INSTALAÇÃO E CONFIGURAÇÃO DE SERVIDORES

TÉCNICO INTEGRADO EM INFORMÁTICA PARA INTERNET

PROFESSOR IURI SOUZA

ROTEIRO DE AULA PRÁTICA 01

INSTALAÇÃO E CONFIGURAÇÃO DO APACHE

Configuração de Rede e Certificados SSL - IP Fixo e Acesso por HTTPS

SUMÁRIO

SUMÁRIO..... 1
INTRODUÇÃO..... 2
CONFIGURAÇÃO DE REDE - IP ESTÁTICO..... 2
Habilitar HTTPS através dos módulos SSL..... 3
CONFIGURAÇÕES BÁSICAS..... 3
Habilitar SSL..... 4
Habilitando o novo arquivo de configuração..... 4
Arquivo ports.conf..... 4
Habilitar/Desabilitar Módulos..... 5
ATIVIDADE PROPOSTA..... 5

INTRODUÇÃO

Por meio desse tutorial você será capaz de fixar um IP ao servidor WEB além de habilitar o seu acesso por meio do protocolo HTTPS, ativando a criptografia a nível de aplicação pelo protocolo SSL.

A fixação de IP é imprescindível a um servidor tendo em vista que irá determinar a sua localização em uma rede além de definir de forma estática e fixa os serviços oferecidos.

Já a configuração HTTPS será importante para proteger os dados trafegados entre cliente e servidor por meio da criptografia SSL.

CONFIGURAÇÃO DE REDE - IP ESTÁTICO

Inicialmente devemos reconhecer o nome da interface de rede que o nosso servidor está usando para se conectar na rede, para isso use o comando:

$ ip address

Exemplo:

```
iurisouza@professor:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
oup default qlen 1000
    link/ether 08:00:27:06:aa:27 brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute enp0s8
       valid_lft 86389sec preferred_lft 86389sec
    inet6 fe80::a00:27ff:fe06:aa27/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Na imagem de exemplo, o nome da interface é **enp0s8**

Acesse o arquivo /etc/network/interfaces

Ao final do arquivo, adicione a seguinte configuração:

Obs.: Não deve ser apagado nada que já exista no arquivo!

```
iface <nome_interface> inet static
        address     <IP>
        netmask     <Máscara de Rede>
        network     <IP da rede>
        gateway     <Gateway Padrão>
        broadcast   <IP de Broadcast>
```

Onde <nome_interface> é o nome identificado anteriormente pelo ip address e as informações da rede devem ser passadas pelo professor.

Salve o arquivo e reinicie sua máquina. Após, verifique se as informações de rede estão ativas através do comando ip address

Obs.: Após a configuração de IP estático sua VM deverá estar conectada OBRIGATORIAMENTE a rede wLabredes5 via modo Placa em modo Bridge.

Habilitar HTTPS através dos módulos SSL.

Inicialmente iremos criar um novo arquivo de configuração para o nosso site.

Obs.: O arquivo antigo não precisa ser desabilitado, apesar de que futuramente isso será aconselhável.

CONFIGURAÇÕES BÁSICAS

Dentro do diretório sites-available, crie um novo arquivo .conf e realize as seguintes configurações.

```
<VirtualHost *:443>

ServerAdmin <email do admin>
ServerName <domínio do servidor>
ServerAlias <alias do dominio>
DocumentRoot <caminho até os arquivos do site>
SSLEngine on #habilita módulo ssl
SSLCertificateFile <caminho para o certificado ssl arquivo.crt>
SSLCertificateKeyFile <caminho para a chame ssl arquivo.key>

</VirtualHost>
```

OBS.: Deve-se criar um diretório dentro de /etc/apache2 para armazenar os arquivos de chaves e certificados SSL. Aconselha-se que esse diretório se chame ssl.

Iremos utilizar o comando `openssl` para criar certificados de autenticação e chaves criptográficas.

Habilitar SSL

```
$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout <caminho até o arquivo de chave> -out <caminho até o arquivo do certificado SSL>
```

Obs.: Os caminhos até os arquivos precisam ser os mesmos dos indicados no VirtualHost.

Habilitando o novo arquivo de configuração.

Utilizar comando `a2ensite` <nome do site.conf> para habilitar

Utilizar comando `a2dissite` <nome do site.conf> para desabilitar

Arquivo ports.conf

Armazena as portas que serão ouvidas pelo servidor. No caso da porta 443 (HTTPS), ela só será aberta no caso dos módulos SSL estarem instalados e habilitados. O sistema Debian, por padrão, mantém este

módulo instalado mas não os habilita. Para isso, precisamos utilizar o comando que segue:

Habilitar/Desabilitar Módulos

Habilitar: `$ sudo a2enmod <módulo>`
Desabilitar: `$ sudo a2dismod <módulo>`

Observação: O apache utiliza os diretório mods-available e mods-enabled para gerenciar os módulos utilizados.

ATIVIDADE PROPOSTA

Instale e habilite os módulos php em seu servidor. Para a instalação deve ser utilizado o mesmo padrão de instalação para pacotes.

Obs.: Verificar a versão do php que será utilizado.