MAC5715 - Descrição do padrão FDP para arquiteturas de rede baseados em Sistemas GNU/Linux

Alex Pires de Camargo

2 de outubro de 2002

Este padrão teve ajuda do documento FDP (**F**DP **D**ocumentation **P**roject), meu trabalho de formatura no BCC, em conjunto com meus colegas Livio Baldini Soares e Rafael Caetano dos Santos, em dezembro de 1999. A motivação deste trabalho de formatura era documentar, para os futuros administradores, a organização da rede, procedimentos de manutenção, e políticas de administração e segurança da rede. Nesse padrão, foi integralmente elaborado um novo texto restrito apenas a estrutura da rede, a nível de distribuição de serviços e alocação de recursos à disposição do usuário.

1 Problema

Montar um ambiente de rede, baseados num sistema Gnu/Linux, para usuários executarem tarefas do dia a dia. Entre as mais comuns:

- Navegação pela Web
- Desenvolvimento de projetos acadêmicos
- Digitação de textos em latex

A única infra-estrutura oferecida pelo ambiente onde a rede será instalada é a infra-estrutura de cabeamento e pontos de rede para servidores e clientes, e um ip fixo, com sua máscara de rede e roteador padrão, bem como um serviço de DNS onde esse ip deverá estar registrado.

2 Solução

Todos os serviços serão baseados em arquitetura cliente-servidor. Dividiremos a especificação do padrão entre servidoes e clientes.

2.1 Servidores

Dado que essa rede deverá prover quase todos os serviço básicos (roteamento por mascaramento, mail, dns) além dos serviços referentes aos dados de usuário e disponibilidade de software, é necessário otimizar a distribuição destes serviços entre várias máquinas. Um maior número de máquinas pode aumentar o desempenho destes serviços, mas dificultar as tarefas de manutenção e monitoramento, bem como custo de implantação. O grau de divisão de carga de serviços nos servidores depende muito de demanda de cada serviço, que pode diferenciar de uma implantação de rede para outra.

2.1.1 Roteador com firewall

No intuito de economizar ips, recurso nem sempre farto, bem como isolar os clientes da rede de ataques externos, todo acesso a hosts fora da rede interna será feito por este servidor. Ele fará o roteamento dos pacotes oruindos da rede interna para fora, mascarando os ip's de origem com o seu, e desfazendo o processo no pacote de resposta. Ele também fará a filtragem de pacotes que passam de dentro pra fora de rede (e vice-versa), para aumentar a segurança dos serviços pela rede oferecidos.

Nesta máquina rodará também uma parte do servidor de emails. A parte que 'conversa' com a rede externa, recebendo email de fora pra dentro e enviando emails de dentro pra fora. Seria uma camada de isolação do sistema de emails do ambiente exterior a rede. Com isso, além da segurança, uma eventual lentidão na entrega de emails externos não comprometeria a entrega dos emails internos, já que os servidores de emails mais populares e principalmente o mais recomendado (qmail) trabalham em esquemas de fila única de email.

2.1.2 Servidor de Disco (homes), nis e email local

Esta máquina ficará encarregada de parte dos serviços servidos ao ambiente interno da rede. Começando por um servidor de nomes, baseados em nis (Network Information Server), que cuidará de distribuir aos clientes informações do tipo logins, senhas, grupos de usuários e grupos de máquinas. As senhas ficam guardadas criptografadas, e distribuídas aos clientes de forma que só os roots locais tenham acesso a estas. O serviço de email principal ficará nessa máquina.

Estar na mesma máquina dos discos tem a vantagem de uma entrega rápida de emails, mas dependendo dos filtros de email aplicados, pode haver uma degradação total no sistema. Sistemas como o qmail permitem que o usuário defina seus próprios filtros de emails, o que torna a máquina suscetível a falta de cuidado ou má intenção dos usuários. O sistema de entrega de email deverá ser connfigurado de tal forma que emails para hosts fora da rede sejam enviados ao roteador, que tem a parte do sistema de correio eletrônico encarregado de fazer a entrega de mail remotos.

Os homes, áreas com os arquivos pessoais dos usuários, deverão ficar nesta máquina. Um servidor nfs deverá estar rodando para exportar o diretório de homes para os clientes.

Nesta máquina deve-se confeccionar e usar scripts de abertura e fechamento de contas. Scripts desse tipo devem no mínimo mexer em áreas de usuários e arquivos do nis e servidor de email, portanto ter todos esses serviços em uma máquina só é uma característica que tende a facilitar a confecção e manutenção desses scripts.

2.1.3 Servidor de software na rede, Web, Impressão

Os outros serviços disponíveis da rede ficarão nesta máquina. Um servidor web (Apache), para disponibilizar as páginas da rede e dos usuários, com definidas políticas de uso de recursos como cgi e php. Essa máquina não terá um ip real na Internet, portanto a porta 80 do roteador deve ser redirecionada para a porta oitenta desta máquina. Nesta máquina pode ser colocado o serviço de software distribuído pela rede, normalmente software que não se encotra nos clientes. Pelos padrões de hierarquia do sistema de arquivos do Linux, esse diretório deve ser montado como /usr/local nos clientes. Outros serviços mais leves, como servidor de impressão e ntp (Network Time Protocol), devem ser instalados e configurados nesse servidor.

2.2 Clientes

Os clientes da rede são máquinas com praticamente todo software disponível instalado localmente. Aqui é importante frisar que o poder computacional disponível está no cliente, pois os usuários não terão acesso aos recursos de processamento dos servidores. Portanto as máquinas devem ser razoavelmente potentes e com um bom espaço em disco disponível. Elas montarão um diretório com um pouco de software e os arquivos pessoais dos usuários. É necessário ter cuidado com a segurança nos clientes. Um root local pode ter acesso a alguns dados de usuários e deixar programas maliciosos rodando escondidos. Como o acesso físico as máquinas é possível, se tornar root num cliente pode ser uma tarefa não muito difícil de se executar. É importante ter-se um sistema de execução de comandos em todos os clientes a partir de um servidor. Um script que usa chaves públicas e privadas de ssh pode cuidar disso, com muito cuidado na distribuição dessas chaves. Isso é vital para manutenção da homogeneidade dos clientes principalmente no que se refere a instalação de software nas máquinas e alterações emergenciais de segurança.

3 Conseqüências

Esse tipo de estrutura tem seus prós e contras, e deve-se levar em conta alguns fatores antes de sua implementação. Coisas a se preocupar:

- **Monitoramento do acesso as máquinas.** Como o acesso físico ao cliente pode facilitar uma tentativa de ganhar privilégios de super usuário na máquina, o ideal é que as máquinas estejam em um ambiente de laboratório, por onde várias pessoas circulam. Estações isoladas em salas de acesso restrito podem dar chance a um usuário mal intencionado de poder abrir a máquina, apagar a BIOS, dar um boot por disquete e trocar a senha de root da estação. O autor do padrão ainda não conhece um bom esquema de autenticação que evitaria um root no cliente se transformar em qualquer usuário e ter acesso a seus arquivos.

- **Custo de manutenção.** Dependendo da complexidade de um cliente pode-se demorar um bom tempo até fazer uma nova instalação. E eventuais problemas de hardware podem deixar clientes parados por um bom tempo. Como o custo dos clientes não é baixo, pode ser difícil ter máquinas a disposição. Aqui mais uma vez mostra-se que o ambiente ideal para essa estrutura é um laboratório, onde o usuário tem a sua disposição vários clientes.

- **Atualizações.** Para facilitar as atualizações o crucial é usar uma distribuição que facilite essa tarefa, principalmente nos servidores. Existe distribuições, como a Debian, que possibilitam upgrades com as máquinas em uso, sem que a rede praticamente não sinta as coisas acontecendo.

- **Hardware dos clientes.** Sobre os clientes já foi comentado o suficiente. Como eles serão o recurso de processamento a disposição dos usuários, só é necessário saber o que esses usuários precisam nesse sentido. Se preocupar com a compatibilidade do hardware usado com a versão do kernel do Linux a ser utilizada (a distribuição passa essa informação, mas sempre é possível ter um kernel específico para os clientes da rede).

- **Hardware dos servidores.** Robutez é importante. As máquinas não precisam ser mais rápidas que os clientes, mas hardware de boa qualidade é muito importante.

  - Gateway: Provavelmente será a máquina mais lenta da rede. Um Pentium 200 consegue tranquilamente lidar com uma banda de 100Mbps, sem ter que tomar muitas decisões de roteamento, que é o caso desta arquitetura. Relembrando, o importante é ter um equipamento robusto.
  - Servidor de Disco: O importante aqui é ter um acesso rápido a rede, discos bem dimensionados e rápidos. Memória é importante, para manter bastante coisa em cache, otimizando o acesso a esses discos. Discos extras para redundâncias (RAID), equipamentos de backup.
  - Servidor de software na rede, Web, backup. Mais uma vez, uma máquina com processamento a nível de um cliente médio cuidará dos serviços. Reafirmando, robustez é importante.