Nginx 在启动后，在 unix 系统中会以 daemon 的方式在后台运行，后台进程包含一个 master 进程和多个 worker 进程。

在 Nginx 中 connection 就是对 tcp 连接的封装，其中包括连接的 socket，读事件，写事件。利用 Nginx 封装的 connection，我们可以很方便的使用 Nginx 来处理与连接相关的事情，比如，建立连接，发送与接受数据等。而 Nginx 中的 http 请求的处理就是建立在 connection之上的，所以 Nginx 不仅可以作为一个web服务器，也可以作为邮件服务器。当然，利用 Nginx 提供的 connection，我们可以与任何后端服务打交道

首先，Nginx 在启动时，会解析配置文件，得到需要监听的端口与 ip 地址，然后在 Nginx 的 master 进程里面，先初始化好这个监控的 socket(创建 socket，设置 addrreuse 等选项，绑定到指定的 ip 地址端口，再 listen)，然后再 fork 出多个子进程出来，然后子进程会竞争 accept 新的连接。此时，客户端就可以向 Nginx 发起连接了。当客户端与服务端通过三次握手建立好一个连接后，Nginx 的某一个子进程会 accept 成功，得到这个建立好的连接的 socket，然后创建 Nginx 对连接的封装，即 ngx\_connection\_t 结构体。接着，设置读写事件处理函数并添加读写事件来与客户端进行数据的交换。最后，Nginx 或客户端来主动关掉连接，到此，一个连接就寿终正寝了。

当然，Nginx 也是可以作为客户端来请求其它 server 的数据的（如 upstream 模块），此时，与其它 server 创建的连接，也封装在 ngx\_connection\_t 中。作为客户端，Nginx 先获取一个 ngx\_connection\_t 结构体，然后创建 socket，并设置 socket 的属性（ 比如非阻塞）。然后再通过添加读写事件，调用 connect/read/write 来调用连接，最后关掉连接，并释放 ngx\_connection\_t。

在 Nginx 中，每个进程会有一个连接数的最大上限，这个上限与系统对 fd 的限制不一样。在操作系统中，通过 ulimit -n，我们可以得到一个进程所能够打开的 fd 的最大数，即 nofile，因为每个 socket 连接会占用掉一个 fd，所以这也会限制我们进程的最大连接数，当然也会直接影响到我们程序所能支持的最大并发数，当 fd 用完后，再创建 socket 时，就会失败。Nginx 通过设置 worker\_connectons 来设置每个进程支持的最大连接数。如果该值大于 nofile，那么实际的最大连接数是 nofile，Nginx 会有警告。Nginx 在实现时，是通过一个连接池来管理的，每个 worker 进程都有一个独立的连接池，连接池的大小是 worker\_connections。这里的连接池里面保存的其实不是真实的连接，它只是一个 worker\_connections 大小的一个 ngx\_connection\_t 结构的数组。并且，Nginx 会通过一个链表 free\_connections 来保存所有的空闲 ngx\_connection\_t，每次获取一个连接时，就从空闲连接链表中获取一个，用完后，再放回空闲连接链表里面。

在这里，很多人会误解 worker\_connections 这个参数的意思，认为这个值就是 Nginx 所能建立连接的最大值。其实不然，这个值是表示每个 worker 进程所能建立连接的最大值，所以，一个 Nginx 能建立的最大连接数，应该是worker\_connections \* worker\_processes。当然，这里说的是最大连接数，对于 HTTP 请求本地资源来说，能够支持的最大并发数量是worker\_connections \* worker\_processes，而如果是 HTTP 作为反向代理来说，最大并发数量应该是worker\_connections \* worker\_processes/2。因为作为反向代理服务器，每个并发会建立与客户端的连接和与后端服务的连接，会占用两个连接。

**二、常用命令**

       nginx 的使用比较简单，就是几条命令。

[复制代码](javascript:void(0);)

nginx -s stop # 快速关闭Nginx，可能不保存相关信息，并迅速终止web服务。

nginx -s quit #平稳关闭Nginx，保存相关信息，有安排的结束web服务。

nginx -s reload #因改变了Nginx相关配置，需要重新加载配置而重载。

nginx -s reopen #重新打开日志文件。

nginx -c filename #为 Nginx 指定一个配置文件，来代替缺省的。

nginx -t #不运行，而仅仅测试配置文件。nginx 将检查配置文件的语法的正确性，并尝试打开配置文件中所引用到的文件。

nginx -v #显示 nginx 的版本。

nginx -V #显示 nginx 的版本，编译器版本和配置参数。

**三、http反向代理配置**

   我们先实现一个小目标：不考虑复杂的配置，仅仅是完成一个 http 反向代理。

  nginx.conf 配置文件如下

[复制代码](javascript:void(0);)

#运行用户

#user somebody;

#启动进程,通常设置成和cpu的数量相等

worker\_processes 1;

#全局错误日志

error\_log D:/Tools/nginx-1.10.1/logs/error.log;

error\_log D:/Tools/nginx-1.10.1/logs/notice.log notice;

error\_log D:/Tools/nginx-1.10.1/logs/info.log info;

#PID文件，记录当前启动的nginx的进程ID

pid D:/Tools/nginx-1.10.1/logs/nginx.pid;

#工作模式及连接数上限

events {

worker\_connections 1024; #单个后台worker process进程的最大并发链接数

}

#设定http服务器，利用它的反向代理功能提供负载均衡支持

http {

#设定mime类型(邮件支持类型),类型由mime.types文件定义

include D:/Tools/nginx-1.10.1/conf/mime.types;

default\_type application/octet-stream;

#设定日志

log\_format main '[$remote\_addr] - [$remote\_user] [$time\_local] "$request" '

'$status $body\_bytes\_sent "$http\_referer" '

'"$http\_user\_agent" "$http\_x\_forwarded\_for"';

access\_log D:/Tools/nginx-1.10.1/logs/access.log main;

rewrite\_log on;

#sendfile 指令指定 nginx 是否调用 sendfile 函数（zero copy 方式）来输出文件，对于普通应用，

#必须设为 on,如果用来进行下载等应用磁盘IO重负载应用，可设置为 off，以平衡磁盘与网络I/O处理速度，降低系统的uptime.

sendfile on;

#tcp\_nopush on;

#连接超时时间

keepalive\_timeout 120;

tcp\_nodelay on;

#gzip压缩开关

#gzip on;

#设定实际的服务器列表

upstream zp\_server1{

server 127.0.0.1:8089;

}

#HTTP服务器

server {

#监听80端口，80端口是知名端口号，用于HTTP协议

listen 80;

#定义使用www.xx.com访问

server\_name www.helloworld.com;

#首页

index index.html

#指向webapp的目录

root D:\01\_Workspace\Project\github\zp\SpringNotes\spring-security\spring-shiro\src\main\webapp;

#编码格式

charset utf-8;

#代理配置参数

proxy\_connect\_timeout 180;

proxy\_send\_timeout 180;

proxy\_read\_timeout 180;

proxy\_set\_header Host $host;

proxy\_set\_header X-Forwarder-For $remote\_addr;

#反向代理的路径（和upstream绑定），location 后面设置映射的路径

location / {

proxy\_pass http://zp\_server1;

}

#静态文件，nginx自己处理

location ~ ^/(images|javascript|js|css|flash|media|static)/ {

root D:\01\_Workspace\Project\github\zp\SpringNotes\spring-security\spring-shiro\src\main\webapp\views;

#过期30天，静态文件不怎么更新，过期可以设大一点，如果频繁更新，则可以设置得小一点。

expires 30d;

}

#设定查看Nginx状态的地址

location /NginxStatus {

stub\_status on;

access\_log on;

auth\_basic "NginxStatus";

auth\_basic\_user\_file conf/htpasswd;

}

#禁止访问 .htxxx 文件

location ~ /\.ht {

deny all;

}

#错误处理页面（可选择性配置）

#error\_page 404 /404.html;

#error\_page 500 502 503 504 /50x.html;

#location = /50x.html {

# root html;

#}

}

}

**四、负载均衡配置**

上一个例子中，代理仅仅指向一个服务器。

但是，网站在实际运营过程中，多半都是有多台服务器运行着同样的app，这时需要使用负载均衡来分流。

nginx也可以实现简单的负载均衡功能。

假设这样一个应用场景：将应用部署在 192.168.1.11:80、192.168.1.12:80、192.168.1.13:80 三台linux环境的服务器上。网站域名叫 www.helloworld.com，公网IP为 192.168.1.11。在公网IP所在的服务器上部署 nginx，对所有请求做负载均衡处理。

**nginx.conf** 配置如下：

[复制代码](javascript:void(0);)

http {

#设定mime类型,类型由mime.type文件定义

include /etc/nginx/mime.types;

default\_type application/octet-stream;

#设定日志格式

access\_log /var/log/nginx/access.log;

#设定负载均衡的服务器列表

upstream load\_balance\_server {

#weigth参数表示权值，权值越高被分配到的几率越大

server 192.168.1.11:80 weight=5;

server 192.168.1.12:80 weight=1;

server 192.168.1.13:80 weight=6;

}

#HTTP服务器

server {

#侦听80端口

listen 80;

#定义使用www.xx.com访问

server\_name www.helloworld.com;

#对所有请求进行负载均衡请求

location / {

root /root; #定义服务器的默认网站根目录位置

index index.html index.htm; #定义首页索引文件的名称

proxy\_pass http://load\_balance\_server ;#请求转向load\_balance\_server 定义的服务器列表

#以下是一些反向代理的配置(可选择性配置)

#proxy\_redirect off;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

#后端的Web服务器可以通过X-Forwarded-For获取用户真实IP

proxy\_set\_header X-Forwarded-For $remote\_addr;

proxy\_connect\_timeout 90; #nginx跟后端服务器连接超时时间(代理连接超时)

proxy\_send\_timeout 90; #后端服务器数据回传时间(代理发送超时)

proxy\_read\_timeout 90; #连接成功后，后端服务器响应时间(代理接收超时)

proxy\_buffer\_size 4k; #设置代理服务器（nginx）保存用户头信息的缓冲区大小

proxy\_buffers 4 32k; #proxy\_buffers缓冲区，网页平均在32k以下的话，这样设置

proxy\_busy\_buffers\_size 64k; #高负荷下缓冲大小（proxy\_buffers\*2）

proxy\_temp\_file\_write\_size 64k; #设定缓存文件夹大小，大于这个值，将从upstream服务器传

client\_max\_body\_size 10m; #允许客户端请求的最大单文件字节数

client\_body\_buffer\_size 128k; #缓冲区代理缓冲用户端请求的最大字节数

}

}

}

## 六、https反向代理配置

一些对安全性要求比较高的站点，可能会使用 HTTPS（一种使用ssl通信标准的安全HTTP协议）。

这里不科普 HTTP 协议和 SSL 标准。但是，使用 nginx 配置 https 需要知道几点：

* HTTPS 的固定端口号是 443，不同于 HTTP 的 80 端口
* SSL 标准需要引入安全证书，所以在 nginx.conf 中你需要指定证书和它对应的 key

其他和 http 反向代理基本一样，只是在 Server 部分配置有些不同。

[复制代码](javascript:void(0);)

#HTTP服务器

server {

#监听443端口。443为知名端口号，主要用于HTTPS协议

listen 443 ssl;

#定义使用www.xx.com访问

server\_name www.helloworld.com;

#ssl证书文件位置(常见证书文件格式为：crt/pem)

ssl\_certificate cert.pem;

#ssl证书key位置

ssl\_certificate\_key cert.key;

#ssl配置参数（选择性配置）

ssl\_session\_cache shared:SSL:1m;

ssl\_session\_timeout 5m;

#数字签名，此处使用MD5

ssl\_ciphers HIGH:!aNULL:!MD5;

ssl\_prefer\_server\_ciphers on;

location / {

root /root;

index index.html index.htm;

}

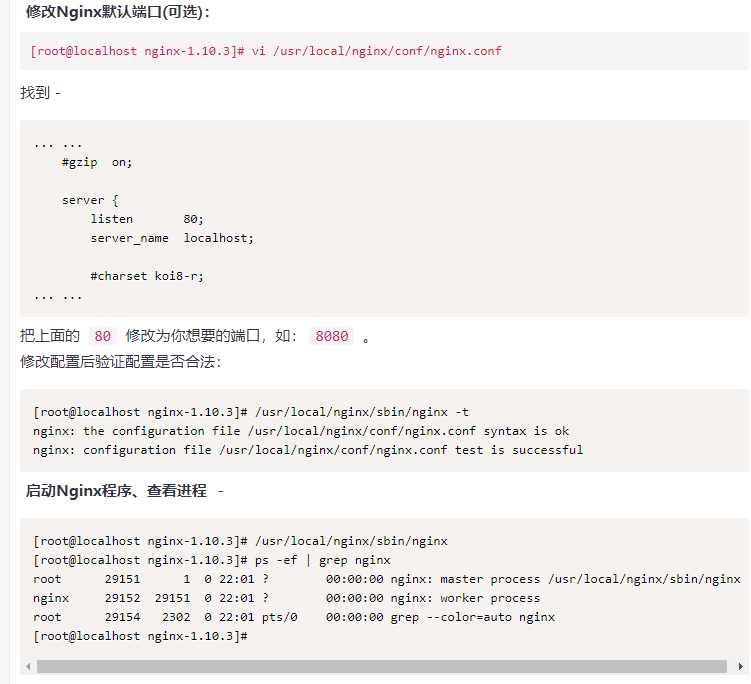
}

[**Windows下Nginx的启动、停止等命令**](https://www.cnblogs.com/qianzf/p/6809427.html)

Windows下Nginx的启动、停止等命令  
在Windows下使用Nginx，我们需要掌握一些基本的操作命令，比如：启动、停止Nginx服务，重新载入Nginx等，下面我就进行一些简单的介绍。  
1、启动：  
C:\server\nginx-1.0.2>start nginx或  
C:\server\nginx-1.0.2>nginx.exe  
  
2、停止：  
C:\server\nginx-1.0.2>nginx.exe -s stop或  
C:\server\nginx-1.0.2>nginx.exe -s quit  
注：stop是快速停止nginx，可能并不保存相关信息；quit是完整有序的停止nginx，并保存相关信息。  
  
3、重新载入Nginx：  
C:\server\nginx-1.0.2>nginx.exe -s reload  
当配置信息修改，需要重新载入这些配置时使用此命令。

4、重新打开日志文件：  
C:\server\nginx-1.0.2>nginx.exe -s reopen  
  
5、查看Nginx版本：  
C:\server\nginx-1.0.2>nginx -v





/usr/local/nginx/sbin/nginx -t

使用configure命令配置构建。 它定义了系统的各个方面，包括允许使用nginx进行连接处理的方法。 最后它创建一个Makefile。 configure命令支持以下参数：

* --prefix = path - 定义将保留服务器文件的目录。 这个同一个目录也将用于由configure(除了库源的路径)和nginx.conf配置文件中设置的所有相关路径。 它默认设置为/usr/local/nginx目录。
* --sbin-path = path - 设置nginx可执行文件的名称。此名称仅在安装期间使用。默认情况下文件名为 prefix/sbin/nginx。
* --conf-path = path - 设置nginx.conf配置文件的名称。 如果需要，nginx可以始终使用不同的配置文件启动，方法是在命令行参数-c file 指定。 默认情况下，该文件名为：prefix/conf/nginx.conf。
* --pid-path = path - 设置将存储主进程的进程ID的nginx.pid文件的名称。 安装后，可以使用pid指令在nginx.conf配置文件中更改文件名。 默认情况下，文件名为：prefix/logs/nginx.pid。
* --error-log-path = path - 设置主错误，警告和诊断文件的名称。 安装后，可以在nginx.conf配置文件中使用error\_log指令更改文件名。 默认情况下，文件名为：prefix/logs/error.log。
* --http-log-path = path - 设置HTTP服务器主要请求日志文件的名称。 安装后，可以使用access\_log指令在nginx.conf配置文件中更改文件名。 默认情况下，文件名为：prefix/logs/access.log。
* --build = name - 设置一个可选的nginx构建名称。
* --user = name - 设置非特权用户的名称，该用户的凭据将由工作进程使用。 安装后，可以使用user指令在nginx.conf配置文件中更改名称。 默认的用户名是：nobody。
* --group = name - 设置由工作进程使用其凭据的组的名称。 安装后，可以使用user指令在nginx.conf配置文件中更改名称。 默认情况下，组名称设置为非特权用户的名称。
* --with-select\_module 和 --without-select\_module — 启用或禁用构建允许服务器使用select()方法的模块。 如果平台似乎不支持更合适的方法(如kqueue，epoll或/dev/poll)，则会自动构建该模块。
* --with-poll\_module 和 --without-poll\_module — 启用或禁用构建允许服务器使用poll()方法的模块。 如果平台似乎不支持更合适的方法(如kqueue，epoll或/dev/poll)，则会自动构建该模块。
* --without-http\_gzip\_module - 禁用构建压缩HTTP服务器响应的模块。 需要zlib库来构建和运行此模块。
* --without-http\_rewrite\_module - 禁用构建一个允许HTTP服务器重定向请求并更改请求URI的模块。 需要PCRE库来构建和运行此模块。
* --without-http\_proxy\_module - 禁用构建HTTP服务器代理模块。
* --with-http\_ssl\_module - 可以构建一个将HTTPS协议支持添加到HTTP服务器的模块。 默认情况下不构建此模块。 OpenSSL库是构建和运行该模块所必需的。
* --with-pcre = path - 设置PCRE库源的路径。库发行版(4.4 - 8.40版)需要从[PCRE站点](http://www.pcre.org/)下载并提取。 其余的由nginx的./configure和make完成。 该库是 location 指令和ngx\_http\_rewrite\_module模块中正则表达式支持所必需的。
* --with-pcre-jit - 使用“即时编译”支持构建PCRE库。
* --with-zlib = path - 设置zlib库的源路径。 库分发(版本1.1.3 - 1.2.11)需要从zlib站点下载并提取。 其余的由nginx的./configure和make完成。 该库是ngx\_http\_gzip\_module模块所必需的。
* --with-cc-opt = parameters - 设置将添加到CFLAGS变量的其他参数。 在FreeBSD下使用系统PCRE库时，应指定--with-cc-opt="-I /usr/local/include"。 如果需要增加select()所支持的文件数，那么也可以在这里指定，如：--with-cc-opt="-D FD\_SETSIZE=2048"。
* --with-ld-opt = parameters - 设置链接过程中使用的其他参数。 当在FreeBSD下使用系统PCRE库时，应指定--with-ld-opt="-L /usr/local/lib"。

原文出自【易百教程】，商业转载请联系作者获得授权，非商业转载请保留原文链接：https://www.yiibai.com/nginx/configure.html#article-start

## 3. 提供静态内容服务(静态网站)

一个重要的Web服务器任务是提供文件(如图像或静态HTML页面)。这里我们来学习如何实现一个示例，根据请求，文件将从不同的本地目录提供：/data/www(可能包含HTML文件)和/ data/images(包含图像)。这将需要编辑配置文件，并使用两个位置块在http块内设置服务器块。

首先，创建/data/www目录，并将一个包含任何文本内容的index.html文件放入其中，并创建/data/images目录并在其中放置一些图像。创建两个目录 -

[root@localhost ~]# mkdir -p /data/www

[root@localhost ~]# mkdir -p /data/images

[root@localhost ~]#

分别在上面创建的两个目录中放入两个文件：/data/www/index.html 和 /data/images/logo.png，/data/www/index.html文件的内容就一行，如下 -

<h2> New Static WebSite Demo.</h2>

接下来，打开配置文件(/usr/local/nginx/conf/nginx.conf)。 默认的配置文件已经包含了服务器块的几个示例，大部分是注释掉的。 现在注释掉所有这样的块，并启动一个新的服务器块：

http {

server {

}

}

通常，配置文件可以包括服务器监听的端口和服务器名称区分的几个server块。当nginx决定哪个服务器处理请求后，它会根据服务器块内部定义的location指令的参数测试请求头中指定的URI。

将以下location块添加到服务器(server)块：

http {

server {

location / {

root /data/www;

}

}

}

该location块指定与请求中的URI相比较的“/”前缀。 对于匹配请求，URI将被添加到root指令中指定的路径(即/data/www)，以形成本地文件系统上所请求文件的路径。 如果有几个匹配的location块，nginx将选择具有最长前缀来匹配location块。 上面的location块提供最短的前缀长度为1，因此只有当所有其他location块不能提供匹配时，才会使用该块。

接下来，添加第二个location块：

http {

server {

location / {

root /data/www;

}

location /images/ {

root /data;

}

}

}

它将是以/images/(位置/也匹配这样的请求，但具有较短前缀，也就是“/images/”比“/”长)的请求来匹配。

server块的最终配置应如下所示：

server {

location / {

root /data/www;

}

location /images/ {

root /data;

}

}

这已经是一个在标准端口80上侦听并且可以在本地机器上访问的服务器( http://localhost/ )的工作配置。 响应以/images/开头的URI的请求，服务器将从/data/images目录发送文件。 例如，响应http://localhost/images/logo.png请求，nginx将发送服务上的/data/images/logo.png文件。 如果文件不存在，nginx将发送一个指示404错误的响应。 不以/images/开头的URI的请求将映射到/data/www目录。 例如，响应http://localhost/about/example.html请求时，nginx将发送/data/www/about/example.html文件。

要应用新配置，如果尚未启动nginx或者通过执行以下命令将重载信号发送到nginx的主进程：

[root@localhost ~]# /usr/local/nginx/sbin/nginx -t

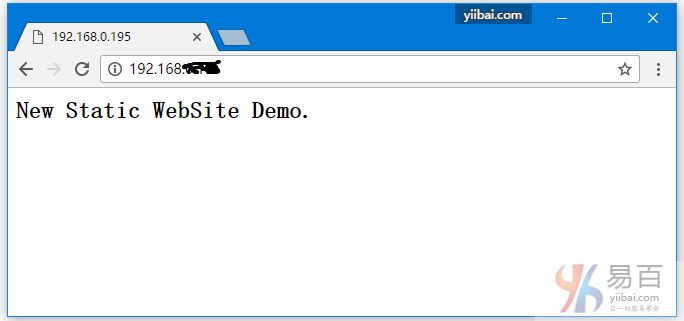
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok

nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful

[root@localhost ~]# /usr/local/nginx/sbin/nginx -s reload

如果错误或异常导致无法正常工作，可以尝试查看目录/usr/local/nginx/logs或/var/log/nginx中的access.log和error.log文件中查找原因。

打开浏览器或使用CURL访问Nginx服务器如下所示 -



完整的nginx.conf文件配置内容如下：

#user nobody;

worker\_processes 1;

#error\_log logs/error.log;

#error\_log logs/error.log notice;

#error\_log logs/error.log info;

#pid logs/nginx.pid;

events {

worker\_connections 1024;

}

http {

include mime.types;

default\_type application/octet-stream;

#log\_format main '$remote\_addr - $remote\_user [$time\_local] "$request" '

# '$status $body\_bytes\_sent "$http\_referer" '

# '"$http\_user\_agent" "$http\_x\_forwarded\_for"';

#access\_log logs/access.log main;

sendfile on;

#tcp\_nopush on;

#keepalive\_timeout 0;

keepalive\_timeout 65;

#gzip on;

## 新服务(静态网站)

server {

location / {

root /data/www;

}

location /images/ {

root /data;

}

}

}

## 4. 设置简单的代理服务器

nginx的一个常见用途是将其设置为代理服务器，这意味着它可作为一个接收请求的服务器，将其传递给代理服务器，从代理服务器中检索响应，并将其发送给客户端。

我们将配置一个基本的代理服务器，它为来自本地目录的文件提供图像请求，并将所有其他请求发送到代理的服务器。 在此示例中，两个服务器将在单个nginx实例上定义。

首先，通过向nginx配置文件添加一个server块来定义代理服务器，其中包含以下内容：

server {

listen 8080;

root /data/up1;

location / {

}

}

这将是一个监听端口8080的简单服务器(以前，由于使用了标准端口80，所以没有指定listen指令)，并将所有请求映射到本地文件系统上的/data/up1目录。 创建此目录并将index.html文件放入其中。 请注意，root指令位于server块上下文中。 当选择用于服务请求的location块不包含自己的root指令时，将使用此root指令。

在上面创建的目录/data/up1中放入一个文件：/data/www/demo.html，文件的内容就一行，如下 -

<h2>About proxy\_pass Page at port 8080</h2>

接下来，使用上一节中的服务器配置进行修改，使其成为代理服务器配置。 在第一个位置块中，将proxy\_pass指令与参数中指定的代理服务器的协议，名称和端口(在本例中为http://localhost:8080)：

server {

location / {

proxy\_pass http://localhost:8080;

}

location /images/ {

root /data;

}

}

我们将修改当前使用/images/prefix将请求映射到/data/images目录下的文件的第二个location块，使其与典型文件扩展名的图像请求相匹配。 修改后的位置块如下所示：

location ~ \.(gif|jpg|png)$ {

root /data/images;

}

该参数是一个正则表达式，匹配所有以.gif，.jpg或.png结尾的URI。正则表达式之前应该是~字符。 相应的请求将映射到/data/images目录。

当nginx选择一个location块来提供请求时，它首先检查指定前缀的location指令，记住具有最长前缀的location，然后检查正则表达式。 如果与正则表达式匹配，nginx会选择此location，否则选择之前记住的那一个。

代理服务器的最终配置将如下所示：

server {

location / {

proxy\_pass http://localhost:8080/;

}

location ~ \.(gif|jpg|png)$ {

root /data/images;

}

}

此服务器将过滤以.gif，.jpg或.png结尾的请求，并将它们映射到/data/images目录(通过向root指令的参数添加URI)，并将所有其他请求传递到上面配置的代理服务器。

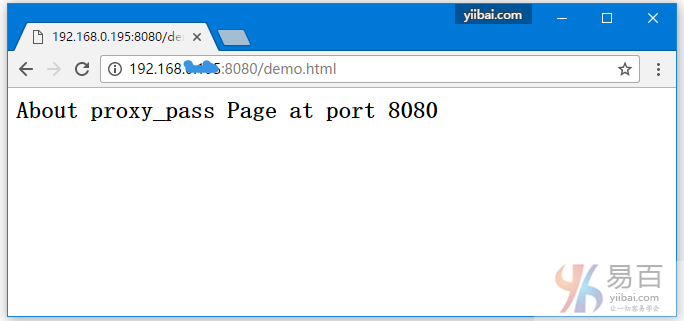
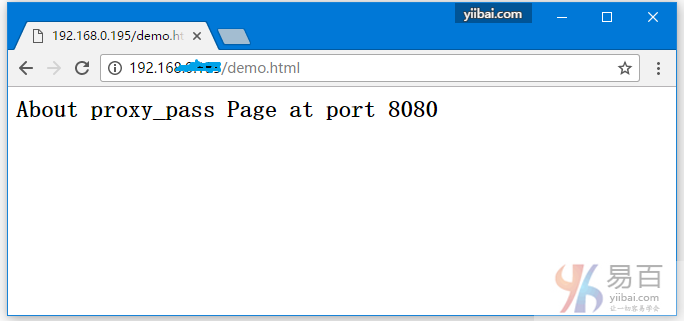
要应用新配置，如果尚未启动nginx或者通过执行以下命令将重载信号发送到nginx的主进程：

[root@localhost ~]# /usr/local/nginx/sbin/nginx -t

nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok

nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful

[root@localhost ~]# /usr/local/nginx/sbin/nginx -s reload

首先测试上面配置的 8080 端口的服务，访问服务的8080端口，得到以下结果：  
  
再次访问 80 端口(这里只是一个代理，它会把请求转发给8080的服务，由8080端口这这个服务处理并返回结果到客户端)，得到以下结果 -  


完整的配置nginx.conf文件内容如下 -

#user nobody;

worker\_processes 1;

#error\_log logs/error.log;

#error\_log logs/error.log notice;

#error\_log logs/error.log info;

#pid logs/nginx.pid;

events {

worker\_connections 1024;

}

http {

include mime.types;

default\_type application/octet-stream;

#log\_format main '$remote\_addr - $remote\_user [$time\_local] "$request" '

# '$status $body\_bytes\_sent "$http\_referer" '

# '"$http\_user\_agent" "$http\_x\_forwarded\_for"';

#access\_log logs/access.log main;

sendfile on;

#tcp\_nopush on;

#keepalive\_timeout 0;

keepalive\_timeout 65;

#gzip on;

## 新服务(服务处理)

server {

listen 8080;

root /data/up1;

location / {

}

}

## 代理配置，数据转发

server {

location / {

proxy\_pass http://localhost:8080/;

}

location ~ \.(gif|jpg|png)$ {

root /data/images;

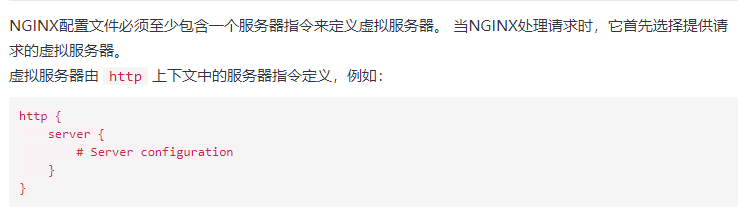
}

}

}



## 设置虚拟服务器



server配置块通常包括一个listen指令，用于指定服务器侦听请求的IP地址和端口(或Unix域套接字和路径)。IPv4和IPv6地址均被接受; 将方括号(。  
下面的示例显示了监听IP地址127.0.0.1和端口8080的服务器的配置：

server {

listen 127.0.0.1:8080;

# The rest of server configuration

}

如果省略端口，则使用标准端口。 同样地，如果省略一个地址，服务器将侦听所有地址。 如果没有包含listen指令，则“标准”端口为80/tcp，“default”端口为8000/tcp，具体取决于超级用户权限。

如果有多个服务器与请求的IP地址和端口相匹配，则NGINX将根据服务器块中的server\_name指令测试请求的主机头域。 server\_name的参数可以是完整(精确)名称，通配符或正则表达式。 通配符是一个字符串，其开头，结尾或两者都包含星号(\*); 星号匹配任何字符序列。 NGINX将Perl语法用于正则表达式; 在它们之前使用波浪号(〜)。 此示例说明了一个确切的名称。

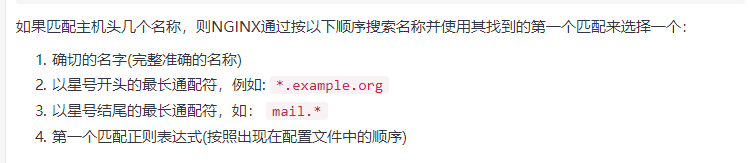
server {

listen 80;

server\_name example.org www.example.org;

...

}



## 2. 配置位置

## 

## 

