Configurando o Centos 7 depois de instalado

April 20, 2015 3 minutes read
Linux
centos • linux • fail2ban • ntp

Instalando o Epel

A primeira coisa a ser feita é instalaar o epel

```
sudo yum install epel-release
```

Agora vamos fazer o update dos pacotes do SO

```
sudo yum update
```

Configurando o Firewall

Um mudança consideravel agora no Centos7 é a remoção do iptables e a adição do FirewallD, como essa maquina vai estar exposta diretamente para a internet nos precisamos de um firewall para bloquear alguns acessos em serviços que deverão estar expostos só em loopback.

Estou usando uma VM na DigitalOcean e por padrão a imagem de Centos7 deles vem com o firewallD desativado, para ativar digite o comando:

```
sudo systemctl start firewalld
```

Para habilitar ele no boot digite:

```
sudo systemctl enable firewalld
```

Um problema do antigo iptables era que para tornar uma regra permante você tinha que salvar usando iptables-save e fazer o iptables ler o arquivo no boot do SO, agora para adiconar uma regra persistente só é preciso colocar um –permanent como argumento da regra, a primeira regra do firewall vai ser para abri a porta do ssh:

```
sudo firewall-cmd --permanent --add-service=ssh
```

Como o ssh esta com login somente por chave não vejo motivo para alterarmos a porta default, mas nos iremos proteger o ssh usando o fail2ban que tem como objetivo impedir um bruteforce na porta 22. Enquanto isso vamos retomar a configuração do firewall, como esse servidor vai ser utilizado como servidor web nos temos que abrir a porta 80:

```
sudo firewall-cmd --permanent --add-service=http
```

Para ver todos os serviços que podemos abrir as portas pela lista default basta digitar:

```
sudo firewall-cmd --get-services
```

Para abrir uma porta que não esta listada nos serviços podemos usar o seguinte comando:

```
sudo firewall-cmd --permanent --add-port=22/tcp
```

Podemos listar as portas abertas de forma permanente com o seguinte comando:

```
sudo firewall-cmd --permanent --list-all
```

Para colocar as novas regras em funcionamento nos precisamos dar um reload no firewalld, para isso digite:

```
sudo firewall-cmd --reload
```

Agora que o FirewallD esta configurados vamos instalar e configurar o Fail2Ban

Fail2Ban

Nos iremos configurar o Fail2ban de maneira que após 4 login com falha o ip que esta tentado logar na maquina irá ficar banido por 1 semana, é muito importante que você esteja autenticando na maquina via chaveou que não erre o login caso contrario seu IP será banido por uma semana =D.

Vamos instalar o pacote:

```
sudo yum install fail2ban fail2ban-firewalld fail2ban-systemd
```

Vamos criar o arquivo de configuração sshd.conf no diretorio conf.d do fail2ban:

```
sudo vi /etc/fail2ban/jail.d/sshd.conf
```

No arquivo colocamos

```
[DEFAULT]
bantime = 345600
banaction = firewallcmd-ipset
backend = systemd
action = %(action_mwl)s
maxretry = 4
[sshd]
enabled = true
```

Agora iremos inicar o fail2ban

```
sudo systemctl start fail2ban
```

Habilitamos o fail2ban para iniciar com o SO

```
sudo systemctl enable fail2ban
```

Para ver os ips banidos pelo fail2ban use o seguinte comando:

```
fail2ban-client status sshd
```

NTP

As vezes o relogio dos servidore ficam meio loucos, para resolver esse problema iremos instalar o ntpclient no servidor.

```
sudo yum install ntp
```

Depois disso iremos iniciar o daemon e configurar para iniciar junto com o SO:

```
sudo systemctl start ntpd
```

```
sudo systemctl enable ntpd
```