GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Nginx Seguro

CONFIGURAÇÃO E PROTEÇÃO DE SERVIÇOS WEB

Abertura

Glaucio Guerra
CTO - MarkWay
glaucio@guerra.academy

- **Desenvolvimento**
- **Infraestrutura (DataCenter / Cloud)**
- **Arquitetura**
- **DevOps**
- **Consultoria especializada**
- **Educação**

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA
https://guerra.academy

Mark Way
https://www.markway.com.br

www.linkedin.com/in/glaucioguerra/

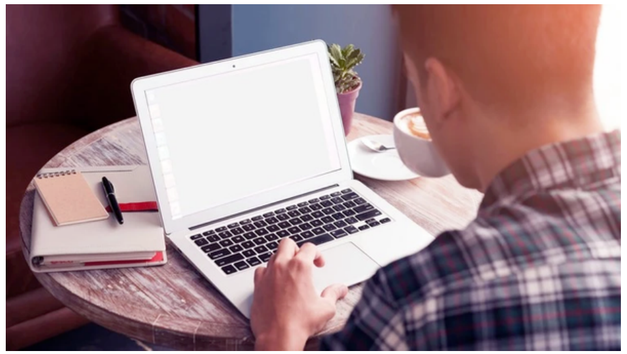
Abertura

- Indicado para iniciantes e profissionais experientes em servidores Web que desejam aprender sobre configuração e otimização do NGINX.
- Compartilha as melhores práticas de mercado relacionadas ao NGINX.
- O livro aborda as funcionalidades do NGINX, oferecendo informações sobre configuração, otimização e segurança.

Versão Impressa: https://amzn.to/48kvGaS **Versão Digital: https://amzn.to/3sNwrZI**

Abertura

Apache Web Server



http://bit.ly/apache-webserver

DevOps - Mão na Massa

https://bit.ly/devops-mao-massa

Go - DevOps & SREs

https://bit.ly/programacao-go-devops

Abertura

- DevOps
- SRE
- Arquitetura
- Podcasts
- Perguntas x Respostas
- Dicas
- Promoções e sorteios de cursos

Primeiros Passos

Introdução

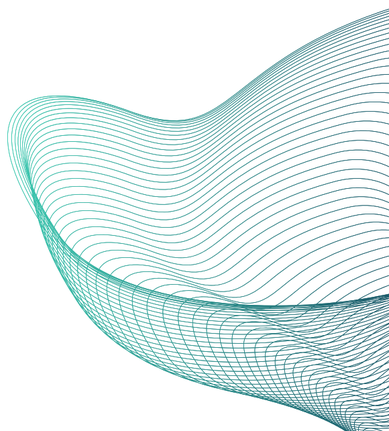
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Introdução

- Nginx, criado por Igor Sysoev em 2002, é um servidor web de código aberto.
- Destacou-se por lidar com muitas conexões simultâneas com baixo uso de recursos.
- Lançado oficialmente como projeto de código aberto em 2004.
- Ganhou popularidade como servidor web de alto desempenho e proxy reverso.
- Em 2011, a empresa Nginx Inc. foi criada para desenvolver soluções, incluindo o Nginx Plus, uma versão comercial com suporte.

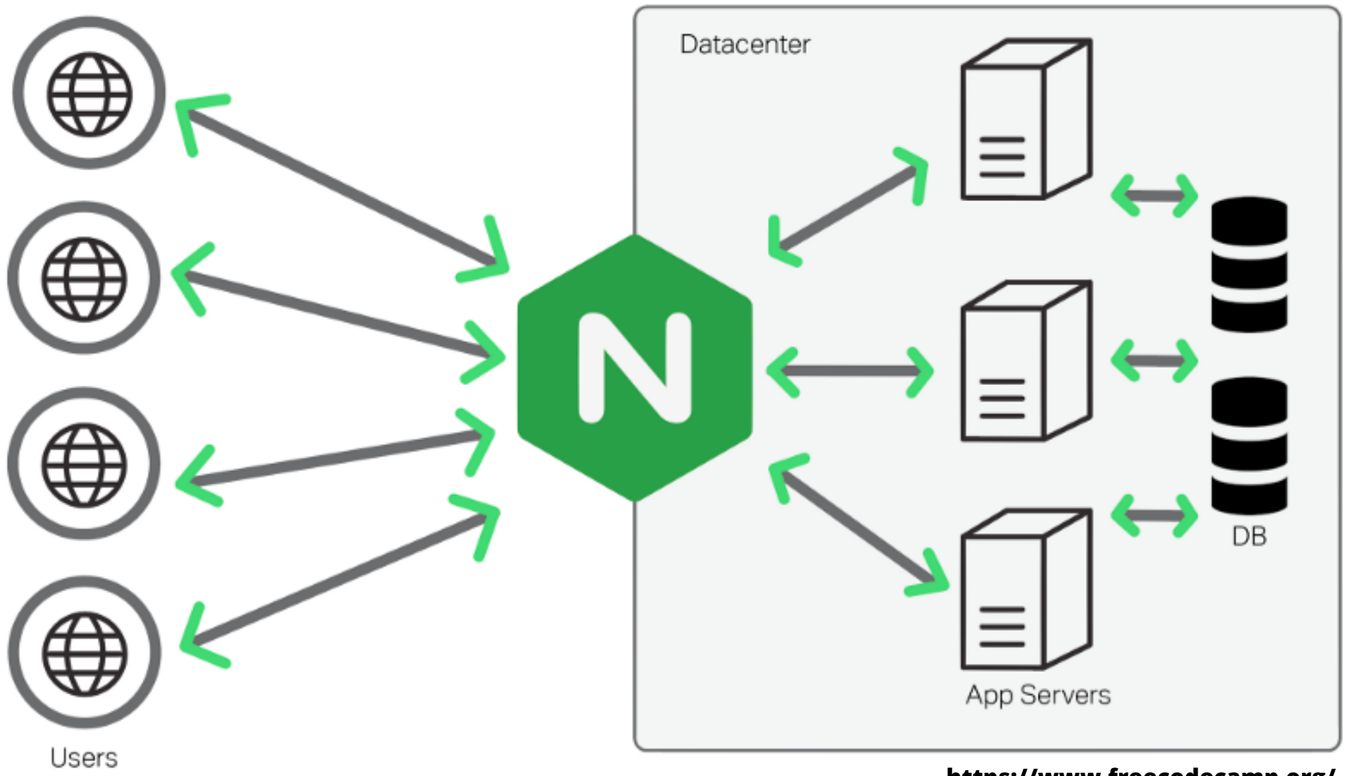
Introdução

Quem utiliza?



Introdução

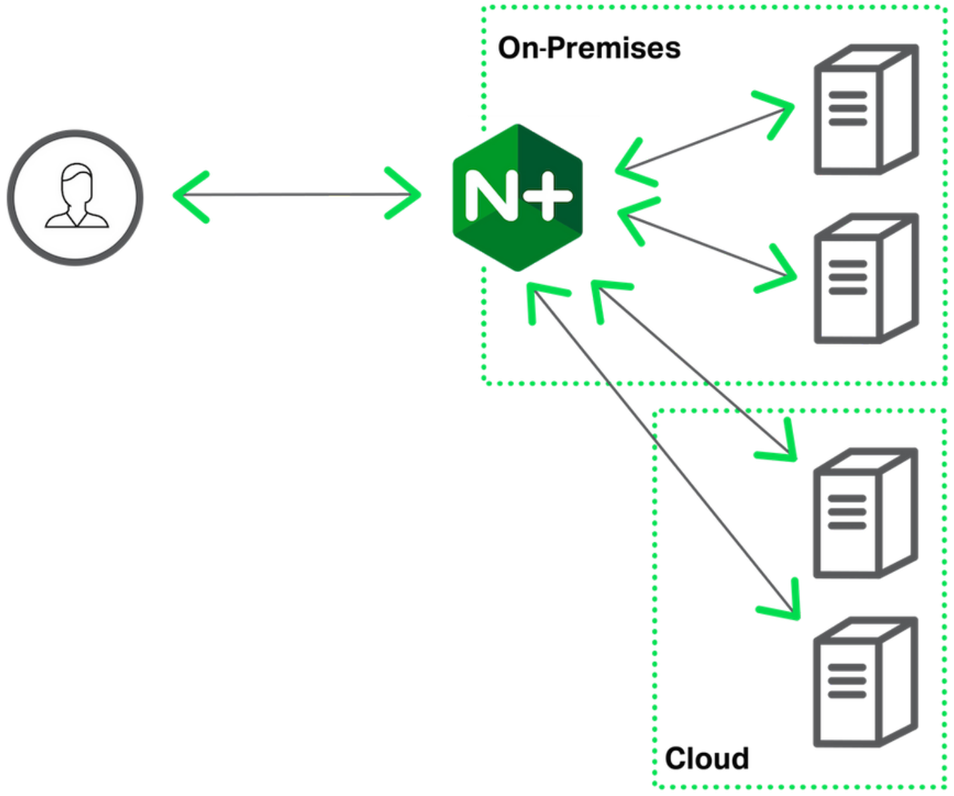
Funcionamento



https://www.freecodecamp.org/

Introdução

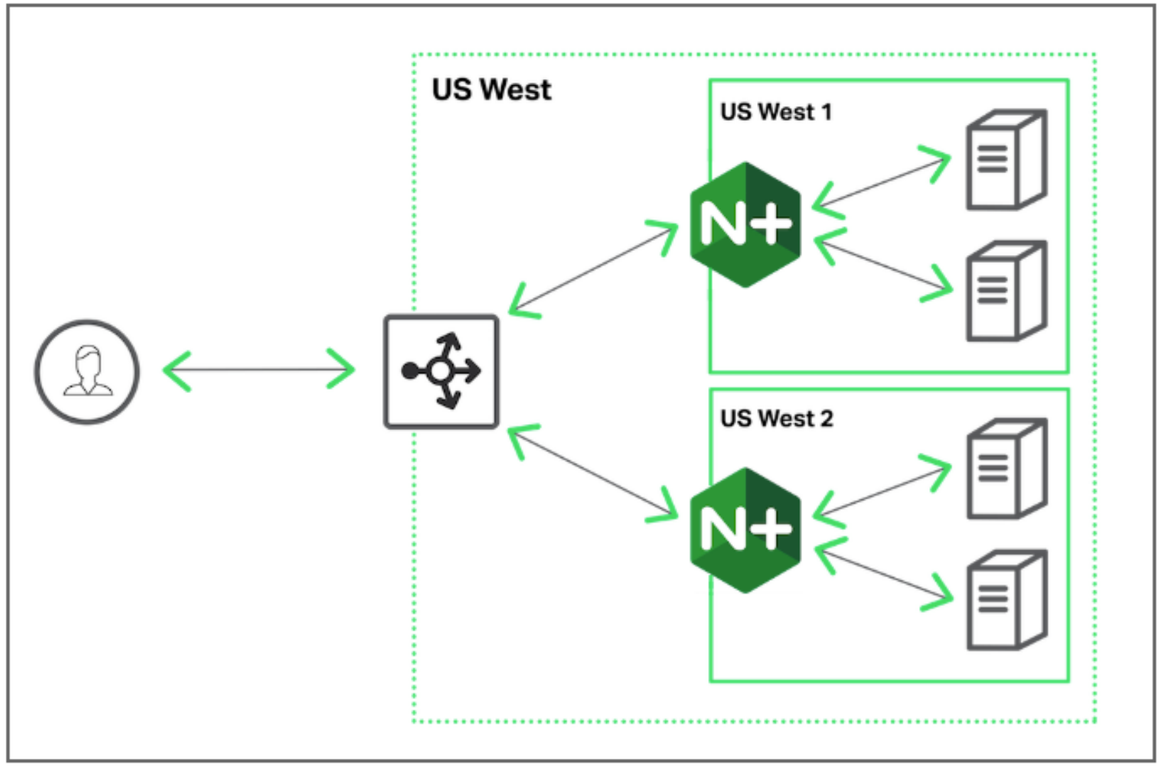
Arquitetura Híbrida



https://www.nginx.com

Introdução

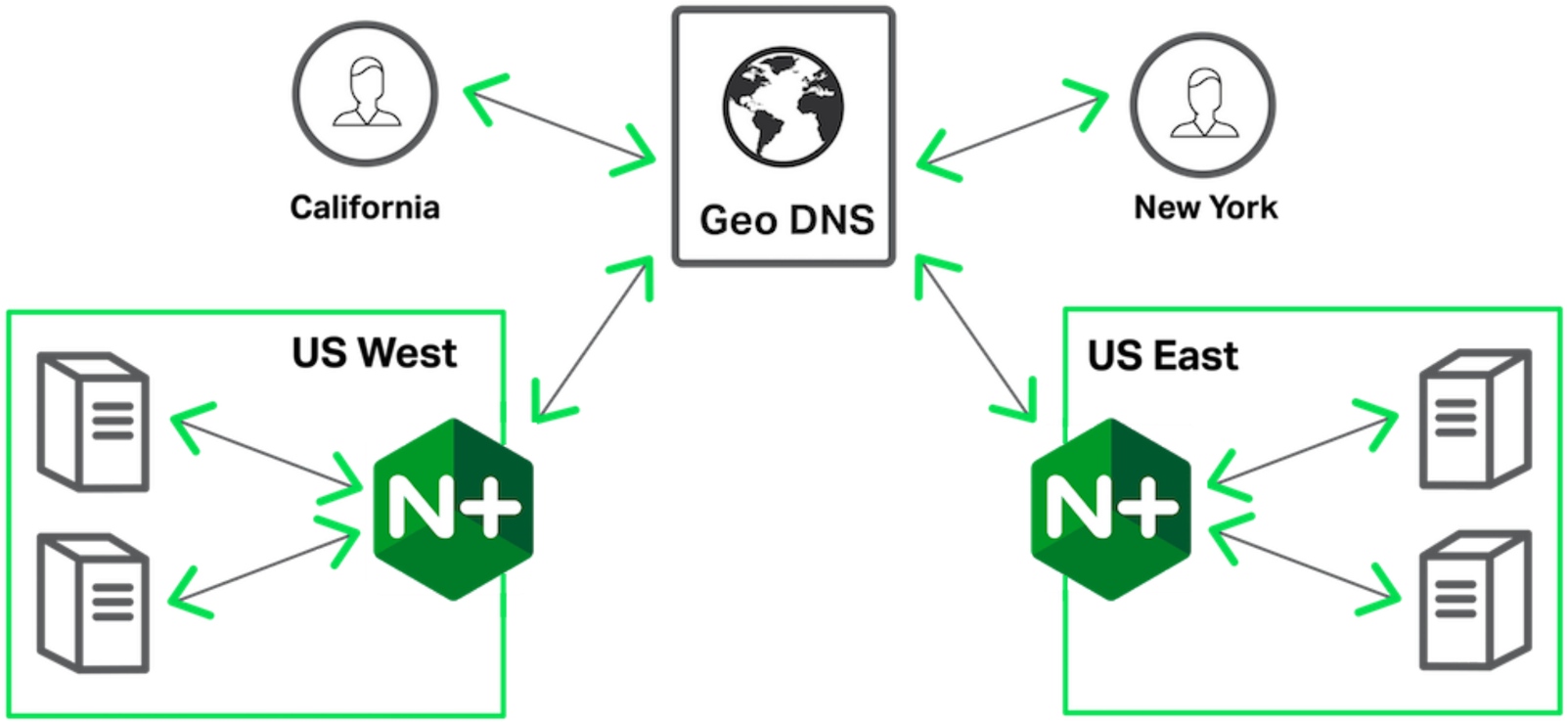
HA - Multi Zones



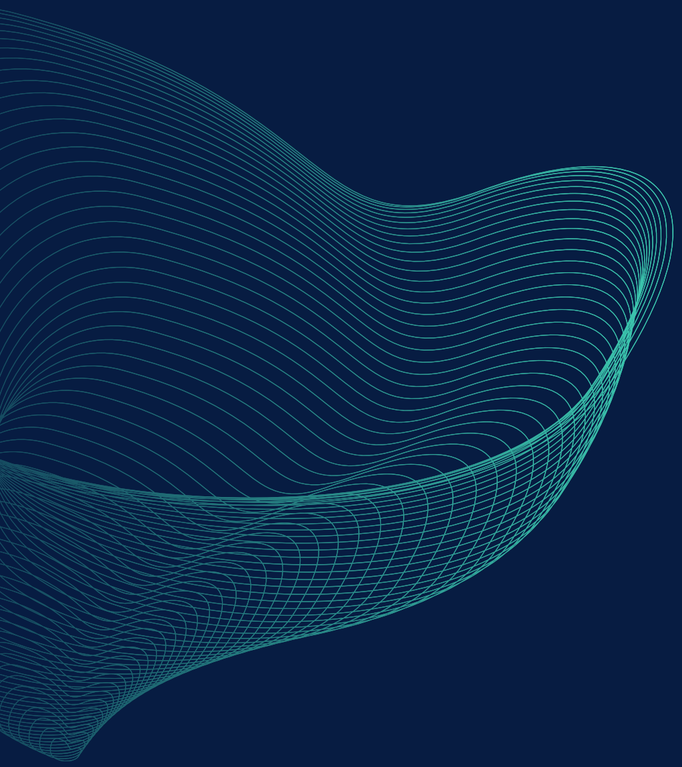
https://www.nginx.com

Introdução

Global Load Balance



https://www.nginx.com



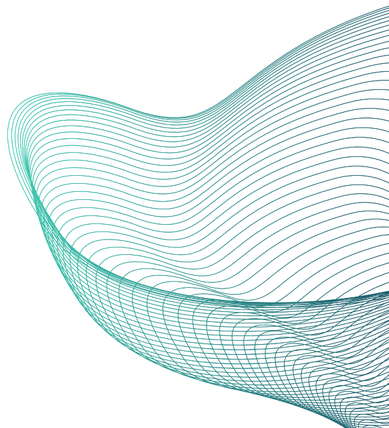
Primeiros Passos

Instalação do Nginx

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

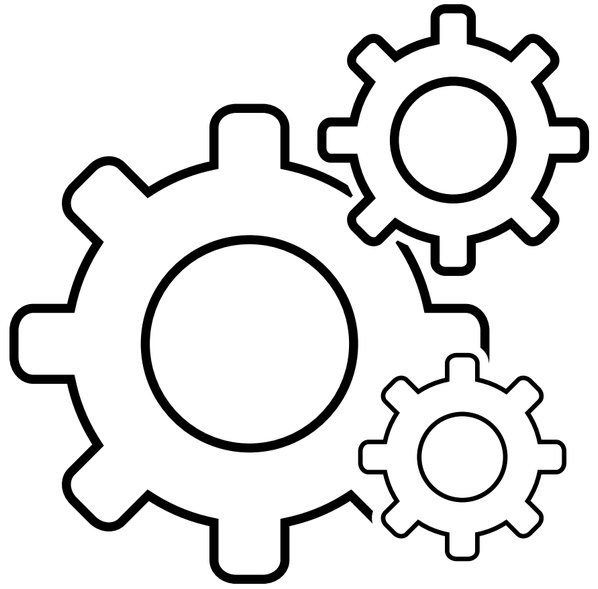
Instalação

- Servidor Ubuntu 20.4
- Acesso a Internet
- 1G de RAM
- 20G Disco
- 2VCPUs



Instalação

- Atualização do S.O
- Instalação do git
- Configuração do repo Nginx
- Instalação do Nginx
- Configuração do primeiro virtual host

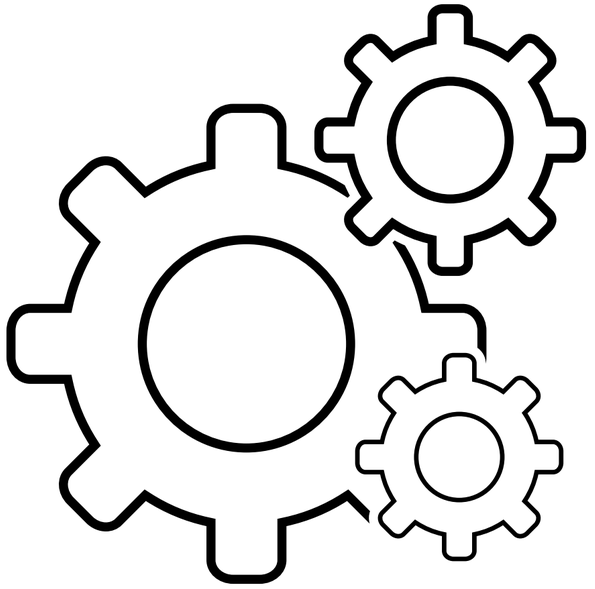


GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Instalação

Atualização do S.O

- sudo apt update && sudo apt upgrade -y
- sudo apt autoremove



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Instalação

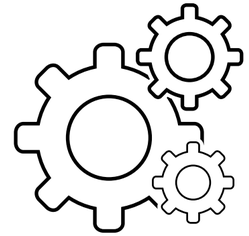
Instalação do Git

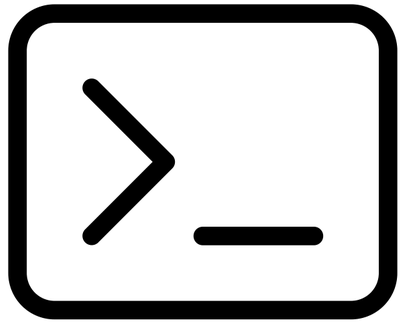
- sudo apt install git
- git --version

https://github.com/glaucioguerra/nginx-descomplicado

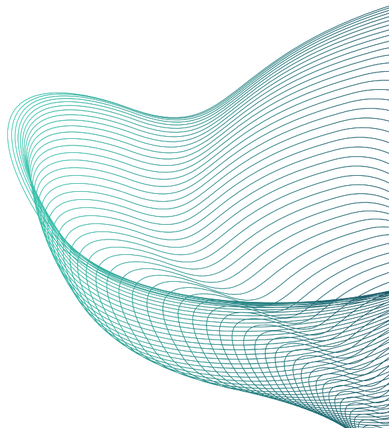
Instalação

Instalação Nginx





Hora do Hands On



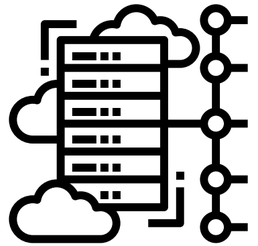
Primeiros Passos

Configuração de Virtual Server

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Virtual Server

Para que serve?



- Permite que um único servidor web hospede vários sites diferentes em um único servidor físico.

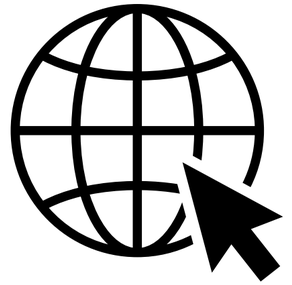
- Cada site pode ter sua própria configuração e comportamento independentes.

- Mesmo compartilhando recursos do servidor, os virtual hosts direcionam solicitações para o site correto com base no nome de domínio

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Virtual Server

- Criar um arquivo de configuração extensão .conf



- Criar diretório de hospedagem dos arquivos estáticos

- Download da aplicação:
  - https://github.com/glaucioguerra/nginx-descomplicado/tree/main/capitulo1/OnePage
  - https://guerra.academy/nicbr/onepage.tar.gz

- Simular criação de um nome de DNS válido (/etc/hosts)

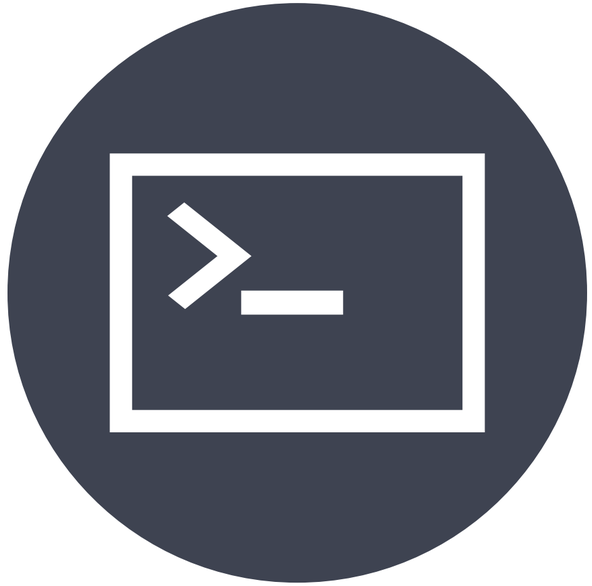
Virtual Server

```
server {
  listen 80;
  server_name meusite.com;
  root /var/www/meusite.com;
  index index.html;
  location / {
     try_files $uri $uri/ = 404;
  }
```

Virtual Server

Comandos básicos:

- nginx -t
- service nginx reload
- service nginx start
- service nginx restart
- git clone

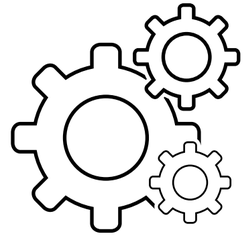


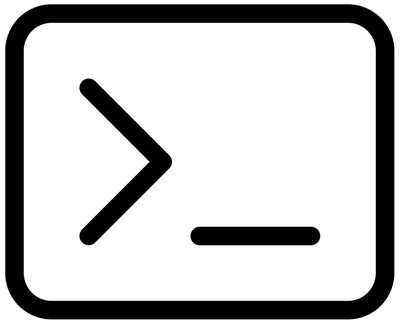
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Virtual Server

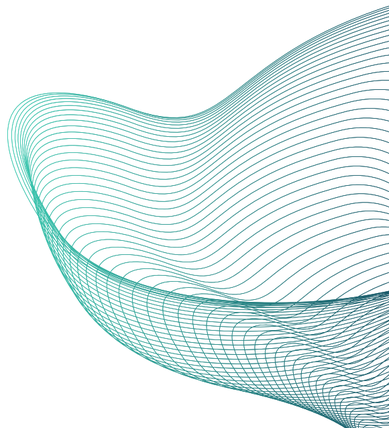
Erros comuns:

Virtual Server





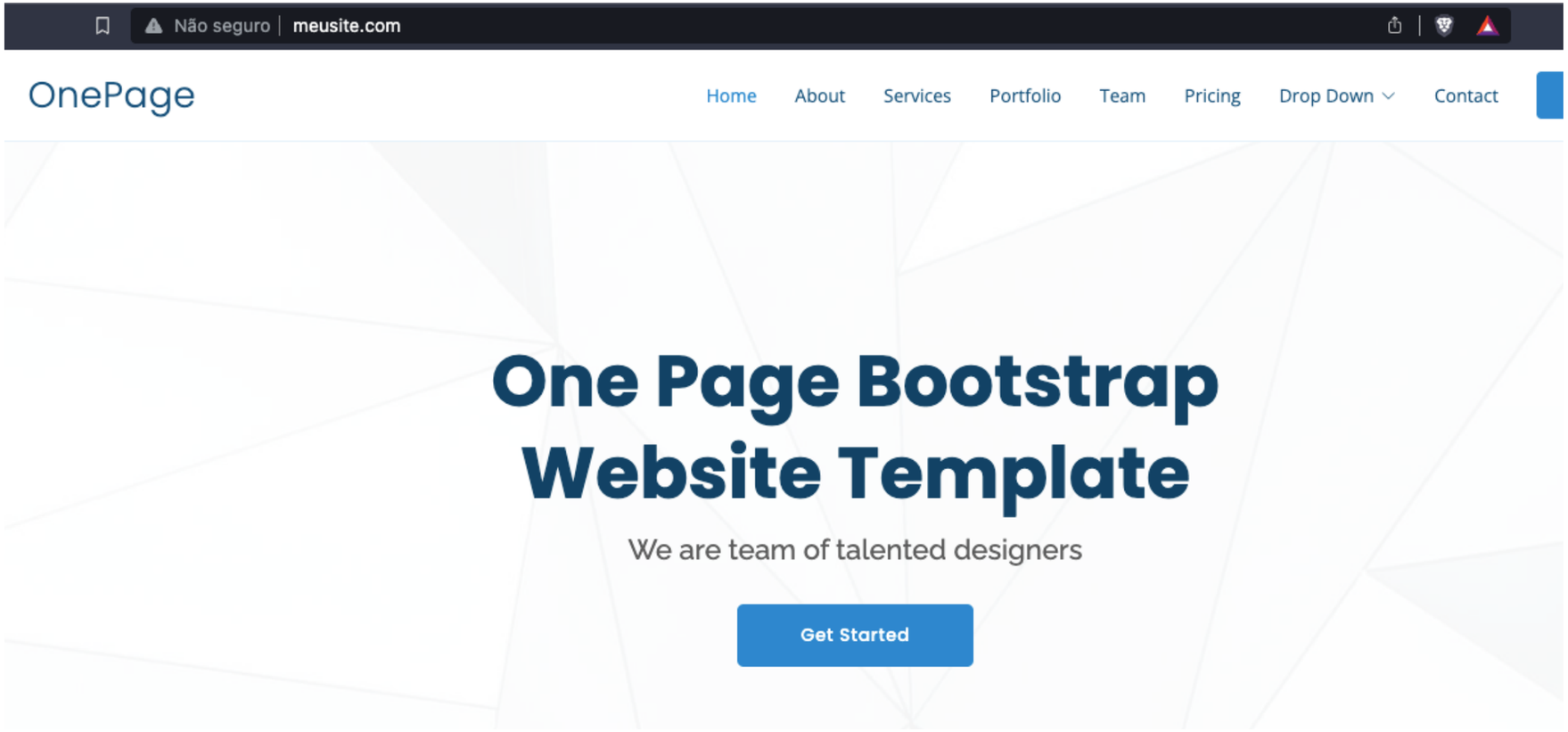
Hora do Hands On



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Virtual Server

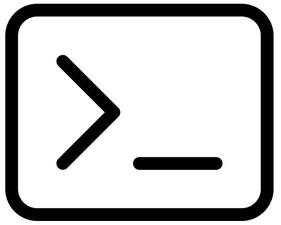
http://meusite.com



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

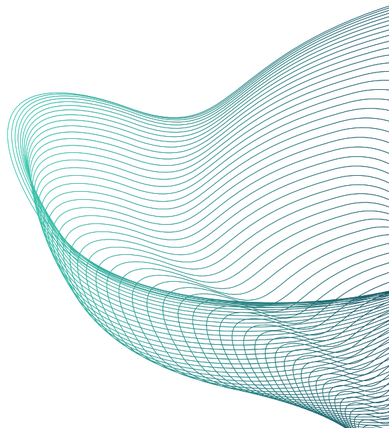
Dica rápida

Criação de alias

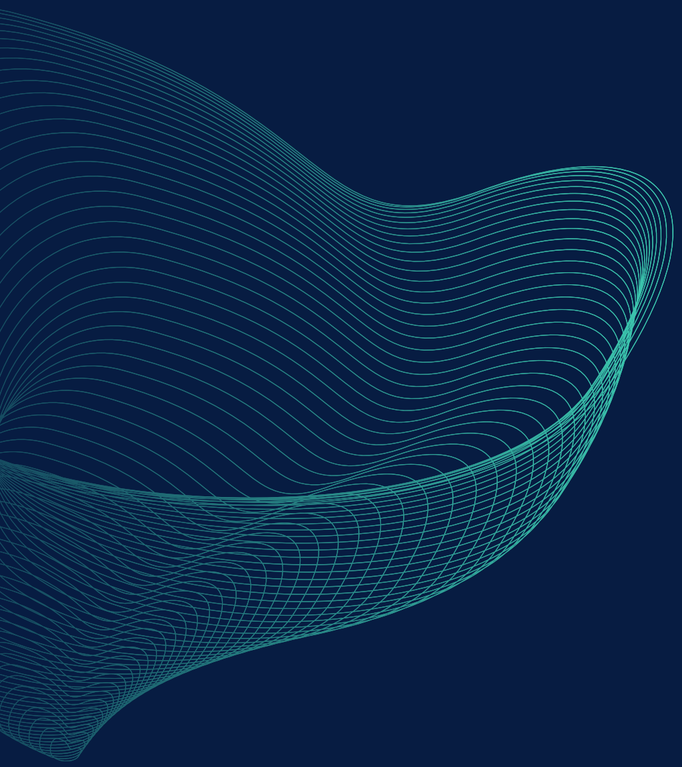


- **Editar ~/.bashrc**

- Adicionar alias: ntr (nginx test e reload)
  - echo "alias seu_alias='nginx -t && service nginx reload'" >> ~/.bashrc



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

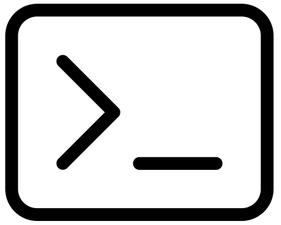


Primeiros Passos

Estrutura de diretórios e arquivos

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Estrutura de diretórios e arquivos



- **/etc/nginx:**
  - Diretório principal de configuração do produto
  - Configurações globais
- **/etc/nginx/conf.d:**
  - Configuração virtual hosts
- **/usr/share/nginx:**
  - Arquivos estáticos
- **/var/log/nginx:**
  - Arquivos de acesso e erros do web server.

Estrutura de diretórios e arquivos

/etc/nginx/nginx.conf:

```
user  nginx;
#qtd de workers (CPU)
worker_processes  auto;
error_log  /var/log/nginx/error.log notice;
pid        /var/run/nginx.pid;
events {
    #n. máximo de conexões por worker
    worker_connections  1024;
}
```

```
http {
    #tabela DE X PARA de tipos de arquivos
    include       /etc/nginx/mime.types;
    #type default caso não seja encontrado no 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  /var/log/nginx/access.log  main;

# cópia direta de um file descriptor para outro
    sendfile        on;
#Envia http response header em um pacote somente (precisa do sendfile)
    #tcp_nopush     on;
# tempo que a conexão se mantém aberta com o client.
    keepalive_timeout  65;

# Compactação de requests
    #gzip  on;
# inclusão de arquivos de configuração (virtual hosts)
    include /etc/nginx/conf.d/*.conf;
}
```

Tópicos avançados

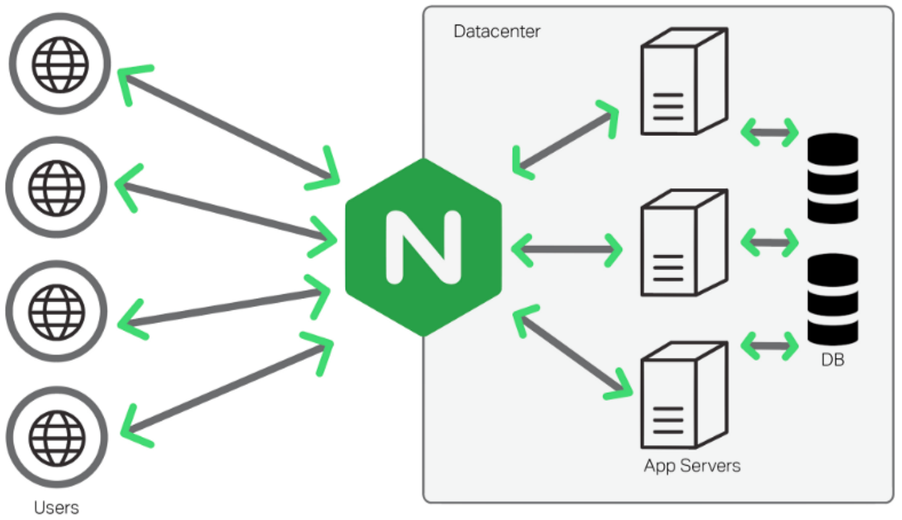
Balanceamento de carga

GUERRA ACADEMY

CRIANDO EXPERTISE EM TECNOLOGIA

Balanceamento de carga

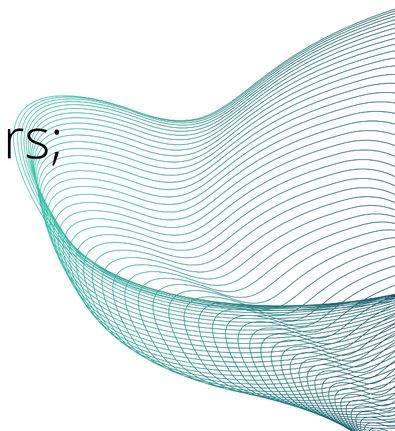
- Distribuição de carga por diversos servidores
- Melhorar Desempenho e escalabilidade
- Caso de uso:
  - Balanceamento entre dois servidores NodeJs
  - Instalação do NodeJs e npm



Balanceamento de carga

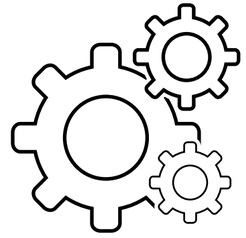
- Instalação do NodeJs
- Configuração de duas apps
- Configuração do balance no Nginx

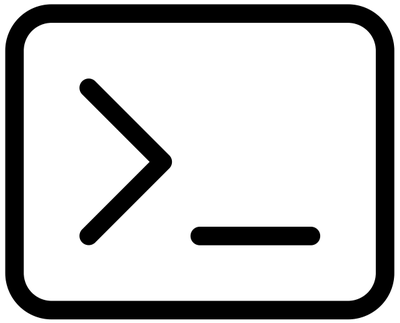
```
upstream node-servers {
    server localhost:3000; # servidor A
    server localhost:3001; # servidor B
}

server {
    listen 80;
    server_name meu-app.com;

    location / {
        proxy_pass http://node-servers;
    }
}
```



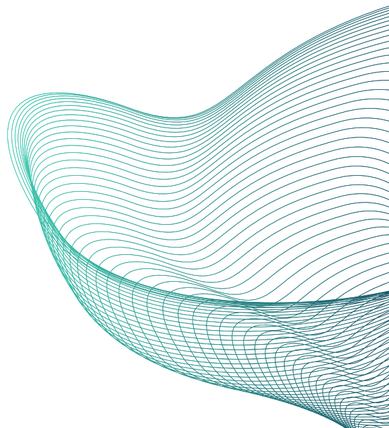
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Balanceamento de carga





Hora do Hands On



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Segurança

Certificado SSL com Let's Encrypt

GUERRA ACADEMY

CRIANDO EXPERTISE EM TECNOLOGIA

SSL com Let's Encrypt

- Tornar a criptografia de sites e aplicativos web mais acessível e fácil de implementar
- O Let’s Encrypt é uma autoridade de certificação (ou CA - Certificate Authority) gratuita
- Os certificados SSL/TLS são uma forma de criptografar a comunicação entre um servidor web e o navegador do usuário
- O certificado emitido pela Let’s Encrypt tem validade de apenas 90 dias, diferentemente do padrão utilizado pelo mercado

SSL com Let's Encrypt

- Certbot:
  - CLI desenvolvido pelo Let’s Encrypt que facilita o processo de obtenção, renovação e gerenciamento de certificados SSL/TLS gratuitos

- Fácil utilização

- Automação no processo de obter e renovar certificado

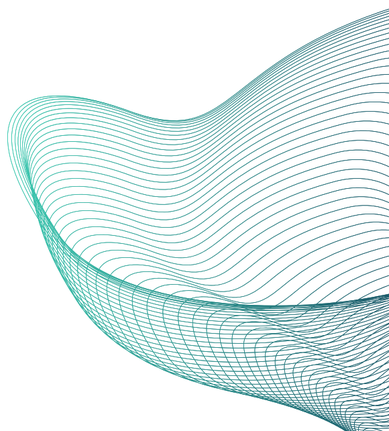
- Gratuito

SSL com Let's Encrypt

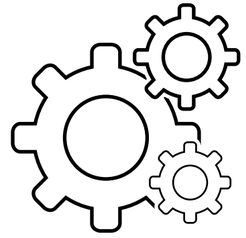
- Domínio válido
- sudo snap install --classic certbot
- sudo ln -s /snap/bin/certbot /usr/bin/certbot
- sudo certbot --nginx

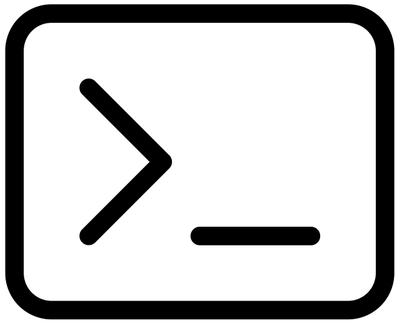
SSL com Let's Encrypt

```
server {
    listen 80;
    # Substitua pelo seu domínio
    server_name agenciasbancarias.com.br;

    root /var/www/agenciasbancarias;
    index index.html;

    # Servir arquivos estáticos diretamente
    location / {
       try_files $uri $uri/ =404;
    }
}
```



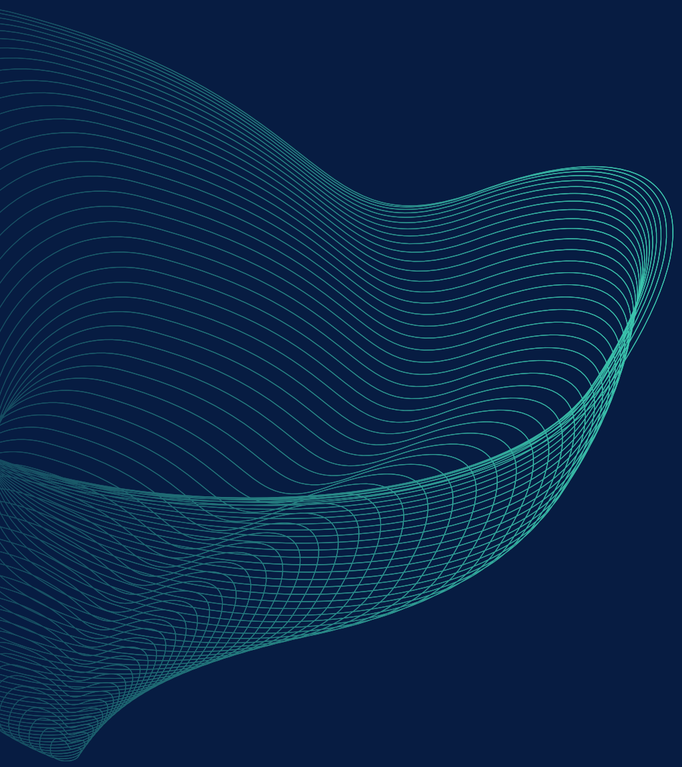
SSL com Let's Encrypt





Hora do Hands On

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA



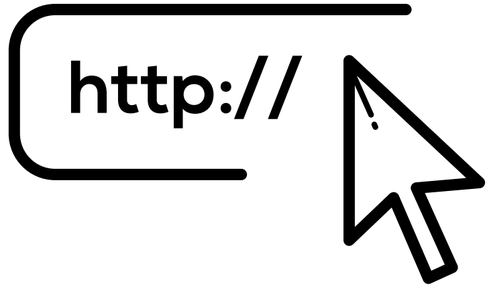
Segurança

Configuração de redirects para SSL

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

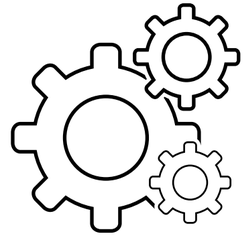
Redirect para SSL

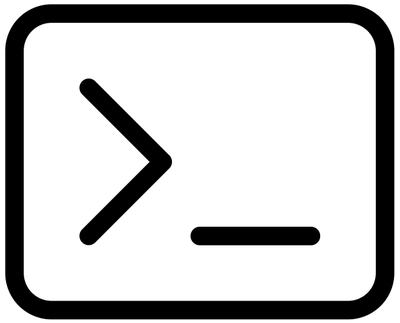
- Redirecionar todos os requets para https
- Manter o site seguro
- Evitar erro 404 para chamadas HTTP
- Configuração de host www



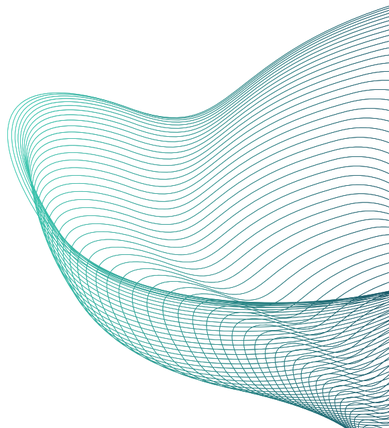
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Redirect para SSL





Hora do Hands On



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Segurança

Autenticação básica

GUERRA ACADEMY

CRIANDO EXPERTISE EM TECNOLOGIA

Autenticação básica

- Gerenciada no Nginx
- Forma eficiente de proteger um endereço
- Utilizada quando recurso não é protegido pela aplicação (conteúdo estático por exemplo)
- Armazenamento via htpasswd

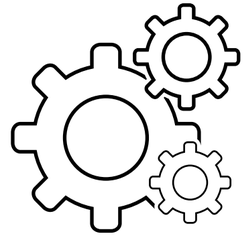
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

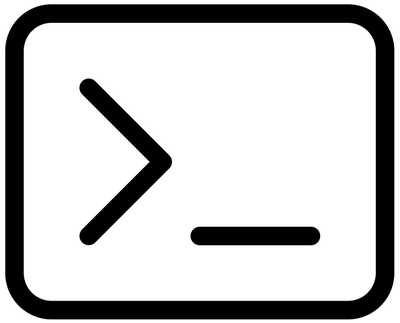
Autenticação básica

- sudo apt-get install apache2-utils
- htpasswd -c /etc/nginx/.htpasswd <username>
- Adicionar ao virtual host meusite.com:
  - auth_basic "Restricted Content";
    auth_basic_user_file /etc/nginx/.htpasswd;
- Reload do serviço

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Autenticação básica





Hora do Hands On

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Segurança

Firewall

GUERRA ACADEMY

CRIANDO EXPERTISE EM TECNOLOGIA

Firewall

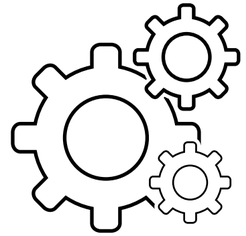
- Geralmente utilizado como Appliance
  - pfsense, Palo alto, Juniper, Check Point, etc.

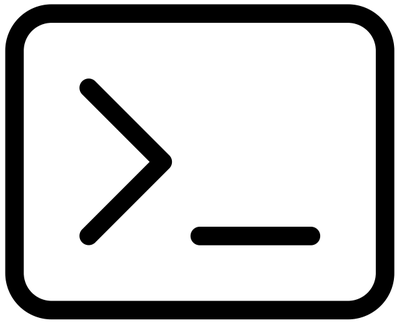
- Firewall Cloud (AWS, Azure, OCI, GCP)

- Firewall embarcado no Nginx: Soluções menores
  - VPS
- UFW - Criação de regras de firewall simples
  - Limitar tráfego de entrada
  - Especificar quais portas serão liberadas
  - 80, 443, 22

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

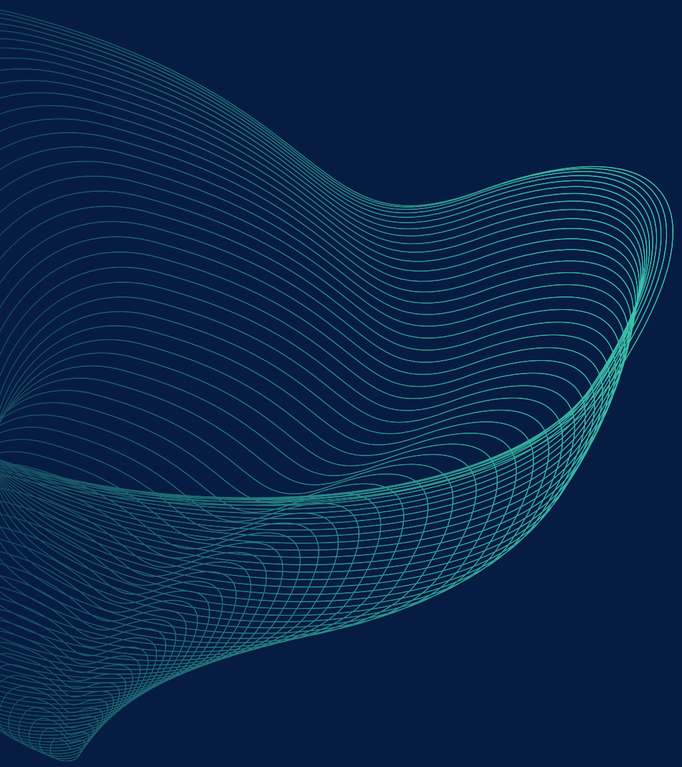
Firewall





Hora do Hands On

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA



Segurança

Web Application Firewall - ModSecurity

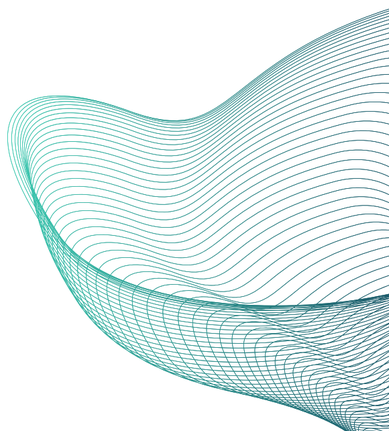
GUERRA ACADEMY

CRIANDO EXPERTISE EM TECNOLOGIA

WAF - ModSecurity

- ModSecurity: WAF OpenSource
- SQL Injection
- Cross-site scripting (XSS)
- Site request Forgery (CSRF)
- OWASP Modsecurity Core Rule Set (CRS)
- https://owasp.org/www-project-modsecurity-core-rule-set/

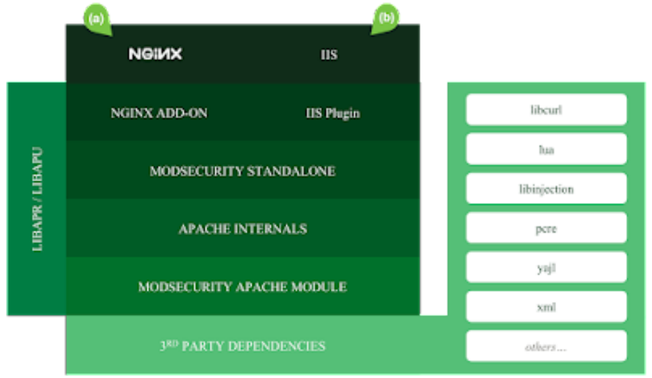
OWASP
ModSecurity
Core Rule Set
THE 1ST LINE OF DEFENSE



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

WAF - ModSecurity

- Compilação a partir do fonte:
  - ModSecurity-connector

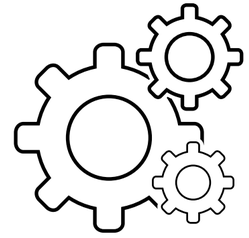


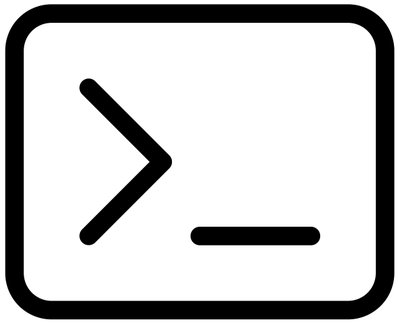
- Habilitar / configurar o mod_security

- Baixar e configurar core rule set:
  - https://github.com/coreruleset/coreruleset/archive/refs/tags/v3.3.5.zip

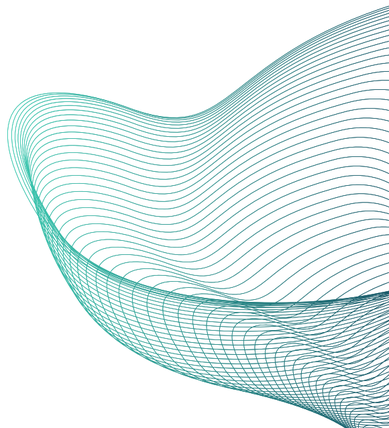
GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

WAF - ModSecurity





Hora do Hands On



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Segurança

Análise DAST - ZAP

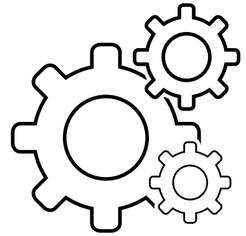
GUERRA ACADEMY

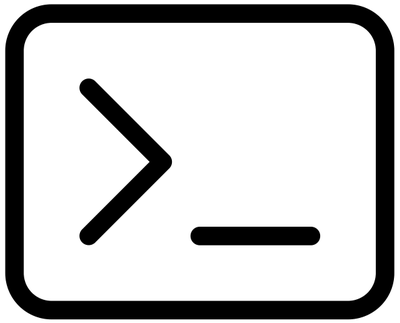
CRIANDO EXPERTISE EM TECNOLOGIA

Análise DAST - ZAP

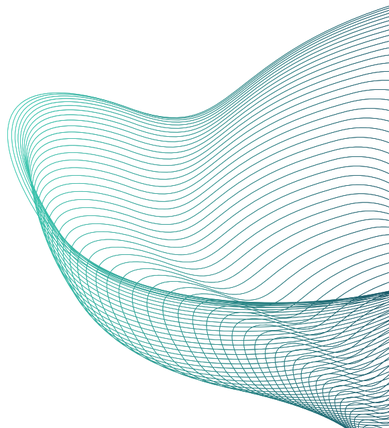
- DAST (Dynamic Application Security Testing)
- Teste de aplicativo em modo de execução
- Ferramenta de teste de segurança OpenSource
- Teste de aplicativos Web e APIs
- Formas de uso: GUI e CLI
- https://www.zaproxy.org/download/

Análise DAST – ZAP





Hora do Hands On



GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Próximos passos

Próximos Passos

- Instalação em containers
- Tuning de S.O
- Compactação
- Algoritmos de Load Balance
- HTTP/2
- Ajustes avançados de SSL
- CDN
- ...

GUERRA ACADEMY
CRIANDO EXPERTISE EM TECNOLOGIA

Versão Impressa: https://amzn.to/48kvGaS

Versão Digital: https://amzn.to/3sNwrZI

Glaucio Guerra
CTO - MarkWay
glaucio@guerra.academy
www.linkedin.com/in/glaucioguerra

http://bit.ly/apache-webserver

https://bit.ly/devops-mao-massa

https://bit.ly/programacao-go-devops

OBRIGADO!

PERGUNTAS?