A *Linuxização* do Departamento de Informática da Universidade do Minho

Grupo de Sistemas Distribuídos*

Departamento de Informática, Universidade do Minho

Largo do Paço, 4709 Braga Codex

`gsd@di.uminho.pt`
`http://gsd.di.uminho.pt/`

Resumo

O Departamento de Informática da Universidade do Minho sempre adoptou o Unix como a sua plataforma de referência. Neste último ano houve uma mudança para um novo edíficio, que levou à criação de vários novos laboratórios pedagógicos, de uma sala aberta aos alunos e ao reforço da infra-estrutura para investigação. Em todos estes casos, o sistema operativo adoptado para servidores é só um: Linux. Este texto descreve as vantagens e novas perspectivas que a adopção do Linux veio trazer, associada à introdução de um sistema de arranque remoto.

Uma Visita Imaginária

Para um aluno de outras universidades que se deslocasse ao Departamento de Informática da Universidade do Minho, estariam reservadas algumas surpresas …

Em primeiro lugar deparava-se com uma sala aberta em os alunos usam cerca de 15 computadores. Começaria por estranhar a ausência de funcionários: a sala e as marcações são geridas por duas organizações de alunos. Por outro lado poderia estranhar o facto de os computadores não parecerem estar divididos por sistema operativo. Há computadores em Linux e em Windows espalhados sem qualquer ordem aparente: *dual-boot* — poderia pensar o visitante — deve ter dado algum trabalho a instalar isto…

Numa observação mais atenta, outra surpresa... As máquinas que não estão em Linux correm Windows95! Não é NT! Como pode ser? E os vírus? E quando os alunos apagam os ficheiros do sistema? E se os alunos instalam jogos??? Toda a gente sabe que máquinas para alunos têm que estar em NT, devidamente protegidas, para que não sejam desconfiguradas ou contaminadas por cada aluno que as use. Mais desconcertado

*ajc,als,cbm,fsm,jop,jpo,psa,rco,vff

ainda ficaria o visitante ao reparar que toda a gente desliga as máquinas "à bruta", sem *shutdown*, e que ninguém se parece preocupar com isso.

Por fim, o supresa final... Se falasse com os utilizadores que escolhem Linux, o visitante verificaria que eles não se preocupam em descobrir a *password* dos outros utilizadores da sua máquina e muito menos a respectiva *password* de *root*. E têm boas razões para isso: em cada máquina só há conta para um utilizador, o próprio aluno. Quanto à *password* de *root*, não é preciso descobri-la, porque é bem conhecida: é a própria *password* do aluno.

Saindo desta sala, o nosso visitante encontraria mais três laboratórios que usam o mesmo sistema. A única diferença é que nestes são dadas aulas, mas o ambiente é o mesmo. Isto quer dizer que os alunos podem sair da aula e continuar o trabalho na sala aberta. Também podem ir para uma aula e continuar aquilo que estavam a fazer na sala aberta, desde que o professor não descubra, claro.

O Arranque Remoto

A explicação para a fábula anterior é simples: as máquinas podem estar sob completo controlo de cada aluno, porque quando vier um novo utilizador este encontrará uma máquina limpa, virgem, como que acabada de instalar. O utilizador anterior pode ter deixado vírus ou cavalos de tróia, pode ter apagado ficheiros importantes, formatado o disco, ou feito um *reset* à máquina sem *shutdown*. Nada disso importa. Para o aluno seguinte a máquina está impecável, e ele pode utilizá-la sem receio.

Este método baseia-se num sistema de arranque remoto inicialmente descrito em [2], e cuja aplicação específica nós descrevemos em [1]. As principais características deste sistema são as seguintes:

- cada posto de trabalho tem uma *boot-prom* que inicia uma sequência de arranque permitindo ao utilizador a escolha do sistema operativo que pretende;
- quando cada posto de trabalho arranca, aparece completamente "limpo", como se tivesse acabado se ser instalado, perfeitamente configurado e livre de vírus;
- cada computador tem um disco, mas este funciona apenas como armazenamento temporário, uma vez que todos os dados dos utilizadores residem num servidor remoto;
- cada utilizador pode usar qualquer dos postos de trabalho, independentemente do sistema operativo escolhido, e ter sempre acesso à sua área de trabalho residente num servidor;
- só podem utilizar os postos de trabalho os utilizadores que tenham conta no servidor.

Antes de mais, o utilizador deve introduzir o seu *login* e *password*, mesmo antes de haver sistema operativo na máquina. Se a autenticação fôr bem sucedida, aparece então um menu com várias opções:

- **Terminal X**: nesta opção é carregado um *kernel* Linux, que arranca sem usar o disco (NFS-root); Aparece um servidor X com uma janela que permite introduzir uma máquina, *login* e *passwd*, permitindo abrir uma sessão X na máquina especificada. Note-se que não se trata de uma sessão `xdm`, mas sim de um túnel `ssh`. Assim, não só resolve o problema de passar pela *firewall*, como se garante comunicação segura.
- **Linux novo**: nesta caso é criada uma partição nativa de Linux, para onde se

carrega uma imagem comprimida de um sistema pré-instalado. O Linux arranca e logo se activa uma sessão X em que aparece o ambiente pessoal do utilizador. Este não voltou sequer a fazer *login*! Basta o que fez antes de haver sistema operativo na máquina. Esta tem duas contas activas: a do próprio aluno e a *root*, com a mesma *password*.

- **Linux Usado**: aqui, apenas se tenta voltar a arrancar pelo mesmo sistema que já estava instalado. Só é util para o próprio, pois só ele sabe as *passwords*.
- **Windows Novo**: neste caso faz o mesmo que para o Linux novo, só que com Windows95. O utilizador faz *logon* e encontra a sua *home* montada como *drive* de rede.
- **Windows Usado**: esta opção só deve ser utilizada pelo mesmo utilizador que instalou esse Windows; é no entanto indispensável devido à tendência que esse sistema tem de exigir *reboots*, inesperados ou não.

Panorâmica da Rede de Laboratórios do DI

Actualmente quase todos os laboratórios do DI podem funcionar como sistemas de acesso público, organizando-se da forma que se pode observar na Figura 1, onde se destacam:

- o servidor de *boot*;
- os servidores de *software*;
- o servidor de áreas de trabalho;
- os *proxies* de HTTP/FTP.

Cada um dos grupos disciplinares do DI tem requisitos diferentes quanto ao *software* necessário à prossecução dos seus objectivos pedagógicos, o que levanta problemas no controlo de versões e na gestão do servidor de *boot* que passaria a ser administrado por diversas de pessoas.

De forma a satisfazer os requisitos de um sistema de acesso público e evitar um potencial problema de administração, distribuiu-se a cada grupo disciplinar um servidor. É neste que deve ser instalado o *software* necessário para assegurar o correcto funcionamento das aulas desse grupo disciplinar e que será posteriormente disponibilizado para qualquer dos laboratórios. Desta forma reduz-se o tamanho das imagens que o servidor de *boot* deve enviar para cada um dos clientes.

Cada utilizador pode durante a sua permanência num determinado posto de trabalho instalar e desinstalar os recursos de *software* que pretender, não compromentendo a configuração do sistema para o próximo utilizador dessa máquina.

A minimização das consequências de acções maliciosas é conseguida limitando a possibilidade de estabelecimento de ligações com outras máquinas através da Internet. Cada laboratório está isolado numa intranet, cujas ligações possíveis são efectuadas através de uma *firewall* que só permite acesso aos servidores de *software*, áreas de trabalho e *proxy* HTTP/FTP do DI.

As Contas dos Alunos

O Departamento de Informática da Universidade do Minho não é responsável por espaço em disco para os alunos, uma vez que existe uma entidade centralizada, o Centro de Informática (CI), que disponibiliza contas para os alunos, com direito a endereço de correio electrónico e a páginas WWW pessoais. Dispõe ainda de diversas salas equipadas com terminais X-Windows ou com computadores pessoais.

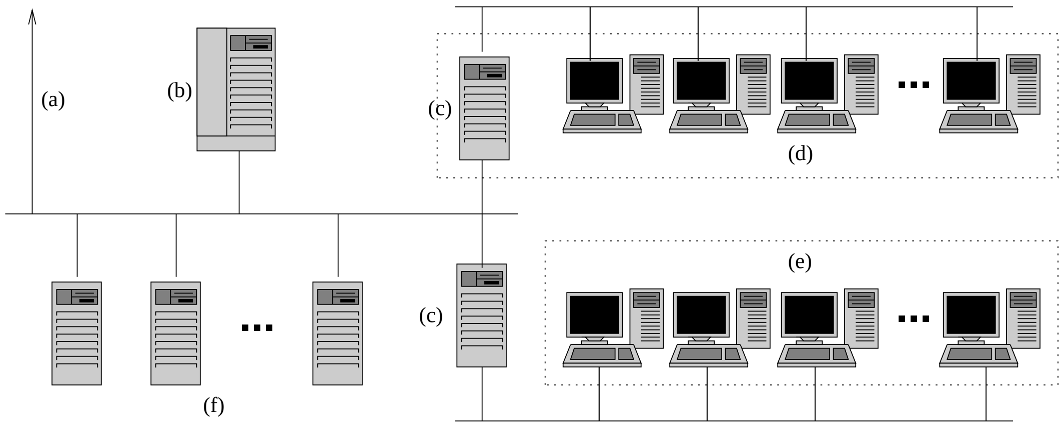

Figura 1: Arquitectura da rede de laboratórios de ensino do DI/UM. (a) Acesso ao exterior; (b) servidor de contas e áreas de trabalho; (c) servidores de *boot*, funcionando também como *firewalls* e *proxies* HTTP/FTP; (d) sala de aula, com o servidor à disposição do docente, para controlo de recursos; (e) sala aberta, com o servidor protegido; (f) servidores de *software* atribuídos aos grupos disciplinares.

Porém, como apoio aos laboratórios e à sala aberta do DI, foi necessário criar um serviço de áreas de trabalho de pequena dimensão para todos os alunos que usam essas instalações.

A solução é puramente baseada no Linux, apesar das contas serem exportadas tanto para clientes Linux como para clientes Windows. Note-se que em qualquer dos ambientes os alunos tem acesso à mesma àrea de trabalho e aos mesmos ficheiros.

Como é evidente, a solução para exportar para os clientes Windows é o `samba`. Talvez menos obviamente, para os clientes Linux a solução é a mesma. Aqui temos um servidor Linux a fingir que é um WindowsNT e um cliente Linux a fingir que é um Windows95, ambos usando um protocolo da Microsoft. Esta solução tem a vantagem de permitir a autenticação por utilizador. Por outro lado dá origem a alguns comportamentos menos adequados, pelo que estamos a pensar mudar para algo mais evoluído, como CODA.

A criação de contas no servidor é instantânea. Basta que o aluno traga o seu cartão de estudante, que é então passado num leitor de cartões. Um programa que desenvolvemos para o efeito consulta uma base de dados fornecida pelos Serviços Académicos, cria a conta no servidor e faz imprimir duas folhas com as regras de utilização. Uma das folhas é assinada e devolvida pelo aluno, a outra fica para ele. Nessa folha encontra-se uma *password* que apesar de gerada aleatoriamente é probabilisticamente parecida com uma palavra portuguesa, para ser mais fácil de memorizar.

O servidor de *boot*

Esta máquina é uma peça fundamental deste sistema, Desempenha várias funções:

- servidor de BOOTP/DHCP para atribuír endereços IP aos clientes;
- servidor de TFTP para fornecer as imagens dos sistemas operativos aos clientes;
- serve como *gateway*/*firewall*, uma vez que os laboratórios estão dentro de uma

rede virtual privada, da qual só se sai por *ip-masquerading*;

- exporta por NFS, só para leitura, as partes do sistema Linux adequadas a serem importadas desta forma (`/usr`, `/opt`);
- exporta por samba, só para leitura, as partes da instalação Windows que podem ser colocádas num *drive* de rede.

Conclusões

Todo o sistema anteriormente descrito funciona sem manutenção. Não há técnicos responsáveis por estas máquinas. Foram inicialmente configuradas pelos docentes do Grupo de Sistemas Distribuidos mas a partir daí o sistema têm-se mantido a si mesmo.

Isto só é possível graças à espantosa robustez do Linux. No servidor de *boot*, tal como no caso do servidor de contas, o Linux mostra-se plenamente à altura do desafio. Esta máquina é um simples PentiumII, e encontra-se a servir quase 60 clientes. Todos os dias serve centenas de arranques, e serve continuamente NFS e samba. Nunca fica sobrecarregado, e nunca teve um *crash*, estando ligado, numa sala fechada à chave, desde o dia em que foi levado para lá.

Também no que diz respeito aos custos, a opção pelo Linux tem um efeito notável: com máquinas relativamente baratas, de marca branca, resolvem-se problemas que com outras soluções custariam muito mais.

Por fim, com esta solução evita-se completamente o uso de WindowsNT, mesmo sem impedir que se use o ambiente Microsoft, nas versões Windows95/98. Muitas vezes o único motivo para usar NT nos postos de trabalho é para impedir os utilizadores de os deconfigurarem. Como nesta solução isso não é problema, não há qualquer motivo para não usar antes o Windows95/98, que até é mais familiar e flexível para a maior parte dos utilizadores. Em termos de licensas, isto faria uma diferença enorme nos custos da maior parte das organizações.

Referências

[1] António Coutinho, António Luís Sousa, Carlos Baquero, Francisco Moura, José Pedro Oliveira, and José Orlando Pereira. Broms: Gestão uniforme de um parque computacional multi-plataforma. *Ingenium*, 2(33):87–91, jan 1999. Revista da Ordem dos Engenheiros.

[2] Marc Vuilleumier Stückelberg, Sandro Viale, and David Clerc. Remote-boot HOWTO. http: //cuiwww.unige.ch/info/pc/remote-boot/howto.html, August 1997.