



Linux para Infraestrutura

Prof. André Nasserála
nasserála@gmail.com

Systemctl

- O comando `systemctl` no Linux é o gerenciador do `Systemd`, que é considerado o gerenciador de “quase tudo” no Linux.
- O sistema `systemd` já é amplamente utilizado nas distribuições mais conhecidas, especialmente nas versões de Kernel superiores a 2.6.
- Para verificar quais serviços estão em execução:
- `$ systemctl status`
- Parar um serviço com o `systemctl`
- `# systemctl stop cron.service`

Systemctl

- Veja o status do serviço quando parado:
- `# systemctl status cron.service`

- Para iniciar um serviço:
- `# systemctl start cron.service`

- Para reiniciar um serviço:
- `# systemctl restart cron.service`

Systemctl

- Para habilitar um serviço durante a carga do sistema, usa-se o comando enable:
 - # systemctl enable cron.service
- Para desabilitar um serviço durante a carga do sistema, usa-se o comando disable:
 - # systemctl disable cron.service
- Para verificar quais serviços estão em execução:
 - \$ systemctl status

DHCP

- **DHCP**, Dynamic Host Configuration Protocol (Protocolo de configuração de host dinâmico), é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede. seja principalmente usado para HTTP, HTTPS e FTP;
- **Resumidamente, o DHCP opera da seguinte forma:**
- Um cliente envia um pacote UDP em broadcast (destinado a todas as máquinas) com um pedido DHCP;
- Os servidores DHCP que capturarem este pacote irão responder com um pacote com configurações onde constará, pelo menos, um endereço IP, uma máscara de rede e outros dados opcionais como o gateway, servidores de DNS, etc.

DHCP

- Para instalar o servidor DHCP em CentOS usamos:
- **# yum install dhcp -y**
- Assim o diretório /etc/dhcp será criado, e dentro dele existirá um arquivo vazio(alguns comentários) de nome dhcpd.conf.
- **# vim /etc/dhcp/dhcpd.conf**

```
Transaction Test Succeeded
Running Transaction
  Installing      : 12:dhcp-4.1.1-12.P1.el6_0.4.x86_64

Installed:
  dhcp.x86_64 12:4.1.1-12.P1.el6_0.4
```

DHCP

- **option domain-name "3wtecinf";**
- **option domain-name-servers 8.8.8.8;**
- **default-lease-time 600;**
- **max-lease-time 7200;**
- **log-facility local7;**
- **subnet 192.168.3.0 netmask 255.255.255.0 {**
- **range 192.168.3.128 192.168.3.254;**
- **option domain-name-servers 192.168.3.1;**
- **option domain-name "3w";**
- **option routers 192.168.3.1;**
- **option broadcast-address 192.168.3.255;**
- **default-lease-time 600;**
- **max-lease-time 7200;**
- **}**

DHCP

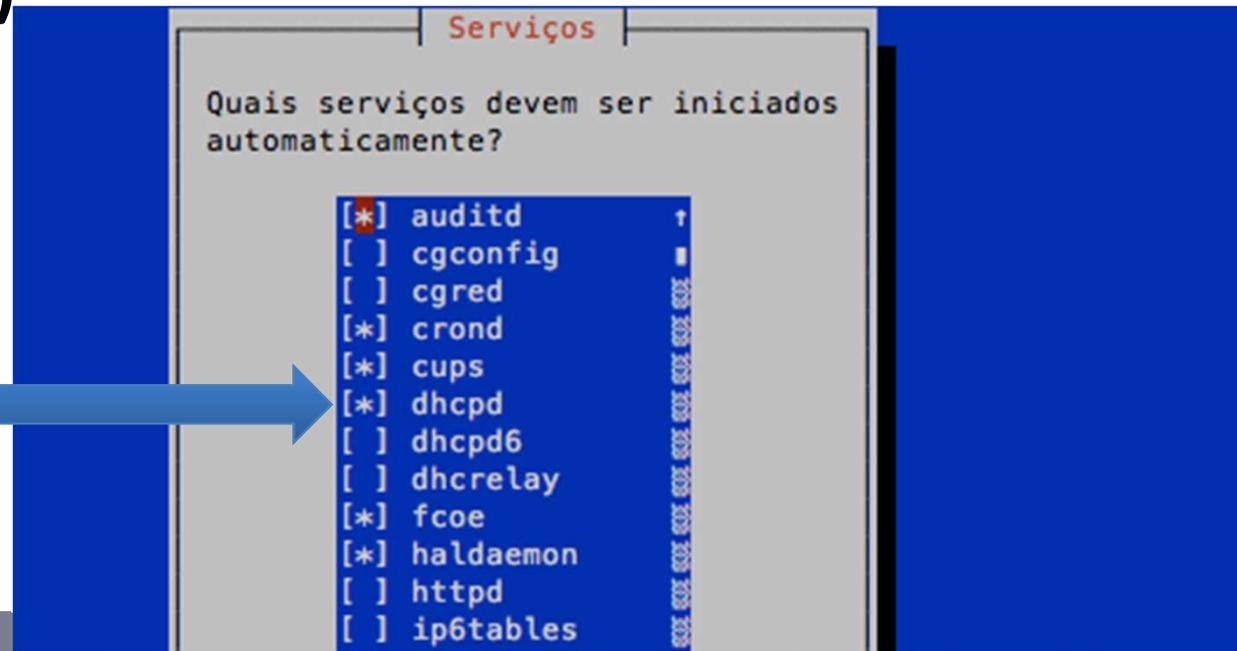
- Nome do Domínio:
- option domain-name "3wtecinf";
- Servidor de DNS:
- option domain-name-servers 8.8.8.8;
- Tempo Padrão de Concessão:
- default-lease-time 600;
- Tempo Maximo de Concessão:
- max-lease-time 7200;
- Nível de LOG
- log-facility local7;

DHCP

- subnet 192.168.3.0 netmask 255.255.255.0 {
- range 192.168.3.128 192.168.3.254;
- option domain-name-servers 192.168.3.1;
- option domain-name "3w";
- option routers 192.168.3.1;
- option broadcast-address 192.168.3.255;
- default-lease-time 600;
- max-lease-time 7200;
- }

DHCP

- Obs: O serviço de DHCP somente inicia se a interface de rede tiver um IP dentro da rede que será distribuída;
- Para inicia-lo por padrão junto com a maquina precisamos marca-lo na lista do ntsysv.
- # ntsysv. (YUM)



SSH

- O Secure Shell ou SSH é, simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota.
- Possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.
- **OpenSSH**: é uma coleção de programas que proveem a criptografia em sessões de comunicações em uma rede de computadores usando o protocolo SSH.
- Ele foi criado com um código aberto alternativo ao código proprietário da suíte de softwares Secure Shell oferecido pela SSH Communications Security. OpenSSH foi desenvolvido como parte do projeto OpenBSD, que foi liderado por Theo de Raadt.

SSH

- Mesmo a instalação mínima podemos usa-lo por padrão, pois o pacote openssh-server já vira instalado. Seu arquivo de configuração é:
- **# vim /etc/ssh/sshd_config**
- Por questões de segurança devemos sempre adicionar ao final desse arquivo a linha:
- **AllowUsers usuario1 usuario2 ... usuarioN;**
- Pois assim negaremos por padrão o acesso remoto via root e somente permitiremos que os usuários listados acessem via SSH;
- **# systemctl restart sshd**

SSH

- **SCP**
- O utilitário scp faz parte de um pacote opcional do OpenSSH e deve ser instalado. Com ele é possível fazer cópias remotas de arquivos entre estações Linux com SSH.
- `# yum install openssh-clients`
- Sua sintaxe:
- **scp**
seu_login@host_remoto:/algun/diretorio/arquivo_remoto
/algun/dir/arquivo_local
- Ou
- **scp** **/algun/dir/arquivo_local**
seu_login@host_remoto:/algun/diretorio/arquivo_remoto

SSH

- Exemplos:
- # scp nasserala@201.15.122.36:/home/nasserala/arquivo.tgz /root/
- # scp * pedro@eletroacre.com.br:/etc/tempo/
- # scp nasserala@192.168.3.1:/home/nasserala/*.sh .

SSH

- Acessando remotamente um servidor:
- **# ssh usuario@host**
- Se estiver rodando em porta diferente da padrão
- **# ssh usuario@host -P 2222**
- Ex:
- **# ssh nasserala@192.168.3.1**
- Executando comandos remotos:
- **# ssh usuario@host "comando"**
- Ex:
- **# ssh nasserala@200.251.75.114 "du -sh /home/djair/*" > resultado.txt**

HTTP com PHP

- O serviço HTTPD do CentOS já vem com todo suporte configurado, assim para ter um servidor WEB com suporte a PHP basta instalar o apache e php via yum e inicia-los:
- **# yum install httpd php -y**
- Informações importantes:
- O document root do apache estará em:
- **/var/www/html**
- Comando:
- **# systemctl start httpd**
- **Abra no navegador e teste.**

HTTP com PHP

- Autenticação com htaccess:
- **Editar:**
- # vi /etc/httpd/conf/httpd.conf
- **Mudar:**
- <Directory "/var/www/html">
-
- Options Indexes FollowSymLinks
-
- AllowOverride **AuthConfig**
-
- Require all granted
- </Directory>

HTTP com PHP

- Arquivos:
- # vi /var/www/html/.htaccess
- AuthName "Acesso Restrito SENAC/Rio Branco"
- AuthType Basic
- AuthUserFile /var/www/html/.htpasswd
- require valid-user

HTTP com PHP

- Sincronizando usuário e senha (script replica.sh):
- `# vi /usr/local/bin/replica.sh`
- `#!/bin/bash`
- `cat /etc/shadow | grep nasserala | cut -d: -f1-2 > /var/www/html/.htpasswd`
- Crontab:
- `0-59/1 * * * * /usr/local/bin/replica.sh`
- TENTA ACESSAR

FTP

- O acesso a um servidor FTP pode ser conseguido de duas formas:
- Anônimo;
- Autenticado;
- Em modo anônimo, clientes remotos podem aceder ao servidor FTP utilizando a conta de utilizador por omissão chamada "anonymous".
- Em modo autenticado o utilizador necessita de um login e uma senha. O acesso do utilizador aos diretórios e arquivos de um servidor FTP depende das permissões definidas para a conta de utilizador.
- Como regra geral, o gestor FTP esconde o diretório raiz do servidor FTP e muda-o para o diretório "Home".

FTP

- VSFTPD
- Instalação do Servidor FTP:
- vsftpd é um serviço disponível no Debian e RHEL. É fácil de instalar, configurar e manter. Para instalar o vsftpd pode executar o seguinte comando:
- **yum install vsftpd -y**

FTP

- Pode-se editar o arquivo de configuração do vsftpd `/etc/vsftpd/vsftpd.conf` para alterar os valores padrão.
- Por padrão apenas o acesso FTP anônimo é permitido.
- Se pretender desativar esta opção, deve alterar a linha:
 - **`anonymous_enable=YES`**
 - para
 - **`anonymous_enable=NO`**

FTP

- Similarmente, por padrão, os utilizadores anônimos não têm permissão para transferir arquivos para o servidor FTP.
- Para alterar esta configuração, deve retirar o comentário da linha:
- **#anon_upload_enable=YES**
- O arquivo de configuração é constituído por muitos parâmetros.
- A informação sobre cada parâmetro está disponível no próprio arquivo de configuração.
- Em alternativa, pode consultar a página do manual, man 5 vsftpd.conf para detalhes de cada parâmetro.

FTP

- Uma vez configurado o vsftpd pode-se dar início ao servidor.
- O seguinte comando pode ser utilizado para correr o servidor vsftpd:
 - **# systemctl start vsftpd**
- Note-se que os valores por padrão no arquivo de configuração são definidos como estão por razões de segurança.
- Cada uma das alterações anteriores torna o sistema um pouco menos seguro, pelo que só devem ser feitas se necessário.