**翻译平台需求**

现在系统效果：

[https://jlccwss.vicp.cc:8085/public/#/login](https://jlccwss:8085/public/#/login)

用户名：admin

密码：admin

# 一期需求（价格4000，目标2月6日完成）

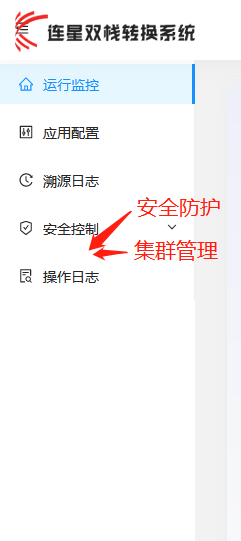
## 1.1页面整体风格按照截图中的修改

或者有其他合适的风格也行，总之换一换。

## 1.2 登录页需求



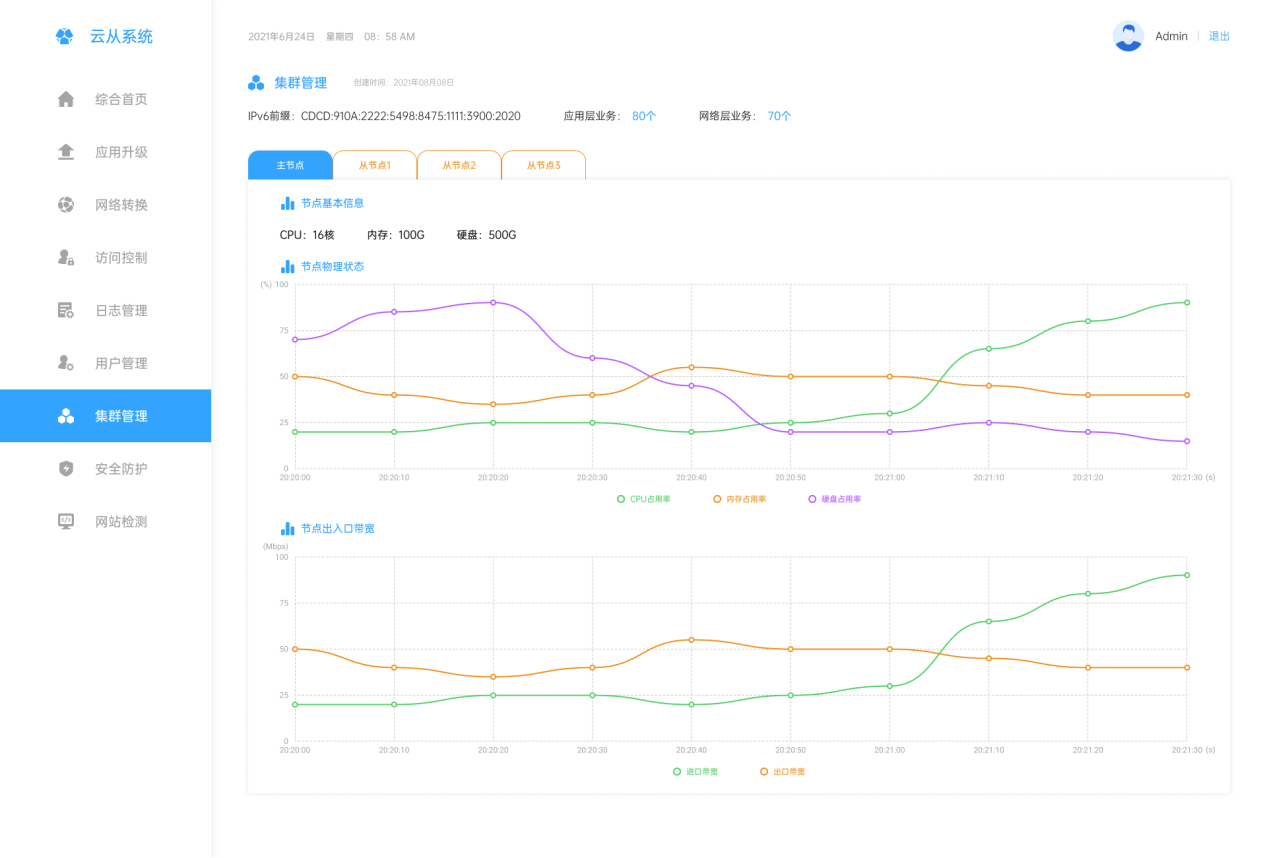
## 1.3 菜单需求



去掉安全控制，安全日志、访问管理移动到一级菜单。安全防护、集群管理加到箭头所示位置。

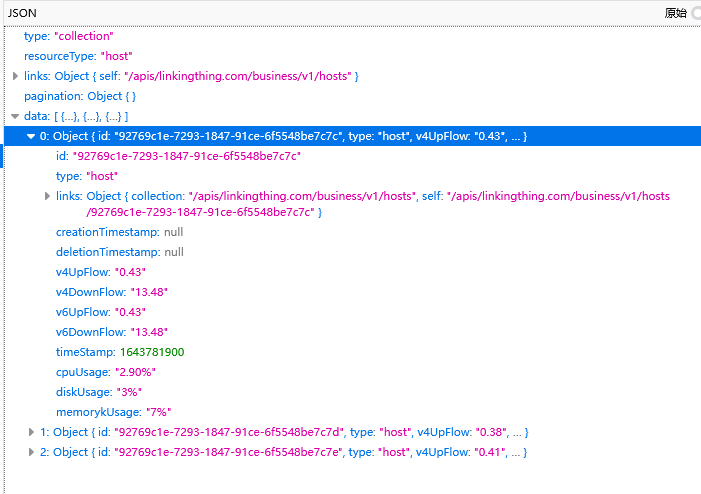
### 1.3.1 新增集群管理

无应用层业务和网络层业务



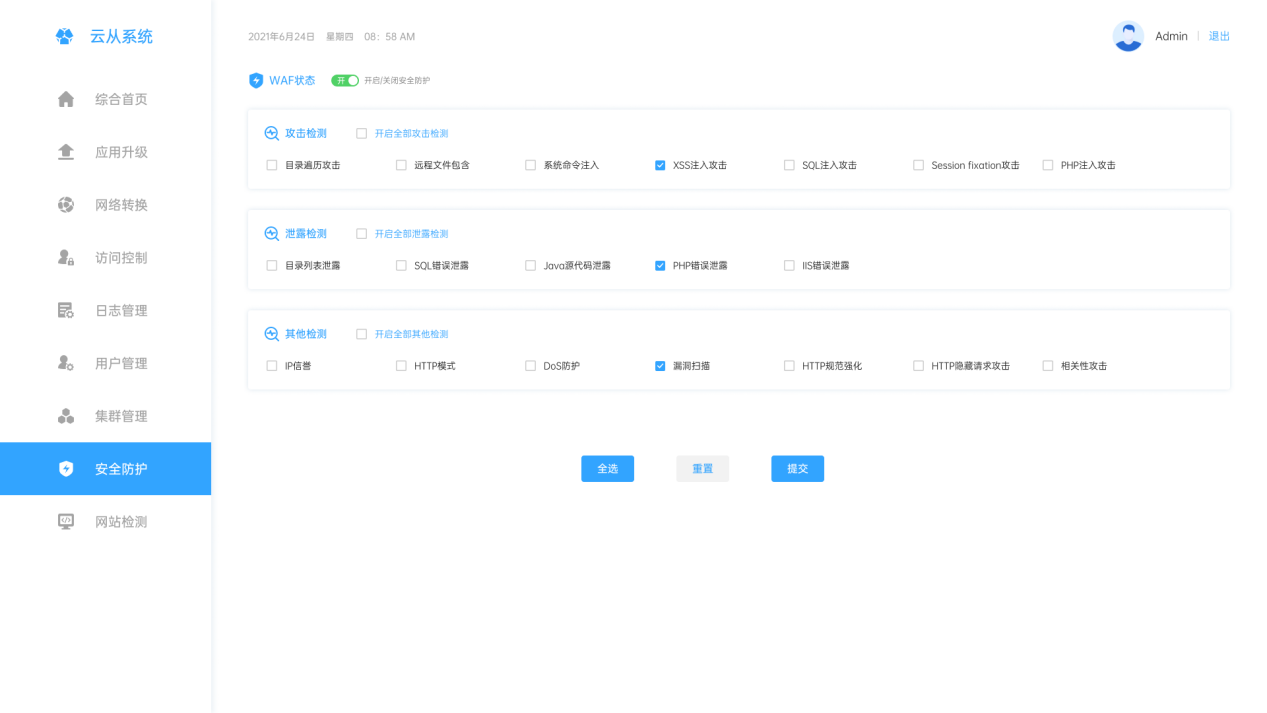
GET <https://xxxx:8085/apis/linkingthing.com/business/v1/hosts>

Response：



cpuUsage、diskUsage、memorykUsage、v4UpFlow、v4DownFlow、v6UpFlow、v6DownFlow、timeStamp一个24个节点的数组。

### 1.3.2 新增安全防护



#### 1.3.2.1 WAF服务启停设置

POST <https://175.47.237.81:8085/apis/linkingthing.com/business/v1/clusters/001/wafs/waf?action=isenabled>

入参举例

{  
 "isEnabled": true  
}

出参举例

{  
 "isSuccess": True  
}

入参参数意义

| 参数名称 | 数据类型 | 表示意义 | 参数值举例 | 备注 |
| --- | --- | --- | --- | --- |
| isEnabled | bool | 启动或者关闭服务 | true/false |  |

#### 1.3.2.2 **WAF设置**

PUT <https://175.47.237.81:8085/apis/linkingthing.com/business/v1/clusters/001/wafs/waf>

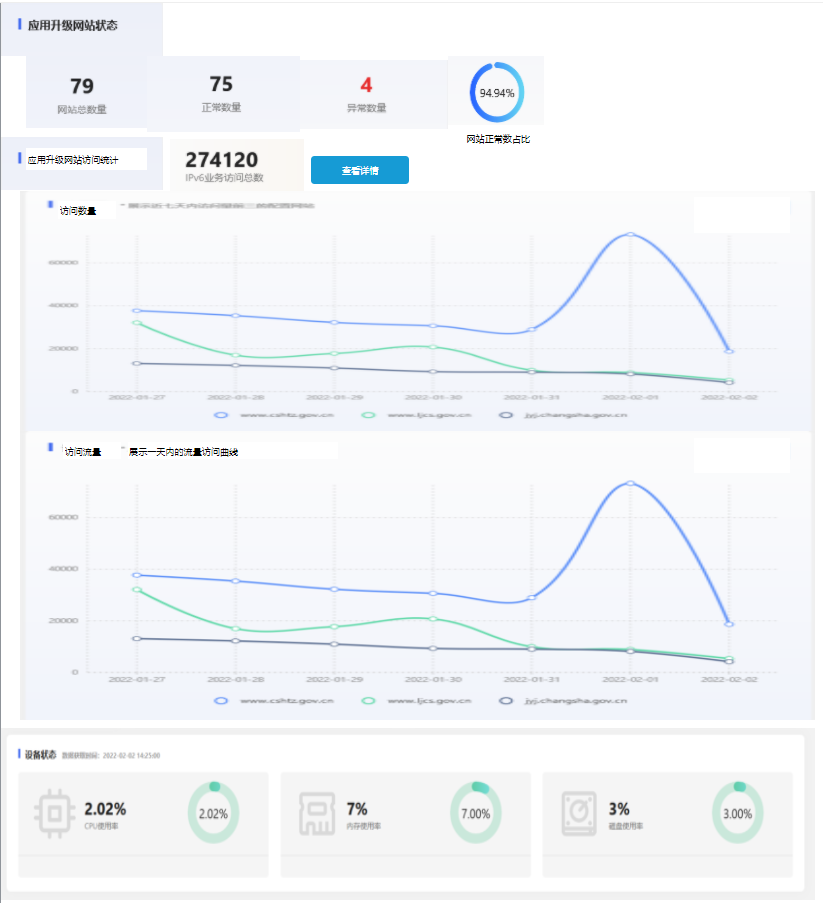
入参举例

{  
 "attackCheck": { //攻击检测  
 "directoryTraversalAttacks": true, // 目录遍历攻击  
 "remoteFileInclusionAttacks": true, // 远程文件包含攻击  
 "unixCommandInjection": true, // 系统命令注入攻击  
 "phpInjectionAttacks": true, // PHP注入攻击  
 "xssAttackDetectedViaLibInjection": true, // XSS注入攻击  
 "sqlInjectionAttacks": true, // SQL注入攻击  
 "possibleSessionFixationAttacks": true // 固定session攻击  
 },  
 "leakageCheck": { // 泄漏检测  
 "directoryListingLeakage": true, // 目录列表泄漏  
 "sqlErrorsLeakage": true, // SQL错误泄漏  
 "javaSourceCodeLeakage": true, // Java源代码泄漏  
 "phpErrorMessageLeakage": true, // PHP错误泄漏  
 "iisErrorsLeakage": true // IIS错误泄漏  
 },  
 "otherCheck": { // 其它检测  
 "ipReputationBlockFlagCheck": true, // IP Reputation检测  
 "httpAllowedRequestMethodsCheck": false, // HTTP 允许方法检测  
 "dosDefendCheck": true, // DDOS检测  
 "vulnerabilityScannerCheck": true, // 漏洞扫描检测  
 "enforceHttpRfcCheck": false, // HTTP规范检测  
 "httpRequestSmugglingAttack": true, // HTTP隐藏攻击检测  
 "correlatedAttackCheck": true // 关联式攻击检测  
 }  
}

出参参数意义

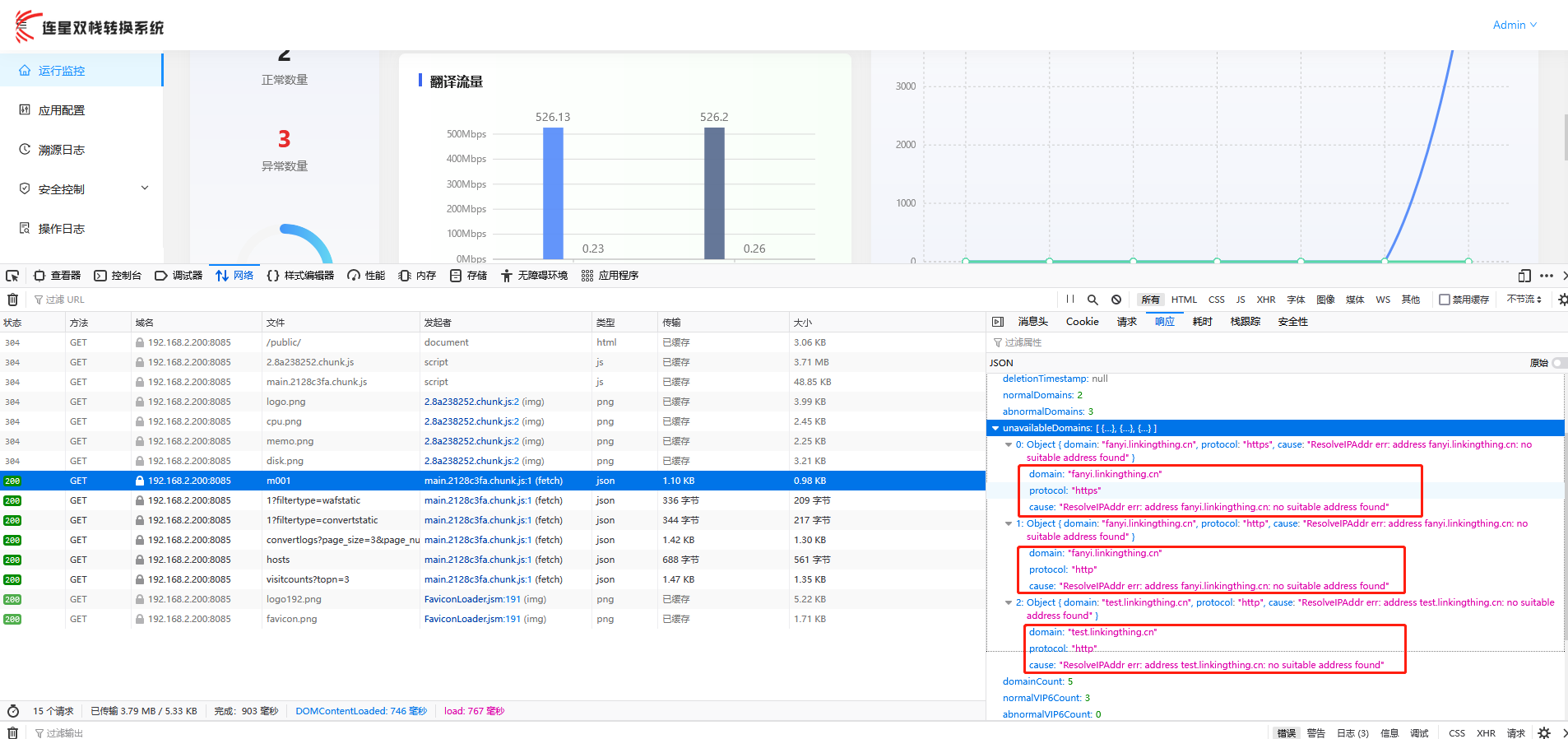


## 1.4 首页

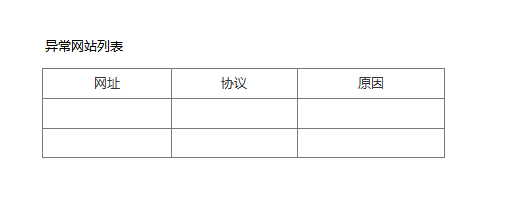


### 1.4.1 点击异常数量，弹出网站异常列表

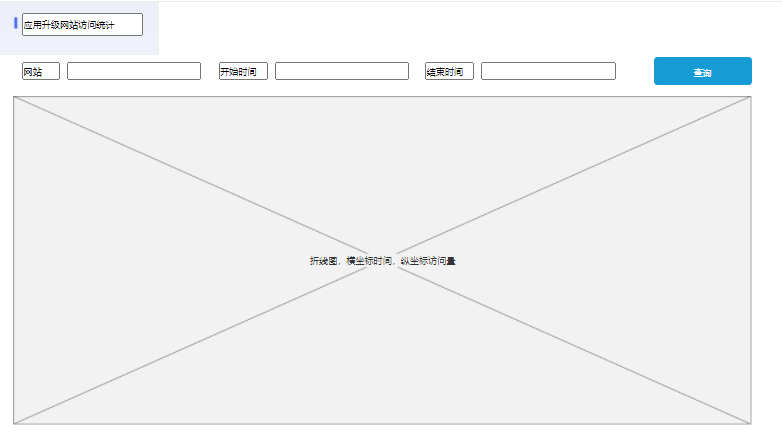
使用现有接口数据实现，如下图



弹窗内容如下：



### 1.4.2 点击查看详情，打开下级页面



接口待补，开始结束精确到天，默认网站值为TOP3中的第一个，时间默认当天。

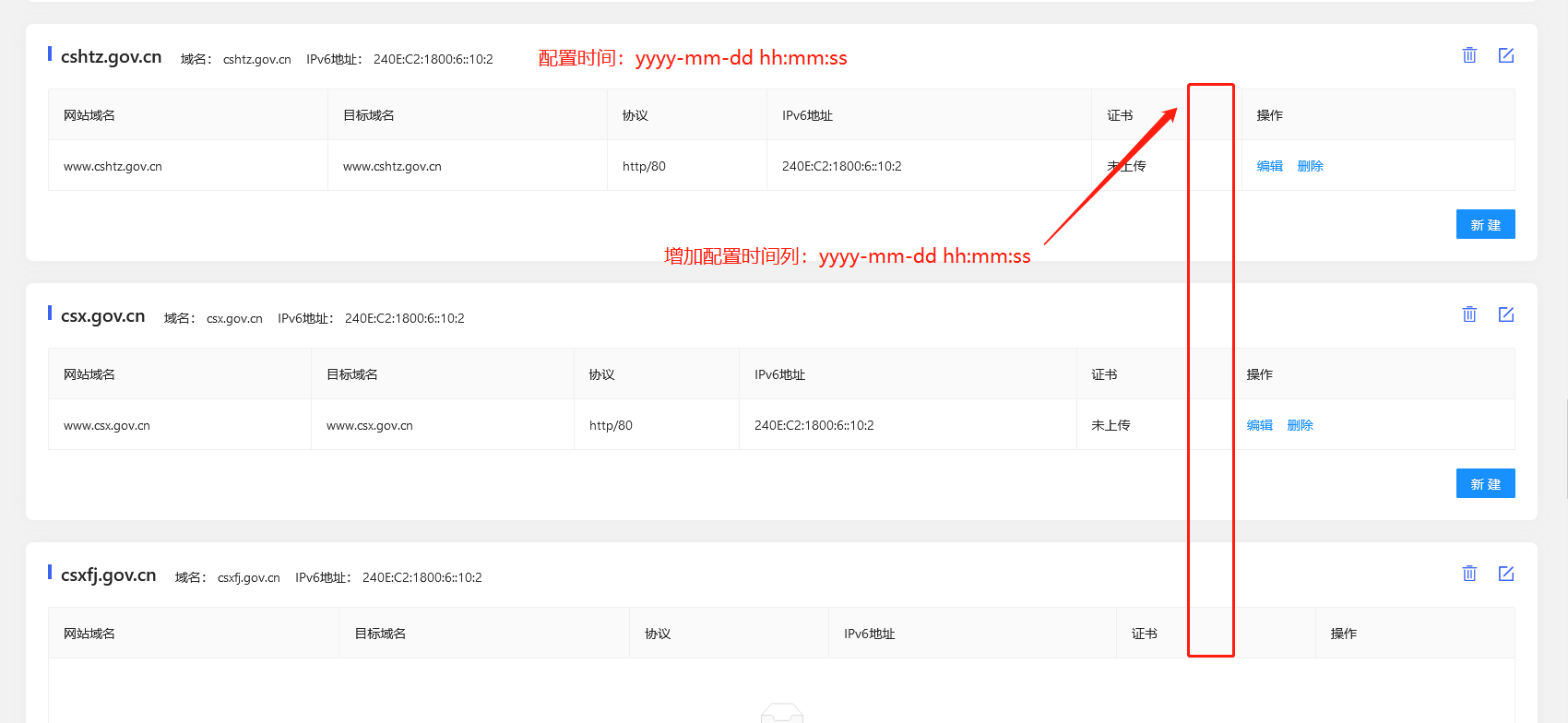
### 1.4.3 首页设备状态

接口：GET https://192.168.2.200:8085/apis/linkingthing.com/business/v1/hosts/hostmax

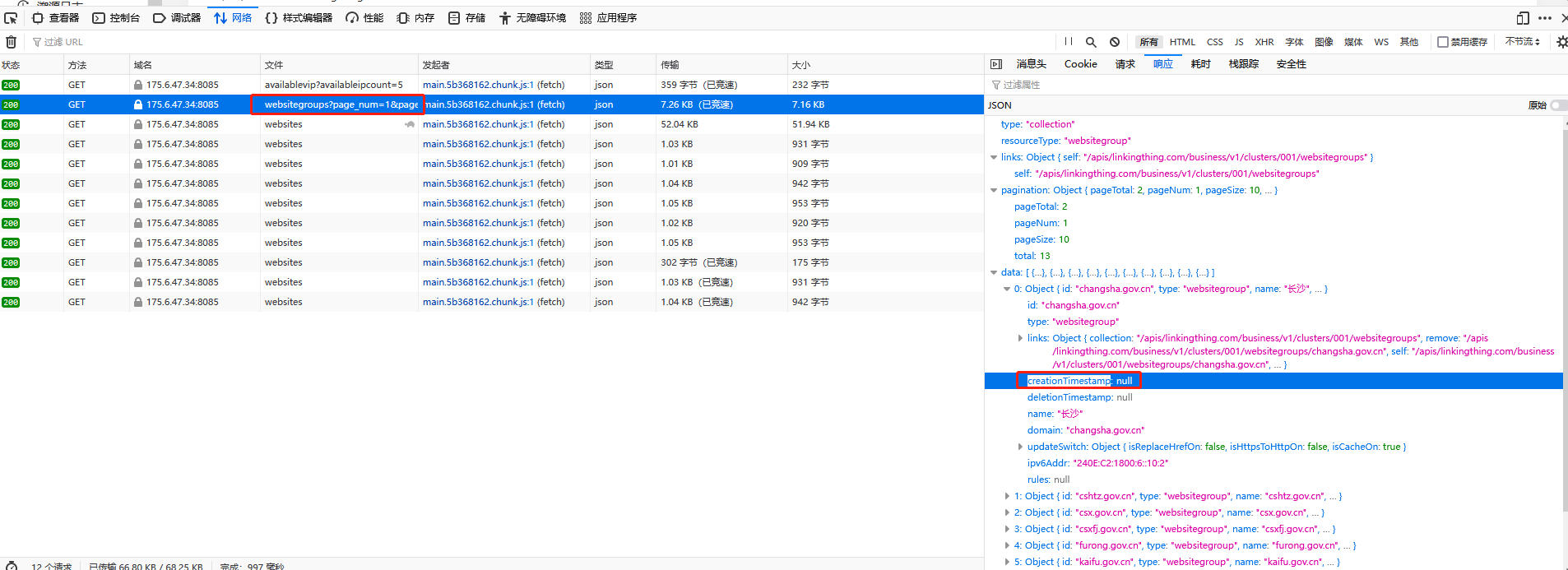
返回：{"id":"hostmax","type":"host","links":{"collection":"/apis/linkingthing.com/business/v1/hosts","self":"/apis/linkingthing.com/business/v1/hosts/f50b4d56-dce5-c15b-9377-98b8559ea25fbogon"},"creationTimestamp":null,"deletionTimestamp":null,"v4UpFlow":"0.20","v4DownFlow":"452.81","v6UpFlow":"0.22","v6DownFlow":"452.86","timeStamp":1643868000,"cpuUsage":"1.29%","diskUsage":"7%","memorykUsage":"74%"}

## 1.5 应用配置

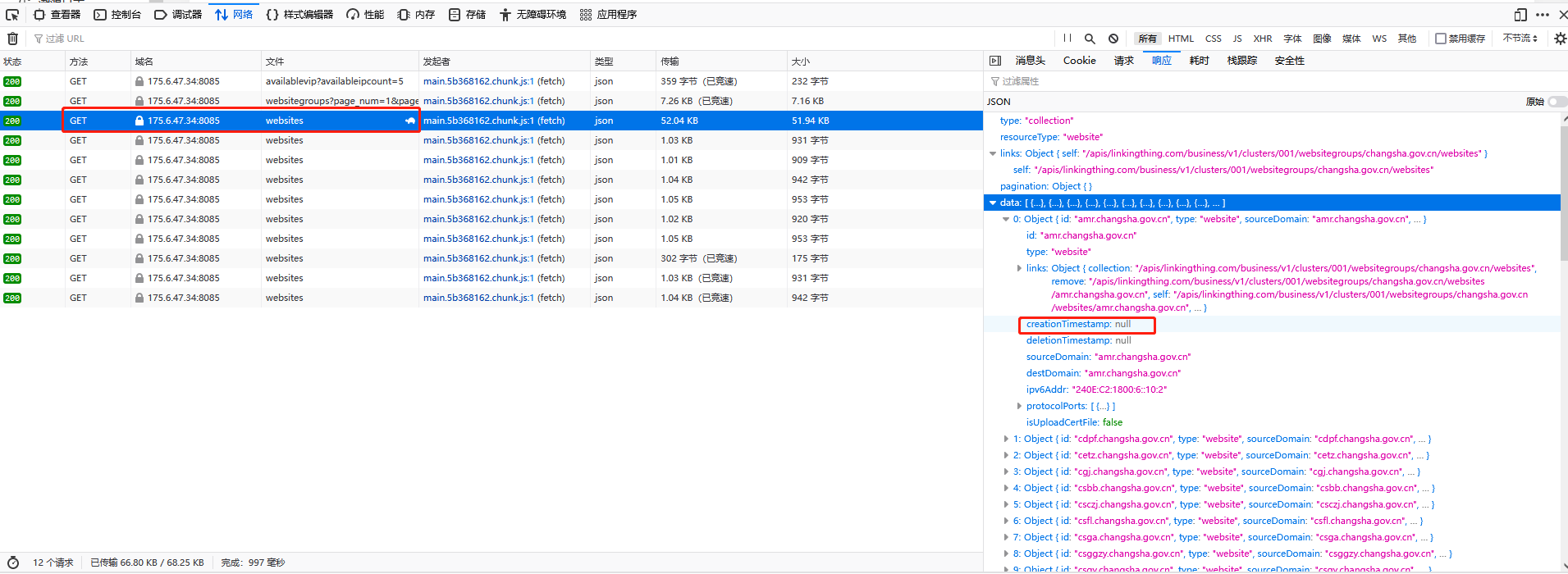
域名配置时间显示，所有的卡片再头部增加配置时间，表格增加配置时间列。里面有一个creationTimestamp：整型。



下图是卡片头的配置时间：



下面是每个卡片列表的配置时间字段：



# 二期需求（价格待定，时间待定）

## 2.1增加批量导入的模板；（2期）

## 2.2增加网站应用域名升级时，提示该网站支持IPv6访问，可对单个域名进行配置；（2期）

## 2.3域名在显示访问量页面同时显示流量（2期）