Lista 3 - Treinamento Rede GNU/Linux

Juliano Garcia de Oliveira Nº USP: 9277086

26 de Janeiro, 2017

Resolução dos exercícios

Servidores

1. O NIS é um sistema de administração e similar ao DNS, que possibilita que todos os computadores de uma rede possa acessar configurações comuns para toda a rede, centralizando o trabalho para o *host* principal. O LDAP é similar, porém é um protocolo que especifica como acessar e procurar informações em um servidor, basicamente. Por exemplo, uma rede tem 10 usuários, e será adicionado um novo usuário. Ao invés de atualizar a informação de login do novo usuário em todos os computadores da rede manualmente, usando o NIS ou o LDAP basta atualizar as informações no servidor do serviço (NIS ou LDAP). Na rede linux, e em redes de tamanho médio ou até de grande porte, o LDAP é melhor que o NIS. Enquanto o NIS é mais simples e funciona bem em LAN's pequenas, o LDAP permite uma organização melhor de informações, o *namespace* é hierárquico e a busca de informações é mais rápida e intuitiva através dos filtros que o protocolo especifica. As informações completas dos usuários de uma rede armazenados em um banco de dados central pode ser acessado e controlado através do LDAP, facilitando a consulta e a obtenção das informações.

2. O Kerberos é um protocolo de autenticação em rede, que funciona através da autenticação e troca de *tickets* entre um cliente e um serviço. O Kerberos autentica e distribui as chaves de acesso e posteriormente um *ticket* que permite um determinado cliente / usuário fazer solicitações para um determinado serviço da rede. A utilização do Kerberos em uma rede (como na Rede Linux) aumenta a segurança e simplifica várias operações e configurações. Como o Kerberos trata da autenticação através de *tickets*, ao invés de configurar manualmente quais usuários tem permissão para usar um determinado serviço, basta configurar no Kerberos, e a configuração será replicada por toda a rede. Como os acessos e identificação de um usuário funcionam a partir de um *ticket* de acesso, o usuário não precisa ficar digitando a senha a cada serviço diferente que precisa usar, simplificando tanto para o usuário tanto para os administradores da rede que podem gerenciar os usuários e os acessos de um modo mais simples.

3. NFS é um protocolo que especifica como é feito o acesso de arquivos por usuários em uma rede. O servidor NFS dispõe de ferramentas que permitem montar discos e/ou diretórios na rede, e exportando certos diretórios para que sejam acessíveis remotamente na rede linux. As alternativas variam de acordo com a rede em questão, sendo que em uma rede que inclua computadores Windows é bastante usado o SAMBA.

4. Apache é um servidor *web* HTTP. Basicamente o *Apache* recebe requisições em HTTP, analisa as requisições verificando integridade / segurança da requisição, e devolve uma página web ,por exemplo, caso essa tenha sido a requisição. O Apache também possui vários módulos para interpretação de diferentes linguagens, por exemplo o *php*, que é *server-side* e funciona com o *Apache*.

5. O mais comum e recomendado no linux é instalar o CUPS, que é o sistema que gerencia e controla a impressão. Ele usa o protocolo IPP, que permite compartilhamento de impressora e impressão em uma rede. Com o CUPS, basta adicionar a impressora como um certo IP na rede e configurar o CUPS para permitir a impressão e o compartilhamento nos IP's corretos (o CUPS por padrão só permite a *loopback* e o 127.0.0.1).

6. SMTP, POP e IMAP são protocolos que tratam do envio de *emails*. O SMTP especifica como é feita a transmissão de *emails*, que está na *layer* do TCP/IP. O POP e o IMAP são protocolos similares que tratam do processo do destinatário receber os *emails*, por causa der algumas limitações do SMTP. Na sua versão mais recente, o protocolo POP cria cópias locais dos *emails* do usuário e os deleta do servidor de *email*. Já o IMAP mantém os *emails* em um sevidor remoto (não localmente), o que permite que o mesmo usuário entre em diferentes provedores de *emails* e consiga ver os mesmos *emails*, até que sejam deletados pelo usuário.

7. SSL é um protocolo de segurança que cria um canal seguro de transmissão na internet ou em uma outra rede qualquer. O SSL faz a encriptação dos dados transmitidos através da rede, que só podem ser decriptados pelo destinatário dos dados que foram transmitidos. É importante pois aumenta a segurança, se não houvesse o SSL o risco de alguém conseguir senhas, números de cartões de crédito e outras informações credenciais seria alta já que o atacante poderia tentar obter esses dados capturando os pacotes transmitidos, sendo que ao usar SSL os pacotes estariam encriptados, e o atacante não conseguiria visualizar as informações (se não tivesse a chave pra descriptação).

Arquivos e Disco

1. O comando *fsck* é usado para verificar a consistência de arquivos do sistema (no linux é o *filesystem(ext2)*), além de fazer reparos. É bastante utilizado pra tentar recuperar sistemas linux que estão corrompidos, ou algum problema relacionado com o disco.

2. RAID 0 possui um foco na performance, já que ao fazer a escrita dos dados uniformemente em todos os arquivos do *array*, a escrita dos dados é mais rápida. Porém como não possui redundância, se um disco do *array* falhar, todos os dados são perdidos. Já o RAID 1 escreve a mesma informação em todos os discos do *array*, e essa redundância garante que não há perda de informação se um disco falhar. Mas é claro, como ao invés de escrever em um disco no RAID 1 se escreve em todos, a performance é menor.