SSL/TLS - Certificates

OpenSSL

Generate self-signed certificates

```
root@vagrant:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx.key
 -out /etc/ssl/certs/nginx.crt
Generating a 2048 bit RSA private key
.....................................................+++
......+++
writing new private key to '/etc/ssl/private/nginx.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

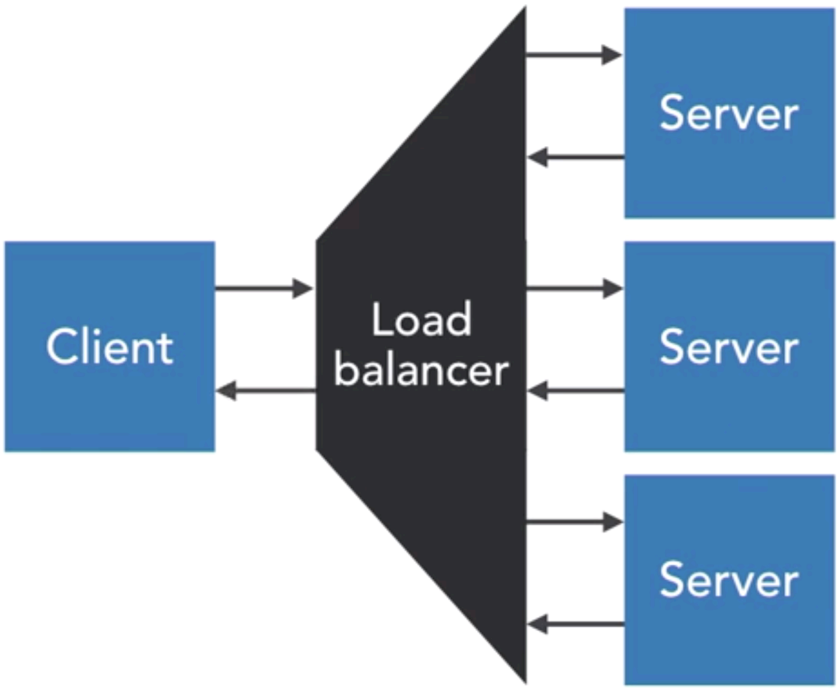
- Use option "-bath" option to above command to avoid prompts.

Reverse Proxy

- Good-case where Requests are served by ONE Webserver on the BackEnd and LoadBalancer is not required in those scenarios.
- **NGINX - Proxy benefits**
  - SSL termination
  - Caching back-end content
-

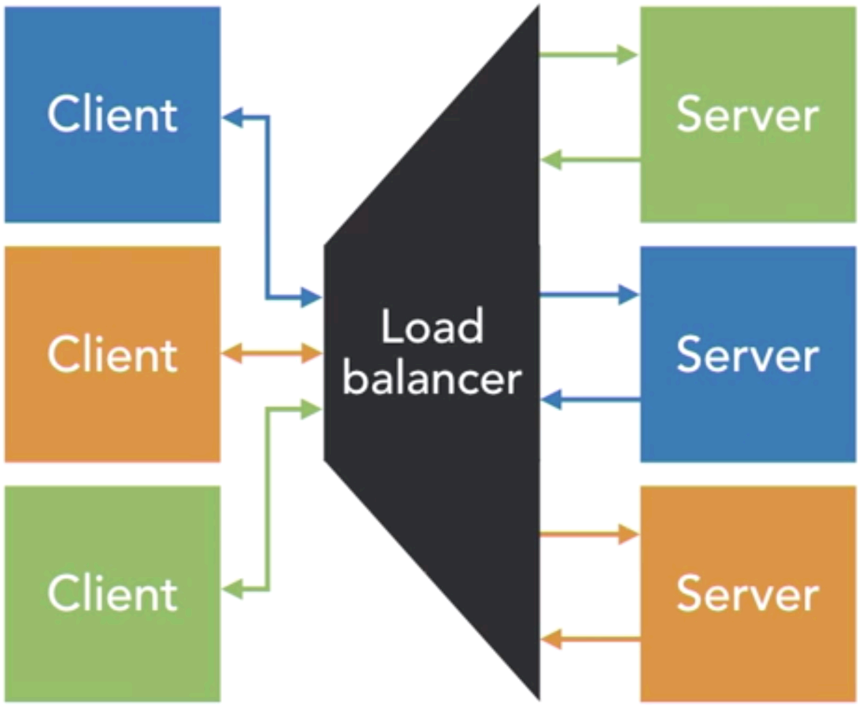
Load Balancers

Load Balancer



Benefits: Session-Persistance

Load Balancer



Load Balancing Directives

Method	Directive	Application
Round Robin	—	Upstream servers connected one at a time
Least Connections	`least_conn`	The upstream server with the fewest connections is favored
IP Hash	`ip_hash`	Connection is made based on the client's IP address
(All)	`weight`	Upstream server with higher weight is favored