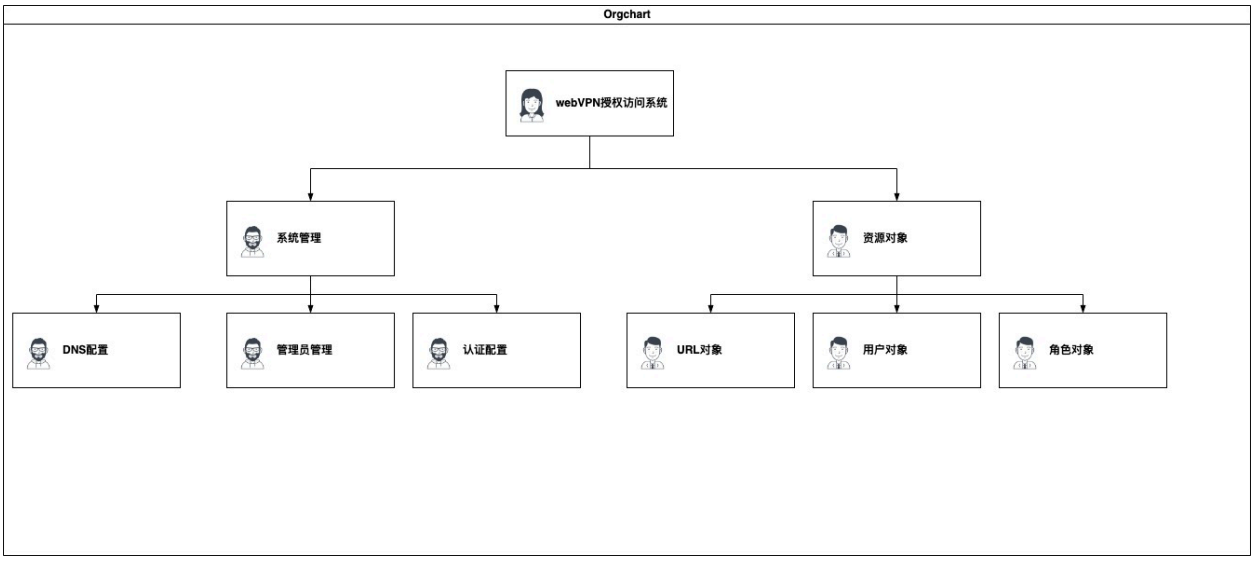
webvpn设计文档

1. 系统结构图



本期主要实现2个功能集，分别为系统管理及资源管理：

1.1.系统管理：

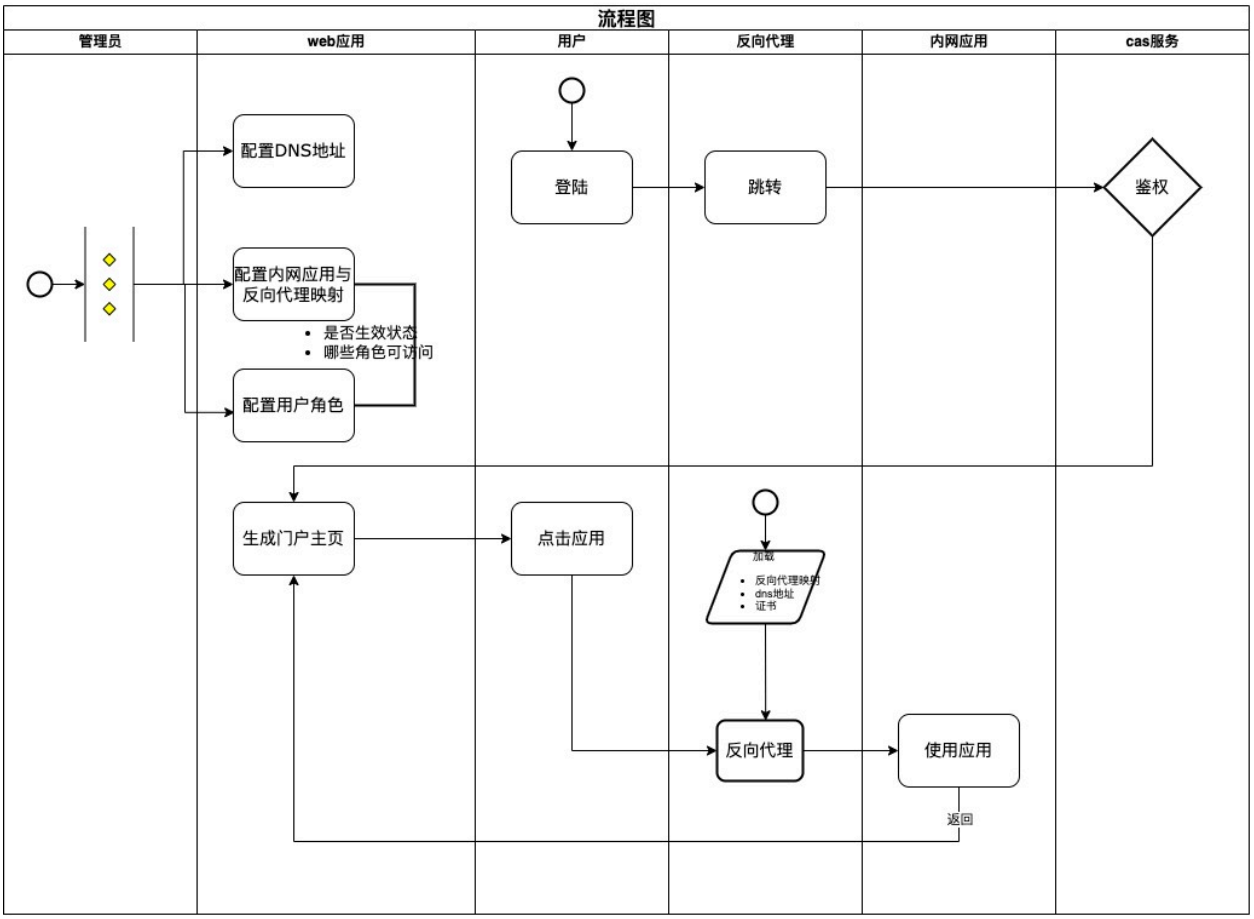
系统管理是配置通用功能的地点，目前包括DNS配置，该DNS配置为局域网DNS服务器地址，用于域名解析。

1.2.资源对象：

资源对象是管理员集中配置资源访问对象的地方，是本次开发的核心工能，主要包括url对象配置、用户对象配置及角色对象配置。

2. 系统流程分析

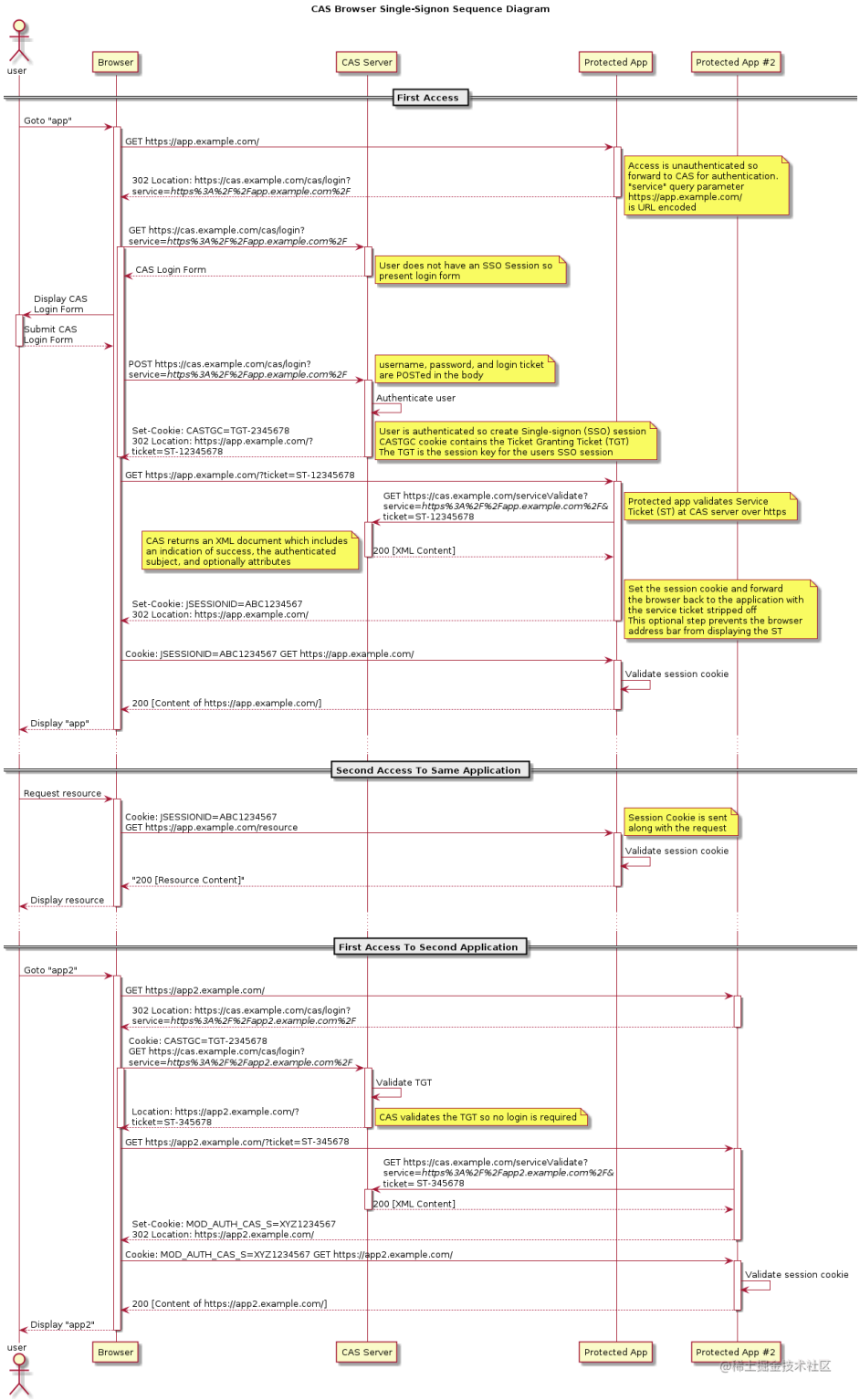
2.1.流程概览



总体流程如上图，管理首先配置校内局域网的DNS服务器地址信息，并通过校内cas服务器同步用户信息，并配置用户角色。每个用户可以配置多个角色。管理员还需要配置校内应用与公网域名的映射关系，反向代理服务器通过映射关系进行反向代理。

2.2.CAS认证流程图

当用户从外网域名登陆web时，将被重定向到cas服务器的登陆界面，并将登陆token写入cookie，cas登陆的流程图如下：

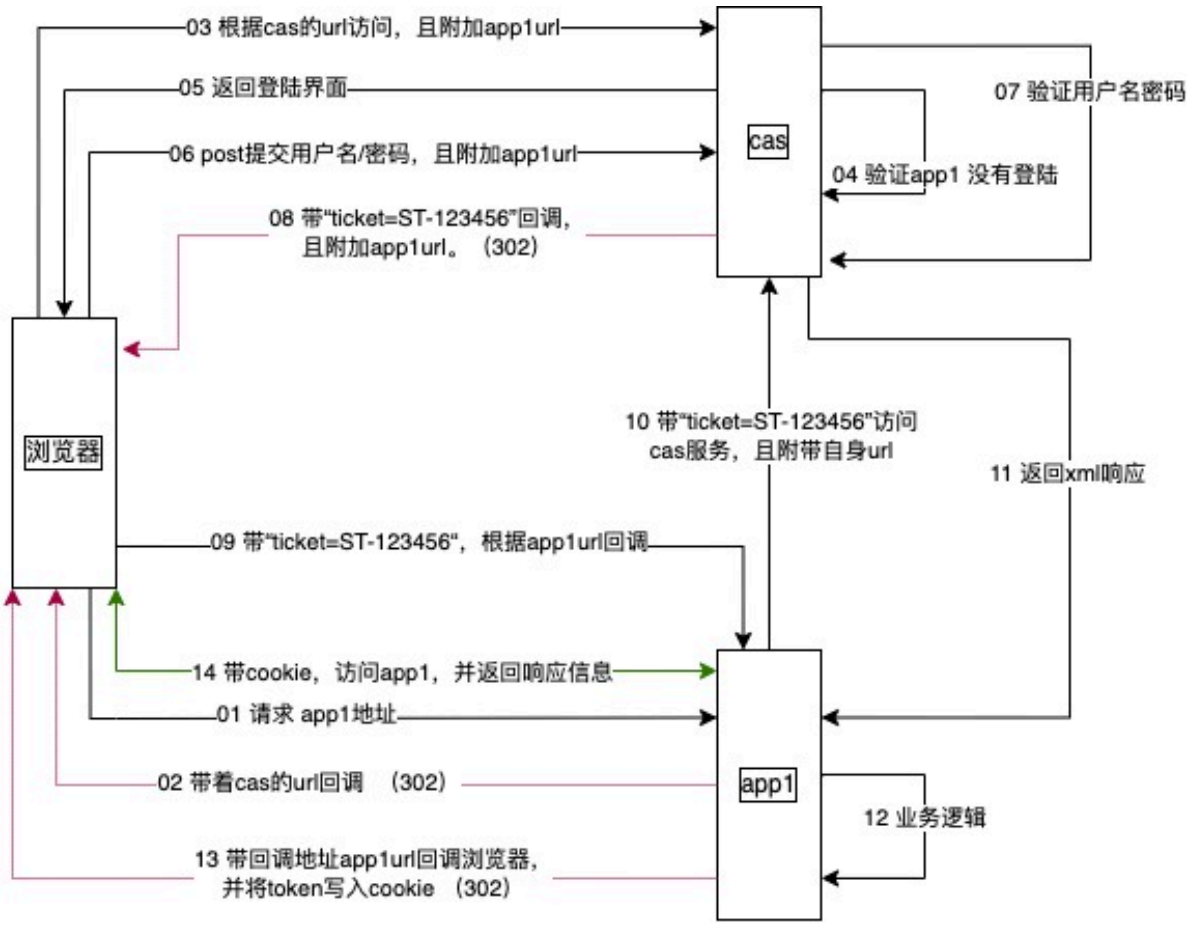


Ticket Granting Ticket(票据授权票据,简称TGT)

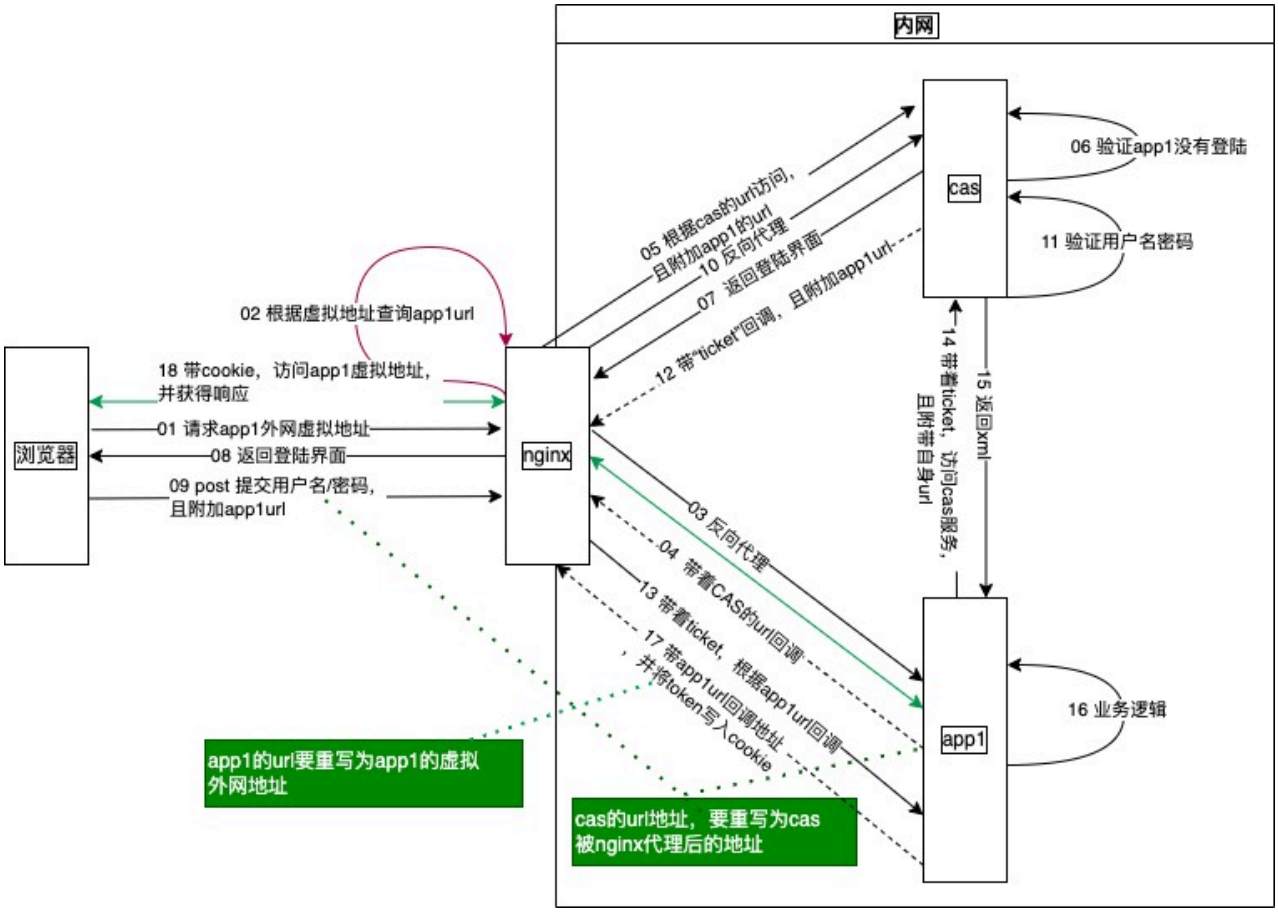
Service Ticket(服务票据,简称ST)

此处需要注意，由于有cas的存在，所以代理服务器由于要拦截用户浏览器到cas的请求响应，所以代理服务器必须位于浏览器与cas之间，又由于cas已经配置了代理应用的地址，且代理应用也与cas对接过，所以代理服务器也要拦截代理应用的请求信息。

2.3.现有CAS认证流程



2.4.WEBVPN项目认证流程图



以下为各流程描述：

序号	描述	其他
1	请求app1的外网虚拟地址（带子域名），此时访问到nginx服务的地址	
2	Nginx根据虚拟地址查询获得app1的内网地址，并根据内网地址反向代理	此处是nginx初始化加载，当2请求到达时应已存在映射关系
3	反向代理到内网中的app1	
4	app1中的CASclient会回调CASServer的url	302，此处要回写CASServer的地址为nginx代理的CASServer地址，因为如果是cas本身的内网地址，则webvpn将对后续访问脱管。
5	回跳到CASServer中	按nginx代理cas的地址跳转

序号	描述	其他
6	Cas服务器进行验证，假定目前没有登陆	
7	Cas服务器响应登陆页面	经nginx代理，此处应该替换登陆页面响应体中的表单地址，替换为nginx的代理后的casserver地址
8	浏览器看到CAS的登陆界面	输入用户名密码
9	点击提交按钮，表单链接由7替换为nginx代理的casserver地址	点击提交按钮，表单带用户名密码
10	反向代理至casserver内网地址	
11	casserver验证用户名密码	假定认证通过
12	casserver回调，附带ticket信息及app1的内网地址	302，此处需要将app1的内网地址重写为反向代理的app1地址（或外网虚拟地址）
13	带着ticket回调app1虚拟地址	
14	App1的casclient调用casserver内网地址，且附带app1外网地址	此处不确定，应该是casserver的内网地址和app1的外网地址，那么需要替换app1的外网地址为内网地址，否则casserver不认识，再将casserver内网地址替换为nginx代理的外网地址，否则代理将脱管
15	返回cas登陆信息，xml格式	返回给app1
16	App1进行业务处理	由casclient记录cookieid等信息
17	带app1的回调地址，回调客户端	由代理改写app1的内网地址为外网虚拟地址
18	写入浏览器cookie，完成鉴权过程	每次请求附带cookie信息，并由代理根据虚拟地址查询反向代理地址。

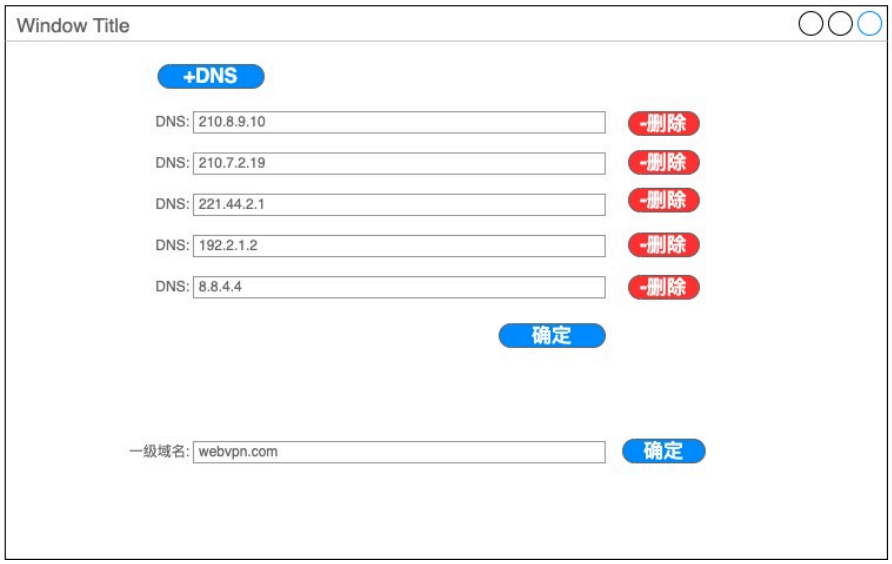
3. 功能描述

3.1.系统管理

一次性加载的配置项，及与系统相关的配置。

3.1.1.DNS配置

- 用于配置用户自建DNS地址，可配置多个，输入格式为ip校验。



- 此处录入一级域名，一级域名为从外网可访问nginx的域名地址，有且仅有一个。

  输入：ip地址

  输出：刷新DNS列表

  异常：统一弹出异常

  输入：一级域名地址

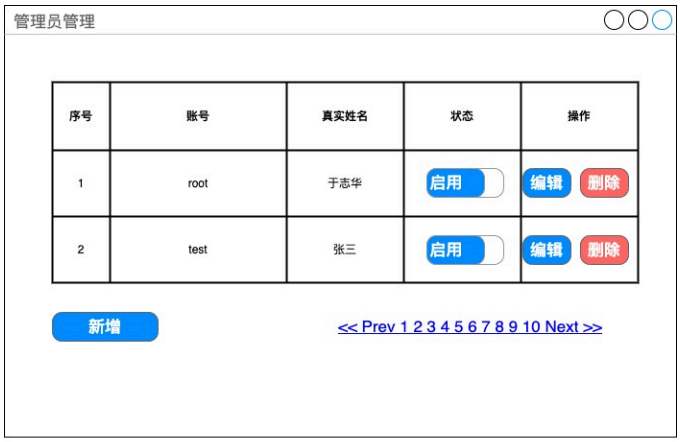
  输出：无

3.1.2.认证配置

配置CAS认证服务器的信息（未完）

3.1.3.管理员管理

管理员是webvpn系统的后台维护帐户，管理员是一类特殊的用户，仅对系统的后台管理开放，并不具有访问被保护app的权限，两者帐户互不相通。



输入：账号、真实姓名、密码、是否启用

输出：管理员列表

异常：统一弹出异常

3.2.资源管理

3.2.1.代理配置

3.2.2.用户对象

3.2.3.角色对象

4. 数据字典

4.1.代理配置表

proxies	
PK	**proxy_id int NOT NULL**
	proxy_name vchar(50) ：代理名称 vir_domain_name 虚拟域名 proxy_ip:内网ip officer : 负责人 officer_phone: 责任人电话 desc：描述 failure：失效判定（次） prefix： int（1） 代理前缀 1:固定关键词，0乱序 ignore：boolean 禁止代理 ture禁止 false 允许

4.2.管理员表

admins	
PK	**admin_id int NOT NULL**
	account vchar(50) NOT NULL password vchar(50) NOT NULL name vchar(50) NOT NULL sts: int(1) 1:启动 0:停用

4.3.域名服务器表

domain_name_servers	
PK	**dns_id int not null**
	dns vachar(50): IP地址格式

4.4.一级域名

有且仅有一条记录

domain_name	
PK	**name vcahr(50) int not null**