# 

# 

# **Assessment**

# **Nginx**

Trainee Name : Aditya Upadhyay

Newers ID : 3978

Mentor Name : Tarun Saxena

College : UPES

1. What is the advantage of using a “reverse proxy server”?

A reverse proxy is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers. Reverse proxies are typically implemented to help increase securiity, performance, and reliability.

A popular website that gets millions of users every day may not be able to handle all of its incoming site traffic with a single origin server. Instead, the site can be distributed among a pool of different servers, all handling requests for the same site. In this case, a reverse proxy can provide a load balancing solution which will distribute the incoming traffic evenly among the different servers to prevent any single server from becoming overloaded.

With a reverse proxy in place, a web site or service never needs to reveal the IP address of their origin server(s). This makes it much harder for attackers to leverage a targeted attack against them, such as a DDoS attack.

1. Why and where Nginx is a better choice than apache.

Nginx is faster than apache. Nginx can support many concurrent accesses. Nginx has features like reverse proxy and load balancer built in. Nginx is lightweight, event driven and asynchronous.

1. What are worker nodes and worker connections? How to calculate the max server capacity using the above two?

​ Worker nodes:​ defines the number of worker processes nginx is running. Default value is number of processor in the system

Worker\_connection:​ specifies the maximum number of connections that a single worker can have open at one time.

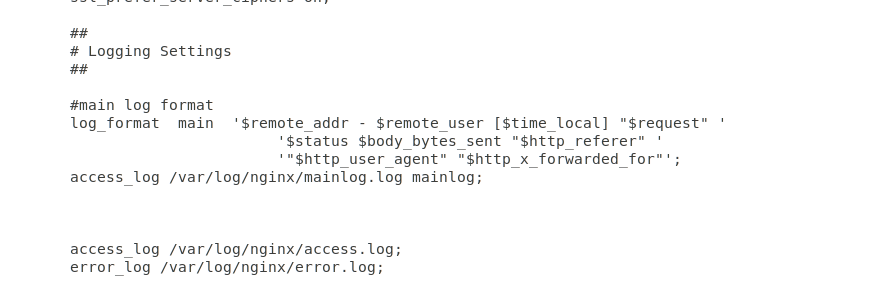
To check number of worker nodes:- grep processor /proc/cpuinfo | wc -l

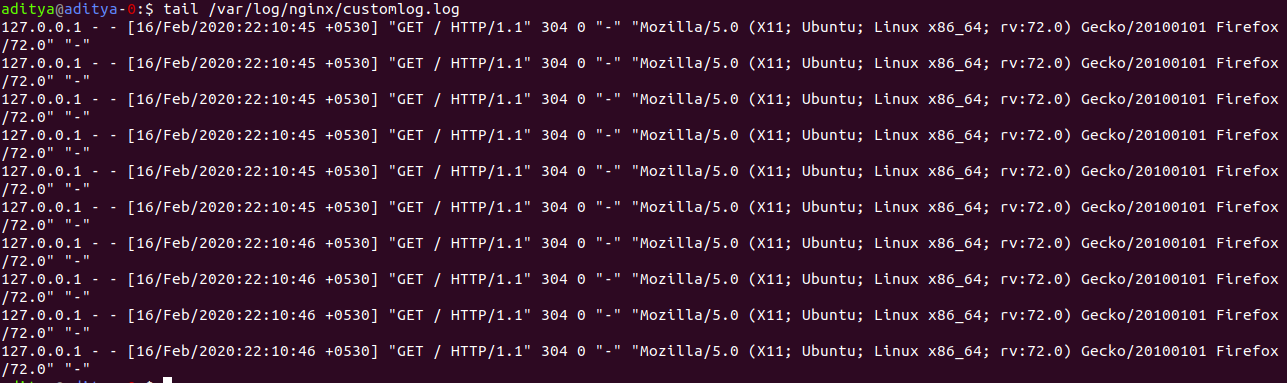
Maximum number of connections = worker\_processes \* worker\_connections

1. From what directory will NGINX automatically load server (virtual host) configurations when using the default /etc/nginx/nginx.conf configuration?

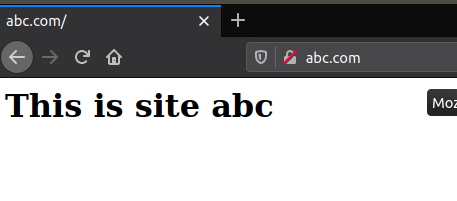
/etc/nginx/conf.d/\*.conf . Nginx will load all .conf files inside conf.d directory.

1. How to configure different log\_format for different “location” block/directive?

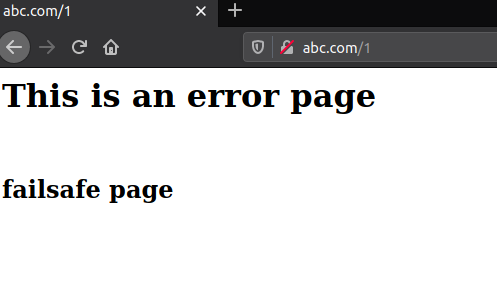


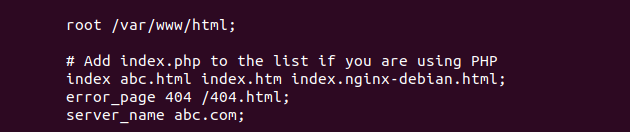


1. Host a site ABC.COM

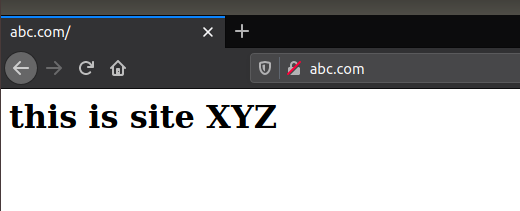


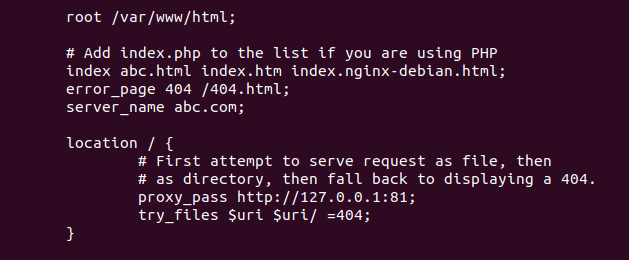
* 1. Create an index page and a fail-safe page. If a page for URI is not available, the fail-safe page is served.

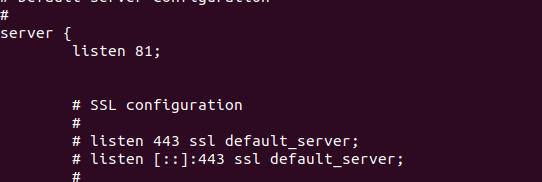




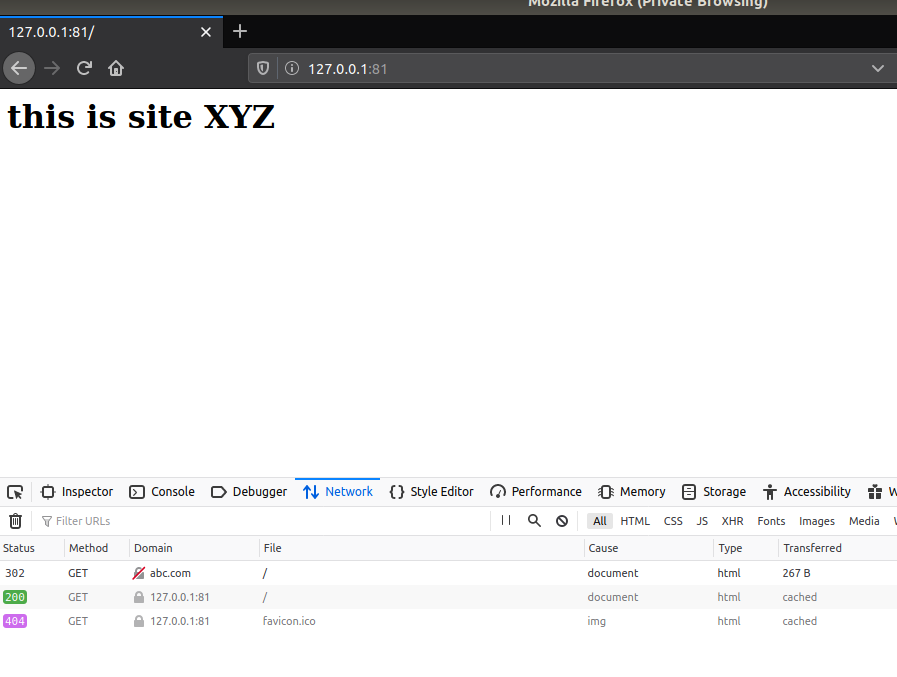
* 1. proxy pass to a website xyz.com on a particular URI.



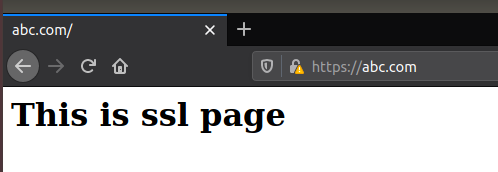


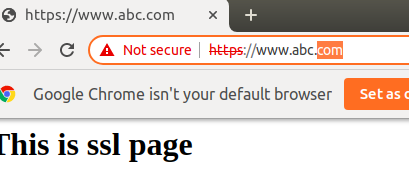


* 1. redirect to above URI on /redirect/



* 1. perform an HTTP to HTTPS redirection including non-www to www redirection.

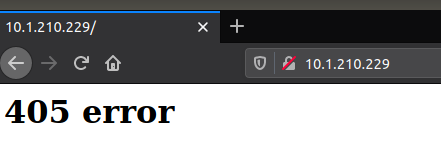


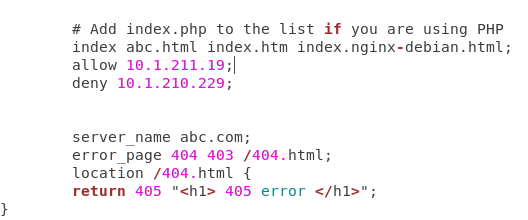


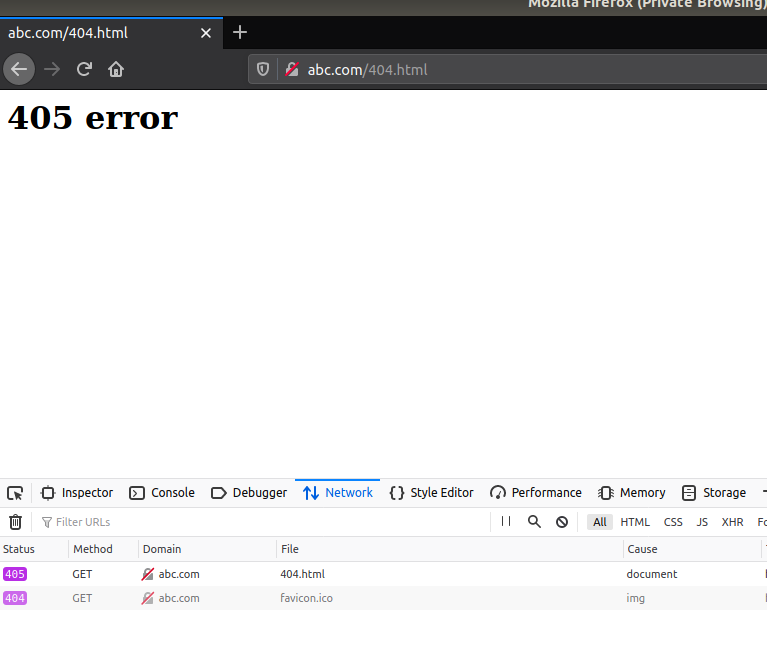




* 1. Allow access to a set of particular IPs on a location block and return 405 to other IPs no matter if the page in that location exists.

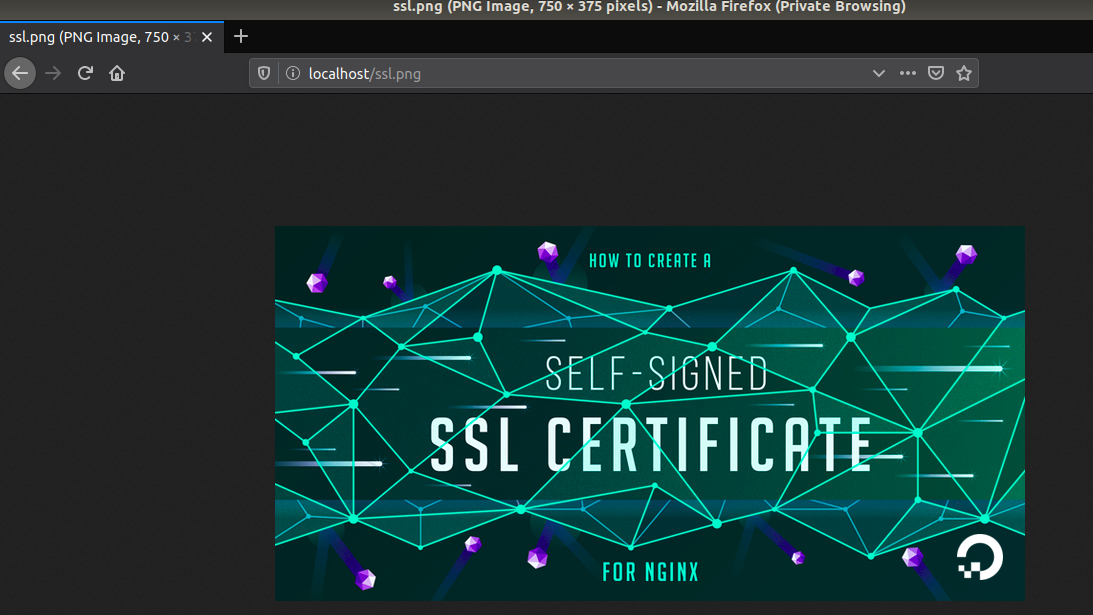


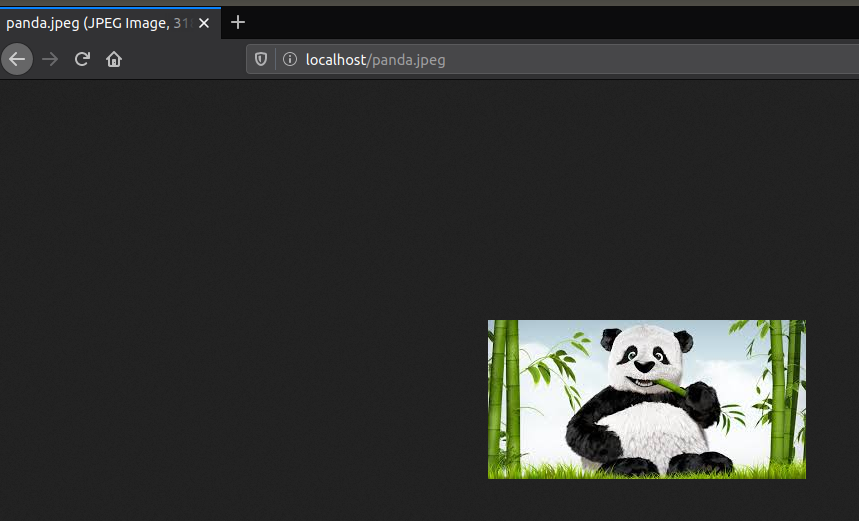


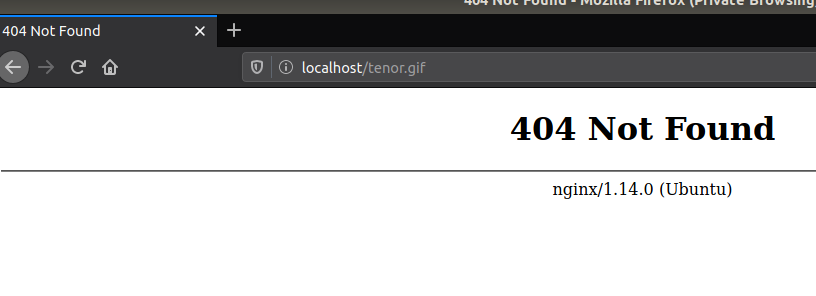


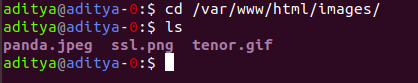
* 1. Place your images at /var/www/html/images. Only accept jpg/png/jpeg. Discard rest



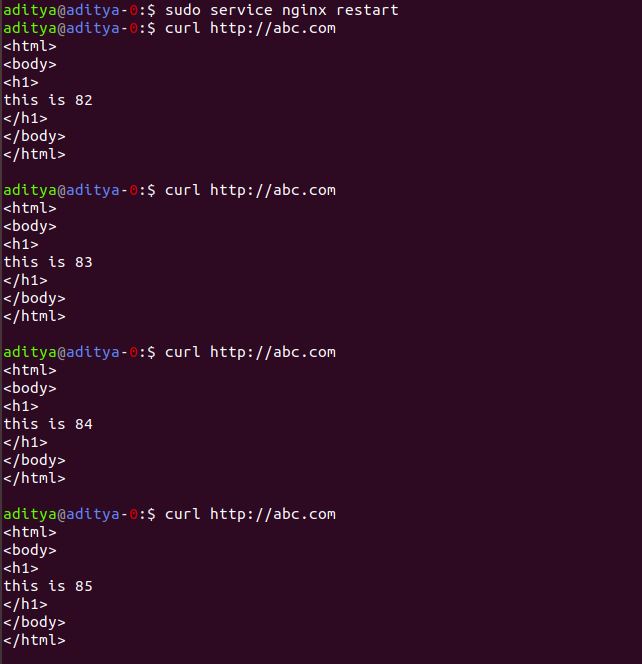








1. Create a load balancer with 5 backends. Explain different types of load balancing methods.



Types of load balancing:

a. Round Robin (Default method)

b. Least Connection:

upstream backend {

least\_conn;

server backend1.example.com;

server backend2.example.com;

}

c. IP Hash:

upstream backend {

ip\_hash;

server backend1.example.com;server backend2.example.com;

}

d. Least Time:

upstream backend {

least\_time header;

server backend1.example.com;

server backend2.example.com;

}

1. Setup Basic Auth (Popup asking for username and password) in a particular location block. (The Basic Auth should not be asked for TTN IP)

