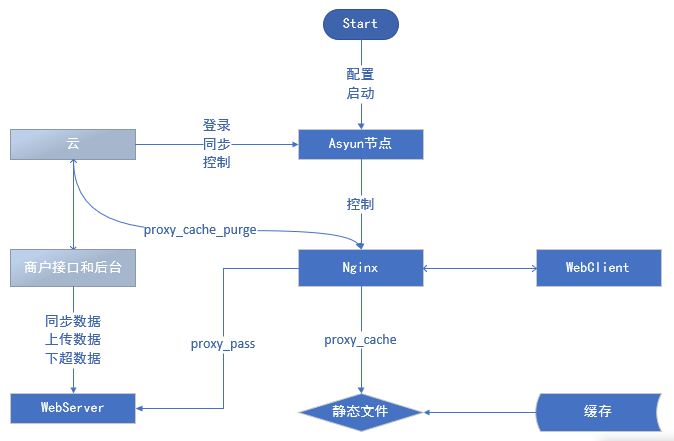
**Asyun节点**

* 1. **架构图**

实现CDN功能的结构图。



* 1. **关系与策略**
* Asyun是基于Nginx与云端的桥梁，与Nginx形成1对1的配置关系。Asyun结点对Nginx进行启用控制和关闭控制, 同步更新云端的配置信息到Nginx配置**。**对服务器的性能数据采集并同步云平台。**功能可用于对Nginx的启用和关闭的策略分析。**
* Nginx静态缓存，通过云端的缓存配置更新或修改Nginx的缓存配置，实时同步缓存的数据大小，动态显示缓存文件及缓存文件的击中率。 **功能可用于云端来对Nginx缓存的周期变化做策略分析。**

**阶段性介绍**

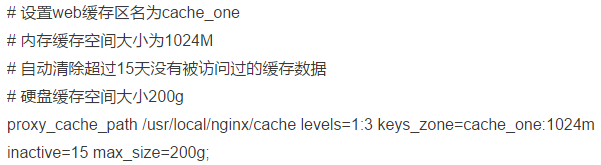
* 1. **控制部分**
* Asyun节点实现登录认证，保障云端接口安全；***系统还未实现，无法测试。***
* Asyun节点实现配置文件更新，用于对Nginx的配置进行动态更新；***已经测试通过。*** 
  1. **数据采集**
* Asyun节点实现性能数据文件上传；***已经测试通过。***
* Asyun节点读取缓存相关数据并采集与传输；***已经测试通过。***
  1. **其它功能**
* Asyun节点与云端的加密通信。***采用对称加密模式，暂时需要完成与云平台功能对接，现在加入加密功能会影响效率。***
* Asyun节点的配置文件。***针对Asyun节点本身的配置项，如：配置远程登录信息（账号、密码、Token），上传数据的时间间格、Nginx的启动路径、缓存的路径、Asyun允许云端控制的端口、网络相关信息(事务数量、连接数量)等。***
* Asyun错误日志与日志文件。***已经完成部份日志。***

**缓存处理**

* 1. **HTTP配置**



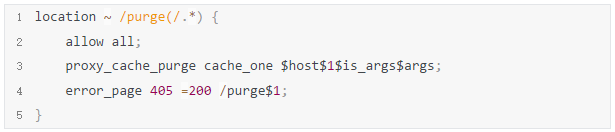
* Nginx模块开发，用于同步Nginx连接远端的相关数据到云端，需记录connect时间、read时间、send时间，网络吞吐量。**功能可用于云端用来对Nginx集群负载分配方案做策略分析。**



* Levels配置可以配置多级，如3到5为最佳；keys\_zone为配置缓存的Key值；max\_size为缓存文件存于硬盘的最大容量；可每时同步此文件目录的容量。**功能可用于云端用来对缓存清理做策略分析。**
  1. **Server缓存配置**



* Proxy\_cache\_key对应的Key值可以用于记录缓存文件的位置，用在于Purge来清理对应的缓存文件。他与Proxy\_cache\_purge的缓存清理文件的key值是相对应的。
* Proxy\_cache\_valid 不同的缓存设置不同的有效时间。
* proxy\_set\_header  自定义http header头，用于发送给后端真实服务器。
* proxy\_pass   指代理后转发的路径，也可以指向负载列表服务器。
  1. **Purge缓存清理**



* Proxy\_cache\_purge只是在域名和路径中间加入purge即可清理掉缓存中的文件。因前面缓存策略已经能处理掉缓存，并且会在指定的时间进行更新。这个功能针对特定的客户需求，备注为可选方案。
  1. **负载均衡配置**



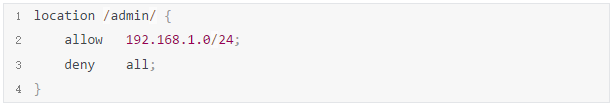
* proxy\_pass指向upstream backen的反向服务器列表，也可以指向地址。
* Backen是用于配置服务器列表，并且跟据服务器列表进行配置权限。其中包括轮询、权重（weight）、ip\_hash（地址的哈希）、fair（负载均衡）、url\_hash（超链接哈希）。

**安全配置**

* 1. **开启HTTPS**



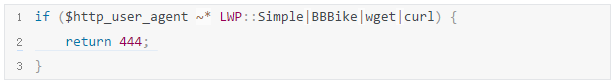
* ssl on： 开启https；
* ssl\_certificate： 配置nginx ssl证书的路径；
* ssl\_certificate\_key： 配置nginx ssl证书key的路径；
* ssl\_protocols： 指定客户端建立连接时使用的ssl协议版本，如果不需要兼容TSLv1，直接去掉即可；
* ssl\_ciphers： 指定客户端连接时所使用的加密算法，你可以再这里配置更高安全的算法；
  1. **添加黑白名单**



* allow：上边表示只允许192.168.1.0/24网段的主机访问，拒绝其他所有
* deny：也可以写成黑名单的方式禁止某些地址访问，允许其他所有，例如
  1. **限制请求方法**



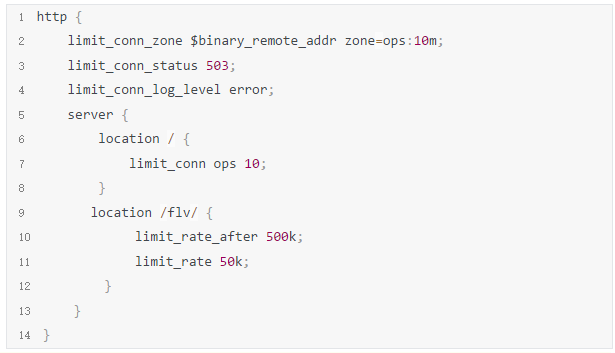
* $request\_method：能够获取到请求nginx的method
* 配置只允许GET\POST方法访问，其他的method返回405
  1. **拒绝User-Agent**



* 防止不法者会利用：wget、curl、python等自动化工具扫描网站。
  1. **图片防盗链**



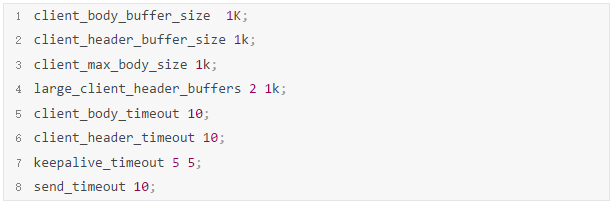
* valid\_referers： 验证referer，其中none允许referer为空，blocked允许不带协议的请求，除了以上两类外仅允许referer为www.ops-coffee.cn或ops-coffee.cn时访问images下的图片资源，否则返回403
  1. **控制并发连接数**



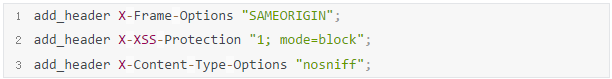
* limit\_conn： 指定一块已经设定的共享内存空间(例如name为ops的空间)，以及每个给定键值的最大连接数。
* limit\_rate\_after：定义当一个文件下载到指定大小（本例中为500k）之后开始限速； limit\_rate：限速下载速度为50k/s。
  1. **控制并发连接数**



* 1. **缓冲区溢出攻击**



* client\_body\_buffer\_size： 默认8k或16k。
* client\_header\_buffer\_size： 表示客户端请求头部的缓冲区大小。
* client\_max\_body\_size： 表示客户端请求的最大可接受body大小，如果请求大于指定的值，客户端将收到一个"Request Entity Too Large" (413)错误，通常在上传文件到服务器时会受到限制。
* large\_client\_header\_buffers 表示一些比较大的请求头使用的缓冲区数量和大小，默认一个缓冲区大小为操作系统中分页文件大小，通常是4k或8k，请求字段不能大于一个缓冲区大小，如果客户端发送一个比较大的头，nginx将返回"Request URI too large" (414)，请求的头部最长字段不能大于一个缓冲区，否则服务器将返回"Bad request" (400)。
* client\_body\_timeout： 表示读取请求body的超时时间，如果连接超过这个时间而客户端没有任何响应，Nginx将返回"Request time out" (408)错误。
* client\_header\_timeout： 表示读取客户端请求头的超时时间，如果连接超过这个时间而客户端没有任何响应，Nginx将返回"Request time out" (408)错误。
* keepalive\_timeout： 参数的第一个值表示客户端与服务器长连接的超时时间，超过这个时间，服务器将关闭连接，可选的第二个参数参数表示Response头中Keep-Alive: timeout=time的time值，这个值可以使一些浏览器知道什么时候关闭连接，以便服务器不用重复关闭，如果不指定这个参数，nginx不会在应Response头中发送Keep-Alive信息。
* send\_timeout： 表示发送给客户端应答后的超时时间，Timeout是指没有进入完整established状态，只完成了两次握手，如果超过这个时间客户端没有任何响应，nginx将关闭连接。
  1. **Header头设置**



* X-Frame-Options： 响应头表示是否允许浏览器加载frame等属性，有三个配置DENY禁止任何网页被嵌入,SAMEORIGIN只允许本网站的嵌套,ALLOW-FROM允许指定地址的嵌套。
* X-XSS-Protection： 表示启用XSS过滤（禁用过滤为X-XSS-Protection: 0），mode=block表示若检查到XSS攻击则停止渲染页面
* X-Content-Type-Options： 响应头用来指定浏览器对未指定或错误指定Content-Type资源真正类型的猜测行为，nosniff 表示不允许任何猜测