



SÃO
PAULO
TECH
SCHOOL

Técnicas de Programação Web

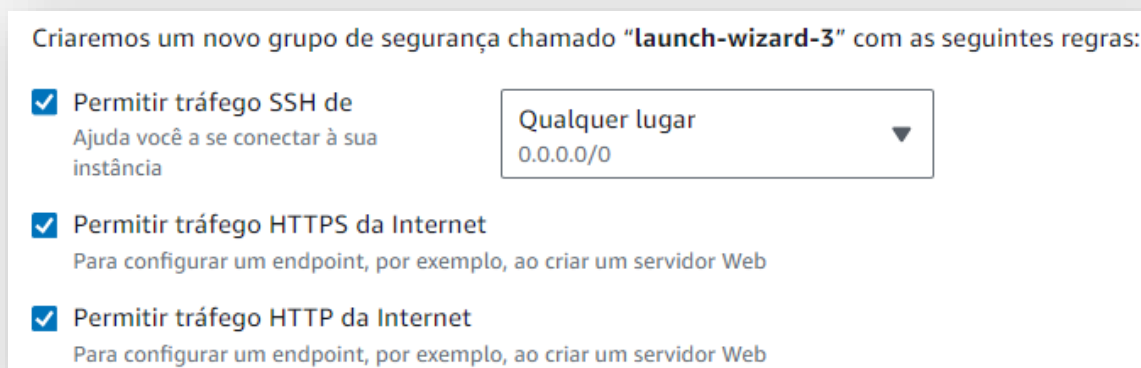
Geração e instalação de certificado
SSL/TLS em uma EC2

Diego Brito

diego.lima@sptech.school

1. Criação da EC2

1. Acesse o painel do **AWS Academy** e inicie o processo de criação de uma instância com acesso à internet, preferencialmente na VPC padrão.
2. Assegure-se de que esta instância receba um **IP público**.
3. Em seguida, configure uma chave de acesso conforme sua preferência; para este tutorial, optaremos pelo uso de um protocolo de acesso SSH.
4. Adicionalmente, configure a instância para permitir o tráfego **HTTP e HTTPS**.



2. NGINX

Acesse a instância, realize uma atualização do sistema e proceda com a instalação do **Nginx**.

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

```
ubuntu@ip-172-31-23-9: ~  
ubuntu@ip-172-31-23-9:~$ systemctl status nginx.service  
• nginx.service - A high performance web server and a reverse proxy server  
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)  
   Active: active (running) since Tue 2024-05-21 11:41:20 UTC; 2min 57s ago  
     Docs: man:nginx(8)  
  Process: 1602 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)  
  Process: 1604 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)  
 Main PID: 1605 (nginx)  
    Tasks: 2 (limit: 1130)  
   Memory: 2.2M (peak: 2.5M)  
      CPU: 16ms  
   CGroup: /system.slice/nginx.service  
           └─1605 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"  
             └─1606 "nginx: worker process"  
  
May 21 11:41:20 ip-172-31-23-9 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy >  
May 21 11:41:20 ip-172-31-23-9 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy s>  
lines 1-16/16 (END)
```

3. Domínio

Nesta etapa, **é necessário** ter um **domínio válido**.

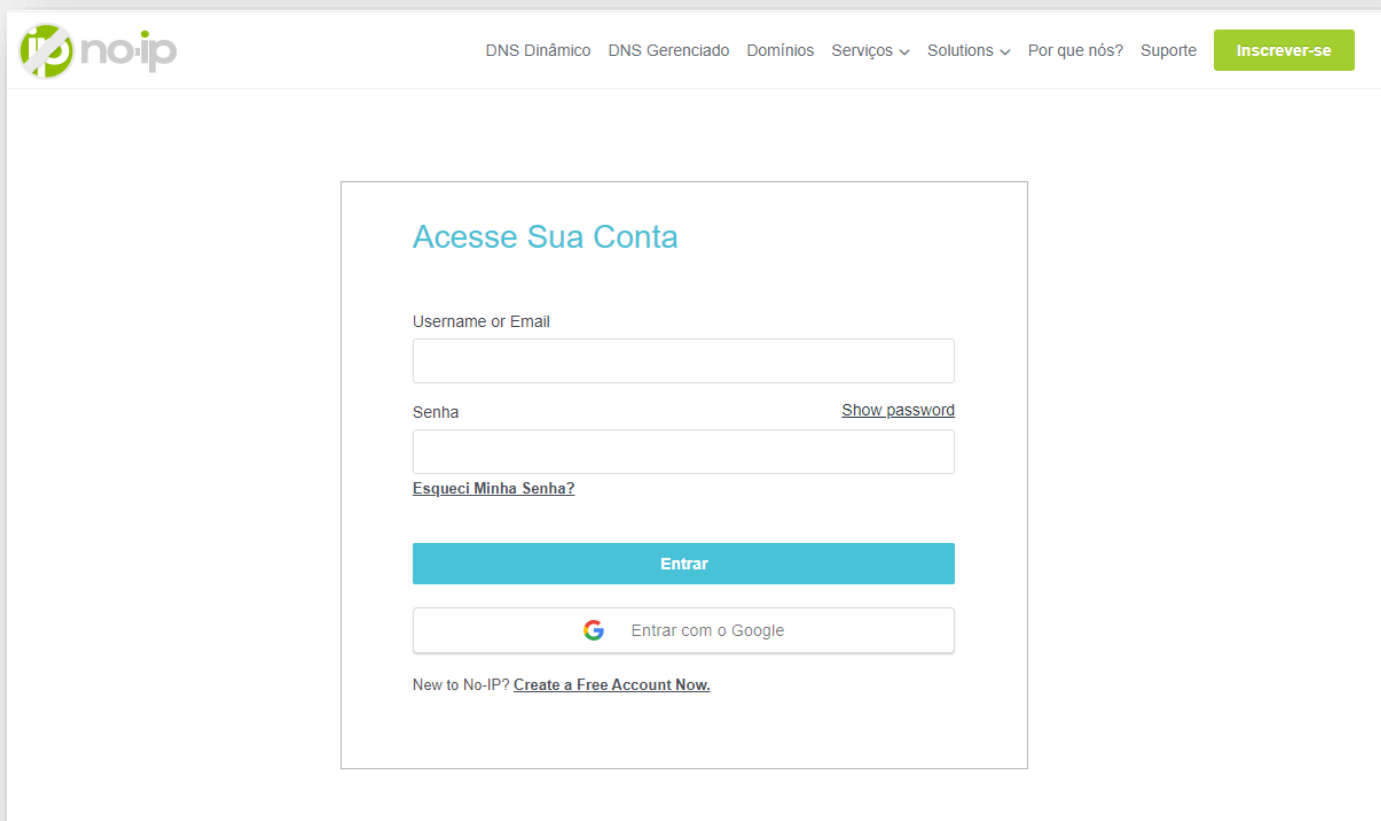
Embora a maioria dos serviços de domínio seja paga, existe uma opção para obter um domínio gratuito, ideal para fins experimentais.

O site NO-IP oferece um domínio grátis que, apesar de não ser o melhor do mercado, atende bem para propósitos de laboratório.

Acesse o NO-IP: <https://www.noip.com!>

3. Domínio

Faça o cadastro como preferir:



The screenshot shows the No-IP website's login interface. At the top, there is a navigation bar with the No-IP logo on the left and a series of links: 'DNS Dinâmico', 'DNS Gerenciado', 'Domínios', 'Serviços', 'Solutions', 'Por que nós?', and 'Suporte'. A green 'Inscrever-se' button is located on the right side of the navigation bar. The main content area features a central box titled 'Acesse Sua Conta'. Inside this box, there are two input fields: 'Username or Email' and 'Senha'. The 'Senha' field has a 'Show password' link to its right. Below the 'Senha' field is a link that says 'Esqueci Minha Senha?'. A blue 'Entrar' button is positioned below the links. At the bottom of the box, there is a button with the Google logo and the text 'Entrar com o Google'. Below the entire box, there is a link that says 'New to No-IP? Create a Free Account Now.'

no-ip

DNS Dinâmico DNS Gerenciado Domínios Serviços Solutions Por que nós? Suporte Inscrever-se


Acesse Sua Conta

Username or Email

Senha [Show password](#)

[Esqueci Minha Senha?](#)

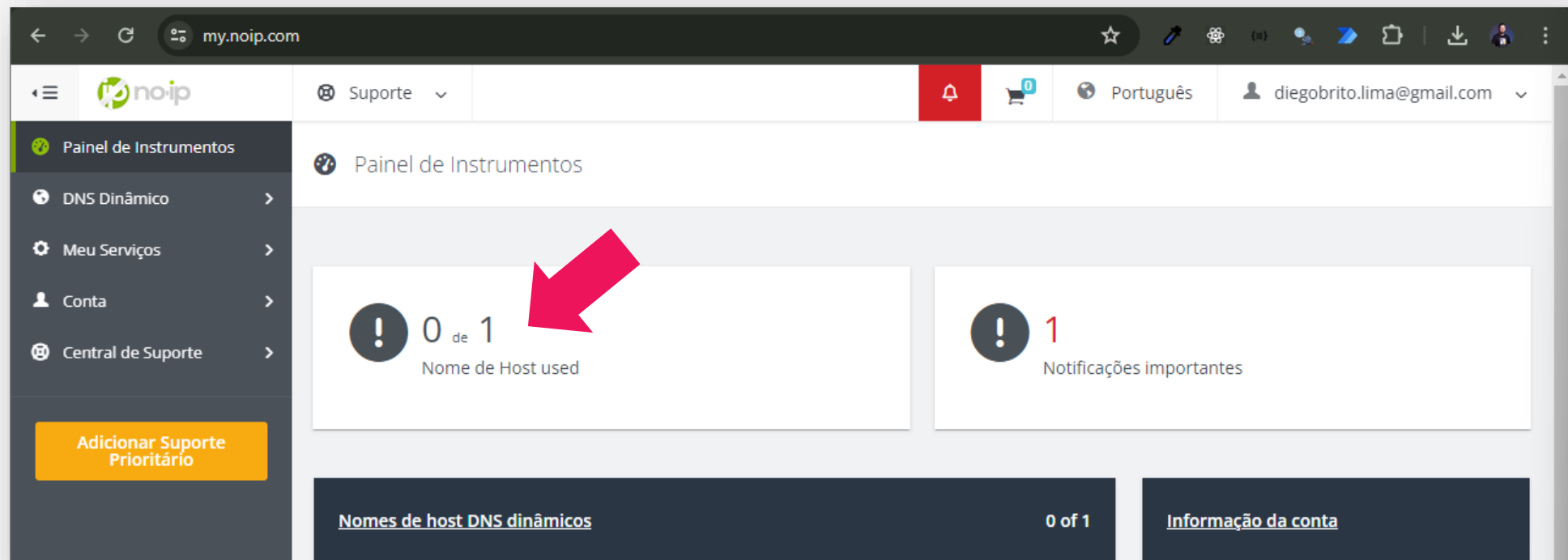
Entrar

 Entrar com o Google

New to No-IP? [Create a Free Account Now.](#)

3. Domínio

No painel clique:



3. Domínio

- Clique em "**Criar Hostname**".
- Selecione um nome para o seu host.
- Em seguida, escolha um domínio a partir do menu suspenso; note que há opções pagas, então, para economizar, opte por um dos primeiros listados.
- Na seção "**Tipo de Registro**", mantenha a configuração padrão, utilizando a opção **DNS Host (A)**.

The image displays two screenshots of a web interface for creating a hostname. The top screenshot shows the 'Nome de Hosts' page with a green 'Criar hostname' button, indicated by a red arrow and the number 1. The bottom screenshot shows the 'Create a Hostname' form. It has a 'Nome de Host' field with the value 'meu-site-maroto' (indicated by a red arrow and the number 2) and a 'Domínio' dropdown menu (indicated by a red arrow and the number 3). The dropdown menu lists several domains, with 'ddns.net' highlighted. Below the dropdown, there is a section for 'Tipo de Registro' with radio buttons for 'DNS Host (A)', 'AAAA (IPv6)', 'DNS Alias (CNAME)', and 'Web Redirect'. The 'DNS Host (A)' option is selected. Below this, there is a link to 'Gerencie seu registro de Round Robin, TXT, SRV e DKIM'. At the bottom, there is a 'Wildcard' section with a 'Compre Enhanced' link and a note 'para ativar a opção Wildcard'.

3. Domínio

Continue na mesma tela de configuração e insira o **IP** da instância que você configurou na **Amazon**. Copie o endereço IP do painel da Amazon e cole-o no campo destinado ao endereço IPv4.

The screenshot shows the AWS Route 53 'Criar hostname' configuration page. It includes a 'Domínio' dropdown menu set to 'zapro.org', an 'IPv4 Endereço' input field containing '3.91.32.119', and a 'Criar hostname' button. A 'Tipo de Registro' section on the left shows 'DNS Host (A)' selected. A notification at the top left states 'Endereço IPv4 público copiado'. Three red arrows with numbers 1, 2, and 3 point to the IP source, the input field, and the create button respectively.

1

2

3

Endereço IPv4 público copiado

3.91.32.119 | endereço aberto

Tipo de Registro

- ☒ DNS Host (A)
- ☐ AAAA (IPv6)

Domínio

zapro.org

IPv4 Endereço


3.91.32.119

hostname with DDNS Key

Criar hostname

3. Domínio

Ao **concluir** esta etapa, a tela exibida deve ser semelhante à seguinte:

Criar hostname		Pesquisar... x		
Nome de Host ▲	Last Update	IP / Alvo	Type	DDNS Key
 site-maroto.zapto.org Active	May 21, 2024 05:09 PDT ⚠	3.91.32.119	A	Create DDNS Key Modificar x

4. Certbot

O **Certbot** é uma ferramenta gratuita que automatiza o processo de obtenção, instalação e renovação de certificados SSL/TLS para websites, utilizando o serviço Let's Encrypt.

Ao rodar o Certbot, ele interage com o serviço **Let's Encrypt**, verifica a autenticidade do servidor e, após a validação, emite um certificado.

O Certbot também configura automaticamente o servidor web (como Apache ou Nginx) para usar o novo certificado e pode agendar renovações automáticas, mantendo o certificado sempre atualizado.

4. Certbot

- Acesse a instância EC2 via SSH.
- Depois, execute o comando a seguir para instalar o Certbot:
sudo apt install certbot python3-certbot-nginx.

```
ubuntu@ip-172-31-23-9: ~  
ubuntu@ip-172-31-23-9:~$ sudo apt install certbot python3-certbot-nginx  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  python3-acme python3-certbot python3-configargparse python3-icu python3-josepy python3-parsedatetime  
  python3-rfc3339  
Suggested packages:  
  python-certbot-doc python3-certbot-apache python-acme-doc python-certbot-nginx-doc  
The following NEW packages will be installed:  
  certbot python3-acme python3-certbot python3-certbot-nginx python3-configargparse python3-icu python3-josepy  
  python3-parsedatetime python3-rfc3339  
0 upgraded, 9 newly installed, 0 to remove and 21 not upgraded.  
Need to get 1097 kB of archives.  
After this operation, 5699 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

- Digite **"Y"** para confirmar e pressione **Enter.**

5. De volta ao NGINX

- É necessário configurar a propriedade **server_name** usando o arquivo de configuração padrão localizado em:
 - **/etc/nginx/sites-available/default.**
- Abra o arquivo e insira o **mesmo nome de host** que você definiu no passo 3 no site NO-IP.
- **Não esqueça de salvar o arquivo!**
- Recarregue o Nginx usando:
 - **sudo systemctl reload nginx.**

P.S.: Se você estiver utilizando o Nginx dentro de um contêiner Docker, o procedimento pode ser diferente.

```
server {  
    listen 80 default_server;  
    listen [::]:80 default_server;  
  
    root /var/www/html;  
  
    index index.html index.htm index.nginx-debian.html;  
  
    server_name site-maroto.zapto.org;  
  
    location / {  
        try_files $uri $uri/ =404;  
    }  
}
```

```
ubuntu@ip-172-31-23-9:~$ sudo nginx -t  
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok  
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

6. De volta ao Certbot

Após recarregar o Nginx, será necessário executar o seguinte comando do Certbot:

```
sudo certbot --nginx -d example.com
```

Neste comando, substitua **example.com** pelo nome do host exato que você configurou no site do NO-IP.

6. De volta ao Certbot

Após rodar o comando:

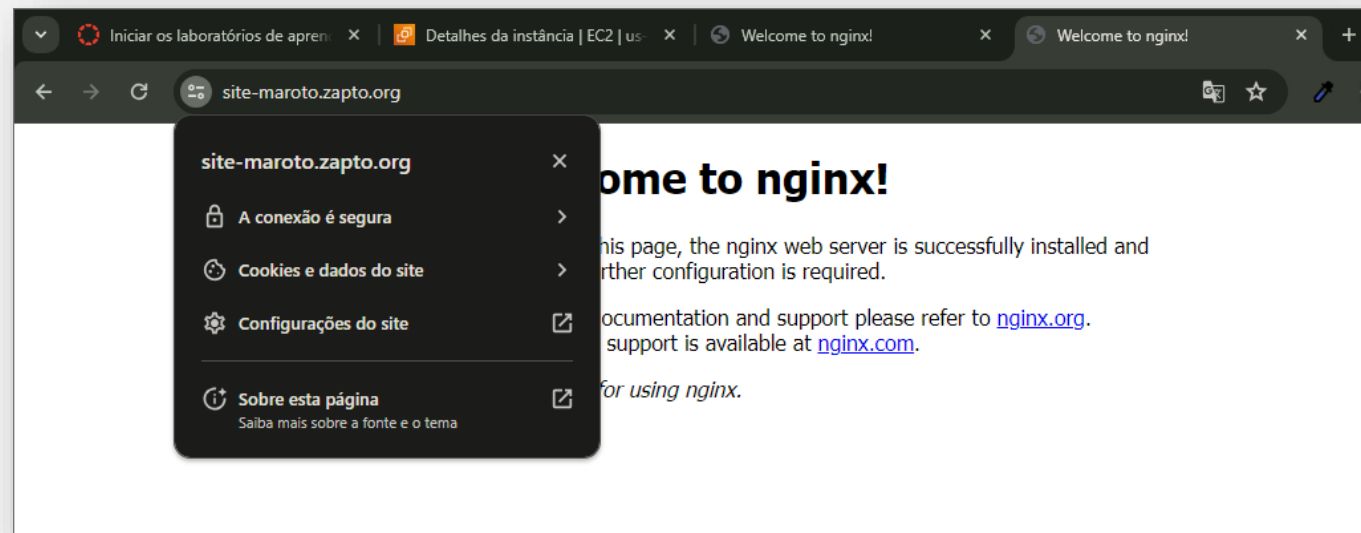
1. Insira um email para receber **notificações sobre o vencimento do certificado.**
2. Aceite os termos de serviço.
3. Decida se deseja compartilhar seu email para receber atualizações sobre melhorias da ferramenta e informações de segurança.

Pronto, seu certificado está configurado!

```
ubuntu@ip-172-31-23-9: ~  
Account registered.  
Requesting a certificate for site-maroto.zapto.org  
  
Successfully received certificate.  
Certificate is saved at: /etc/letsencrypt/live/site-maroto.zapto.org/fullchain.pem  
Key is saved at: /etc/letsencrypt/live/site-maroto.zapto.org/privkey.pem  
This certificate expires on 2024-08-19.  
These files will be updated when the certificate renews.  
Certbot has set up a scheduled task to automatically renew this certificate  
  
Deploying certificate  
Successfully deployed certificate for site-maroto.zapto.org to /etc/nginx/sites-enabled/default  
Congratulations! You have successfully enabled HTTPS on https://site-maroto.zapto.org/  
  
-----  
If you like Certbot, please consider supporting our work by:  
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate  
* Donating to EFF: https://eff.org/donate-le  
-----  
ubuntu@ip-172-31-23-9:~$
```

7. Teste de acesso

Ao acessar o endereço registrado, observamos que o nosso site de teste foi carregado corretamente e exibe o ícone famoso do cadeado (ou algo relacionado a isso), indicando que um certificado foi instalado com sucesso em nosso servidor.



8. Configuração Nginx

Se retornarmos ao arquivo de configuração do **Nginx**, veremos que o Certbot realizou alguns ajustes automaticamente, como por exemplo, configurar o **redirecionamento do tráfego da porta 80 para a porta 443**.

Além disso, o arquivo agora contém os caminhos para os certificados que foram instalados na máquina.

Simples, não é?

```
server {  
    root /var/www/html;  
    index index.html index.htm index.nginx-debian.html;  
    server_name site-maroto.zapto.org;  
    location / {  
        try_files $uri $uri/ =404;  
    }  
  
    listen [::]:443 ssl ipv6only=on; # managed by Certbot  
    listen 443 ssl; # managed by Certbot  
    ssl_certificate /etc/letsencrypt/live/site-maroto.zapto.org/fullchain.pem; # managed by Certbot  
    ssl_certificate_key /etc/letsencrypt/live/site-maroto.zapto.org/privkey.pem; # managed by Certbot  
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot  
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot  
}  
server {  
    if ($host = site-maroto.zapto.org) {  
        return 301 https://$host$request_uri;  
    } # managed by Certbot  
  
    listen 80 default_server;  
    listen [::]:80 default_server;  
  
    server_name site-maroto.zapto.org;  
    return 404; # managed by Certbot  
}  
~
```

9. Congrats - Links

NGINX em container:

[How To Install TLS/SSL on Docker Nginx Container With Let's Encrypt](#)

TLS para NGINX com Load Balance:

<https://www.cyberciti.biz/faq/configure-nginx-ssl-tls-passthru-with-tcp-load-balancing/>

TLS para NGINX com Load Balance [2]:

<https://www.digitalocean.com/community/tutorials/how-to-set-up-nginx-load-balancing-with-ssl-termination>

Configuração de um HTTPS server com NGINX:

https://nginx.org/en/docs/http/configuring_https_servers.html

Abraço!



Agradeço a sua atenção!

Por: Diego Brito

diego.lima@sptech.school



SÃO
PAULO
TECH
SCHOOL