## Pacote padrão usado pelo ftp é o Very Secure FTP Deamon (vsftpd).

## Pacote para configuração de servidor de e-mail usado pelo Fedora (sendmail), pelo rhel (postfix) e há também o exim.

## Pacote do servidor web apache é o httpd.

## Pacote para servidor de impressão é o cups.

## Pacote para o Windows File Server é o samba.

## Pacote usado para NFS é nfs-utils.

## Pacote para servidor de DNS é o bind.

## Pacote usado para servidor NTP é o ntpd.

## systemd é o responsável por gerenciar serviços, usado no Fedora e Ubuntu, e System V no RHEL.

## O xinetd tem por principal função carregar serviços/deamon somente quando necessários, era muito utilizado antigamente quando a memória ainda era cara.

## Algumas dicas de segurança:

- Nao permitir login direto como root

- Restringir portas através de firewall

- Utilizar TCP Wrappers e adicionar os hosts/ip que podem acessar no arquivo /etc/hosts.allow e /etc/hosts/deny. Pacote usado é libwrap

- SELinux (Security Enhanced Linux) aumenta a segurança garantindo que os serviços acessem apenas o conteúdo apontado nos arquivos de configuração.

- Nos próprios arquivos de configuração dos serviços.

## O recurso sar (disponível no pacote sysstat) observa atividades no sistema, memória, cpu, etc. Sendo executado 24 horas de minutos em minutos.

## chkconfig é usado para definir serviços de inicialização ou status de serviço no rhel. ex chkconfig ssh on (habilita o sshd para iniciar automáticamente)

## observações SSH

- Quando acessamos um servidor remotamente, recebemos uma chave pública do servidor e é armazenada dentro de .ssh/know\_hosts.

- A opção PermitRootLogin informa se é permitida a conexão via ssh como usuário root.

- executando comandos remotos. ex ssh root@10.10.10.10 "cat /etc/hosts" ou localhost. Para espaços é necessário usar aspas.

- A opção X11Forwarding habilita a utilização de interfaces gráficas em conexões remotas, para isso a conexão deve ser feita usando ssh -X.

## rsync = Comando utilizado para realização de backup, espelhamento, similar ao scp, porém ele avalia se já existe o arquivo igual no lugar, e caso positivo não sobrescreve.

ex; rsync -avl /usr/share/man/man1 localhost:/tmp/ (copia o conteúdo do diretório man1 para o /tmp/ da máquina local)

rsync -avl --delete usuario@10.10.10.10:/usr/share/man/man1 /tmp/ (espelha as duas bases, caso no diretório local tenha algum arquivo a mais que o diretório remoto, será excluído.

## sftp = Usado para transferência de arquivos, a diferença entre o sftp e o ftp é que a transmissão via sftp é criptografada. ex; sftp [usuario@sftp.exemplo.com](mailto:usuario@sftp.exemplo.com) .

get e put são usados para enviar e pegar os arquivos.

## ssh-keygen = Gera uma chave pública e privada, a privada fica armazenada no servidor local e a publica enviada para o host remoto. Com isso é possível fazer autenticação em um servidor remoto sem autenticar com uma senha (senha de rede por exemplo).

ex; ssh-keygen (suponha que foi gerado dentro de ~/.ssh/id\_rsa e id\_rsa.pub)

ssh-copy-id -i ~/.ssh/id\_rsa.pub usuario@192.0.0.7

## rsyslog = Responsável pelo gerenciamento de logs do sistema, com ele é possível enviar os logs de um servidor local para um servidor remoto. Para configurar o rsyslog enviando logs para um servidor remoto, primeiro temos que editar o arquivo /etc/rsyslog.conf no cliente adicionando um @servidordelogoremoto e no lado servidor habilitar a coleta de informações /etc/sysconfig/rsyslog. Feito isso reniciar o serviço do rsyslog e checar se o iptables permite a conexão na porta definida,a padrão é a 514.

## logwatch = Serviço de envio dos logs coletados no sistema por e-mail.