

# Virtualização e Alta Disponibilidade

## Caso Prático Gil

Luciano Rocha  
Nuno Carvalho

Grupo de Investigação de Linux  
Departamento de Informática  
Universidade do Minho

<http://gil.di.uminho.pt/membros/strange/opcao3/>

23 de Fevereiro de 2005



# Introdução

- 1 Motivações
- 2 Objectivos
  - Sistema base funcional
  - Paravirtualização
  - Replicação de Dados
  - Monitorização e Migração
  - Serviços Visíveis
  - Administração Centralizada
  - Cópias de Segurança
- 3 Solução Final
  - Rede
- 4 Problemas
- 5 Conclusão e Futuro
  - Conclusão
  - Futuro
- 6 Discussão



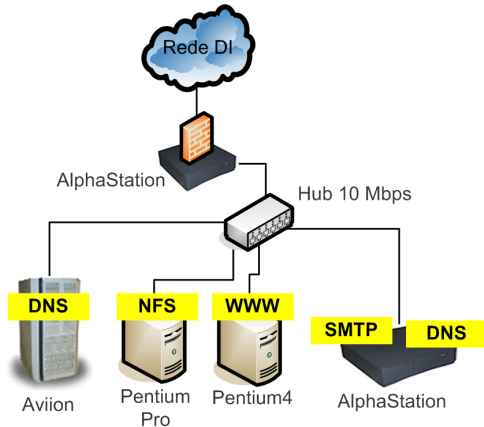
# Motivações

## Deficiências existentes

- problemas de *hardware*
- interdependências não satisfeitas
- software desatualizado
- problemas logísticos
- dados inseguros

## Novas necessidades

- aproveitar novo *hardware*
- acomodar novos projectos



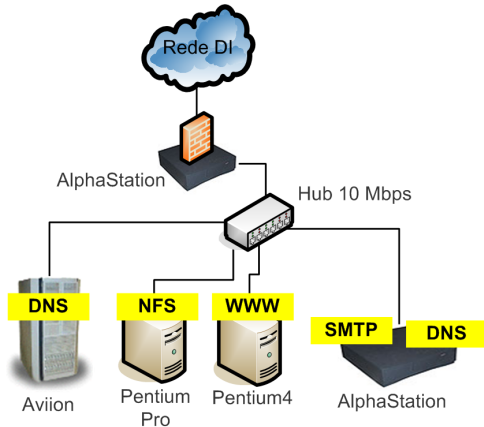
# Motivações

## Deficiências existentes

- problemas de *hardware*
- interdependências não satisfeitas
- software desatualizado
- problemas logísticos
- dados inseguros

## Novas necessidades

- aproveitar novo *hardware*
- acomodar novos projectos



# Sistema base funcional

## Objectivos

- sistema actual
- de fácil administração
- e nosso conhecido

## Fedora Core 3

- *LVM*  
Flexibilidade na alocação de espaço  
Alteração dinâmica sem interrupção de serviço
- *Ext3*  
Sistema de ficheiros *journalled*  
Alteração de tamanho com manutenção dos dados
- *Yum*  
Instalação e administração de pacotes simplificada



Turing



Knuth



# Sistema base funcional

## Objectivos

- sistema actual
- de fácil administração
- e nosso conhecido

## Fedora Core 3

- *LVM*  
Flexibilidade na alocação de espaço  
Alteração dinâmica sem interrupção de serviço
- *Ext3*  
Sistema de ficheiros *journalled*  
Alteração de tamanho com manutenção dos dados
- *Yum*  
Instalação e administração de pacotes simplificada



Turing



Knuth



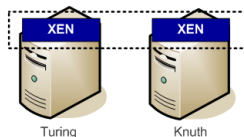
# Paravirtualização

## Objectivos

- criação e integração facilitada de novos sistemas
- garantias de performance, isolamento e segurança

## Xen

- virtualiza o hardware
- baixo impacto de performance
- controle de recursos - memória e processador
- permite guardar e recuperar, ou migrar, as máquinas virtuais
- não restrito a Linux ou x86.



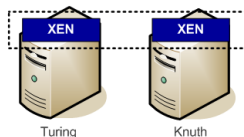
# Paravirtualização

## Objectivos

- criação e integração facilitada de novos sistemas
- garantias de performance, isolamento e segurança

## Xen

- virtualiza o hardware
- baixo impacto de performance
- controle de recursos - memória e processador
- permite guardar e recuperar, ou migrar, as máquinas virtuais
- não restrito a Linux ou x86.





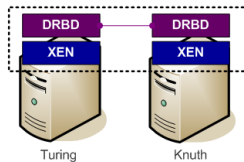
# Replicação de Dados

## Objectivos

- replicação contínua da informação vital

## DRBD

- replicação de um dispositivo de armazenamento via rede
- sincronismo garantido
- desempenho adequado



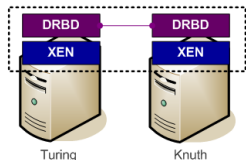
# Replicação de Dados

## Objectivos

- replicação contínua da informação vital

## DRBD

- replicação de um dispositivo de armazenamento via rede
- sincronismo garantido
- desempenho adequado



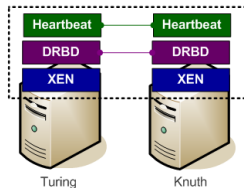
# Monitorização e Migração

## Objectivos

- monitorização da *liveness* das réplicas
- migração em caso de falhas

## Heartbeat

- monitorização via vários canais de comunicação
- verificação de disponibilidade a vários níveis
- reagir a mudanças de estado
- *scripts* próprias para a solução
  - mudança para nodo primário *DRBD*
  - activação dos volumes partilhados
  - arranque das máquinas virtuais



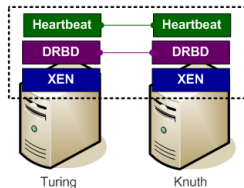
# Monitorização e Migração

## Objectivos

- monitorização da *liveness* das réplicas
- migração em caso de falhas

## Heartbeat

- monitorização via vários canais de comunicação
- verificação de disponibilidade a vários níveis
- reagir a mudanças de estado
- *scripts* próprias para a solução
  - mudança para nodo primário *DRBD*
  - activação dos volumes partilhados
  - arranque das máquinas virtuais



# Serviços Visíveis

## Objectivos

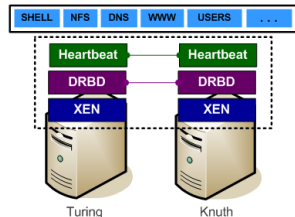
- fornecimento de serviços fundamentais
- migrar serviços existentes para a nova base

## Sistemas hóspedes

- Debian

```
debootstrap -arch i386 sid /mnt
http://.../debian
```
- Fedora Core

```
yum -installroot=/mnt -y groupinstall Base
```



# Serviços Visíveis

## Objectivos

- fornecimento de serviços fundamentais
- migrar serviços existentes para a nova base

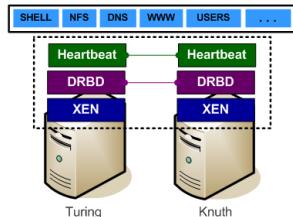
## Sistemas hóspedes

- Debian

```
debootstrap -arch i386 sid /mnt  
http://.../debian
```

- Fedora Core

```
yum -installroot=/mnt -y groupinstall Base
```



# Administração Centralizada

## Objectivos

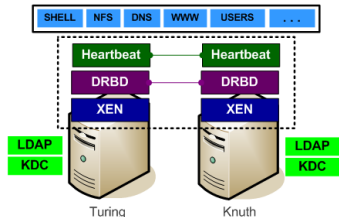
- centralização da informação para os vários serviços
- redução de etapas de administração
- manutenção facilitada

## LDAP

- serviço de directorias extensível
- suportado por vários serviços
- informação centralizada

## Kerberos

- *Single Sign-On*
- autenticação mútua
- integração com *NFSv4*



# Administração Centralizada

## Objectivos

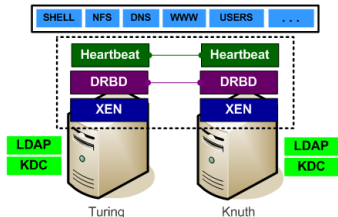
- centralização da informação para os vários serviços
- redução de etapas de administração
- manutenção facilitada

## LDAP

- serviço de directorias extensível
- suportado por vários serviços
- informação centralizada

## Kerberos

- *Single Sign-On*
- autenticação mútua
- integração com *NFSv4*





# Administração Centralizada

## Objectivos

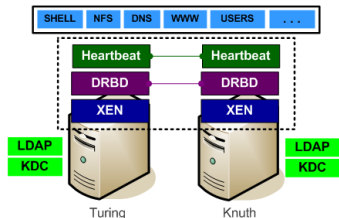
- centralização da informação para os vários serviços
- redução de etapas de administração
- manutenção facilitada

## LDAP

- serviço de directorias extensível
- suportado por vários serviços
- informação centralizada

## Kerberos

- *Single Sign-On*
- autenticação mútua
- integração com *NFSv4*



# Cópias de Segurança

## Objectivos

- garantir a contínua disponibilidade dos dados
  - contra falhas humanas
  - contra falhas catastróficas

## Metodologia

- 1 exportar uma imagem cifrada usando o GNBD
- 2 gravar as alterações usando o rdiff-backup
- 3 gravar a imagem em DVD-ROM

## Políticas

- cópia incremental diária
- cópia total quinzenal



# Cópias de Segurança

## Objectivos

- garantir a contínua disponibilidade dos dados
  - contra falhas humanas
  - contra falhas catastróficas

## Metodologia

- 1 exportar uma imagem cifrada usando o GNBD
- 2 gravar as alterações usando o rdiff-backup
- 3 gravar a imagem em DVD-ROM

## Políticas

- cópia incremental diária
- cópia total quinzenal



# Cópias de Segurança

## Objectivos

- garantir a contínua disponibilidade dos dados
  - contra falhas humanas
  - contra falhas catastróficas

## Metodologia

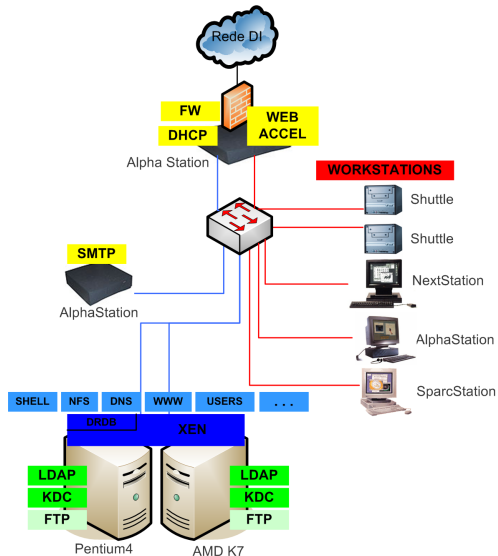
- 1 exportar uma imagem cifrada usando o GNBD
- 2 gravar as alterações usando o rdiff-backup
- 3 gravar a imagem em DVD-ROM

## Políticas

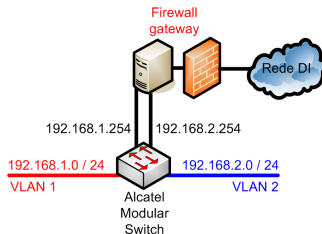
- cópia incremental diária
- cópia total quinzenal



# Solução Final



# Segmentos de Rede



- Para maior segurança a rede foi segmentada utilizando uma tecnologia de *VLANs*
- Todo o acesso passa pela *firewall*, quer tráfego entre o DI, como tráfego entre as *VLANs*
- Redirecionamento utilizando *iptables* e *web accelerator*



# Mapeamento Entre Portas e Endereços IP

Reencaminhamento de novas ligações:

## A nível 3

Porta	Serviço	Destino	Máquina
53	DNS	192.168.1.2	intsrv
25	SMTP	192.168.1.1	mail
22	SSH	192.168.1.18	shell
20	FTP [data]	192.168.1.17	ftp
21	FTP [control]	192.168.1.17	ftp

## A nível 7

- *Squid* para tráfego HTTP



# Mapeamento Entre Portas e Endereços IP

Reencaminhamento de novas ligações:

## A nível 3

Porta	Serviço	Destino	Máquina
53	DNS	192.168.1.2	intsrv
25	SMTP	192.168.1.1	mail
22	SSH	192.168.1.18	shell
20	FTP [data]	192.168.1.17	ftp
21	FTP [control]	192.168.1.17	ftp

## A nível 7

- *Squid* para tráfego HTTP





# Problemas Encontrados (e Resolvidos)

## Interoperabilidade

- Instabilidade de DRBD sob o Xen
- A versão de OpenLDAP distribuída no FC3 depende de TLS/Futex, incompatível com o Xen

## Logísticos

- Foi necessário manter sempre parte do sistema a funcionar, limitando a acessibilidade
- Antiguidade de alguns sistemas em uso tornou difícil encontrar componentes e versões de software para esses sistemas



# Problemas Encontrados (e Resolvidos)

## Interoperabilidade

- Instabilidade de DRBD sob o Xen
- A versão de OpenLDAP distribuída no FC3 depende de TLS/Futex, incompatível com o Xen

## Logísticos

- Foi necessário manter sempre parte do sistema a funcionar, limitando a acessibilidade
- Antiguidade de alguns sistemas em uso tornou difícil encontrar componentes e versões de software para esses sistemas



# Conclusão

## Obteve-se uma infra-estrutura dinâmica

- Máquinas virtuais
- Servidores redundantes
- Informação replicada

## Serviços já disponíveis

- |         |                          |
|---------|--------------------------|
| 1 dns   | 5 e-mail                 |
| 2 www   | 6 ldap e kerberos        |
| 3 shell | 7 firewall               |
| 4 ftp   | 8 <i>web accelerator</i> |



# Conclusão

## Obteve-se uma infra-estrutura dinâmica

- Máquinas virtuais
- Servidores redundantes
- Informação replicada

## Serviços já disponíveis

- |         |                          |
|---------|--------------------------|
| 1 dns   | 5 e-mail                 |
| 2 www   | 6 ldap e kerberos        |
| 3 shell | 7 firewall               |
| 4 ftp   | 8 <i>web accelerator</i> |



## Possíveis melhoramentos

- exportação das máquinas virtuais
- monitorização e migração de carga
- exportação da informação pessoal via Internet
- implementação de IPv6





Questões?

