Recuperação de Desastres Facilitada

Recuperação de Desastres Facilitada

ou

Seguro contra perda total bom, bonito (não muito) e barato!

Recuperação de Desastres Facilitada

ou

Seguro contra perda total bom, bonito (não muito) e barato!

Danton Nunes, engenheiro e encrenqueiro
danton.nunes@inexo.com.br

Estudo de caso de replicação da infraestrutura de TI de uma empresa usando um datacenter remoto e a Internet.

Estudo de caso de replicação da infraestrutura de TI de uma empresa usando um datacenter remoto e a Internet.

Queremos mostrar que ter um mecanismo de retomada dos negócios em caso de desastre no CPD principal pode estar ao alcance de empresas pequenas e médias e mesmo de pessoas físicas cujo trabalho depende da integridade de seus recursos de TI (profissionais liberais, artistas, espiões, ...).

Estudo de caso de replicação da infraestrutura de TI de uma empresa usando um datacenter remoto e a Internet.

Queremos mostrar que ter um mecanismo de retomada dos negócios em caso de desastre no CPD principal pode estar ao alcance de empresas pequenas e médias e mesmo de pessoas físicas cujo trabalho depende da integridade de seus recursos de TI (profissionais liberais, artistas, espiões, ...).

Orquestração de tecnologias:

- **Redes virtuais privativas (VPNs);**
- **Replicação em tempo quase real;**
- **Virtualização de servidores.**
- **Volumes lógicos, especialmente retratos instantaneos.**

Estudo de caso de replicação da infraestrutura de TI de uma empresa usando um datacenter remoto e a Internet.

Queremos mostrar que ter um mecanismo de retomada dos negócios em caso de desastre no CPD principal pode estar ao alcance de empresas pequenas e médias e mesmo de pessoas físicas cujo trabalho depende da integridade de seus recursos de TI (profissionais liberais, artistas, espiões, ...).

Orquestração de tecnologias:

- **Redes virtuais privativas (VPNs);**
- **Replicação em tempo quase real;**
- **Virtualização de servidores.**
- **Volumes lógicos, especialmente retratos instantaneos.**

IMPORTANTE: replicação não substitui o bom e velho BACKUP!

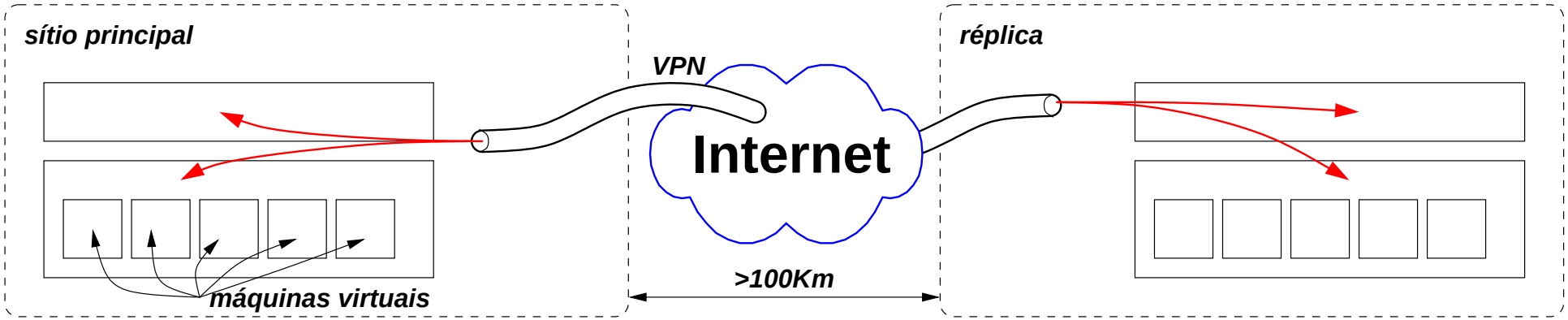
Estudo de caso de replicação da infraestrutura de TI de uma empresa usando um datacenter remoto e a Internet.

Queremos mostrar que ter um mecanismo de retomada dos negócios em caso de desastre no CPD principal pode estar ao alcance de empresas pequenas e médias e mesmo de pessoas físicas cujo trabalho depende da integridade de seus recursos de TI (profissionais liberais, artistas, espiões, ...).

Orquestração de tecnologias:

- **Redes virtuais privativas (VPNs);**
- **Replicação em tempo quase real;**
- **Virtualização de servidores.**
- **Volumes lógicos, especialmente retratos instantaneos.**

IMPORTANTE: replicação não substitui o bom e velho BACKUP!



Tecnologia: Rede Virtual Privativa (VPN)

Por que VPN?

Tecnologia: Rede Virtual Privativa (VPN)

Por que VPN?

- O protocolo de replicação segue o paradigma "peer−to−peer" e não o mais comum cliente−servidor;

Tecnologia: Rede Virtual Privativa (VPN)

Por que VPN?

− O protocolo de replicação segue o paradigma "peer−to−peer" e não o mais comum cliente−servidor;

− A rede da empresa tem acesso à Internet por um desses serviços GPON com CGNAT (Carrier Grade Network Address Translation), que não permite protocolos "peer−to−peer";

Tecnologia: Rede Virtual Privativa (VPN)

Por que VPN?

− O protocolo de replicação segue o paradigma "peer−to−peer" e não o mais comum cliente−servidor;

− A rede da empresa tem acesso à Internet por um desses serviços GPON com CGNAT (Carrier Grade Network Address Translation), que não permite protocolos "peer−to−peer";

− A VPN garante privacidade por causa da criptografia e também oferece compressão de dados, aumentando a banda passante efetiva.

Tecnologia: Rede Virtual Privativa (VPN)

Por que VPN?

− O protocolo de replicação segue o paradigma "peer−to−peer" e não o mais comum cliente−servidor;

− A rede da empresa tem acesso à Internet por um desses serviços GPON com CGNAT (Carrier Grade Network Address Translation), que não permite protocolos "peer−to−peer";

− A VPN garante privacidade por causa da criptografia e também oferece compressão de dados, aumentando a banda passante efetiva.

Solução encontrada: openvpn!

pode não ser a coisa mais bonita ou elegante do universo, mas o canal é cifrado, tem compressão, e, o mais importante, ATRAVESSA CGNAT!

Tecnologia: Virtualização

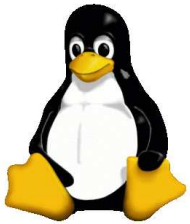
Tecnologia: Virtualização

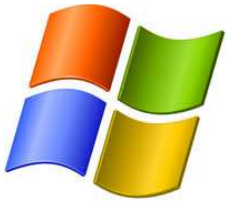
Os servidores usados na empresa são máquinas virtuais que rodam em hospedeiros Linux com qemu−kvm.

Tecnologia: Virtualização

Os servidores usados na empresa são máquinas virtuais que rodam em hospedeiros Linux com qemu−kvm.

Há máquinas de vários sabores:

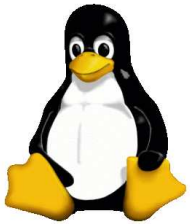


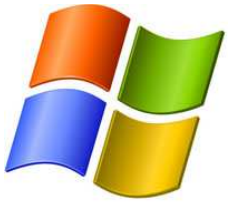


Tecnologia: Virtualização

Os servidores usados na empresa são máquinas virtuais que rodam em hospedeiros Linux com qemu−kvm.

Há máquinas de vários sabores:



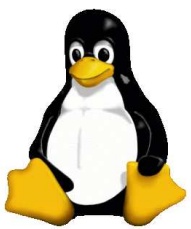


Há sistemas legados que não tem a menor ideia de que se trata replicação.

Tecnologia: Virtualização

Os servidores usados na empresa são máquinas virtuais que rodam em hospedeiros Linux com qemu−kvm.

Há máquinas de vários sabores:



Há sistemas legados que não tem a menor ideia de que se trata replicação.

Nesse cenário faz muito mais sentido replicar os volumes dos hospedeiros do que dos hóspedes, pois não há necessidade de alterar qualquer coisa neles.

Tecnologia: Virtualização

Os servidores usados na empresa são máquinas virtuais que rodam em hospedeiros Linux com qemu−kvm.

Há máquinas de vários sabores:

Há sistemas legados que não tem a menor ideia de que se trata replicação.

Nesse cenário faz muito mais sentido replicar os volumes dos hospedeiros do que dos hóspedes, pois não há necessidade de alterar qualquer coisa neles.

sistemas legados →

Tecnologia: Replicação

Tecnologia: Replicação

Neste caso empregamos o DRBD, da empresa austríaca LINBIT.
− pró: é fácil de usar.
− contra: é exclusivamente para Linux.

Tecnologia: Replicação

Neste caso empregamos o DRBD, da empresa austríaca LINBIT.
− pró: é fácil de usar.
− contra: é exclusivamente para Linux.

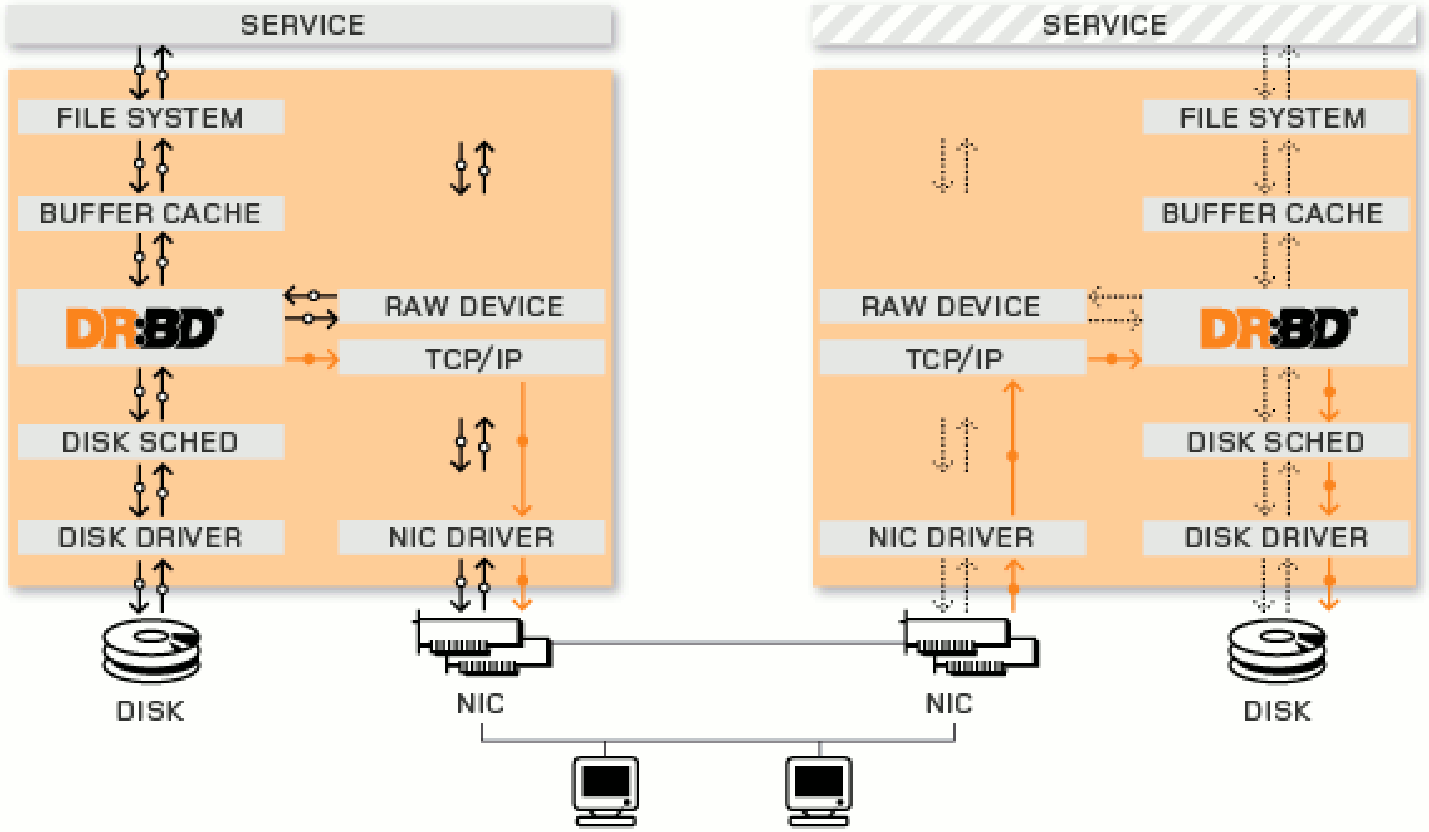


imagem copiada do site da LINBIT www.drbd.org

Tecnologia: Replicação

Neste caso empregamos o DRBD, da empresa austríaca LINBIT.
− pró: é fácil de usar.
− contra: é exclusivamente para Linux.

O DRBD intercepta as mensagens para o disco e as copia pela rede para o replicador.

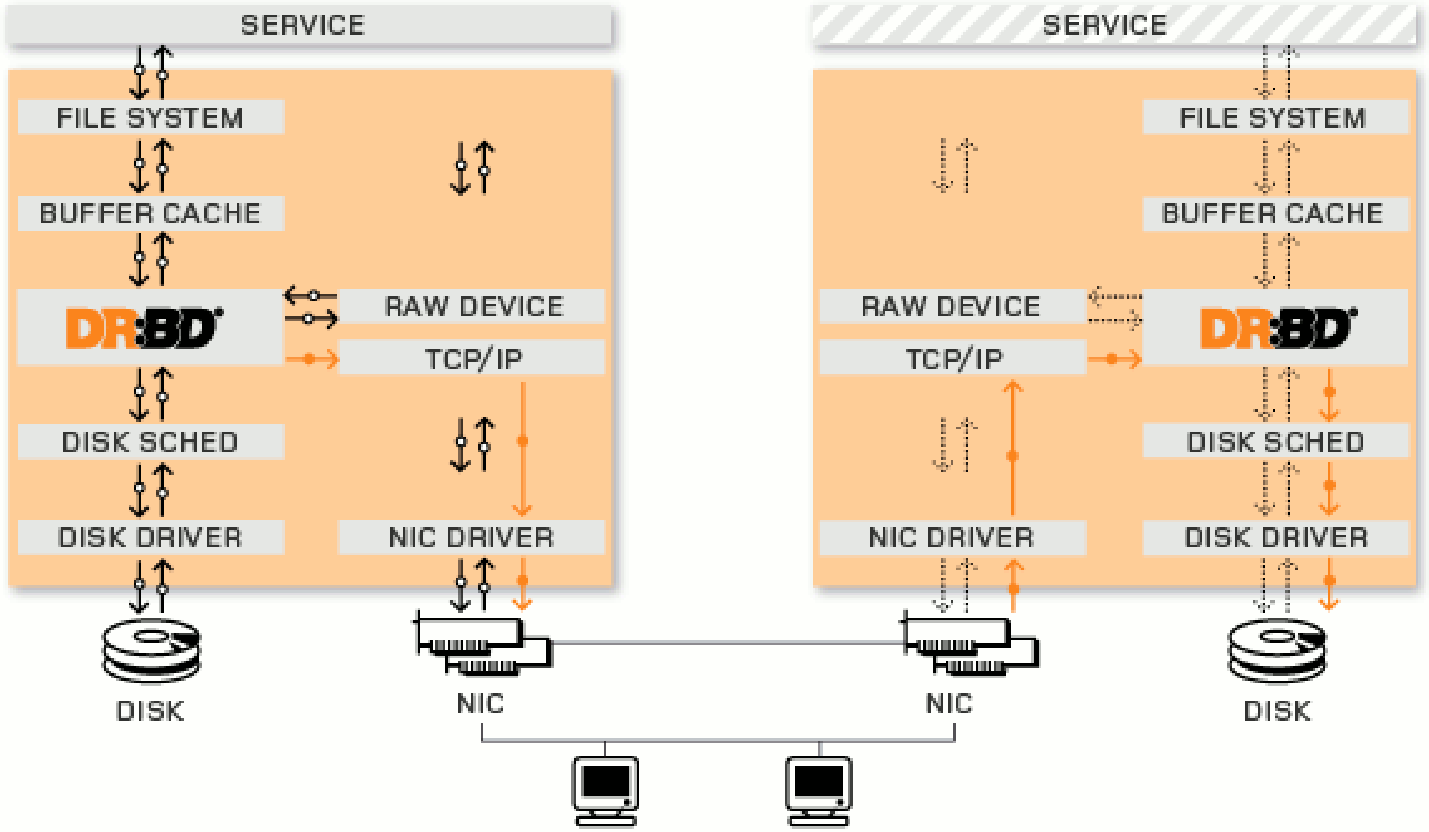


imagem copiada do site da LINBIT www.drbd.org

Tecnologia: Replicação

Neste caso empregamos o DRBD, da empresa austríaca LINBIT.
− pró: é fácil de usar.
− contra: é exclusivamente para Linux.

O DRBD intercepta as mensagens para o disco e as copia pela rede para o replicador.

A interceptação é feita no kernel e as transferências pela rede são tratadas na *userland.*

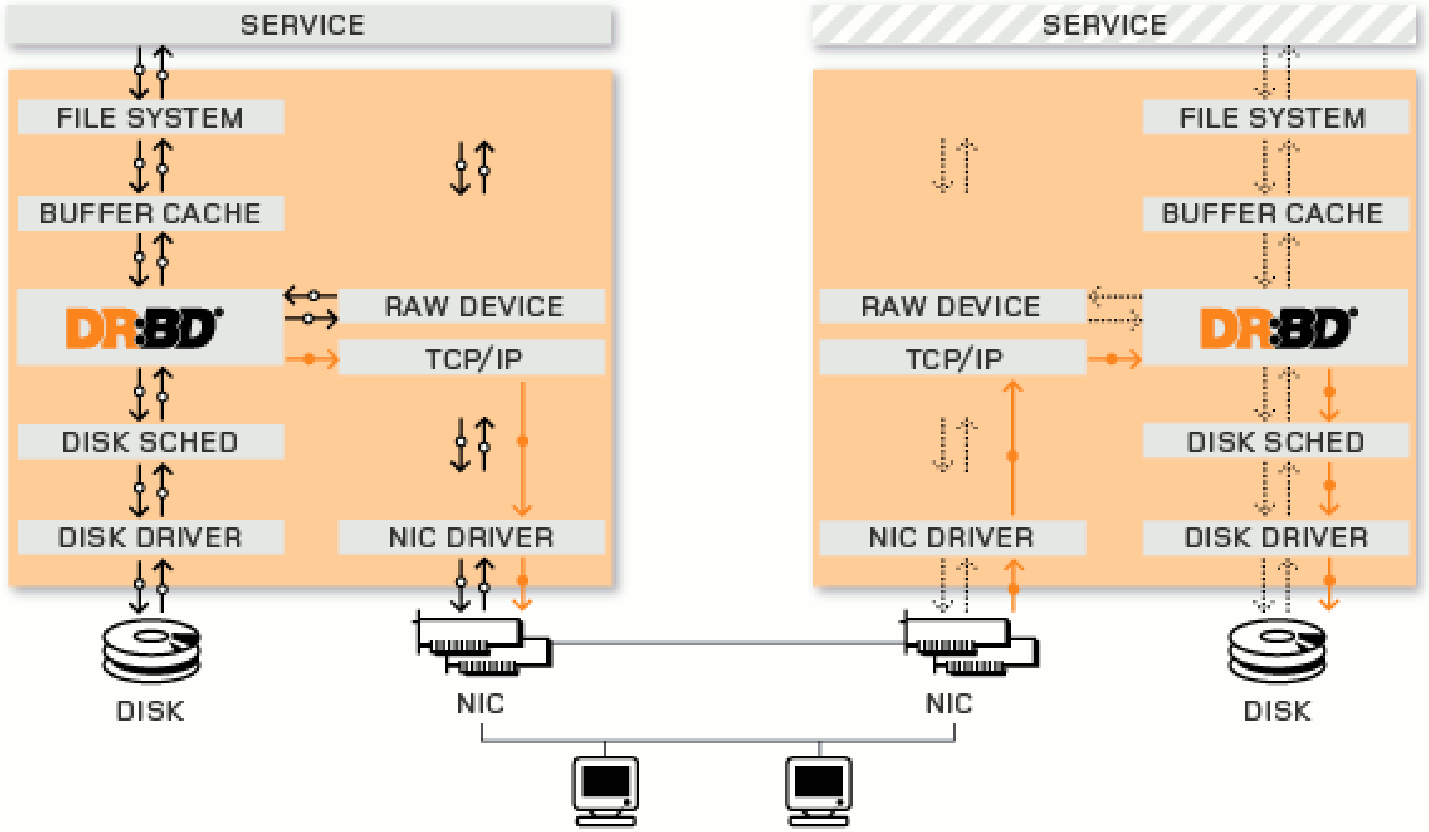


imagem copiada do site da LINBIT www.drbd.org

Tecnologia: Replicação

Neste caso empregamos o DRBD, da empresa austríaca LINBIT.
− pró: é fácil de usar.
− contra: é exclusivamente para Linux.

O DRBD intercepta as mensagens para o disco e as copia pela rede para o replicador.

A interceptação é feita no kernel e as transferências pela rede são tratadas na *userland.*

O sistema replica volumes, tais como partições de disco ou volumes lógicos.

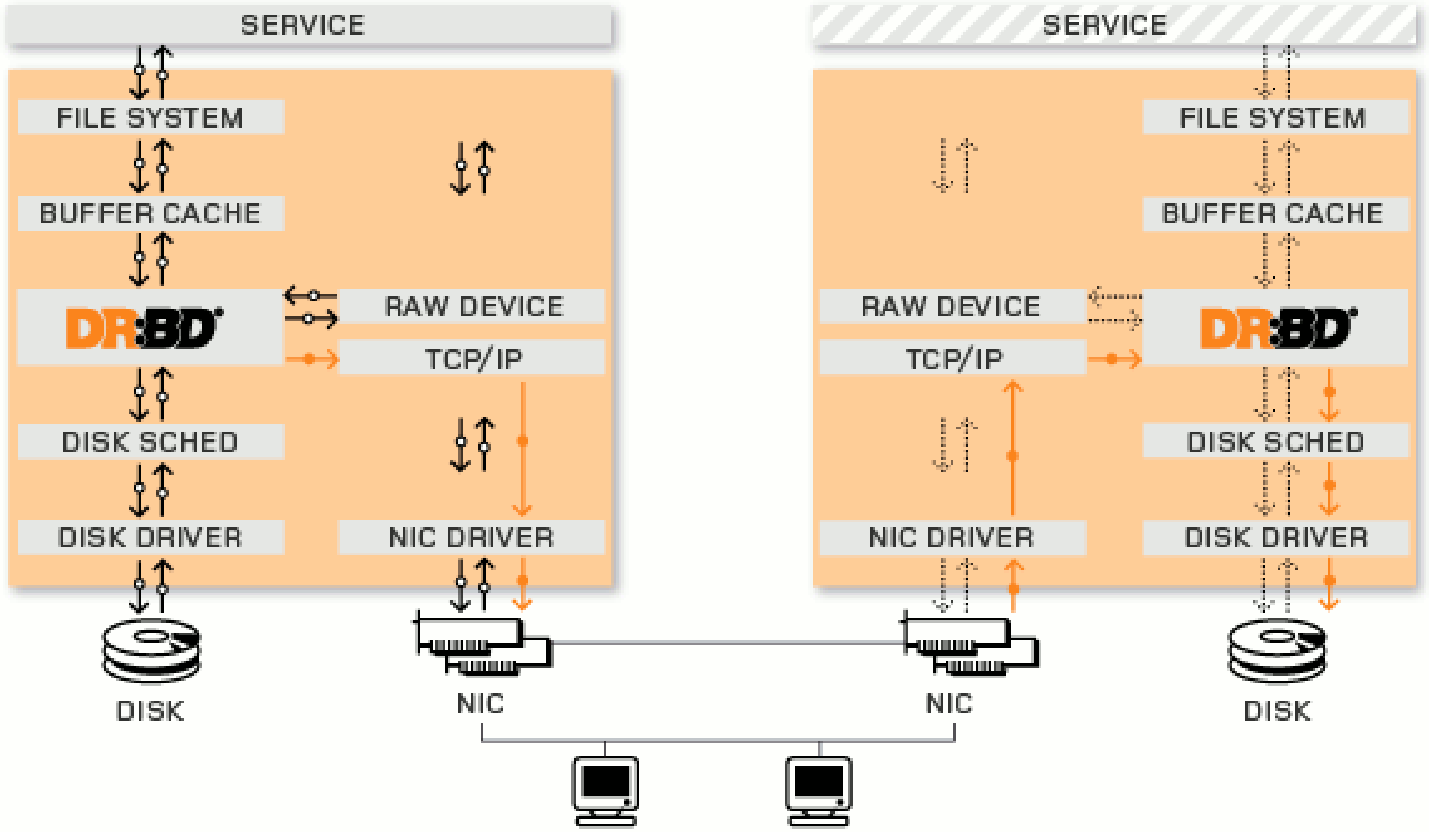


imagem copiada do site da LINBIT www.drbd.org

Como funciona a replicação com o DRBD

Recursos *(resources)*

São os objetos da replicação.

Como funciona a replicação com o DRBD

Recursos *(resources)*

São os objetos da replicação.

uso esperto de snapshots!

Dados: volumes lógicos, partições, discos inteiros...
Meta−dados: estado da sincronização. interno ou externo.

Como funciona a replicação com o DRBD

Recursos *(resources)*

São os objetos da replicação.

uso esperto de snapshots!

Dados: volumes lógicos, partições, discos inteiros...
Meta−dados: estado da sincronização. interno ou externo.

Papeis: Primario (dados originais) e Secundario (copia)
Os papeis podem ser alterados administrativamente. Na recuperação eles se invertem.

Como funciona a replicação com o DRBD

Recursos *(resources)*

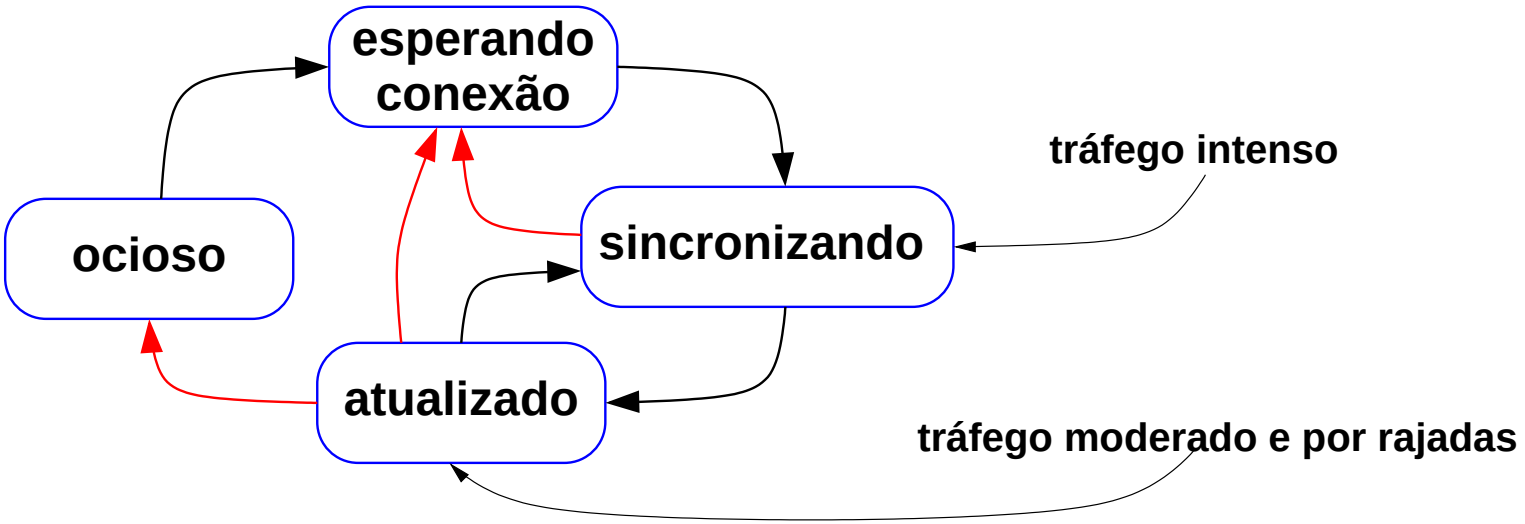
São os objetos da replicação.

uso esperto de snapshots!

Dados: volumes lógicos, partições, discos inteiros...
Meta−dados: estado da sincronização. interno ou externo.

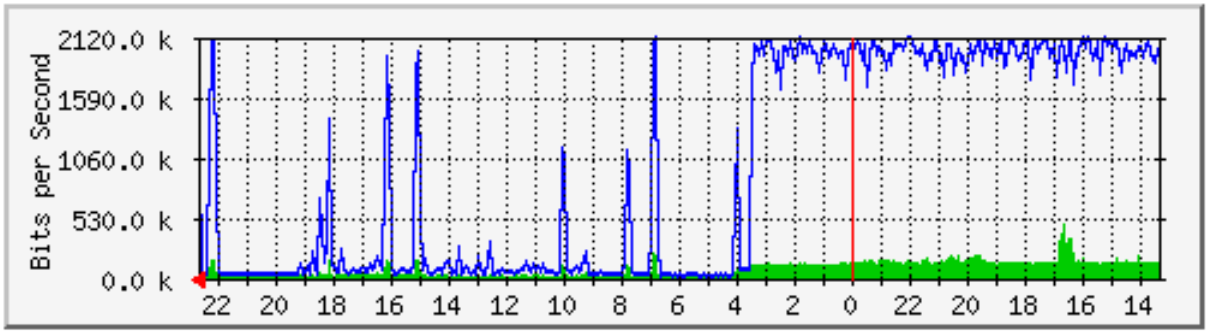
Papeis: Primario (dados originais) e Secundario (copia)
Os papeis podem ser alterados administrativamente. Na recuperação eles se invertem.

Estados:



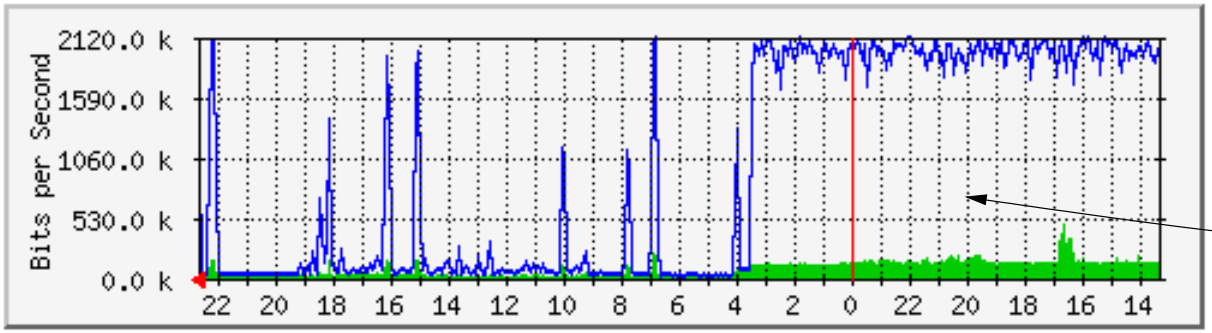
Como funciona a replicação com o DRBD

Medindo o tráfego da replicação com o bom e velho MRTG



Como funciona a replicação com o DRBD

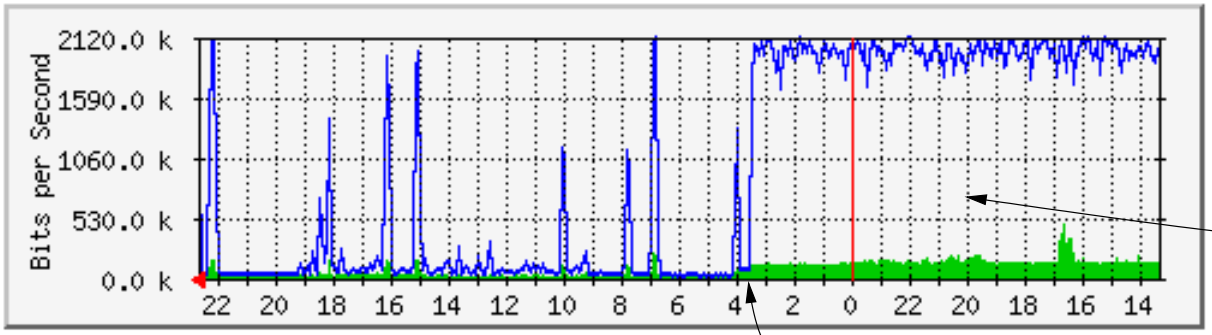
Medindo o tráfego da replicação com o bom e velho MRTG



Fase de sincronização

Como funciona a replicação com o DRBD

Medindo o tráfego da replicação com o bom e velho MRTG

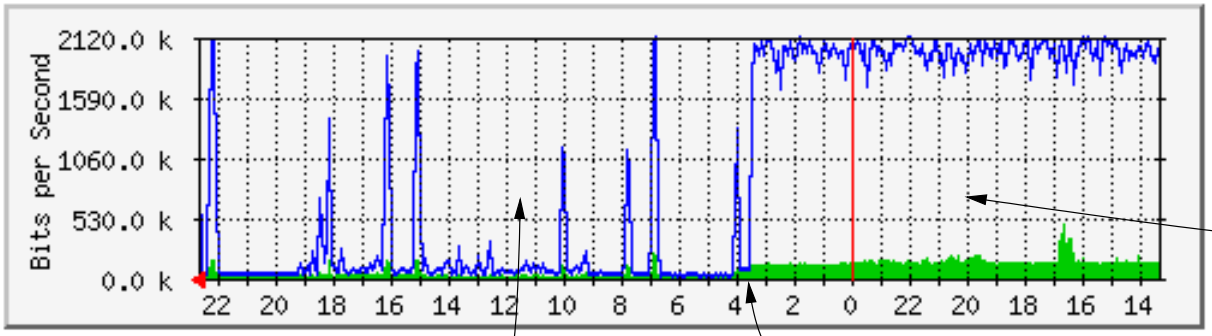


Fase de sincronização

Transição da sincronização para atualizado às 3:30 AM

Como funciona a replicação com o DRBD

Medindo o tráfego da replicação com o bom e velho MRTG



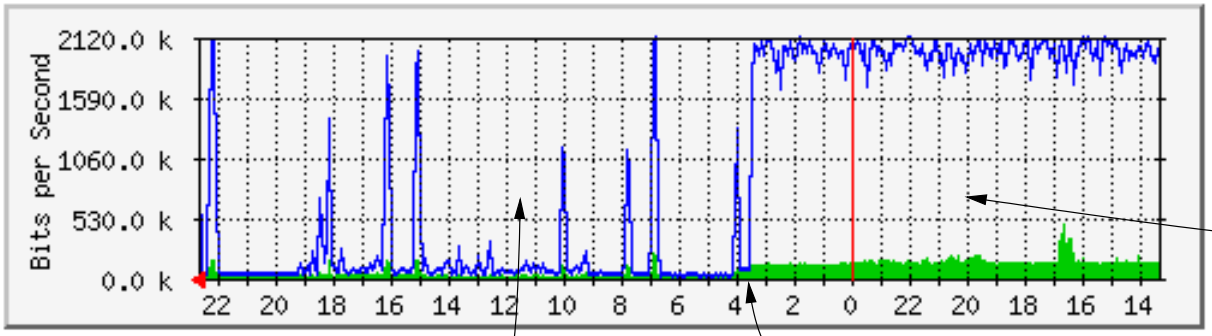
Fase de sincronização

atualizações

Transição da sincronização para atualizado às 3:30 AM

Como funciona a replicação com o DRBD

Medindo o tráfego da replicação com o bom e velho MRTG

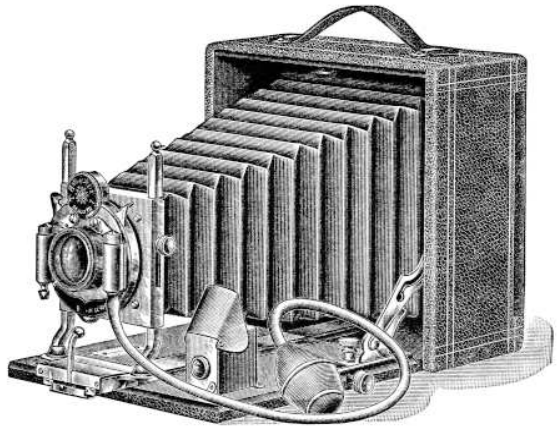


Fase de sincronização

atualizações

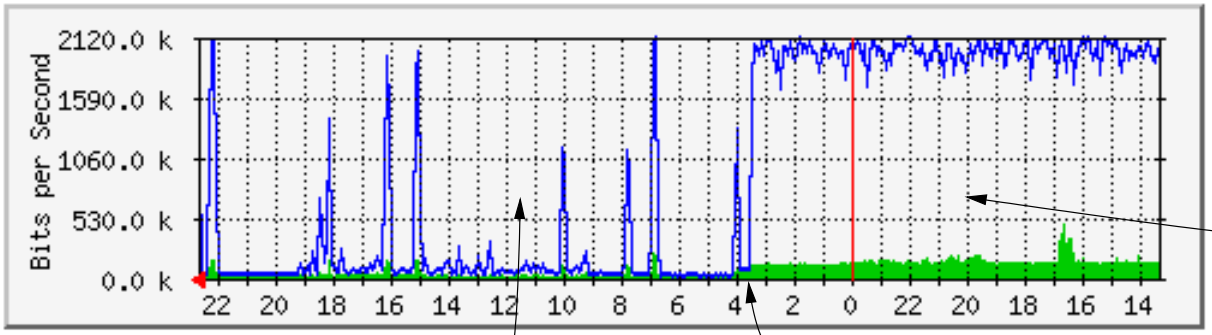
Transição da sincronização para atualizado às 3:30 AM

Uso esperto de snapshots de volumes lógicos:



Como funciona a replicação com o DRBD

Medindo o tráfego da replicação com o bom e velho MRTG



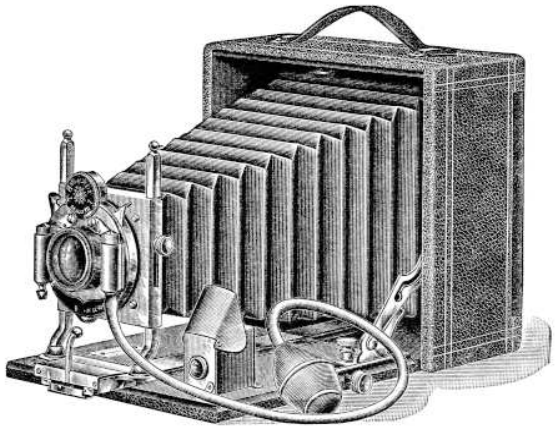
Fase de sincronização

atualizações

Transição da sincronização para atualizado às 3:30 AM

Uso esperto de snapshots de volumes lógicos:

Antes de começar a atualização faz−se uma copia instantanea do volume no secundario. Se alguma coisa MUITO errada acontecer durante a sincronização ainda teremos uma copia consistente, porém desatua−lizada. Mas isso é bem melhor do que nada!



O caso real

2 computadores em cada sitio, com um volume total de dados de aprox. 7TB.

O caso real

2 computadores em cada sitio, com um volume total de dados de aprox. 7TB.

Acesso à Internet no sitio principal via GPON com CGNAT, devidamente driblada com o uso de VPNs.

O caso real

2 computadores em cada sitio, com um volume total de dados de aprox. 7TB.

Acesso à Internet no sitio principal via GPON com CGNAT, devidamente driblada com o uso de VPNs.

Banda das VPNs limitada a 2Mbps. Medições das escritas nos volumes a replicar mostraram que com isto a chance de sair de atualização de volta para sincronização ficou menor que uma ocorrencia por mês.

O caso real

2 computadores em cada sitio, com um volume total de dados de aprox. 7TB.

Acesso à Internet no sitio principal via GPON com CGNAT, devidamente driblada com o uso de VPNs.

Banda das VPNs limitada a 2Mbps. Medições das escritas nos volumes a replicar mostraram que com isto a chance de sair de atualização de volta para sincronização ficou menor que uma ocorrencia por mês.

Uma vantagem em limitar a banda é fazer com que a replicação não provoque muita carga no servidor. Os usuários reclamam se ficar lento...

O caso real

2 computadores em cada sitio, com um volume total de dados de aprox. 7TB.

Acesso à Internet no sitio principal via GPON com CGNAT, devidamente driblada com o uso de VPNs.

Banda das VPNs limitada a 2Mbps. Medições das escritas nos volumes a replicar mostraram que com isto a chance de sair de atualização de volta para sincronização ficou menor que uma ocorrencia por mês.

Uma vantagem em limitar a banda é fazer com que a replicação não provoque muita carga no servidor. Os usuários reclamam se ficar lento...

A outra é o cu$to!

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

Toyota−based replication

São Paulo **S.José dos Campos**

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

Toyota−based replication

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

Toyota−based replication

São Paulo

S.José dos Campos

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

Toyota−based replication

O caso real

Carga inicial feita pela rede local do sitio principal, caso contrario a sincronização tomaria mais de um mês!

Toyota−based replication

São Paulo **S.José dos Campos**

e aí estão eles, no conforto do gabinete de 19"

Conclusões

Conclusões

É pereitamente possível manter a réplica da infraestrutura de TI em local remoto, sincronizada com a matriz, e pronta para entrar em ação em caso de desastre.

Conclusões

É pereitamente possível manter a réplica da infraestrutura de TI em local remoto, sincronizada com a matriz, e pronta para entrar em ação em caso de desastre.

A combinação (ou orquestração, como está na moda) de tecnologias prontamente disponíveis permite implementar a replicação com baixo custo.

Conclusões

É pereitamente possível manter a réplica da infraestrutura de TI em local remoto, sincronizada com a matriz, e pronta para entrar em ação em caso de desastre.

A combinação (ou orquestração, como está na moda) de tecnologias prontamente disponíveis permite implementar a replicação com baixo custo.

Não é necessário usar enlaces LAN−to−LAN; VPNs sobre acessos "vagabundos" resolvem.

Conclusões

É pereitamente possível manter a réplica da infraestrutura de TI em local remoto, sincronizada com a matriz, e pronta para entrar em ação em caso de desastre.

A combinação (ou orquestração, como está na moda) de tecnologias prontamente disponíveis permite implementar a replicação com baixo custo.

Não é necessário usar enlaces LAN−to−LAN; VPNs sobre acessos "vagabundos" resolvem.

O esquema implementado pressupõe que as alterações no conteúdo dos volumes sejam graduais. Alterações massivas (p.ex. copiar para dentro de um deles um HD inteiro de 1/4 de Tera, como eu fiz) fazem o estado do recurso voltar de atualizado para sincronizando.

Conclusões

É pereitamente possível manter a réplica da infraestrutura de TI em local remoto, sincronizada com a matriz, e pronta para entrar em ação em caso de desastre.

A combinação (ou orquestração, como está na moda) de tecnologias prontamente disponíveis permite implementar a replicação com baixo custo.

Não é necessário usar enlaces LAN−to−LAN; VPNs sobre acessos "vagabundos" resolvem.

O esquema implementado pressupõe que as alterações no conteúdo dos volumes sejam graduais. Alterações massivas (p.ex. copiar para dentro de um deles um HD inteiro de 1/4 de Tera, como eu fiz) fazem o estado do recurso voltar de atualizado para sincronizando.