MONSTA

MONITORAMENTO DE REDES IP

INSTALANDO O CERTIFICADO LET'S ENCRYPT NO MONSTA

Índice

A instalação padrão do Monsta permite o acesso à plataforma de monitoramento através dos protocolos HTTP e HTTPS. Entretanto, a porta HTTPS não possui um certificado válido para operar e obriga o usuário a aceitar o certificado atual a cada conexão efetuada.

Para resolver essa situação, faz-se necessário a instalação de um certificado assinado por uma Autoridade de Certificação válida, também conhecida como CA. Para este tutorial, vamos utilizar os serviços do Let's Encrypt (www.letsencrypt.org).

CRIANDO UM CERTIFICADO UTILIZANDO O MODO MANUAL

Utilize este método para criar um certificado nas seguintes condições:

a) Seu servidor do Monsta não possui acesso à porta 80 e 443 pela internet;
b) Você está utilizando o Monsta em uma porta diferente de 80 e 443.

Instalando o certbot

⚠ ATENÇÃO:

1. Para esse procedimento você precisará ter acesso as configurações do DNS de seu domínio.
2. O servidor Linux onde o Monsta está instalado necessita de acesso à internet.

Logado no servidor Linux do Monsta como root, instale os pacotes epel-release e certbot-nginx:

```
yum install -y epel-release
yum install -y certbot-nginx
```

Criando o certificado

⚠ ATENÇÃO: Substitua o domínio monsta.meudominio.com.br pelo que você vai utilizar. Esse domínio deve resolvido na internet.

Crie um registro do tipo A em seu DNS com o endereço IP apontando para monsta.meudomínio.com.br. Após, utilize o comando certbot para criar o certificado e responda as perguntas solicitadas conforme abaixo:

```
certbot certonly --manual --preferred-challenges dns -d monsta.meudominio.com.br --agree-tos --no-eff-email
Enter email address: meu_email@meudominio.com.br
```

```
Are you OK with your IP being logged?
(Y)es/(N)o: Y

Please deploy a DNS TXT record under the name
_acme-challenge.monsta.meudominio.com.br with the following value:

chave_para_incluir_no_registro_TXT
```

ATENÇÃO: Antes de continuar, adicione um novo registro no seu servidor DNS com a chave informada. Após efetuado e ativado o registro, pressione "Enter" para continuar.

Se o certificado for criado sem problemas, a seguinte mensagem deverá ser exibida:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/privkey.pem
   Your cert will expire on 2018-11-07. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - 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
```

Configurando o certificado no Nginx

Edite o arquivo /opt/monsta/etc/nginx.cfg e execute os seguintes passos:

1. Localize a linha com o parâmetro "listen 443;" e adicione abaixo dela o seguinte parâmetro:

server_name monsta.meudominio.com.br;

2. Localize os parâmetros ssl_certificate e ssl_certificate_key e altere-os conforme exemplo abaixo:

ssl_certificate /etc/letsencrypt/live/monsta.meudominio.com.br/fullchain.pem;

```
ssl_certificate_key /etc/letsencrypt/live/monsta.meudominio.com.br/privkey.pem;
```

Testando as alterações

Execute o comando abaixo para testar se as alterações estão corretas:

```
/usr/bin/env LD_LIBRARY_PATH=/opt/monsta/lib /opt/monsta/bin/nginx -t -c /opt/monsta/etc/nginx.cfg
```

Se tudo estiver certo, o comando deverá retornar a seguinte informação:

```
nginx: [alert] could not open error log file: open() "/opt/monsta/nginx/logs/error.log" failed (2: No such file or directory)
nginx: the configuration file /opt/monsta/etc/nginx.cfg syntax is ok
nginx: configuration file /opt/monsta/etc/nginx.cfg test is successful
```

Aplicando as configurações

Reinicie o nginx com o comando abaixo:

```
kill `pidof nginx`
```

A partir de agora seu servidor do Monsta possuirá um certificado válido para acesso pelo protocolo https. Esse certificado vale por 90 dias.

Renovando o Certificado

Para este método, a renovação do certificado deverá ser feita manualmente.

⚠ **ATENÇÃO: Substitua o domínio monsta.meudominio.com.br pelo que você vai utilizar. Esse domínio deve resolvido na internet.**

Acesse o servidor Linux, onde o Monsta está instalado, com o usuário root. Para renovar o certificado, vamos utilizar o comando certbot. Responda as perguntas conforme demonstrado abaixo:

```
certbot certonly --manual --preferred-challenges dns -d monsta.meudominio.com.br --agree-tos --no-eff-email

What would you like to do?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: Keep the existing certificate for now
2: Renew & replace the cert (limit ~5 per 7 days)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):  2
```

```
Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y


Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue

Pressione enter
```

Se o certificado for criado sem problemas, a seguinte mensagem deverá ser mostrada:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/privkey.pem
   Your cert will expire on 2018-11-07. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - 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
```

Após, para carregar o novo certificado, reinicie o Nginx com o comando:

```
kill `pidof nginx`
```

CRIANDO UM CERTIFICADO UTILIZANDO O MODO HTTP

Utilize este método para criar um certificado com a seguinte condição:

a) Seu servidor do Monsta possui, obrigatoriamente, acesso as portas 80 e 443 pela internet;

Instalando o certbot

⚠ ATENÇÃO: O servidor Linux onde o Monsta está instalado necessita ter acesso à internet.

Logado no servidor Linux do Monsta como root, instale os pacotes epel-release, certbot-nginx e nginx-all-modules:

```
yum install -y epel-release
yum install -y nginx-all-modules
yum install -y certbot-nginx
```

Configurando o Nginx

Crie um apontamento para o arquivo de configuração do nginx do Monsta:

```
ln -sf /opt/monsta/etc/nginx.cfg /etc/nginx/nginx.conf
```

Edite o arquivo /etc/nginx/nginx.conf, localize a linha com o parâmetro "listen 443;" e adicione abaixo dela o seguinte parâmetro:

server_name monsta.meudominio.com.br;

Testando as alterações

Execute o comando abaixo para testar se as alterações estão corretas:

```
/usr/bin/env LD_LIBRARY_PATH=/opt/monsta/lib /opt/monsta/bin/nginx -t -c /opt/monsta/etc/nginx.cfg
```

Se tudo estiver certo, o comando deverá retornar a seguinte informação:

```
nginx: [alert] could not open error log file: open() "/opt/monsta/nginx/logs/error.log" failed (2: No such file or directory)
nginx: the configuration file /opt/monsta/etc/nginx.cfg syntax is ok
nginx: configuration file /opt/monsta/etc/nginx.cfg test is successful
```

Reinicie o servidor Nginx com o comando abaixo:

```
kill `pidof nginx`
```

Criando o certificado

ATENÇÃO: Substitua o domínio monsta.meudominio.com.br pelo que você vai utilizar. Esse domínio deve resolvido na internet.

Uilize o comando certbot para criar o certificado e responda as perguntas solicitadas conforme abaixo:

```
certbot --nginx -d monsta.meudominio.com.br  --agree-tos --no-eff-email

Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): meu-email@meudominio.com.br

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
```

Se o certificado foi criado corretamente, você verá a seguinte mensagem:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/monsta.meudominio.com.br/privkey.pem
   Your cert will expire on 2018-11-11. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - 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
```

Renovando o Certificado

Quando utilizado o método por http, é possível configurar a renovação automática do certificado.

Para fazer isso, logue-se como root no servidor onde o Monsta está instalado e execute os procedimentos abaixo:

1. Edite o arquivo do crontab:

```
crontab -e
```

2. Adicione o comando para renovar o certificado para que seja executado diariamente. Escolha o horário que seja mais conveniente:

```
10 0 * * * /usr/bin/certbot renew --quiet
```

3. Salve o arquivo.

Após esses passos, o certificado do Monsta será renovado sempre de forma automática.

APÊNDICE A | Contato

Monsta Tecnologia Ltda

Site: **http://www.monsta.com.br**
Downloads: **http://www.monsta.com.br/download.html**
E-mail: **suporte@monsta.com.br**


MONSTA
MONITORAMENTO DE REDES IP