台

打开浏览器（推荐Chrome、firefox），输入地址 `http://serverIP:serverPort/` 进入到管理控制台登录页面。

例如：将ALB部署在172.20.140.137端口默认为9000，登录地址则为： `http://172.20.140.137:9000`

输入用户名密码登录管理控制台。

- 用户名为： `admin`
- 初始密码为： `apusic$alb`

3.2 使用ALB创建反向代理

前提条件：

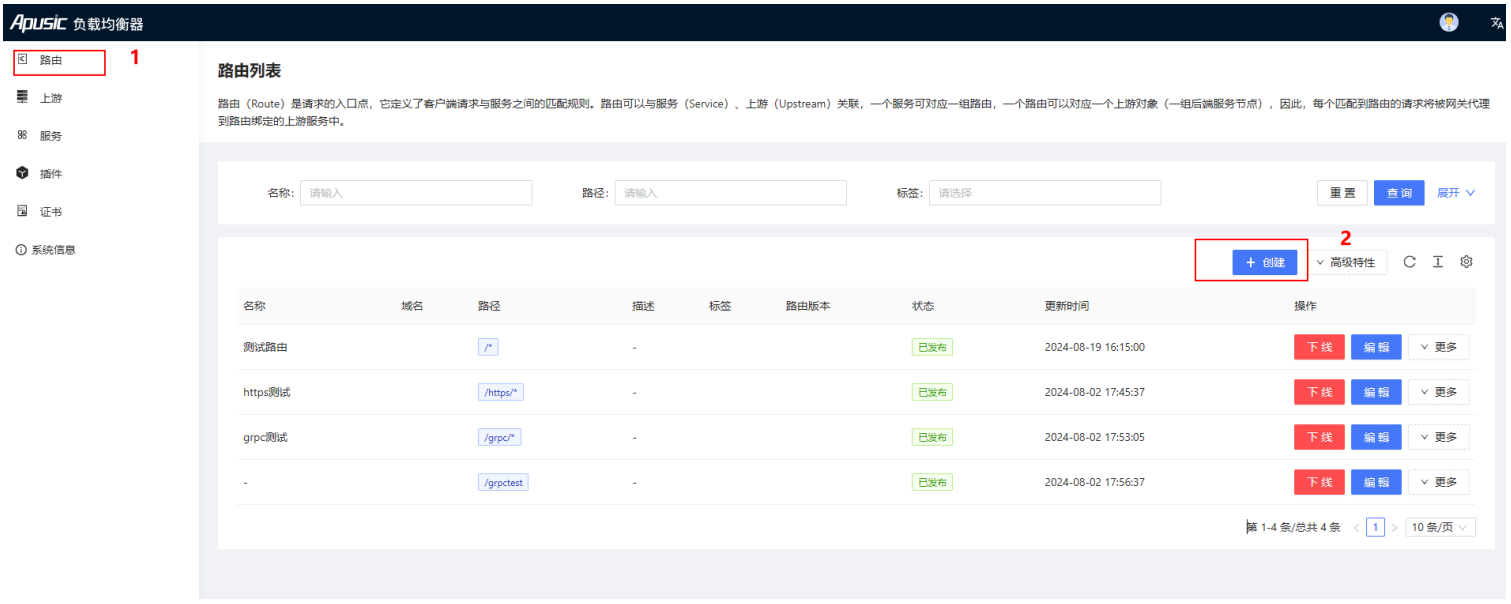
- 已经部署好的ALB
- 已经部署好的后端服务

操作步骤：

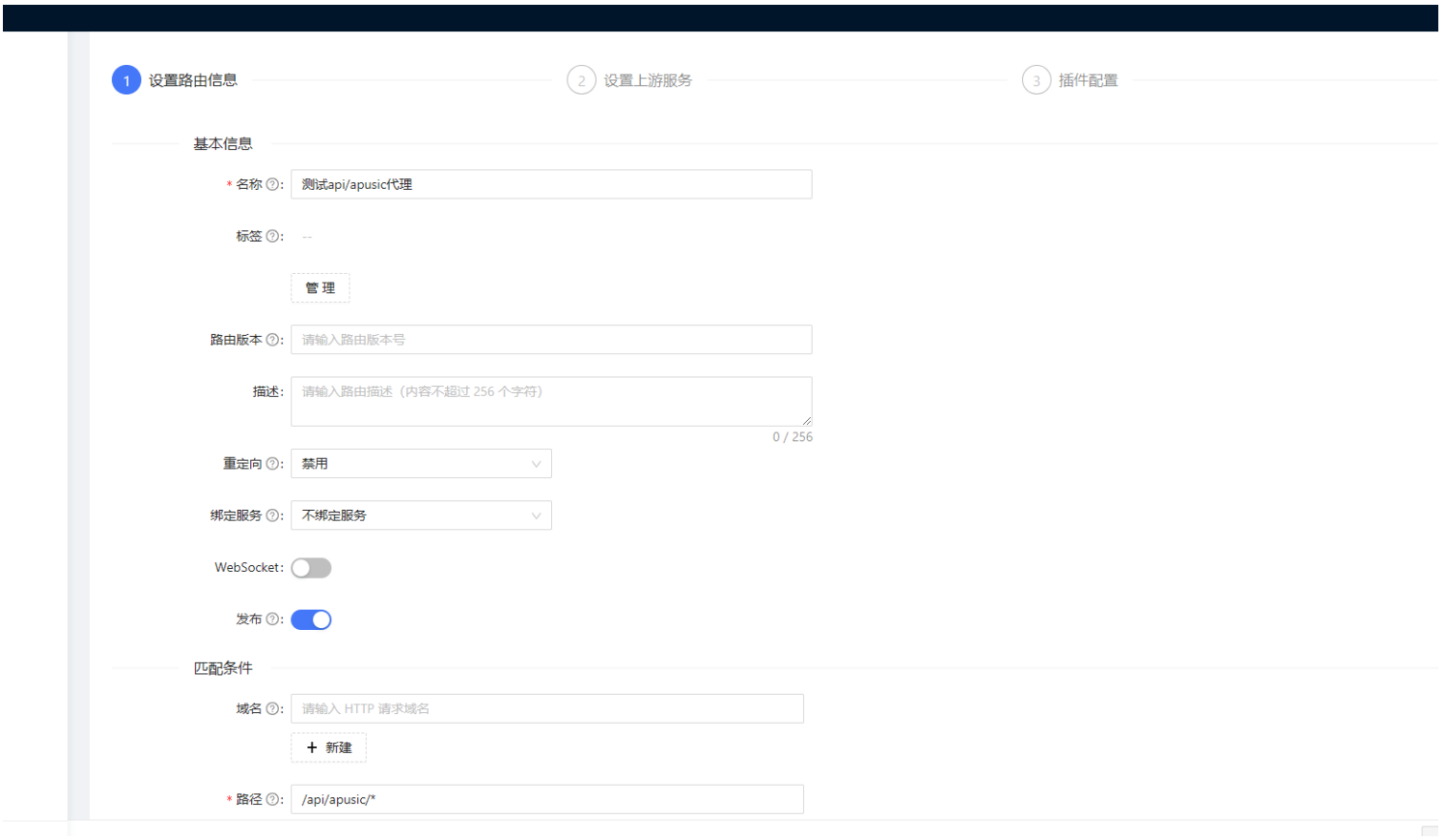
1. 登录ALB管理页面，点击“创建路由”按钮。
2. 填写路由信息，包括路由名称、代理url前缀等信息，点击下一步
3. 填写后端服务信息，包括节点地址和端口、负载均衡算法等信息，点击下一步
4. 插件配置这块点击下一步
5.

如： 配置代理url前缀为`/api/apusic`，后端服务地址为`http://172.21.32.42:8000`，其配置过程如下：

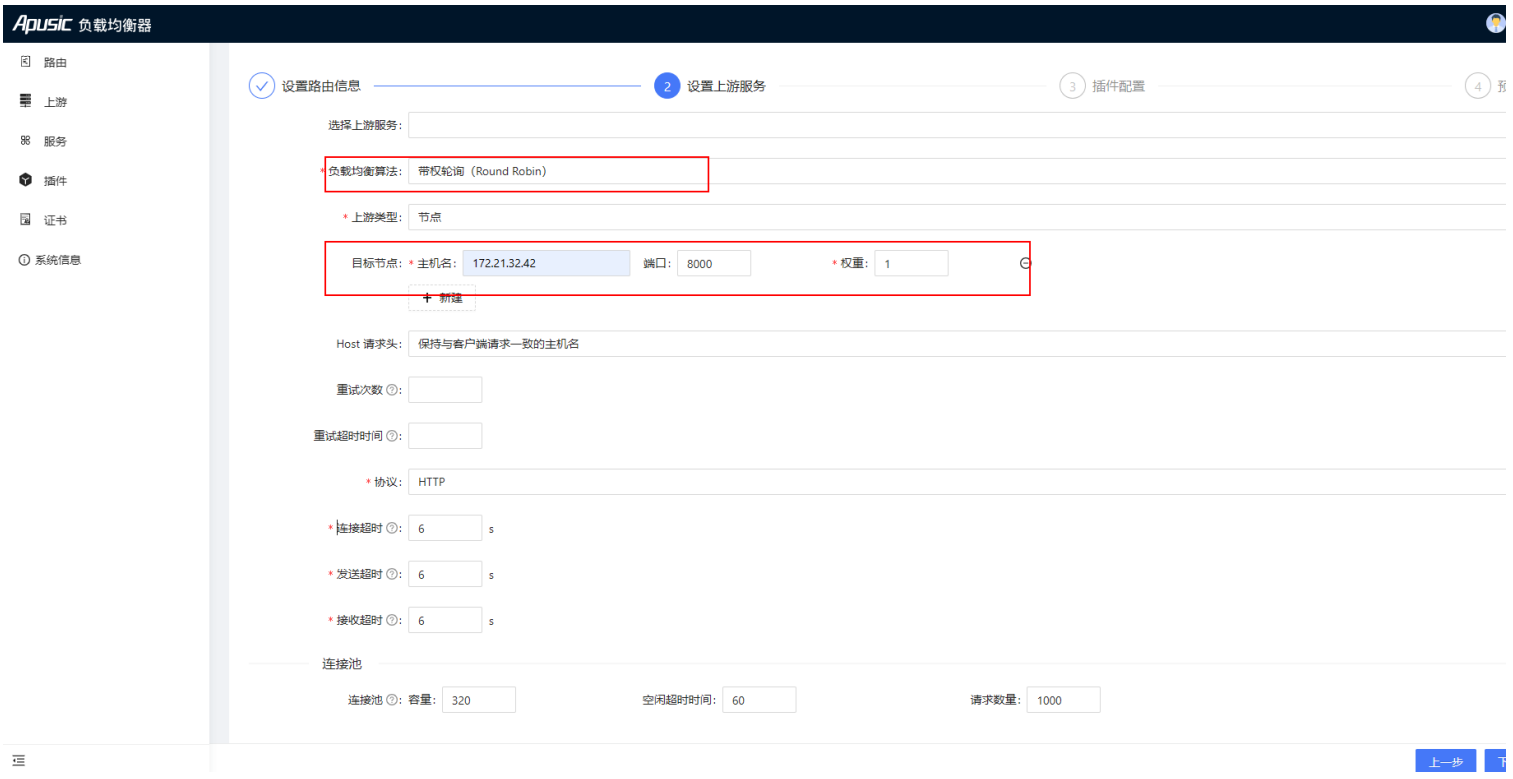
1、点击创建路由



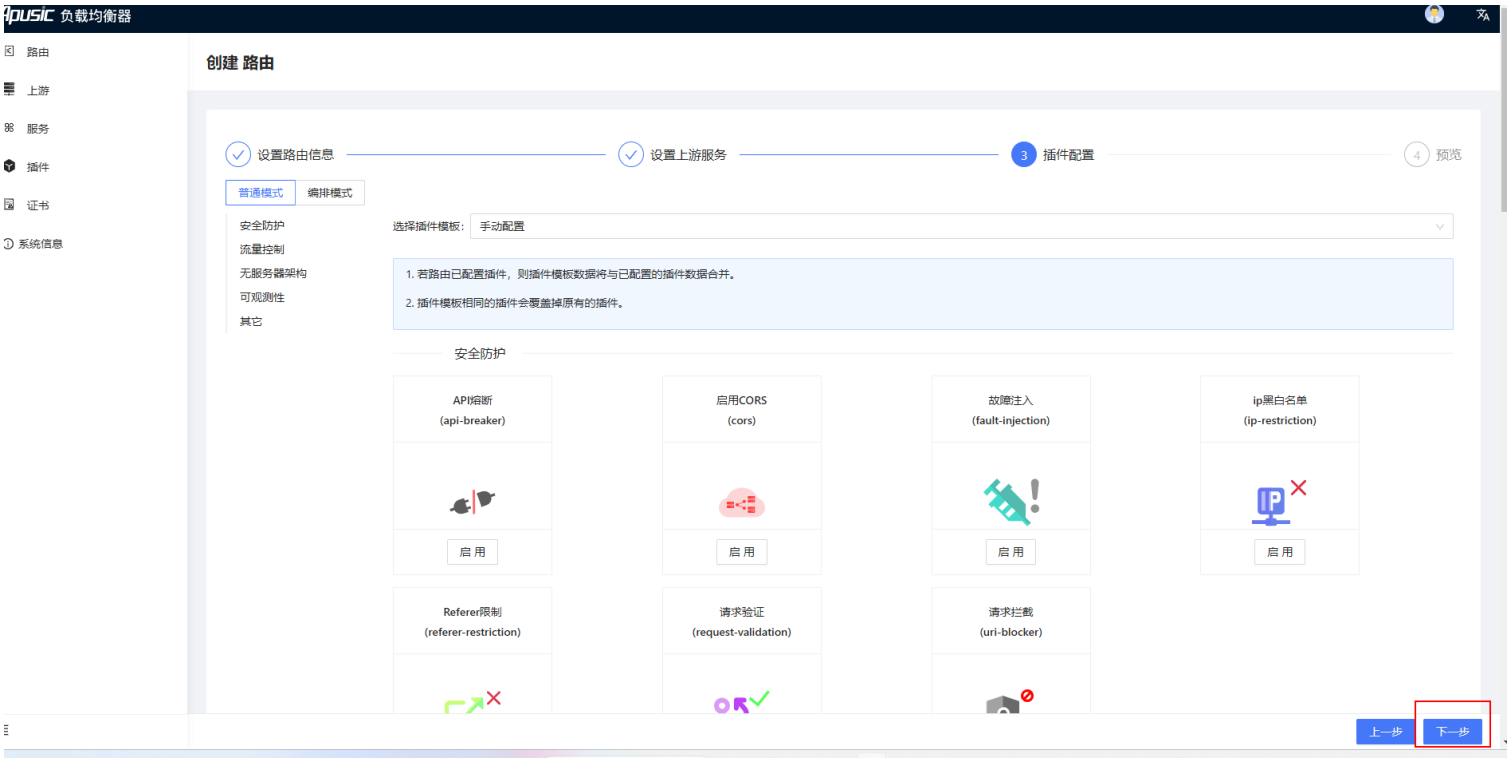
2、填写路由信息，并点击下一步



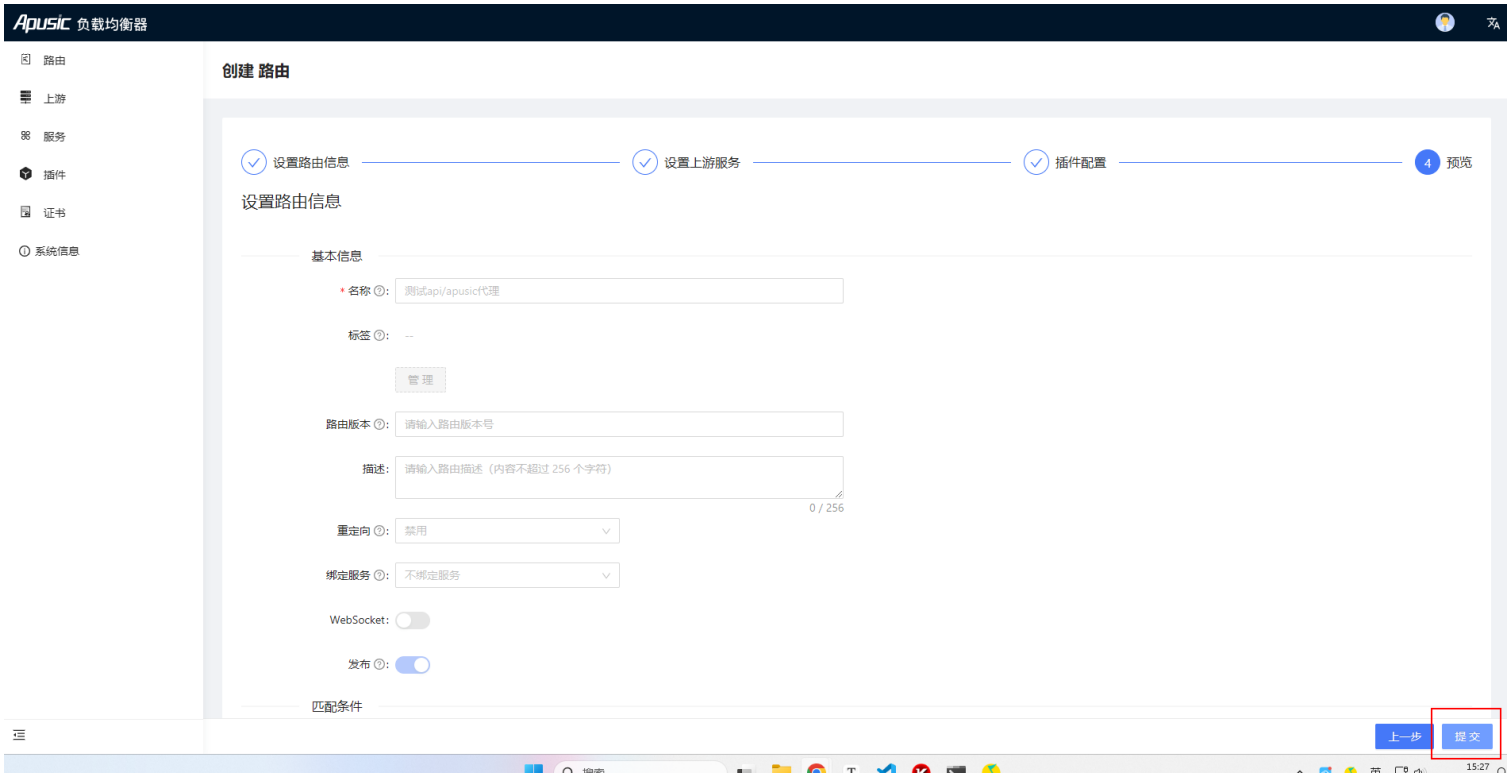
3、填写后端服务信息，并点击下一步



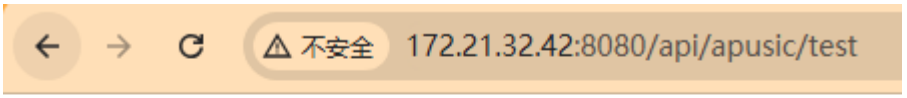
4、插件跳过，点击下一步


Apusic 负载均衡器
路由
上游
服务
插件
证书
系统信息
创建 路由
设置路由信息
设置上游服务
3 插件配置
4 预览
普通模式
编排模式
安全防护
流量控制
无服务器架构
可观测性
其它
选择插件模板:
手动配置
1. 若路由已配置插件，则插件模板数据将与已配置的插件数据合并。
2. 插件模板相同的插件会覆盖掉原有的插件。
安全防护
API熔断
(api-breaker)
启用CORS
(cors)
故障注入
(fault-injection)
ip黑白名单
(ip-restriction)
启 用
Referer限制
(referer-restriction)
请求验证
(request-validation)
请求拦截
(uri-blocker)
上一步
下一步

5、预览点击提交即可


Apusic 负载均衡器
路由
上游
服务
插件
证书
系统信息
创建 路由
设置路由信息
设置上游服务
插件配置
4 预览
设置路由信息
基本信息
* 名称:
测试api/apusic代理
标签:
管 理
路由版本:
请输入路由版本号
描述:
请输入路由描述（内容不超过 256 个字符）
0 / 256
重定向:
禁用
绑定服务:
不绑定服务
WebSocket:
发布:
匹配条件
上一步
提 交

6、使用ALB代理入口测试访问后端 注：当前演示环境的ALB代理的入口修改为8080端口。



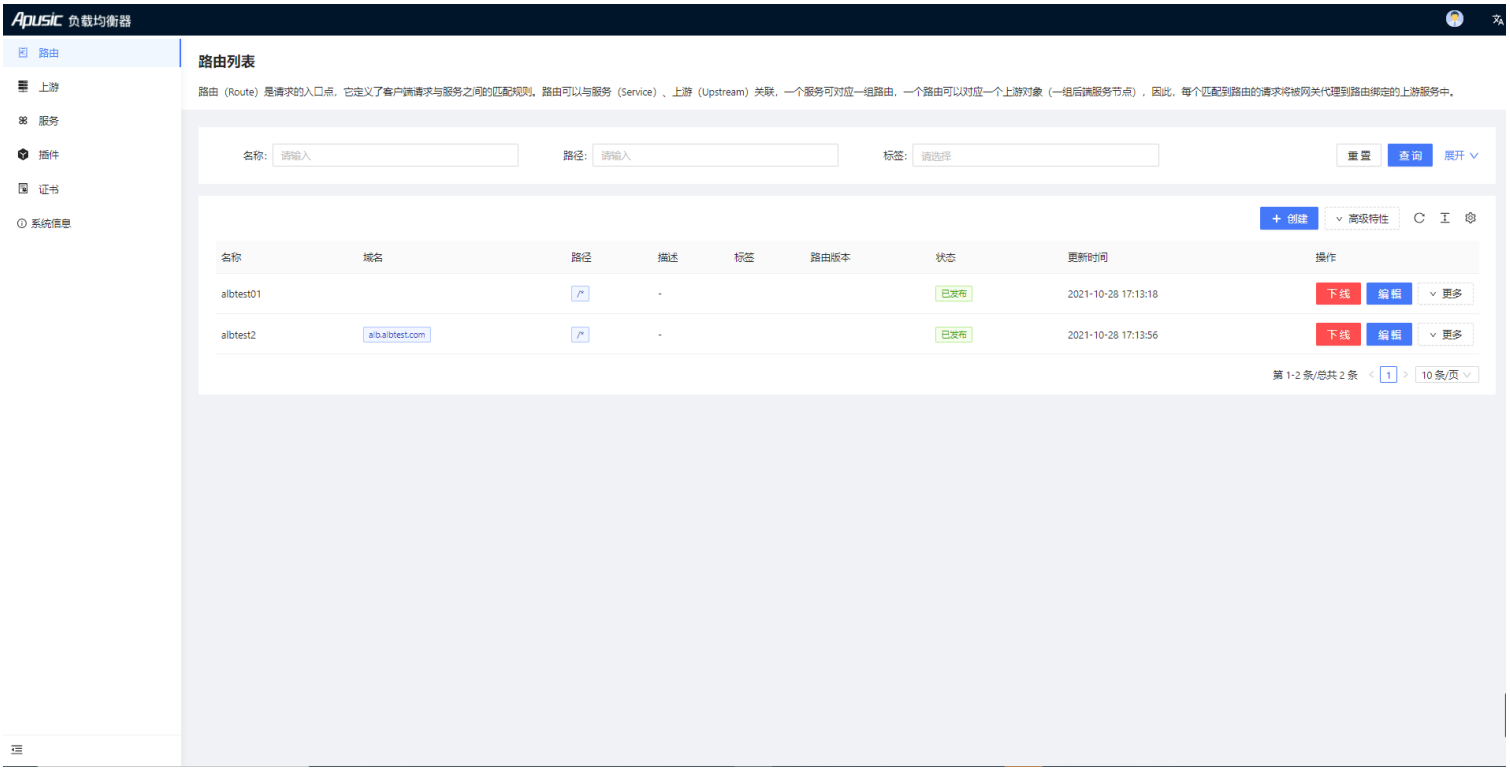

```
Current IP Address: 172.21.32.42
Requested URL: /api/apusic/test
Request Method: GET
```

4 产品功能介绍

4.1 路由

路由（Route）是请求的入口点，它定义了客户端请求与服务之间的匹配规则。路由可以与服务（Service）、上游（Upstream）关联，一个服务可对应一组路由，一个路由可以对应一个上游对象（一组后端服务节点），因此，每个匹配到路由的请求将被网关代理到路由绑定的上游服务中。

路由列表如下图所示：



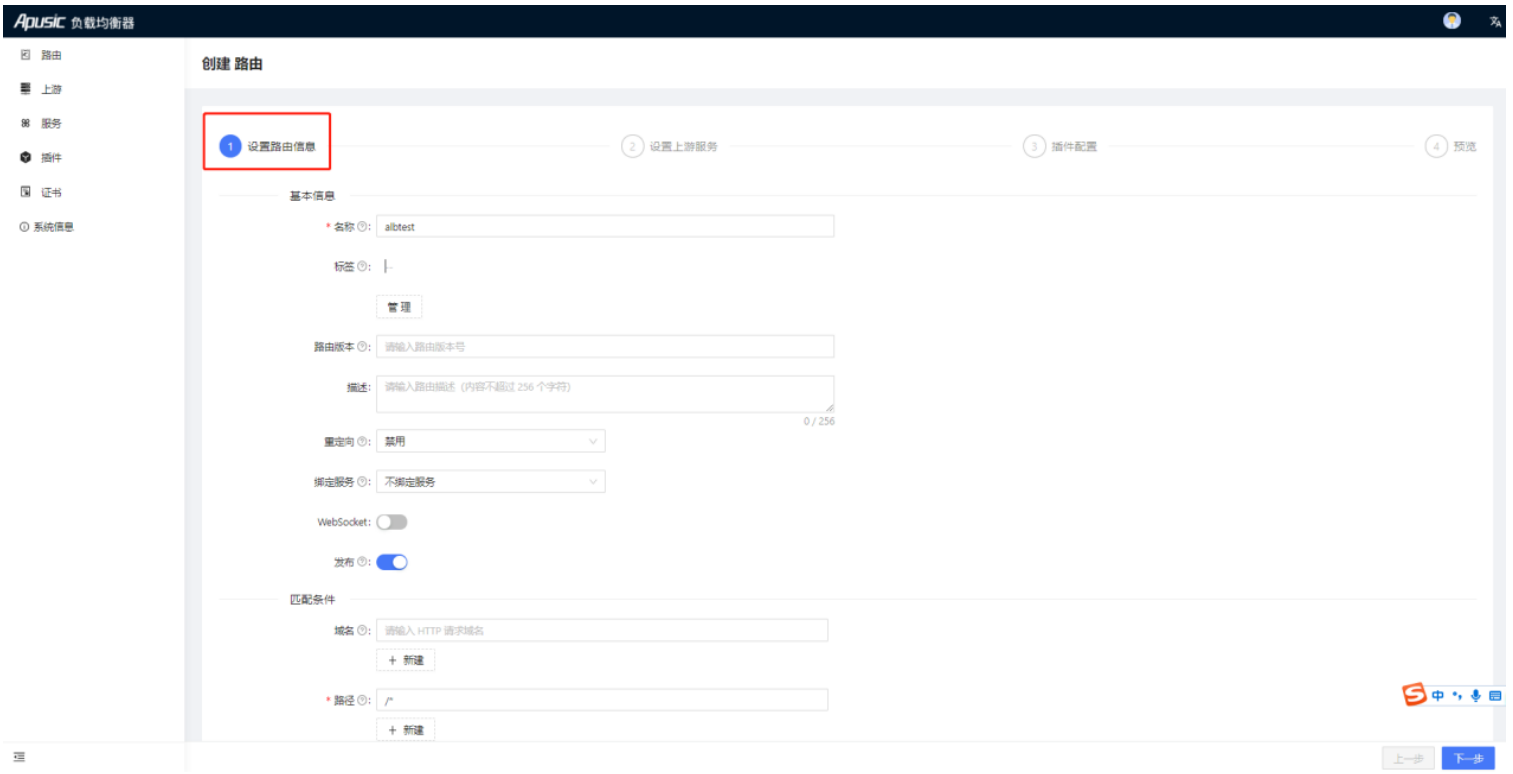
4.1.1 创建路由

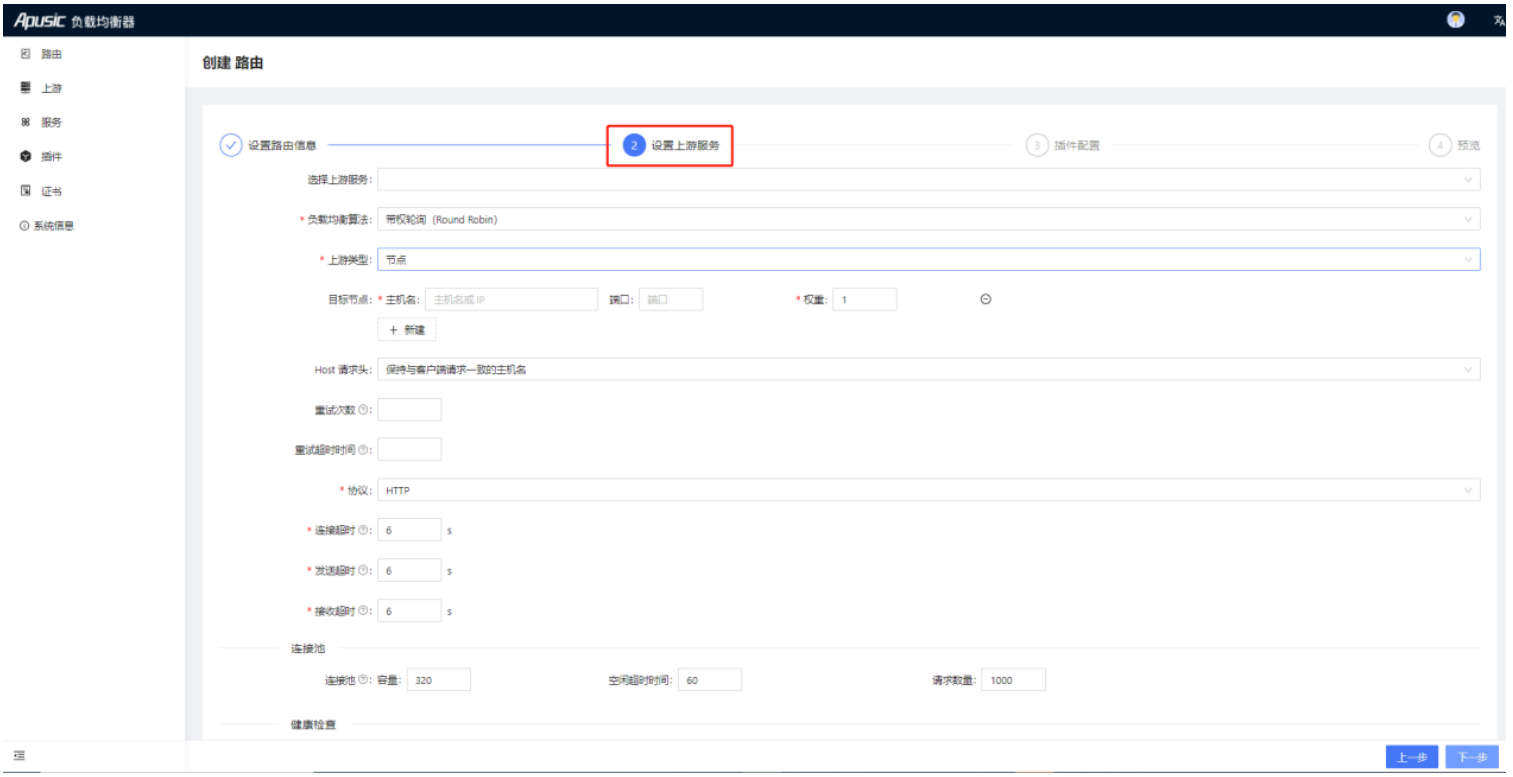
可通过两种方式创建路由：

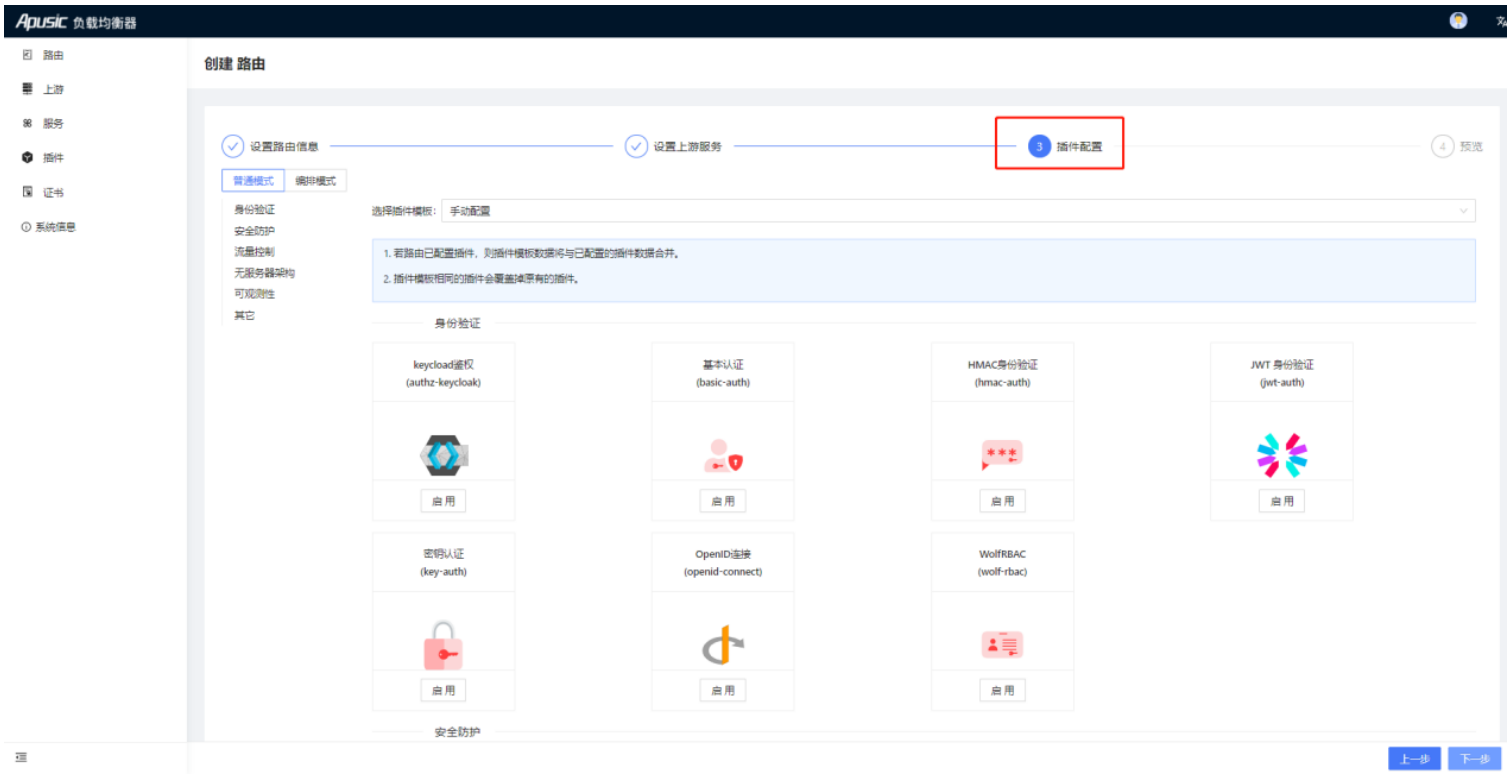
- 界面创建
- 使用编辑器创建

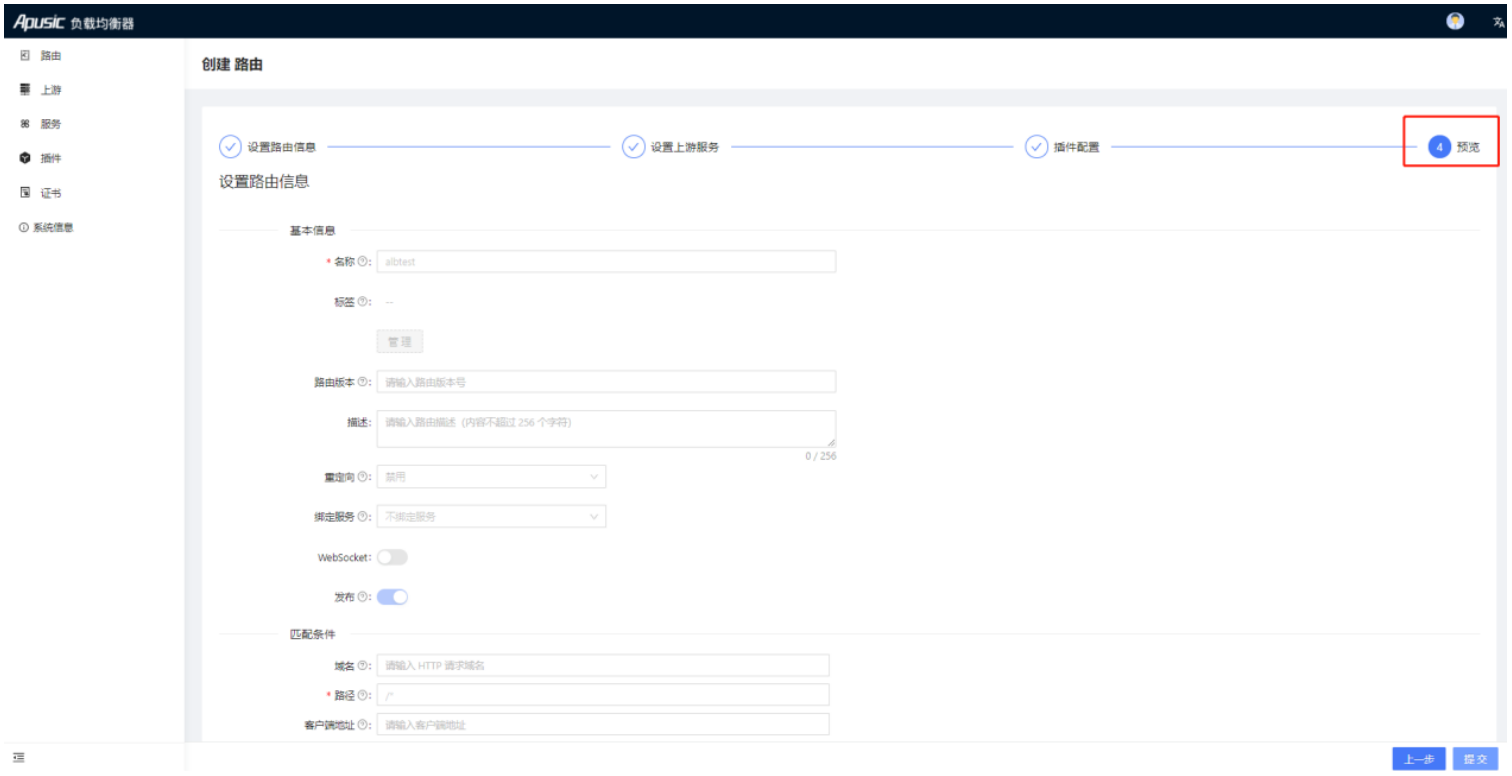
分为四个步骤：

1. 定义API请求
2. 定义API后端服务
3. 插件配置
4. 预览


Apusic 负载均衡器
路由
上游
服务
插件
证书
系统信息
创建 路由
1 设置路由信息
2 设置上游服务
3 插件配置
4 预览
基本信息
* 名称：allbtest
标签：
管理
路由版本：请输入路由版本号
描述：请输入路由描述（内容不超过 256 个字符）
0 / 256
重定向：禁用
绑定服务：不绑定服务
WebSocket：
发布：
匹配条件
域名：请输入 HTTP 请求域名
+ 新建
* 路径：/*
+ 新建
上一步
下一步


Apusic 负载均衡器
路由
上游
服务
插件
证书
系统信息
创建 路由
设置路由信息
2 设置上游服务
3 插件配置
4 预览
选择上游服务：
* 负载均衡算法：带权轮询（Round Robin）
* 上游类型：节点
目标节点：* 主机名：主机名或 IP 端口：端口 * 权重：1
+ 新建
Host 请求头：保持与客户端请求一致的主机名
重试次数：
重试超时时间：
* 协议：HTTP
* 连接超时：6 s
* 发送超时：6 s
* 接收超时：6 s
连接池
连接池：容量：320 空闲超时时间：60 请求数量：1000
健康检查
上一步
下一步





4.1.2 界面创建路由

以界面创建为例介绍路由的创建过程

1. **设置路由信息**：

填写路由基本信息

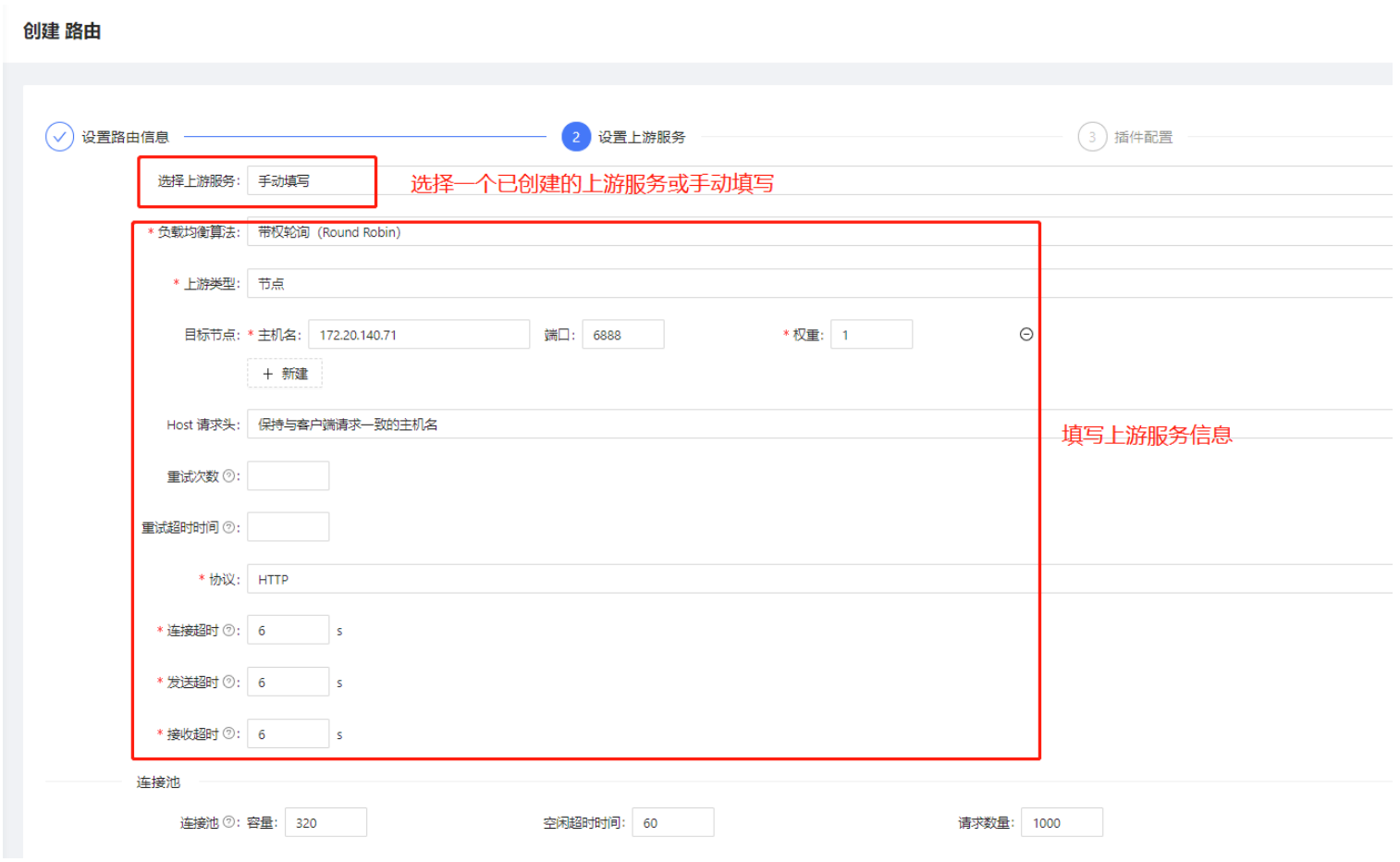
- 名称：必输项，自定义路由名称，不允许配置重名路由
- 发布：默认开启，开启状态下路由才会生效

填写请求信息：

- 域名：alb服务器域名
- 路径：必输项，默认所有路径/*，可以是路由的详细路径或者泛路径（以/*结尾）
- 客户端地址：允许访问的客户端IP或IP网段
- 优先级：必输项，默认为0，路由配置相同时取优先级高的路由
- 请求改写：对客户端的请求的协议、路径、域名、请求头进行改写

4.1.3 定义API后端服务

配置上游信息：



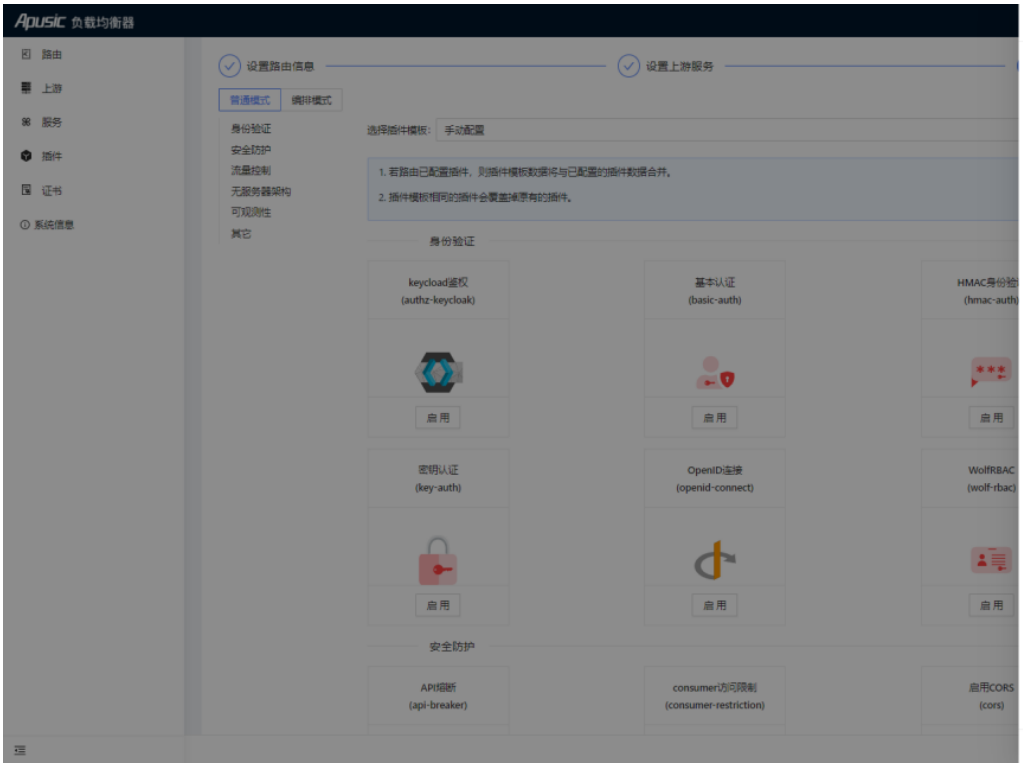
- 选择上游服务：选择已经添加的上游服务时不可编辑上游，手动填写才能编辑上游服务
- 负载均衡算法：必选项，默认带权轮询
- 上游类型：必选项，默认为节点
- 目标节点：必输项，输入目标服务器主机名或者IP地址、端口
- 权重：必输项，输入上游服务器的权重，权重高的节点承受的流量多，权重配置为0时熔断该节点
- 协议类型：必选项，选择客户端请求的类型
- 超时时间：必输项，默认超时时间为6S

4.1.4 插件配置

插件配置根据自定义可选择普通方式或插件编排方式选择插件：

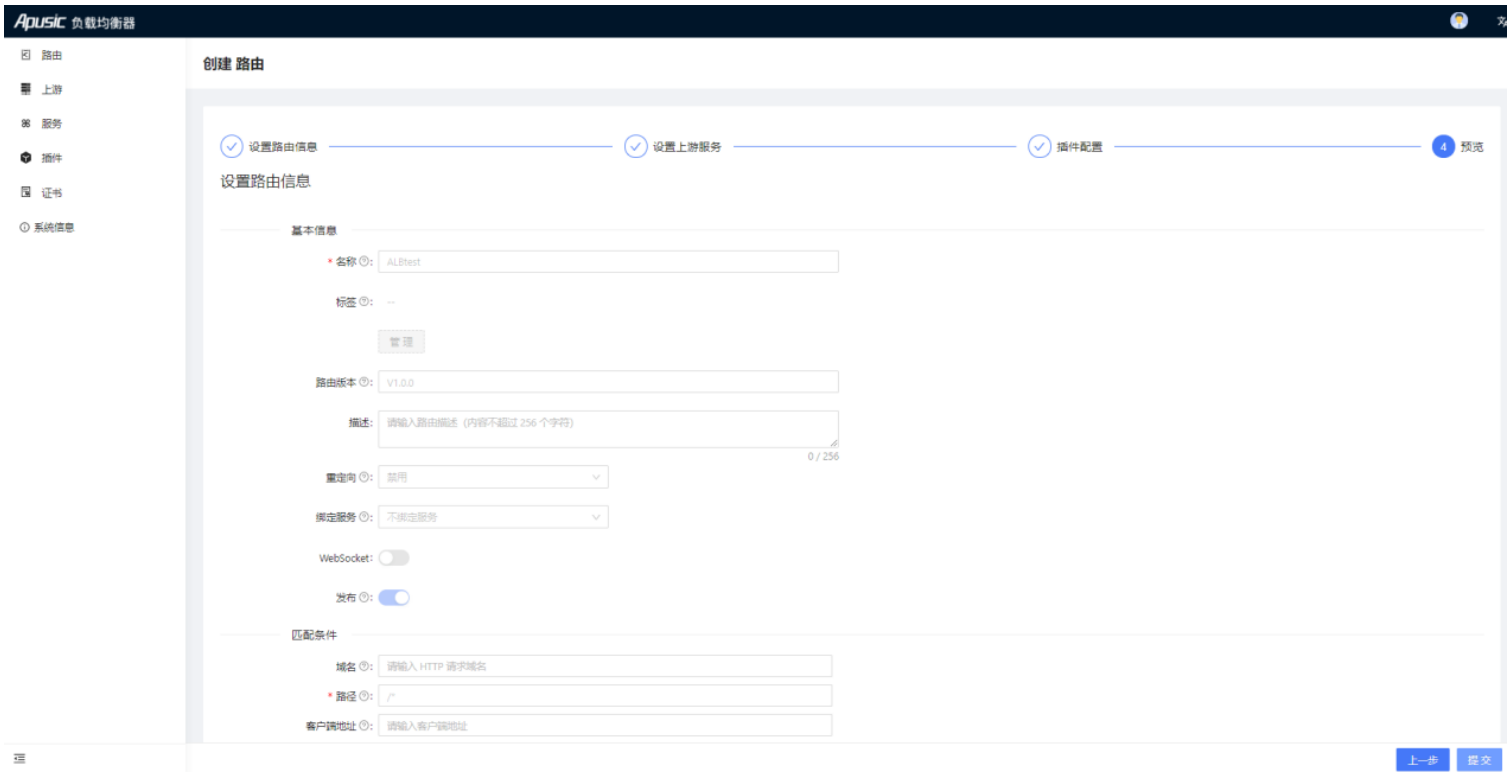

定义 API 请求
定义 API 后端服务
3 插件配置
4 预览
普通模式
插件编排
两种模式
1.普通方式
2.插件编排
选择插件模板：
手动配置
1. 若路由已配置插件，则插件模板数据将与已配置的插件数据合并。
2. 插件模板相同的插件会覆盖掉原有的插件。
认证
通用
日志
监控
协议转换
安全
流量控制
报文转换
插件分类
认证
keycload鉴权
(authz-keycloak)
OpenID连接
(openid-connect)
点击启用
点击启用
选择对应插件点击启用
通用
批量请求
(batch-requests)
回显
(echo)
系统信息上报
(server-info)
后附加函数
(serverless-post-functio
上一步
下一步

启用插件：


Apusic 负载均衡器
路由
上游
服务
插件
证书
系统信息
设置路由信息
设置上游服务
普通模式
编排模式
身份验证
安全防护
流量控制
无服务器架构
可观测性
其它
选择插件模板：
手动配置
1. 若路由已配置插件，则插件模板数据将与已配置的插件数据合并。
2. 插件模板相同的插件会覆盖掉原有的插件。
身份验证
keycload鉴权
(authz-keycloak)
基本认证
(basic-auth)
HMAC身份验证
(hmac-auth)
启用
密钥认证
(key-auth)
OpenID连接
(openid-connect)
WolfRBAC
(wolf-rbac)
安全防护
API熔断
(api-breaker)
consumer访问限制
(consumer-restriction)
启用CORS
(cors)

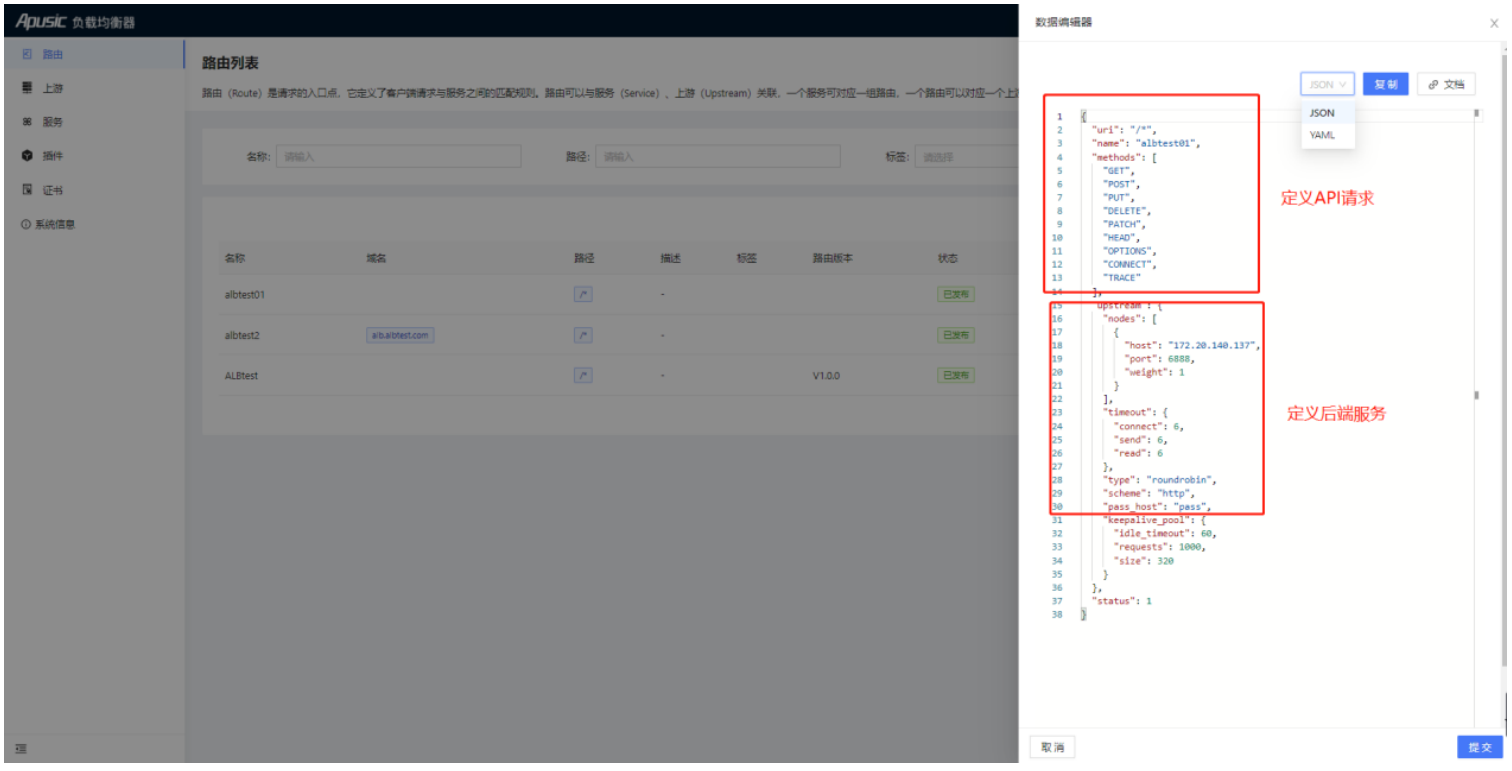

插件配置
名称：
basic-auth
启用：
数据编辑器
表单
本插件无需配置
取消
提交

4.1.5 预览



4.1.6 查看路由

点击路由列表右侧【查看】操作按钮，通过JSON格式或YAML格式查看创建的路由详细信息

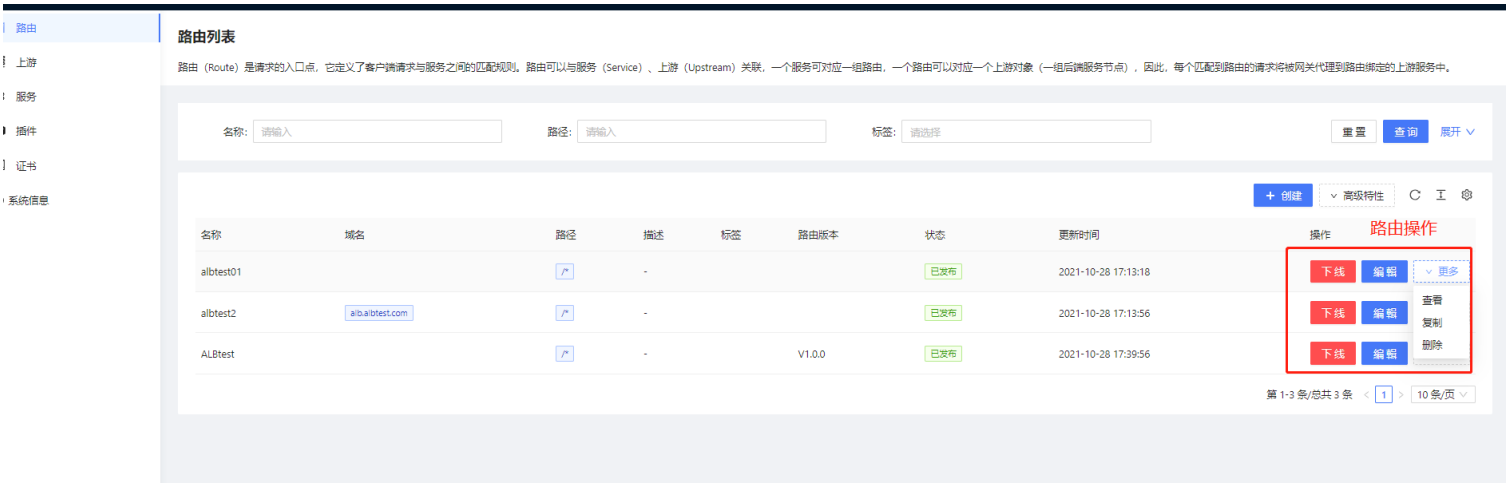


示例Json数据:

```
{
    "uri":"/\*",
    "name":"testALB",
    "methods":[
        "GET",
        "POST",
        "PUT",
        "DELETE",
        "PATCH",
        "HEAD",
        "OPTIONS",
        "CONNECT",
        "TRACE"
    ],
    "upstream":{
        "nodes":{
            "172.18.100.159":1
        },
        "timeout":{
            "connect":6,
            "send":6,
            "read":6
        },
        "type":"roundrobin",
        "scheme":"http",
        "pass_host":"pass",
        "keepalive_pool":{
            "idle_timeout":60,
            "requests":1000,
            "size":320
        }
    },
    "status":1
}
```

4.1.7 路由操作

在路由列表中实现对路由的发布、下线、编辑、查看、删除、复制

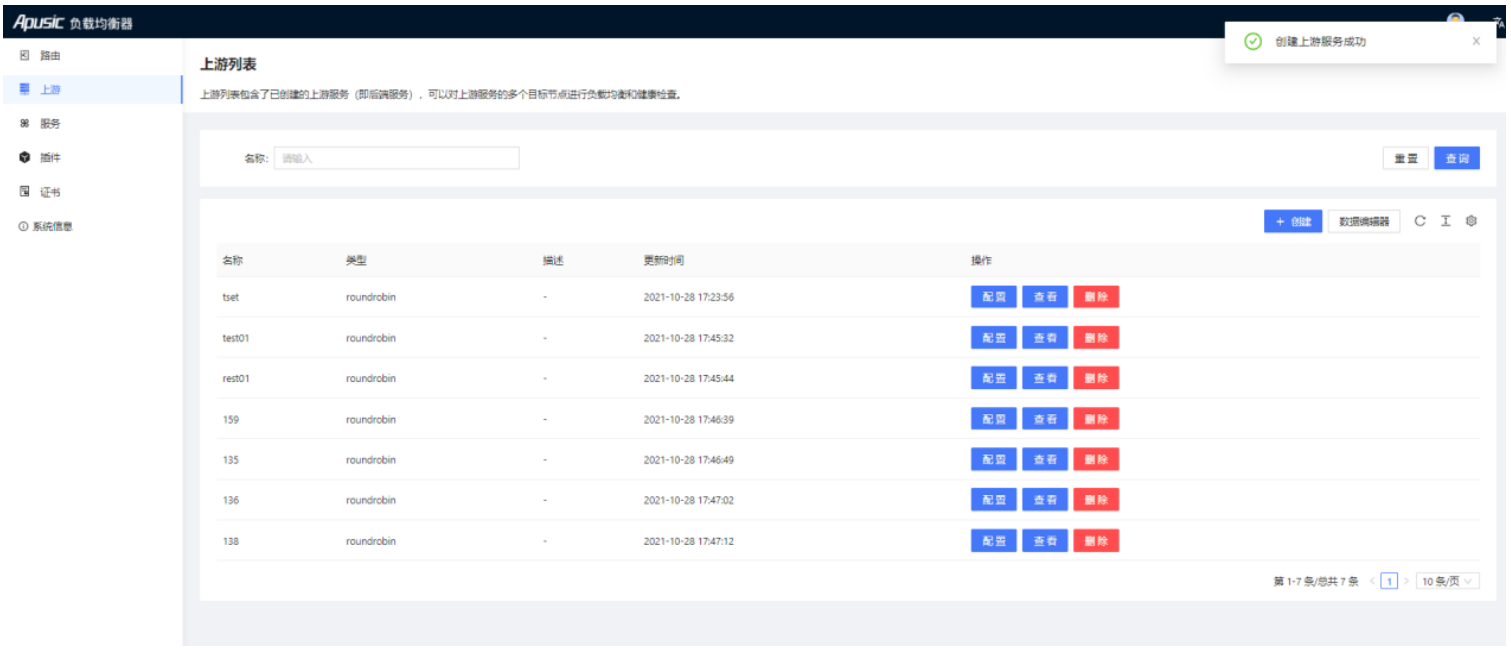


- 编辑：编辑路由基本信息或上游服务节点信息，动态生效无需重启
- 查看：通过JSON格式或YUML格式查看路由
- 复制：复制路由所有信息，名称不可与原名称相同
- 下线\发布：路由下线和发布动态生效，无需重启ALB
- 删除：删除路由信息不保存

4.2 上游

上游列表包含了已创建的上游服务（即后端服务），可以对上游服务的多个目标节点进行负载均衡和健康检查。

4.2.1 上游列表

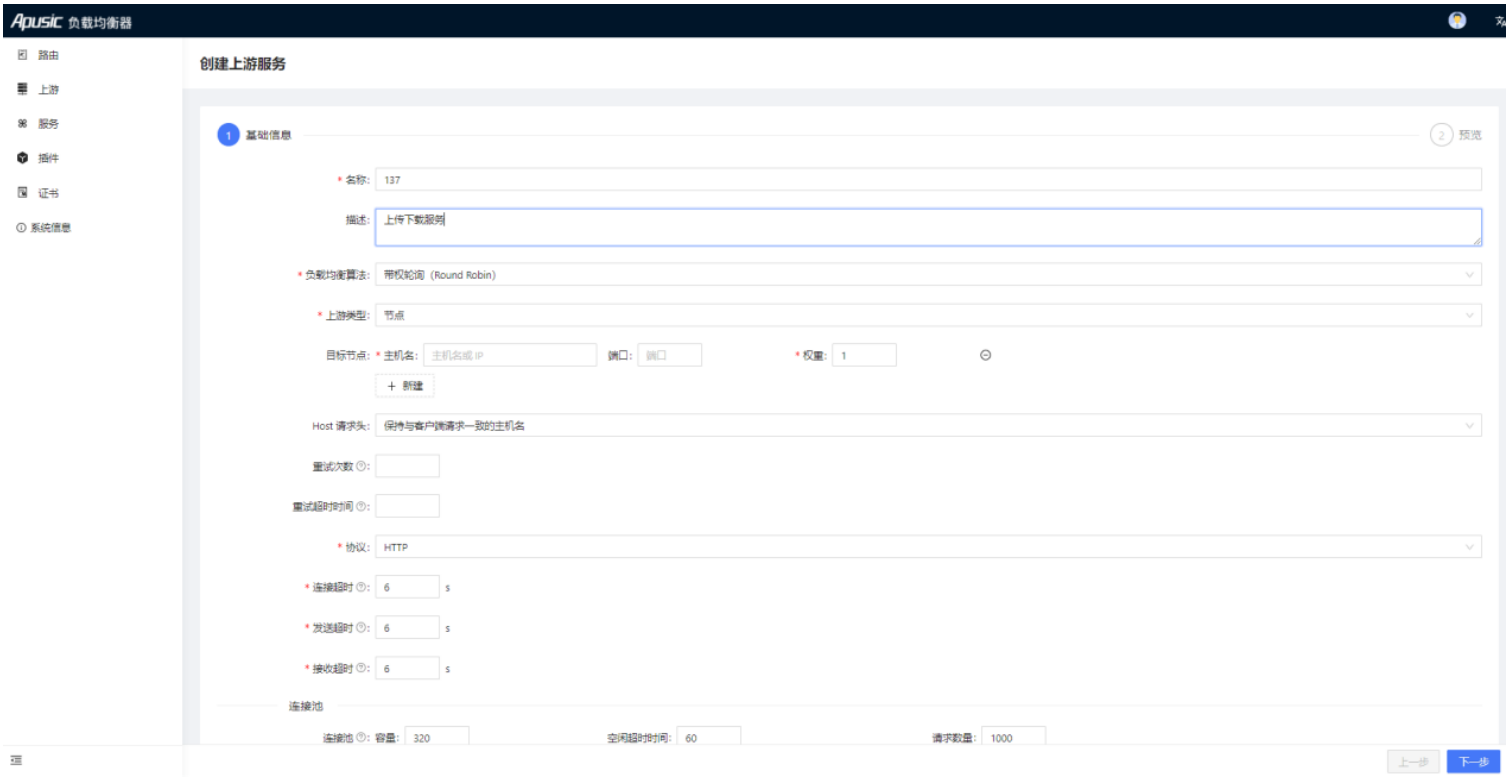


4.2.2 创建上游

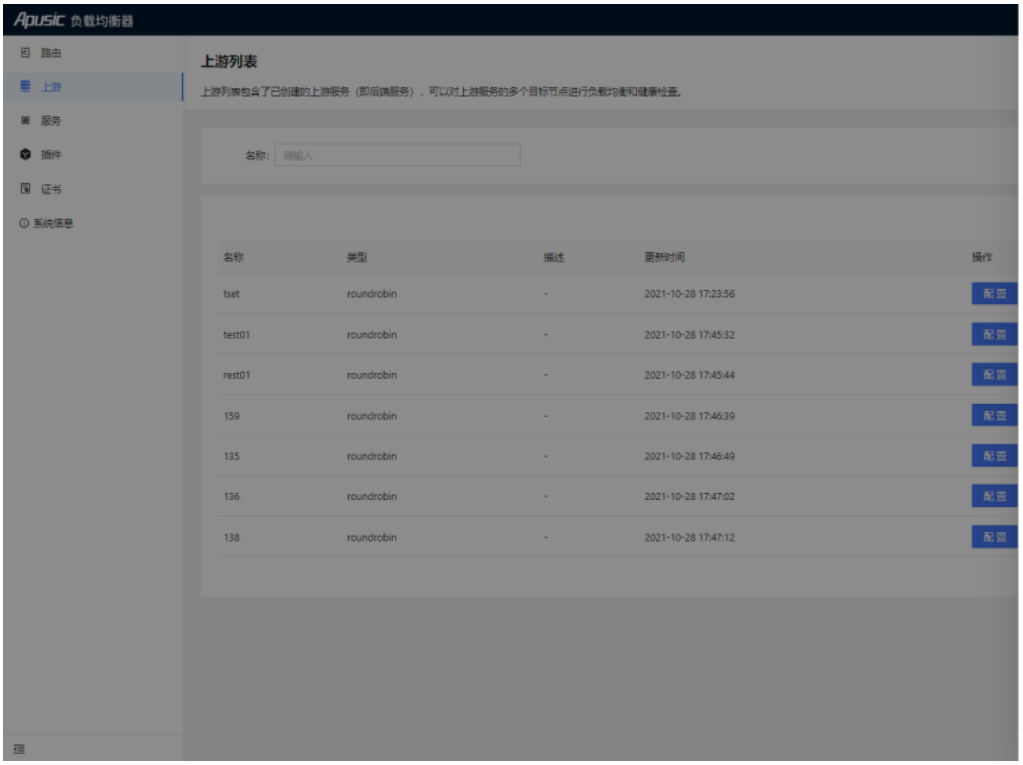
可以通过两种方式进行上游的创建：

- 界面创建
- 使用编辑器创建

下图是使用界面创建：



下图是使用编辑器创建：



4.3 服务

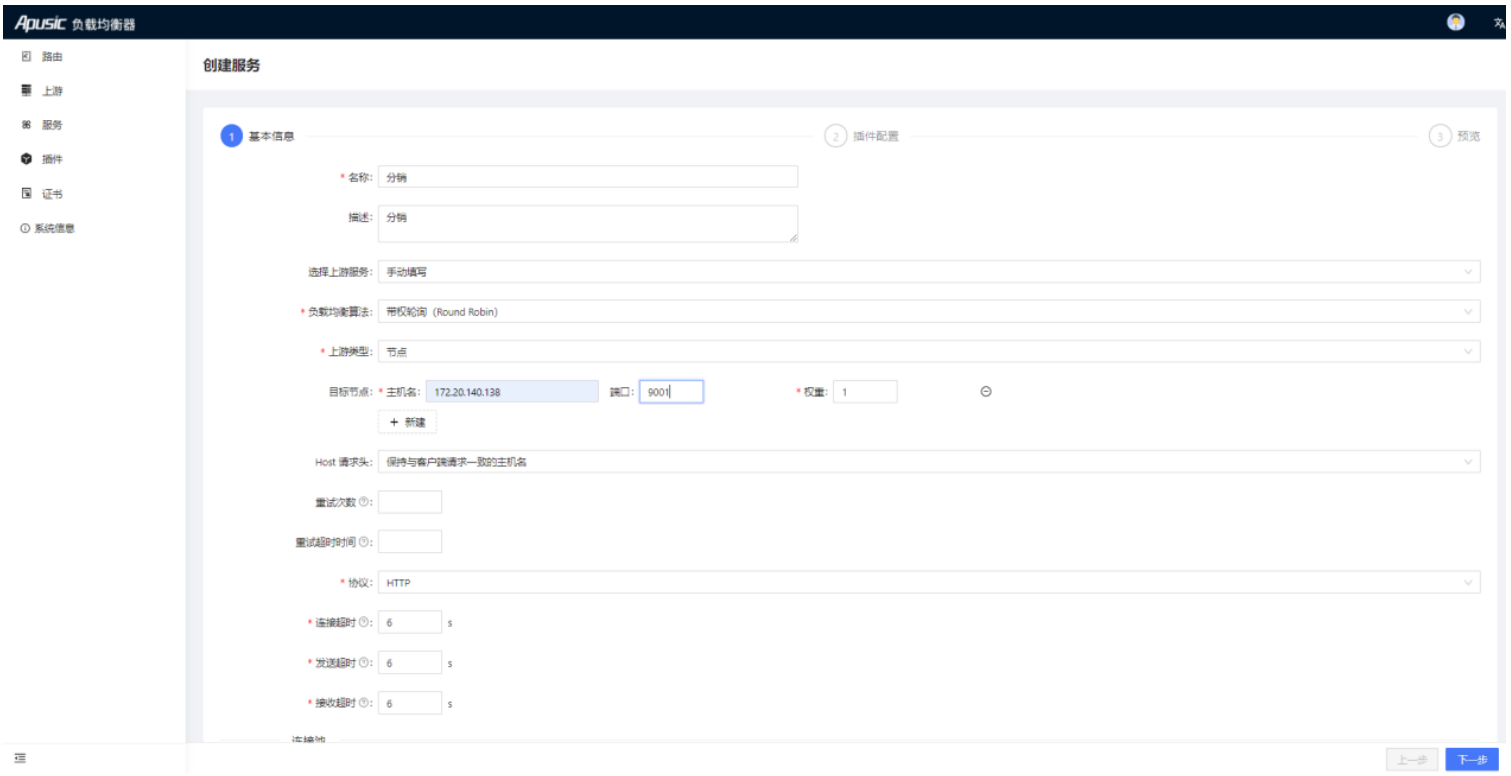
服务由路由中公共的插件配置、上游目标信息组合而成。服务与路由、上游关联，一个服务可对应一组上游节点、可被多条路由绑定。

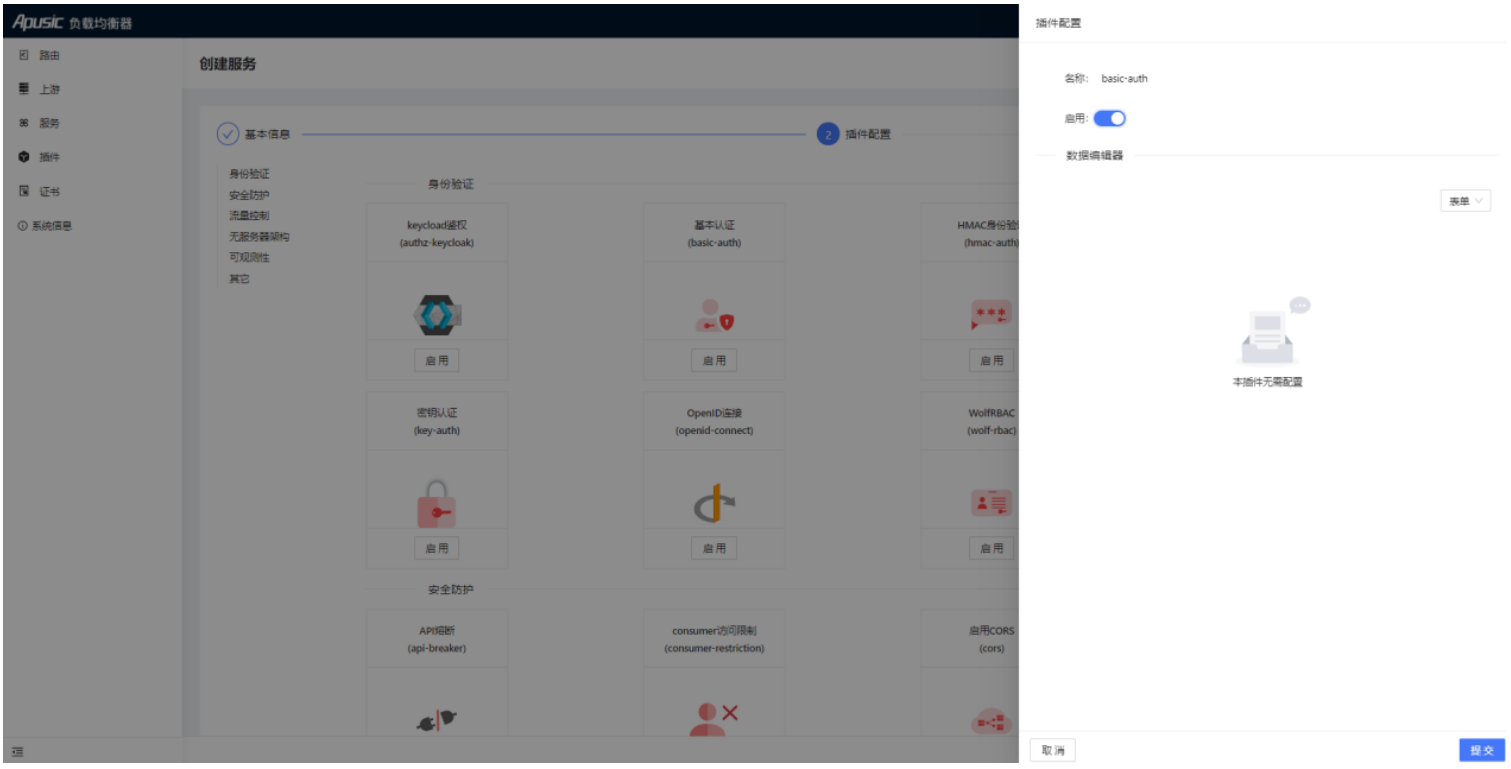
服务列表

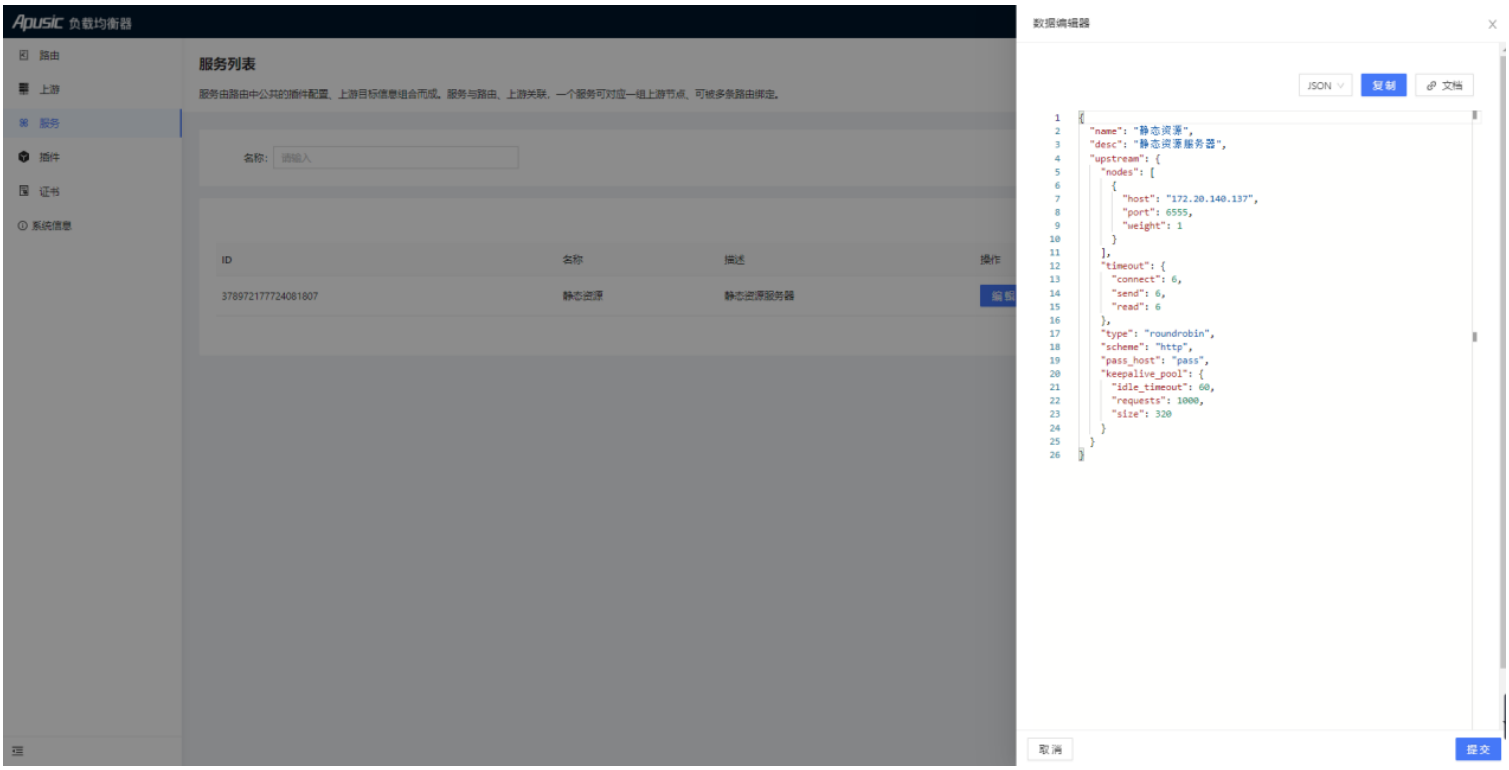
创建服务

可通过两种方式创建服务。

- 界面创建
- 使用编辑器创建







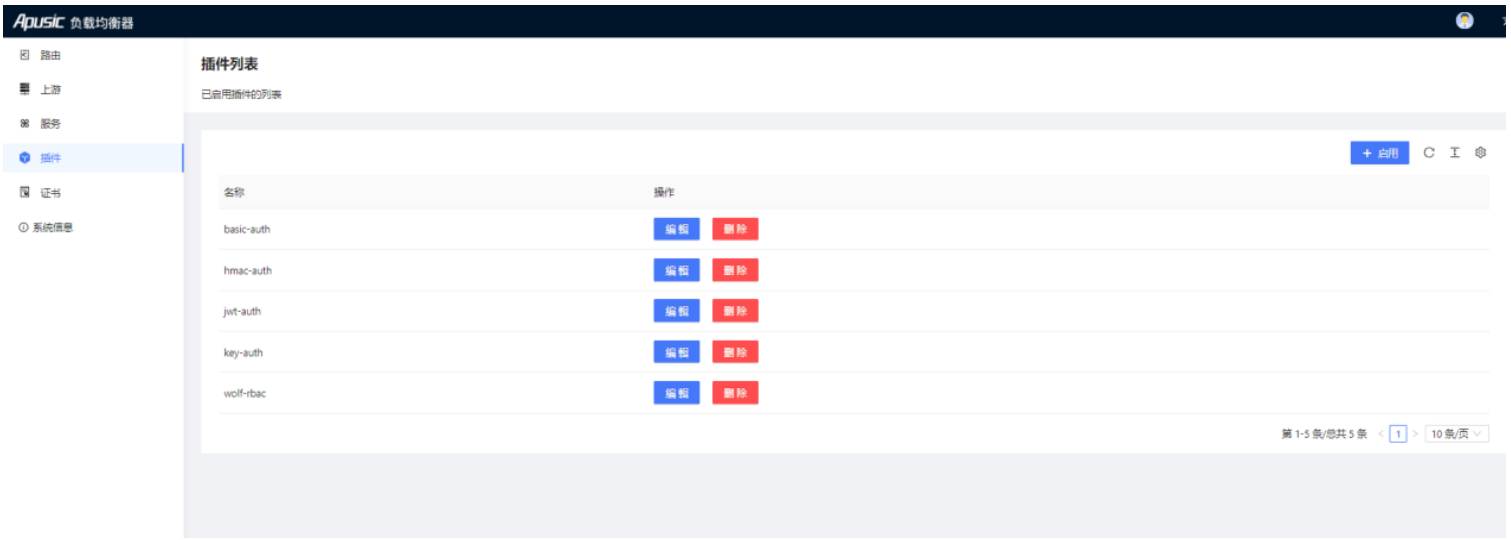
4.4 插件

已启用插件的列表

- 内置插件：
  - 认证：keycloak鉴权、openID连接
  - 通用：批量请求、回显、重定向、前后附加函数等
  - 日志：错误日志、HTTP日志、kafka日志、阿里云日志、TCP日志等
  - 监控：节点状态、prometheus、skywalking等
  - 协议转换：dubbo代理
  - 安全：启用CORS、ip黑白名单、referer限制、请求拦截等
  - 流量控制：API熔断、限制并发连接、限制请求次数等
  - 报文转换：故障注入、gPRC转码、响应信息重写等
- 自定义插件：

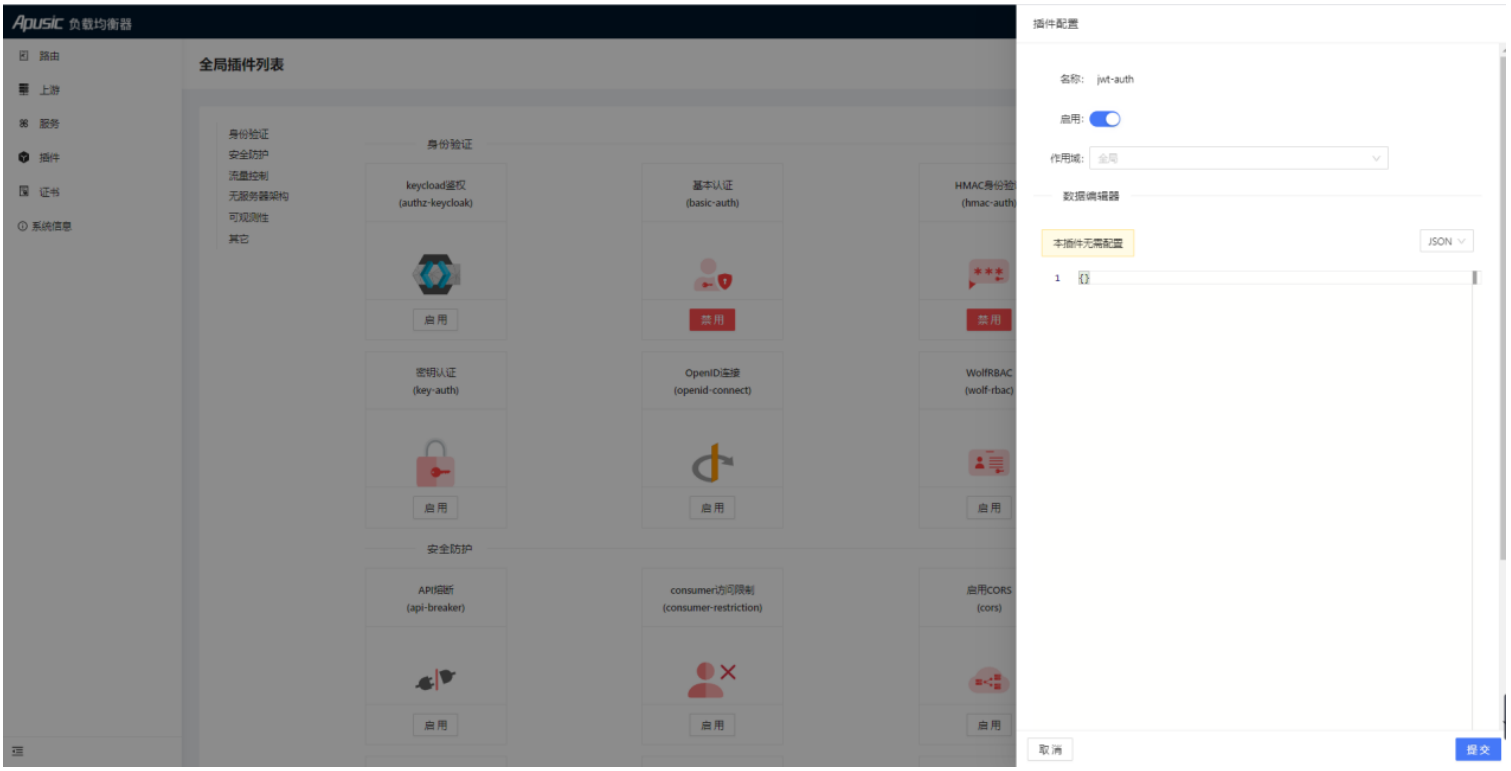
可以根据实际业务编写插件，插件允许在常见阶段进行挂载生效，例如init, rewrite，access，balancer,header filter，body filter 和 log 阶段。

插件列表



启用插件

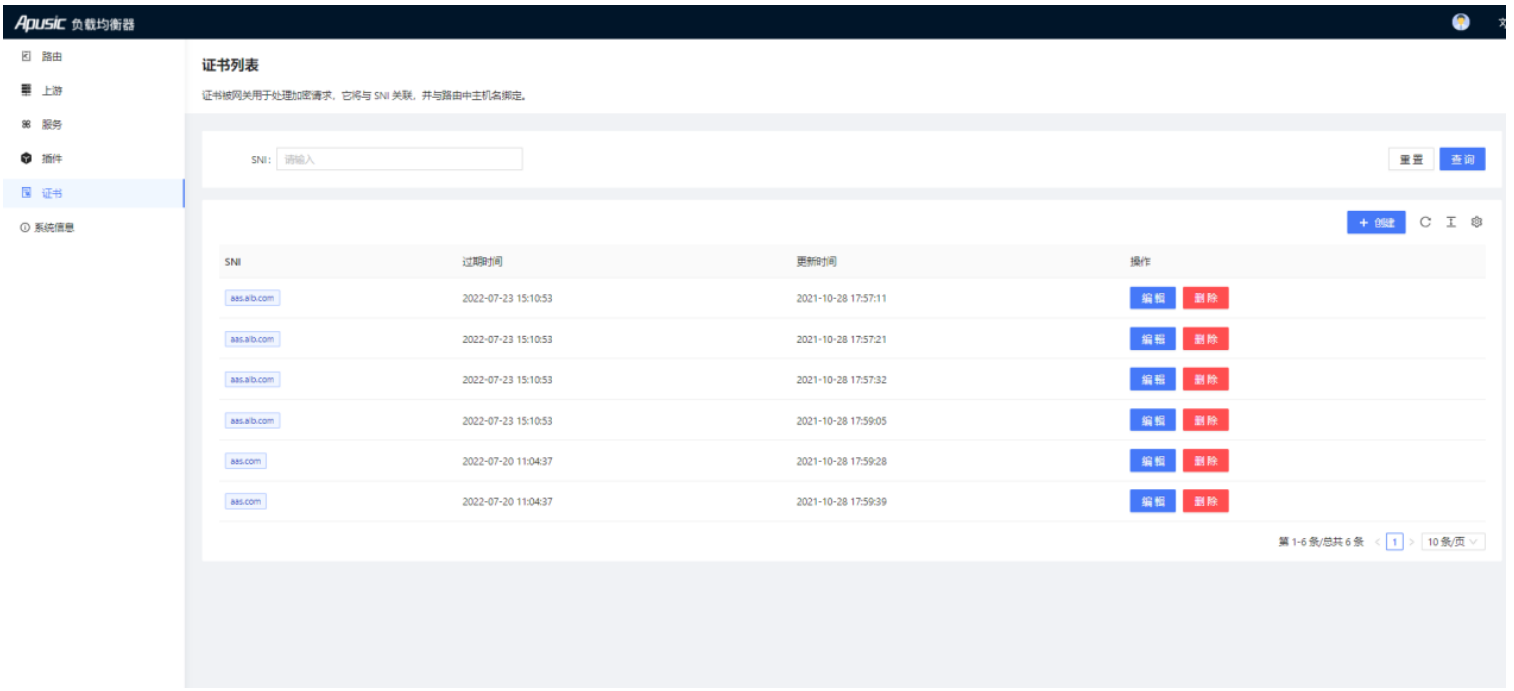
在配置列表中可以选择插件进行启用



4.5 证书

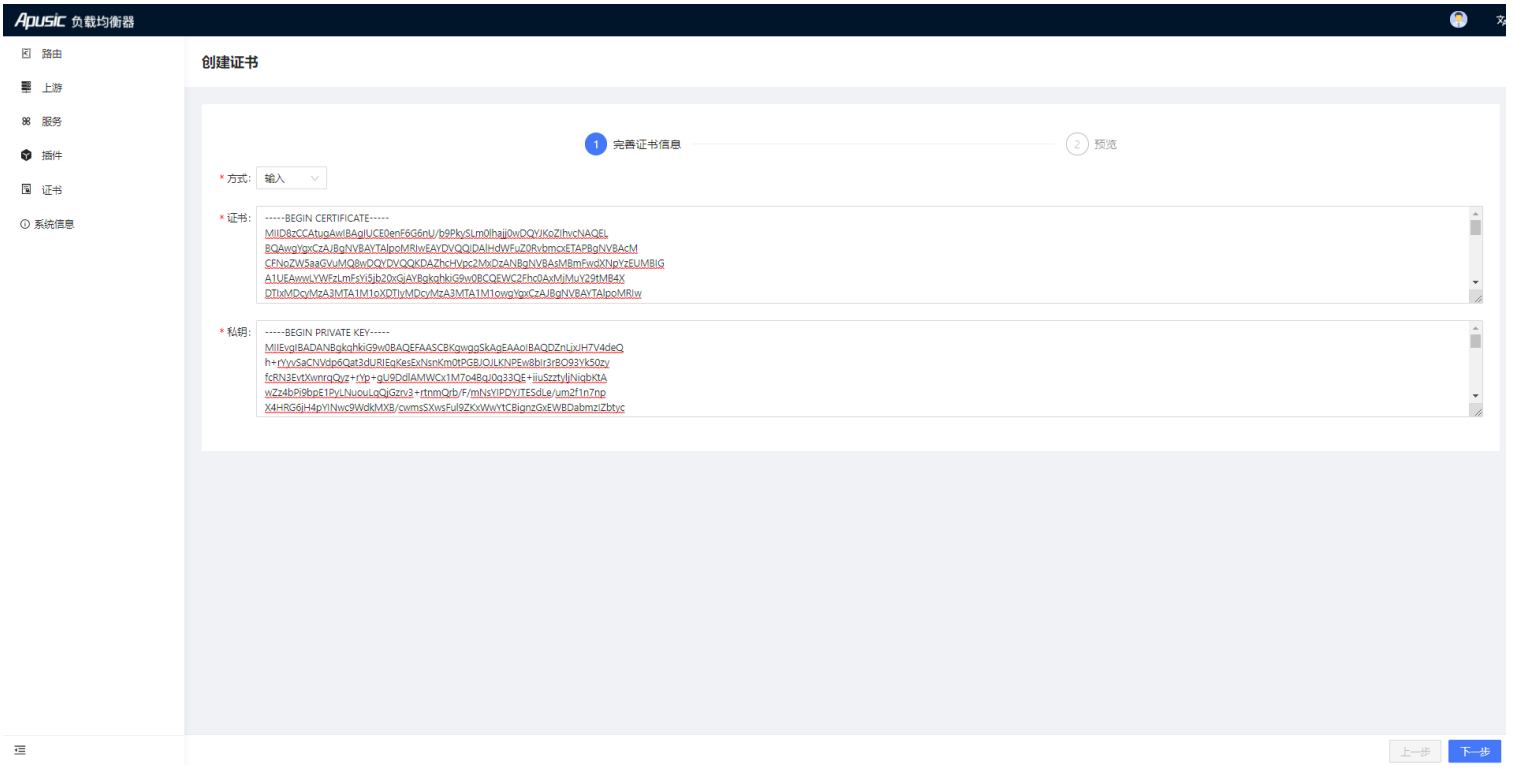
证书被网关用于处理加密请求，它将与 SNI 关联，并与路由中主机名绑定。

** 证书列表**

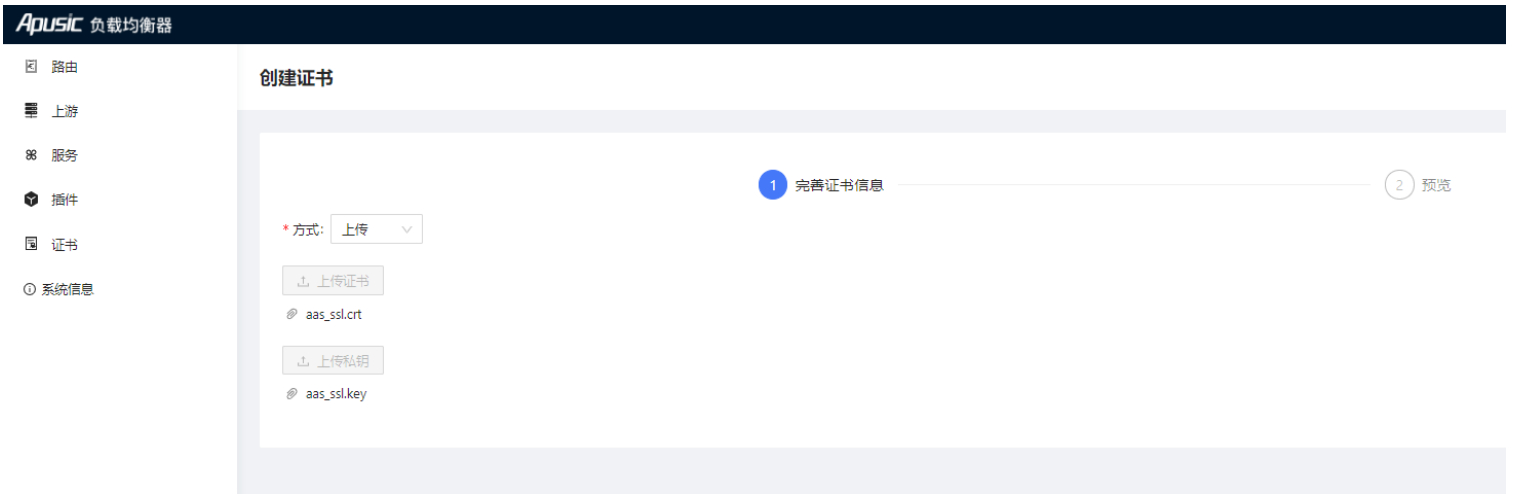


创建证书

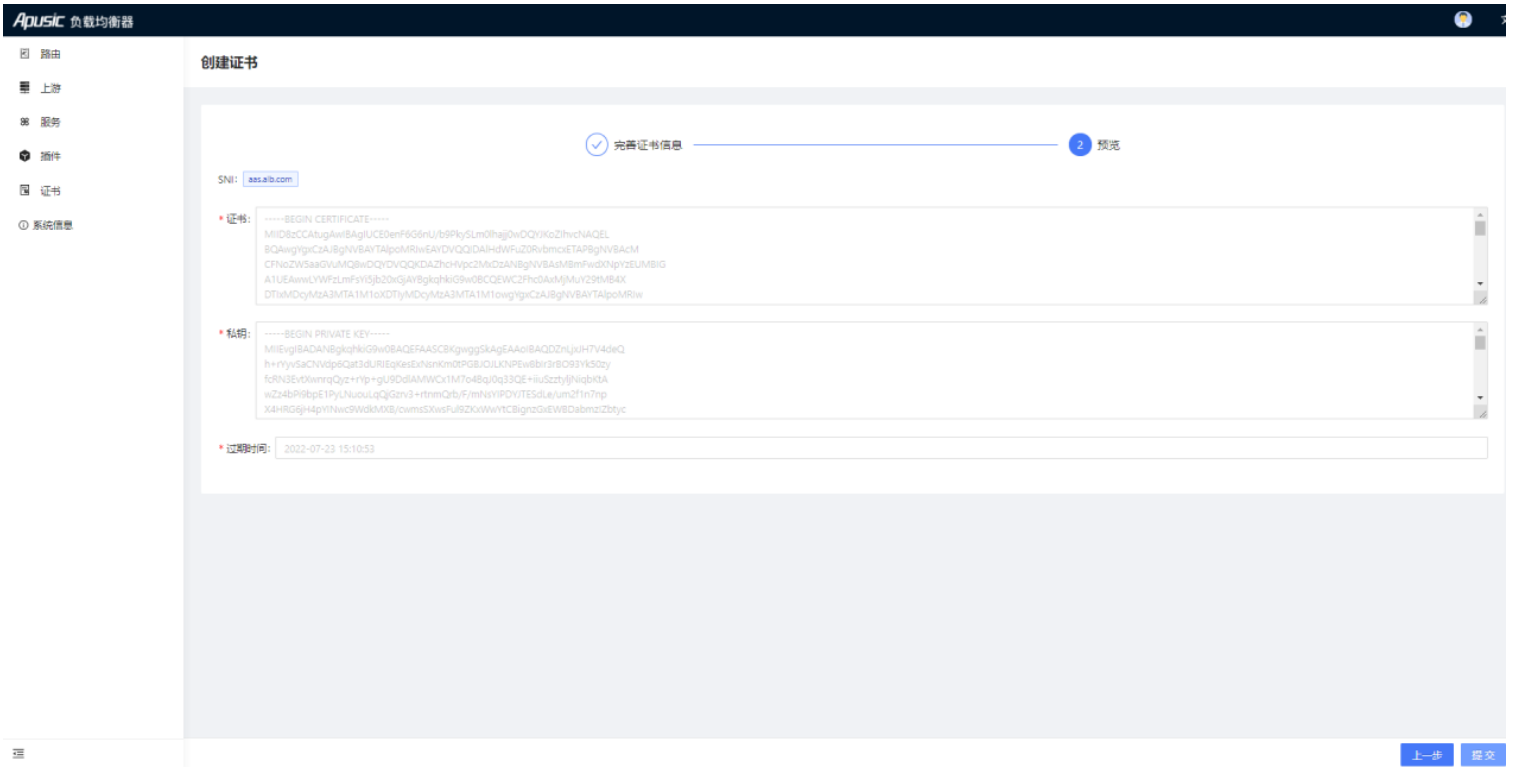
- 输入证书



- 上传证书



- 预览



4.6 系统信息

显示控制台以及ALB节点的信息。

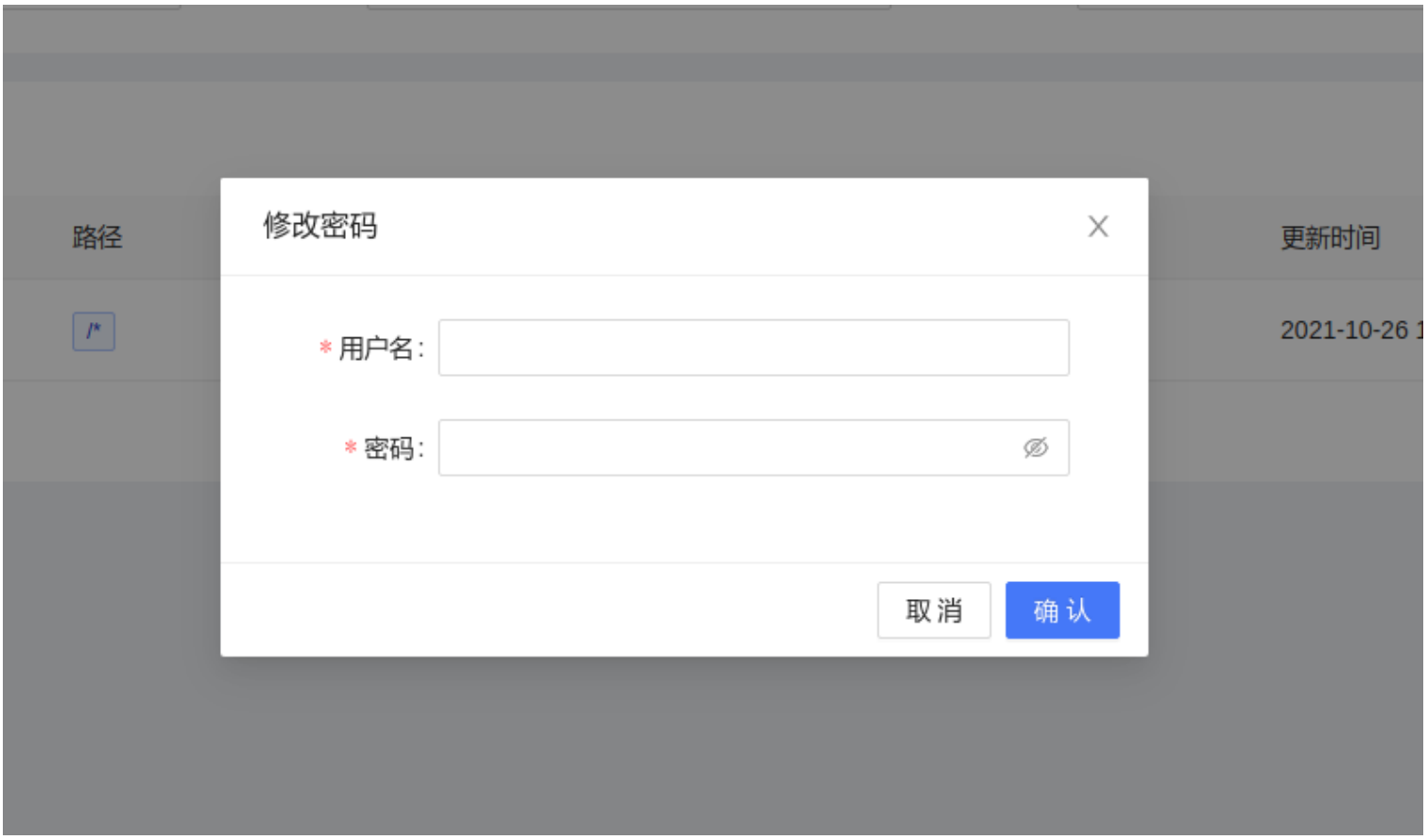
信息页

4.7 密码与安全

密码修改说明：为了保证系统的安全，要求密码**长度需6位**及以上，并且必须包含**特殊字符**。

管控台密码修改

点击右上角头像，选择修改密码，输入登录用户名和新密码即可。



忘记密码

若忘记密码，则需要通过修改配置文件中的密码设置项进行修改，修改步骤为：

1. 用编辑器打开配置文件：`安装目录/alb-dashboard/conf/conf.yaml`
2. 跳转至57行，修改password为新密码项，如下图示：

```
54  expire_time: 3600    # jwt token expire time, in second
55  users:               # yamllint enable rule:comments-indentation
56    - username: admin  # username and password for login `manager api`
57      password: apusic$alb
58    - username: user
59      password: user
```

5 产品使用介绍

5.1 产品端口修改

若系统已有服务占用了80、443、9000端口，会导致alb启动失败，可以通过配置修改端口。

5.1.1 修改http或https的端口

1. 修改配置文件：`安装目录/alb-standard/conf/config.yaml`
2. 修改配置文件内容：

```
soft: ALB/2.0.1
alb:
  admin_key:
    - name: "admin"
      key: edd1c9f034335f136f87ad84b625c8f1  # using fixed API token
has security risk, please update it when you deploy to production
environment
      role: admin
  node_listen: 80        # http默认的网关访问入口

  ssl:
    listen_port: 443     # https访问网关的入口
```

3. 如上，修改对应的 `node_listen` 、 `ssl.listen_port` 端口即可。
4. 重新启动ALB： `./bin/start-alb.sh`

5.1.2 修改WEB管理控制台端口

1. 修改配置文件：`安装目录/alb-dashboard/conf/config.yaml`
2. 修改配置文件内容：

```
conf:
  listen:
    host: 0.0.0.0
    port: 9000   # WEB管理控制台默认端口
```

3. 如上，修改对应的 `listen.port` 端口即可。
4. 重新启动ALB： `./bin/start-alb.sh`

5.2 ALB迁移nginx配置文件

ALB支持兼容nginx的server、upstream等配置内容，可以直接把对应匹配提取问单独的配置，并开启alb导入nginx配置，进行导入即可。

5.2.1 开启支持导入nginx的配置文件

- 修改配置文件，支持导入nginx配置文件

```
nginx_config_include:
  nginx_config_include_enable: true      # 开启nginx配置导入
  nginx_config_include_path: "安装目录/alb-
standard/conf/nginx_conf/*.conf"   #待导入的nginx配置文件存放文件夹
```

- 创建 **安装目录**`/alb-standard/conf/nginx_conf` 目录， `mkdir conf/nginx_conf`

5.2.2 导入nginx配置文件

根据上面创建的nginx配置存放文件夹： **安装目录**`/alb-standard/conf/nginx_conf/` ，把nginx的upstream或者server块内容的配置文件即可。如下配置 nginx_test.conf

```
upstream test_server {
    server 172.21.33.14:8999;
}

server {
    listen 8989;
    server_name test.com;

    location / {
        root /var/www/html;
        index index.html;
    }

    location /api/ {
        proxy_pass http//test_server/api/;
    }
}
```

注：

1. 配置文件仅支持server和upstream块内容。

5.3 国密支持

国密算法仅可通过Nginx配置文件实现，具体操作方法为：

1. 开启ALB支持Nginx Server配置块导入

2. 编写国密证书的Server内容文件并放入配置文件夹
3. 重启ALB

5.3.1 开启ALB支持Nginx Server配置块导入

1. 进入ALB安装目录，编辑 **安装目录**`/alb-standard/conf/config.yaml` 文件，设置 nginx_conf_include_enable 修改为true，并确定nginx配置文件目录

```
php:
  php_enable: false
  php_root_path: "/var/www/html"
  php_listen_port: 9092
  php_server_name: "example.com"
  php_fastcgi_pass: "127.0.0.1:9001"

nginx_config_include:
  nginx_config_include_enable: true
  nginx_config_include_path: "/opt/alb-2.0-kylin-arm/alb_install_dir/alb/conf/nginx_conf/*.conf"
```

2. 创建配置导入目录： `mkdir` **安装目录**`/alb-standard/conf/nginx_conf`

5.3.2 编写国密证书的Server内容文件并放入配置文件夹

编写国密双证书的server.conf文件，并放入 **安装目录**`/alb-standard/conf/nginx_conf` ，如下图为样例：

```
server {

    listen       9443 ssl;

    server_name  www.xxxx.com;
    ssl_certificate /opt/nginx_test/cert/fxqlndxpay.com-sign-cert.pem;
    ssl_certificate_key /opt/nginx_test/cert/fxqlndxpay.com-sign-privatekey.key;
    ssl_certificate /opt/nginx_test/cert/fxqlndxpay.com-enc-cert.pem;
    ssl_certificate_key /opt/nginx_test/cert/fxqlndxpay.com-enc-private-key.key;


    #ssl_protocols TLSv1.2 TLSv1.3 GMTLS;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;


    location / {

        root   /var/www/html;

        index  index.html index.htm;

    }

}
```

国密双证书文件

导入完后，重启ALB生效

5.4 非root启动ALB

很多客户要求使用非root启动alb，在使用root用户安装完毕alb标准版后，可以通过修改安装包的权限使得alb可以使用非root用户启动。

1. 使用root用户安装完毕alb标准版

2. 安装目录使用chown修改权限
3. 修改alb进程配置的用户为非root
4. 修改alb进程权限，支持非root监听80端口
5. 导入license并启动。

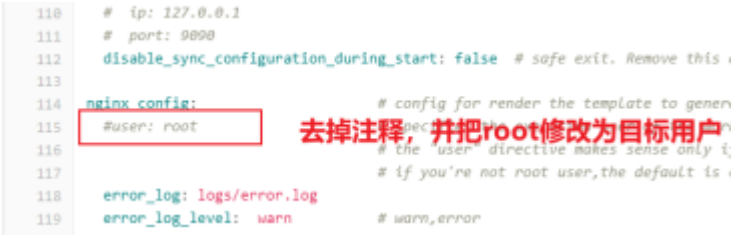
5.4.1 安装目录使用chown修改权限

1. 使用useradd创建用户alb_app，如果已经有用户，则使用已经有的用户名
2. 使用chown修改alb安装目录拥有者为目标用户

```
chown -R alb_app:alb_app alb-2.0-kylin-x86
chown -R alb_app:alb_app /opt/alb-apusic
```

5.4.2 修改alb进程配置的用户为非root用户名

1. 切换到非root用户alb_app，`su alb_app`
2. 使用vim修改文件：`vim 安装目录/alb-standard/conf/config-default.yaml`



5.4.3 修改alb进程权限，支持非root监听80端口

1. 切换到root用户
2. 使用命令：`setcap cap_net_bind_service=+eip /opt/alb-apusic/openresty/nginx/sbin/nginx`
3. 切换回目标用户alb_app
4. 重启ALB即可

5.5 ALB开机自启动

1、修改启动脚本安装目录的start.sh的变量cur_dir修改为脚本的绝对路径

```
#!/bin/bash

#cur_dir=$(pwd)
cur_dir=/opt/alb-2.0-centos-x86
alb_packages="$cur_dir/alb_packages"
# 默认安装在当前目录下alb_install_dir
install_package=${1:-"$cur_dir/alb_install_dir"}
install_soft="alb"

if [[ ! -d $alb_packages || ! -d $install_package ]];then
    alb_packages="$cur_dir/asg_packages"
    install_package="$cur_dir/asg_install_dir"
    install_soft="asg"
fi
```

2、在/etc/rc.d/rc.loacl里添加alb启动脚本路径

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.
touch /var/lock/subsys/local
/opt/alb-2.0-centos-x86/start.sh
~
~
~
```

5.6 Prometheus监控

ALB标准版提供Prometheus监控功能，默认不启用，如需启用，请切换到utils/exporter目录，执行：`./start-exporter.sh`，启动ALB的exporter。

5.6.1 启动说明

启动ALB的exporter必须要在alb配置文件中开启stub_status功能，如下：

```
server {
  listen 8080;              # node_status的端口
```

```
  location /node_status { # 必须要使用node_status
        stub_status on;   # 开启stub_status
        access_log off;
        allow 127.0.0.1;
    }
}
```

在执行start-exporter脚本后，要求输入

- node_status对应的server监听端口，默认为8080.
- exporter监听端口，默认为9113

如下为输入过程：

```
root@root:/utils/expoter$ ./start-exporter.sh
input alb server listening port(请输入node_status监听端口)：
alb server listening port(ALB node_status端口)：  8080
input exporter listening port(请输入监听端口)：
exporter listening port is 9113
exporter are running now!(exporter启动成功)
```

5.6.2 Prometheus监控数据获取

通过start-exporter成功后，可以通过浏览器或者prometheus访问: `http://IP:9113/metrics` 获取监控数据。

注： 如果上面修改了exporter的监听端口，上面url中的9113也一并修改。

6 ALB主备搭建

6.1 前提准备

两台机器好ALB和keepalived软件，其中ALB的安装路径为：/opt/alb-2.0-centos-x86 本文操作的两台机器分别为：

- A： 172.21.32.118、
- B： 172.21.32.11
- IP：172.21.32.198为keepalived的虚拟IP地址。
- 其中A节点作为主节点，B节点作为备节点。

6.2 操作步骤汇总

1. 修改ALB启动方式和数据库连接
2. 配置keepalived软件
3. 启动ALB、和keepalived

6.3 修改A节点启动方式脚本

切换到安装目录 /opt/alb-2.0-centos-x86，编辑start.sh脚本，如下所示，修改150行为下面注释所示

```
nohup_run_etcd() {
    # etcd 不支持arm架构
    if [ "$system_arch" = "arm" ];then
        export  ETCD_UNSUPPORTED_ARCH=arm64
    fi
    # 注释下面一样,
    # nohup etcd --data-dir $etcd_data_dir >> $etcd_log_path 2>&1 &
    # 改为这一行.
    nohup etcd --data-dir $etcd_data_dir  --listen-client-
urls="http://172.21.32.118:2379" --advertise-client-
urls="http://172.21.32.118:2379" >> $etcd_log_path 2>&1 &
}
```

这是一行内容，不能换行

上面的IP地址：172.21.32.118需要改为主节点的IP地址。

6.4 修改AB两个节点的数据库配置

- 修改alb连接数据库的配置 `vim 安装目录/alb-dashboard/conf/config.yaml` ,在文件结尾加入下面三行：

```
etcd:
  host:
    - "http://172.21.32.118:2379"
```

- 修改alb管控台的数据库配置 `vim 安装目录/alb-dashboard/conf/conf.yaml`，修改第10行的配置：为节点A的IP地址,如下所示

```
etcd:
  endpoints:           # 支持多个地址，支持集群
   - 172.21.32.118:2379  # 主节点的IP地址
```

修改完成后，执行stop.sh然后start.sh启动两个alb节点

6.5 主节点配置keepalived（A节点）

创建 `/etc/keepalived/keepalived.conf` 文件，在主节点A节点添加下面内容（附件文件keepalivedmaster.conf）

- interface enp0s31f6这个网卡enp0s31f6修改为当前节点物理网卡名称。
- 在virtual_ipaddrss中，把虚拟IP填上。

```
! Configuration File for keepalived

global_defs {
   router_id alb
}

vrrp_script chk_http_port {
   script "/etc/keepalived/checkalb.sh"
   interval 2 #（检测脚本执行的间隔）
   weight 2
}

vrrp_instance VI_1 {
    # state BACKUP
    state MASTER
    # 备份服务器上将 MASTER 改为 BACKUP
    interface enp0s31f6
```

```
    virtual_router_id 51
    # 主、备机的 virtual_router_id 必须相同
    priority 100
    # 主、备机取不同的优先级，主机值较大，备份机值较小
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        172.21.32.198 # 请根据需要，修改这个虚拟IP地址
    }
    track_script {
        chk_http_port
    }
}
```

6.6 主节点（A节点）创建健康检测脚本

创建健康检查脚本 `/etc/keepalived/checkalb.sh`，并添加下面内容

```
#!/bin/bash
alb_count=$(ps -ef|grep "alb: main process" |wc -l)
#1.判断ALB是否存活,如果不存活停止keepalived
if [ $alb_count -eq 0 ];then
    sleep 3
    #2.等待3秒后再次获取一次alb状态
    alb_count=$(ps -ef|grep "alb: main process" |wc -l)
    #3.再次进行判断， 如alb还不存活则停止Keepalived,让地址进行漂移,并退出脚本
    if [ $alb_count -eq 0 ];then
        echo "alb is down"
        exit 1
    fi
fi
```

6.7 从节点B配置keepavlied（B节点）

创建 `/etc/keepalived/keepalived.conf` 文件，在从节点B节点添加下面内容（附件文件keepalived-backup.conf）

- 注： interface enp0s31f6这个网卡enp0s31f6修改为当前节点物理网卡名称。

```
! Configuration File for keepalived
global_defs {
    router_id alb
}
vrrp_script chk_http_port {
    script "/etc/keepalived/checkalb.sh"
    interval 2 #（检测脚本执行的间隔）
    weight 2
}
vrrp_instance VI_1 {
    state BACKUP
    # state MASTER
    # 备份服务器上将 MASTER 改为 BACKUP
    interface enp0s31f6
    virtual_router_id 51
    # 主、备机的 virtual_router_id 必须相同
    priority 90
    # 主、备机取不同的优先级，主机值较大，备份机值较小
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        172.21.32.198 # 请根据需要，修改这个虚拟IP地址
    }
    track_script {
        chk_http_port
```

```
    }
}
```

6.8 备节点创建健康检测脚本

创建健康检查脚本`/etc/keepalived/checkalb.sh`，并添加下面内容

```
#!/bin/bash
alb_count=$(ps -ef|grep "alb: main process" |wc -l)
#1.判断ALB是否存活,如果不存活停止keepalived
if [ $alb_count -eq 0 ];then
    sleep 3
    #2.等待3秒后再次获取一次alb状态
    alb_count=$(ps -ef|grep "alb: main process" |wc -l)
    #3.再次进行判断, 如alb还不存活则停止Keepalived,让地址进行漂移,并退出脚本
    if [ $alb_count -eq 0 ];then
        echo "alb is down"
        exit 1
    fi
fi
```

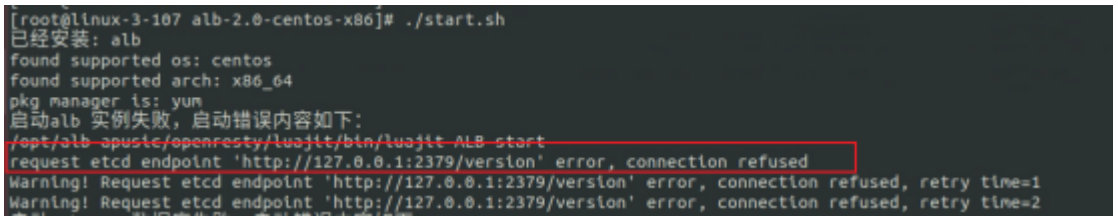
6.9 启动keepalived

- 在A、B两个节点使用命令启动keepalived： keepalived -f /etc/keepalived/keepalived.conf
- 使用虚拟IP访问ALB的管理控制台和代理地址。

7 常见问题与解决

7.1 ETCD连接失败

当执行start脚本后，出现以下etcd连接失败问题，可以通过修改启动脚本，延时启动alb。



7.1.1 问题解决

1、修改启动脚本start.sh，等待etcd启动完成。

如上图所示，在338行插入sleep 15，保存退出后，重启ALB

7.2 DNS is Empty（缺失dns服务器）

所在机器环境无DNS，则需要手动开启内置的DNS配置。

> *配置文件地址：* `安装目录/alb-standard/conf/config.yaml`

去掉前面的注释，即可开启DNS。

注意dns_resolver对齐到上面的enable_control

```
alb:
  enable_control: false   #开启会监听9090端口。

# 如果出现 local DNS is empty，那么把下面三行注释去掉即可，注意对齐到上面的
enable_control。
  dns_resolver:
```

```
    - 8.8.8.8
    - 114.114.114.114
php:
  php_enable: false
```

全国统一服务热线

4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。

Apusic 金蝶天燕

云计算国家标准制定企业

金蝶集团旗下基础软件企业

信息技术应用创新核心企业

官网：www.apusic.com