Aplicação Remote Desktop & Sincronização de Dados

Relatório do Trabalho Final de Curso

Licenciatura em Engenharia Informática

Orientador: José Guerreiro Faísca

Aluno: Rui Pedro Coelho

N.º 20062017

Lisboa, 2011

Agradecimentos

Desejo expressar o meu agradecimento pelo precioso apoio que pessoas e instituições me deram para a realização deste trabalho:

- Ao Sr. Professor José Guerreiro Faísca, pela disponibilidade, ensinamentos prestados e incentivo, sem os quais este percurso teria sido bem mais difícil e longo;

- O meu agradecimento especial aos Professores do Curso de Engenharia Informática da Universidade Lusófona pela formação;

- De um modo geral, a todos os amigos e colegas, que através de sugestões, dúvidas e críticas, me ajudaram a clarificar e completar este trabalho;

- E por último, mas não menos importantes, ao Hélvio, à Margarida, à Sónia, à Judite e especialmente à Deolinda, pelo incondicional apoio e incentivo que sempre manifestaram e que, tanto me ajudou a ultrapassar os obstáculos ao longo deste tão longo percurso que conduziu à elaboração deste trabalho.

Índice

Resumo **4**

Abstract **5**

1-Introdução **6**

2-Revisão Bibliográfica **7**

3-Métodos e Técnicas **8**

3.1 Técnicas **9**

3.2 Processo de Instalação **10**

3.3 Requisitos de Software e Hardware **10**

4-Organização e Estruturas de Redes **11**

4.1 Tipologias de Redes **12**

4.2 Protocolo de Redes TCP **13,14**

5-Segurança na Rede **14,15,16**

6-Resultados **17,18**

7-Conclusões **19**

8-Referencias **20**

Índice de Figuras

Fig.1 desenho da arquitectura 10

Fig.2 instalação dos certificados de segurança 16

Fig.3 alerta de erro do certificado a quando da tentativa de conexão Remote Desktop 16

Fig.4 ficheiros utilizados para teste pasta 1 17

Fig.5 ficheiros utilizados para teste pasta 2 17

Fig.6 resultado da sincronização com utilização da ferramenta Desynchronize 18

Índice de Tabelas

Tab.1atribuição de IP da rede 11

Resumo

Este projecto baseia-se no estudo de varias ferramentas de backup e de sincronização de dados. Estas ferramentas permitem a execução de backup e sincronização de dados em tempo real, onde as suas eficiências falam por si no mundo das TI, tendo sido permitido através de vários testes elaborados e de uma avaliação de desempenho de cada uma das ferramentas testadas.

Este estudo foi realizado num ambiente de virtualização de sistemas, por se tratar de uma aplicação que é executada dentro de um ambiente Remote Desktop Services "RDS". Por si só, cada uma destas ferramentas testadas tem o seu grau de complexidade que permitiu tirar uma melhor ilação para projectos futuros. A arquitectura deste projecto foi desenhada com base em implementações Microsoft, onde teremos oportunidade de ver ao longo do projecto.

Abstract

This project is based on the study of many backup tools and data synchronization. These tools allow to perform backup and synchronization of data in real time, where the efficiencies speak for themselves in IT world, having been granted through various tests and developed a performance of each tested tools.

This study was conducted in an environment of system virtualization, because it is an application that runs inside a Remote Desktop Services environment "RDS". By itself, each of these tools have tested the degree of complexity that allowed us to take a better implication for future projects. The architecture of this project was designed based on Microsoft implementations, where we shall see throughout the project.

1-Introdução

Este trabalho tem como objectivo dar uma visão geral sobre o que é uma aplicação “Remote Desktop e Sincronização de Dados”.

Remote Desktop é um pacote de roles cliente/servidor que nos permite ter acesso ao ambiente da área de trabalho remota de uma dada máquina ou rede e, assim, controlá-la através do rato e teclado local. Esta aplicação é uma role que é suportada pelos diversos sistemas operativos, podendo também ser designado por software. É usada para executar o controlo do sistema remoto e ainda em tarefas de administração de sistemas como: Unix, Windows e outros ambientes de redes diversas.

Neste contexto, define-se “Backup e Sincronização de Dados” como um processo que permite a partir de um ambiente remoto, cliente/servidor ou num ambiente local efectuar backup de dados e sincroniza-los. Os dados podem ser copiados e sincronizados a partir de um directório para outro ou de um computador para outro, mantendo o diferencial, ou seja, usando metas de comparação de bit a bit que faz com que o processo efectue simplesmente a cópia e sincronização dos bits diferentes.

Desta forma, na primeira parte do trabalho serão abordados aspectos sobre Remote Desktop e Sincronização de Dados, e ainda serão apresentados os respectivos “prints screen”.

E por fim, na segunda parte, é desenvolvido a conclusão deste trabalho.

2- Enquadramento teórico Revisão Bibliográfica

O Windows Server 2008 R2 passou por uma série de actualizações que permitiram tirar proveito da virtualização e acesso remoto. É uma solução muito flexível, e com cenário de novas implementações. As capacidades do "RDS" são essências para perceber as funções dos principais componentes da arquitectura e como eles se complementam para efectuar uma conexão "RDS".

Existem cinco componentes principais da arquitectura "Remote Desktop Service", sendo que todos eles necessitam de um servidor de licenciamento "RDS". Cada componente suporta um conjunto de recursos desenhados para atingir uma determinada solução, e todos estes componentes juntos formam um conjunto de ferramentas para aceder aplicações ou terminais de serviço Remote Desktop. O Windows 2008 R2 oferece um conjunto de funcionalidades essências para a construção de uma arquitectura "Remote Desktop".

Os cinco componentes principais da arquitectura deste projecto são: "CONTOSO-DC, RDSH, CONTOSO-CLNT, RDWA e RDCB".

O Rsync é um software livre, desenvolvido para backup e sincronização de dados. Este software funciona nas mais diversas plataformas, desde os sistemas Unix às mais recentes plataformas como Linux, Windows e Osx. O Rsync é um software que pode ser usado como um método inteligente de backup de arquivos de um local para outro, independente de usar uma rede local ou network.

Rsync é uma ferramenta com uma característica especial que não se encontra na maioria dos programas desenvolvidos para backup e sincronização de dados. O Rsync pode copiar ou exibir o conteúdo do directório e copiar arquivos, opcionalmente, usando compressão e recursão.

3-Métodos e Técnicas

A solução para a realização deste projecto, foi desenhada com base em implementações Microsoft para “Remote Desktop e Sincronização de Dados”, uma vez que o Windows Server 2008 R2 já contempla as “Roles” e “Features” que executam com muita qualidade e perfeição as metas desejadas para este projecto.

3.1 Técnicas.

Para realização deste projecto foi utilizado dois sistemas operativos da família Microsoft: Windows Server 2008 R2 e Windows Seven Professional. Foi também utilizado um Hypervisor da família Oracle “Virtual Box” e dois software de backup e sincronização de dados que são: O Desynchronize e o Yintersync. Ferramentas estas que pertencem a familia Rsync. Estas ferramentas foram instaladas nos servidores da aplicação e testadas num ambiente virtual para a conclusão deste estudo.

O Rsync é uma ferramenta que usa um algoritmo inventada pelo australiano Andrew Tridgell programador para uma transmissão eficiente de uma estrutura como um arquivo através de um link de comunicação quando o computador “cliente” tem já tem um arquivo, mas não idêntico a versão do arquivo do existente no computador “servidor”.

No momento da transacção o computador cliente parte o arquivo em vários blocos de tamanho fixo que não se sobrepõem e calcula os dois tamanhos para cada bloco. Actualmente o Rsync utiliza o método MD5, em vez do MD4 que é era uma versão mais fraca. O MD5 “Message Digest Algorithm”, é um algoritmo de hash de 128 bits unidireccional desenvolvido pela RSA Data Security, Inc., descrito na RFC 1321, e muito utilizado por softwares com protocolo ponto-a-ponto (P2P, ou Peer-to-Peer, em inglês) na verificação de integridade de arquivos e logins. Foi desenvolvido em 1991 por Ronald Rivest para suceder ao MD4 que tinha alguns problemas de segurança. Por ser um algoritmo unidirecional, uma hash md5 não pode ser transformada novamente no texto que lhe deu origem. O método de verificação é, então, feito pela comparação das duas hash (uma da mensagem original confiável e outra da mensagem

recebida). O MD5 também é usado para verificar a integridade de um arquivo através, por exemplo, do programa md5sum, que cria a hash de um arquivo. Isto pode-se tornar muito útil para downloads de arquivos grandes, para programas P2P que constroem o arquivo através de pedaços e estão sujeitos a corrupção dos mesmos. Como autenticação de login é utilizada em vários sistemas operativos Unix e em muitos sites com autenticação.

3.2 Processo de instalação de software

O processo de instalação dos sistemas operativos e softwares de backup e sincronização de dados foram elaborados da seguinte forma:

- Na primeira fase, Download e instalação do Hypervisor "Virtual Box", consiste em instalar o Virtual Box, admitindo já ter feito o download do mesmo, e aconselha-se que seja a versão mais recente e a seguir proceder com a instalação ate a sua conclusão;

- A segunda fase consiste na alteração da BIOS para ambientes virtuais e habilitar a opção que faz com que o processador suporta sistemas operativos que correm a 64 bits;

- A terceira fase baseia-se na criação das respectivas máquinas virtuais;

- A quarta fase resume-se na instalação dos sistemas operativos nas respectivas máquinas virtuais;

- A quinta fase consiste na configuração dos servidores;

- Por fim, a ultima fase, resume-se na instalação de software para backup e sincronização de dados.

3.3 Requisitos de Software e Hardware

Para o desenvolvimento deste projecto foram utilizados os seguintes requisitos de software:

- Um Hypervisor;

- Dois Sistemas Operativos: “Windows 2008 R2 e Windows Seven Profissional”.

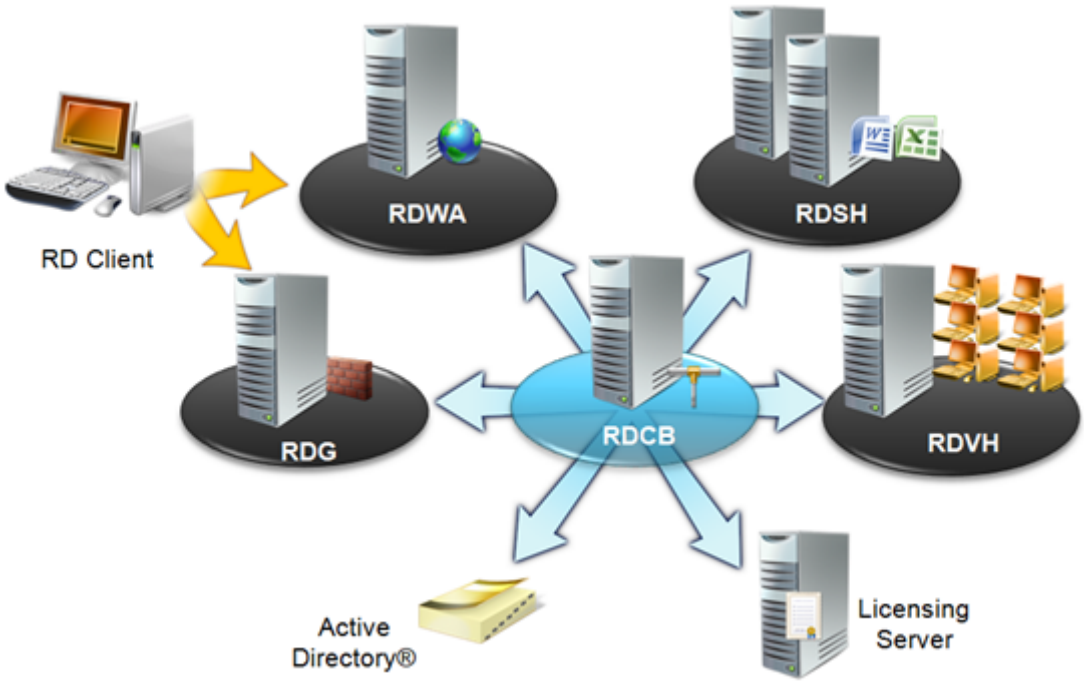
-Dois programas que efectuam Backup e Sincronização de Dados: Dsyncronize, yintersync.

É também importante referir os requisitos de hardware utilizados para o desenvolvimento do mesmo:

- Um computador.

- Cinco máquinas virtuais (VM), que correm num sistema virtualizado.

Fig.1desenho da arquitectura



É de salientar que todos estes requisitos foram muito importantes para a realização deste projecto.

4-Organização e Estrutura de Rede

Para a realização deste estudo, a organização e estrutura da rede foi desenhada com base nas configurações Microsoft para uma rede local que permite usar o protocolo IPv4.

4.1 Tipologias de Redes.

Tab.1 atribuição de IP da rede

Nome do computador	Requisito do sistema operacional	Configurações IP	Configurações de DNS
CONTOSO-DC	Windows Server 2008 R2	Endereço IP: 10.0.0.1 Máscara de sub-rede: 255.255.255.0 Gateway padrão: 10.0.0.1	Configurado pela função de servidor DNS
RDSH-SRV	Windows Server 2008 R2	Endereço IP: 10.0.0.2 Máscara de sub-rede: 255.255.255.0 Gateway padrão: 10.0.0.1	Preferencial: 10.0.0.1
CONTOSO-CLNT	Windows 7	Endereço IP:	Preferencial:

		10.0.0.3 Máscara de sub-rede: 255.255.255.0 Gateway padrão: 10.0.0.1	10.0.0.1
RDCB-SRV	Windows Server 2008 R2	Endereço IP: 10.0.0.5 Máscara de sub-rede: 255.255.255.0 Gateway padrão: 10.0.0.1	Preferencial: 10.0.0.1
RDWA-SRV	Windows Server 2008 R2	Endereço IP: 10.0.0.6 Máscara de sub-rede: 255.255.255.0 Gateway padrão: 10.0.0.1	Preferencial: 10.0.0.1

4.2 Protocolo de Redes.

Á realização deste estudo suporta o protocolo TCP-IP e de dois tipos de IP protocolo, que são; IPv4 e IPv6. Estes dois tipos protocolos têm características diferentes.

De uma forma simples, o TCP/IP é o principal protocolo de envio e recebimento de dados, uma espécie de comunicador que fornece o endereço e o nome e permite a localização do outro computador devido ao recebimento das mesmas informações, sendo usado para estabelecer esta relação tanto na internet quanto em uma intranet. TCP significa Transmission Control Protocol (Protocolo de Controle de Transmissão) e o IP Internet Protocol (Protocolo de Internet), esses dois foram os primeiros a ser definidos.

Entrando em termos um pouco mais técnicos, este conjunto de protocolos também pode ser visto como um modelo de camadas, no qual cada uma delas é responsável pela execução de uma quantidade (grupo) de tarefas, e entregando um conjunto de actividades definidas para o protocolo da camada logo acima.

Quanto mais alta a camada, mais próxima ao utilizador ela se encontra e são aquelas que trabalham com dados mais abstractos (esta é a chamada “camada de aplicação”) e para as camadas em níveis mais baixos restam funções com um nível de abstracção menor. O TCP faz parte da camada de mais alto nível do IP.

Para entrar em detalhes ainda um pouco mais específicos, IP é um protocolo responsável pela entrega de pacotes para todos os outros protocolos TCP/IP e oferece um sistema de entrega de dados sem conexão. O TCP garante a entrega e sequencial dos pacotes. No caso de a rede perder ou corromper um pacote TCP/IP durante a transmissão, é tarefa do TCP copiar estes dados

O protocolo IPv4 os endereço IP são compostos por 4 blocos de 8 bits (32 bits no total), que são representados através de números de 0 a 255, como "200.156.23.43" ou "64.245.32.11".

As faixas de endereços iniciados com "10", com "192.168" ou com "172.16" até "172.31" são reservadas para uso em redes locais e por isso não são usados na internet. Os routers que compõem a grandes redes são configurados para ignorar estes pacotes, de forma que as inúmeras redes locais que utilizam endereços na lista "192.168.0.x" (por exemplo) podem conviver pacificamente.

O protocolo IPv6 fornece o endereçamento de ponta a ponta, necessário para a conexão com rede corporativa. As organizações que ainda não estão preparadas para implantar totalmente um IPv6 nativo podem usar a tecnologia de transição IPv6 para aceder os recursos de IPv4 na rede corporativa. Os clientes do Direct Access podem usar as tecnologias de transição Teredo e IPv6 de 6to4 para ligar-se à Internet de IPv4. O IPv6 ou o tráfego das tecnologias de transição de IPv6 devem estar disponíveis no servidor do Direct Access e ter permissão para passar pelo firewall de rede do perímetro.

5-Segurança na Rede

Este sistema usa os seguintes métodos de segurança: SSL, PKI, IPsec

Com o aumento do uso da Internet para fins comerciais, tornou-se imprescindível a criação de meios que possibilitem a comunicação entre duas pessoas, através da rede, em total segurança. Dentre os diversos protocolos de segurança existente, existe um muito importante, que merece nossa atenção.

Trata-se do SSL (Secure Socket Layer). Ele permite que aplicativos cliente/servidor possam trocar informações em total segurança, protegendo a integridade e a veracidade do conteúdo que trafega na Internet. Tal segurança só é possível através da autenticação das partes envolvidas na troca de informações.

PKI (Infra-estrutura de chave pública). Uma PKI é exigida para emitir certificados para a autenticação de par do protocolo IPsec entre clientes de DirectAccess e servidores. Isso é feito normalmente pela implantação de certificados de computador para clientes de DirectAccess e

servidores. Não são necessários certificados externos. O servidor de DirectAccess também exige um certificado de SSL adicional, que precisa ter um ponto de distribuição de CRL (lista de certificados revogados) acessível por meio de um FQDN (nome de domínio totalmente qualificado) que possa ser resolvido publicamente.

IPsec. O DirectAccess usa IPsec para fornecer autenticação de pares e criptografia a comunicações pela Internet.

IPsec (**IP Security Protocol**, mais conhecido pela sua sigla,) é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja a mesma da origem) e autenticidade das informações ou *identity spoofing* (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet.

Segundo a RFC 6071, IPsec é uma suíte de protocolos que promove a segurança no nível da camada IP para comunicações pela Internet.[1] Opera sob a camada de rede (ou camada 3) do modelo OSI. Outros protocolos de segurança da internet como SSL e TLS operam desde a camada de transporte (camada 4) até a camada de aplicação (camada 7).

Isto torna o IPsec mais flexível, como pode ser usado protegendo os protocolos TCP e UDP, mas aumentando a sua complexidade e despesas gerais de processamento, porque não se pode confiar em TCP (camada 4 do modelo OSI) para controlar a confiabilidade e a fragmentação. O IPsec é parte obrigatória do IPv6, e opcional para o uso com IPv4. O padrão foi desenhado para ser indiferente às versões do IP, à distribuição actual difundida e às implementações do IPv4.

Fig.2 Instalação dos certificados de segurança

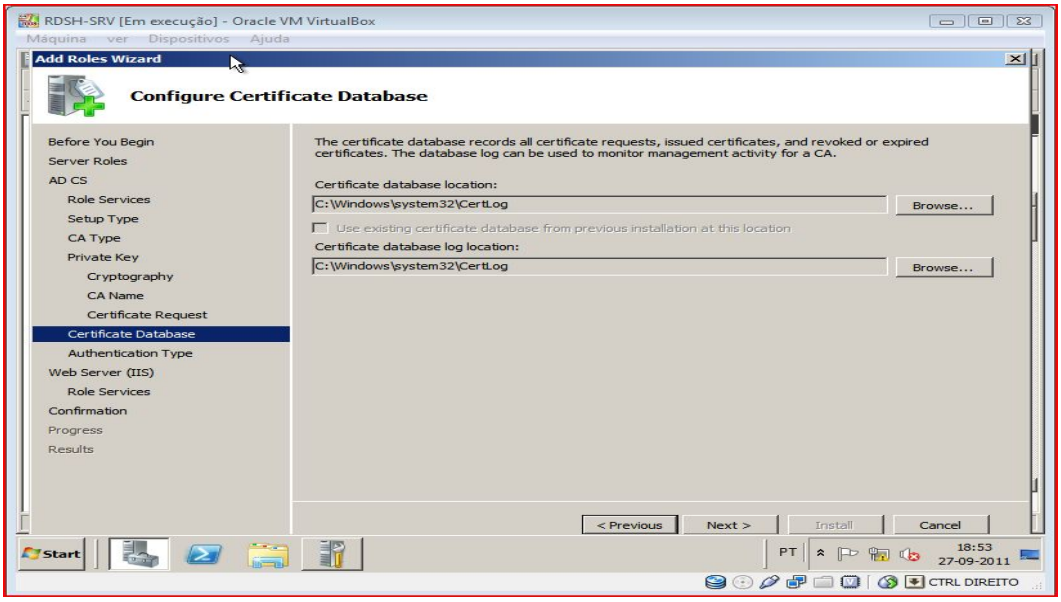
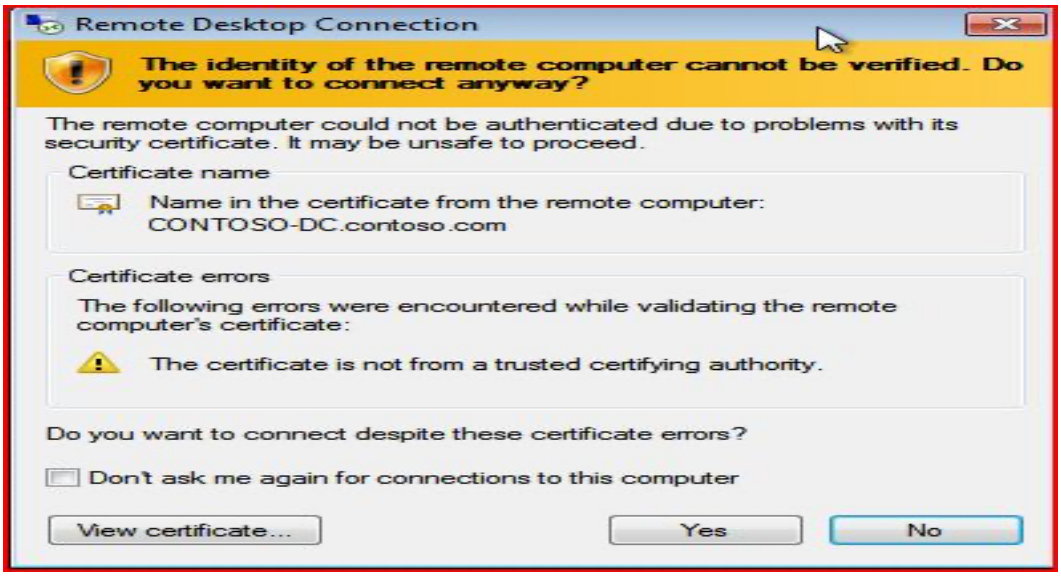


Fig.3 alerta de erro do certificado a quando da tentativa de conexão Remote Desktop.



6-Resultados

Fig.4 ficheiros utilizados para teste “pasta 1”

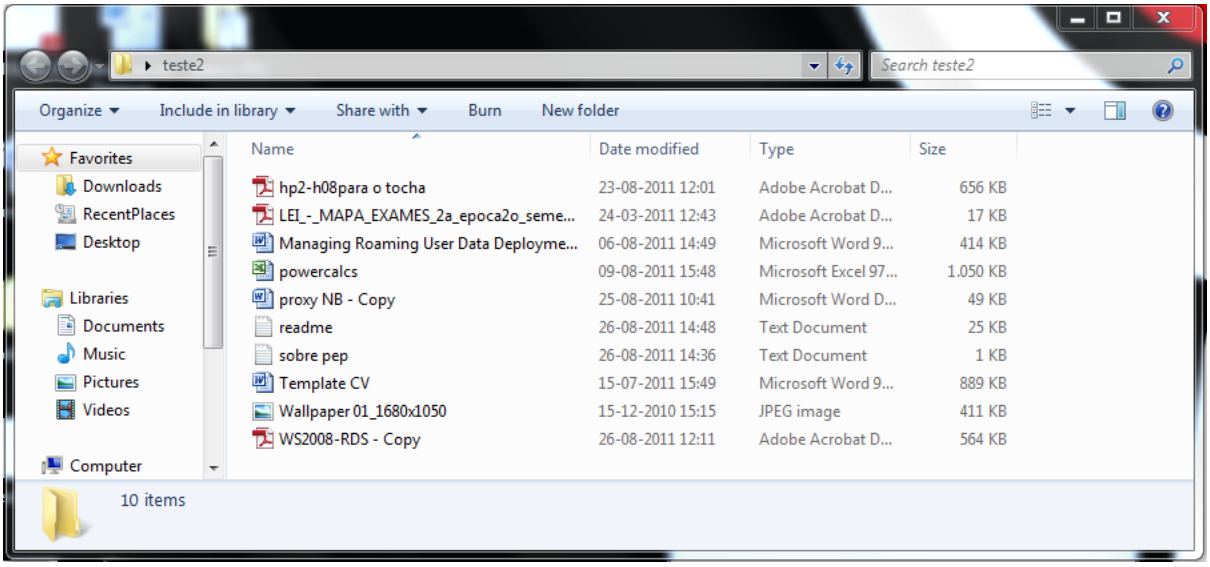


Fig.5 ficheiros utilizados para teste “pasta 2”

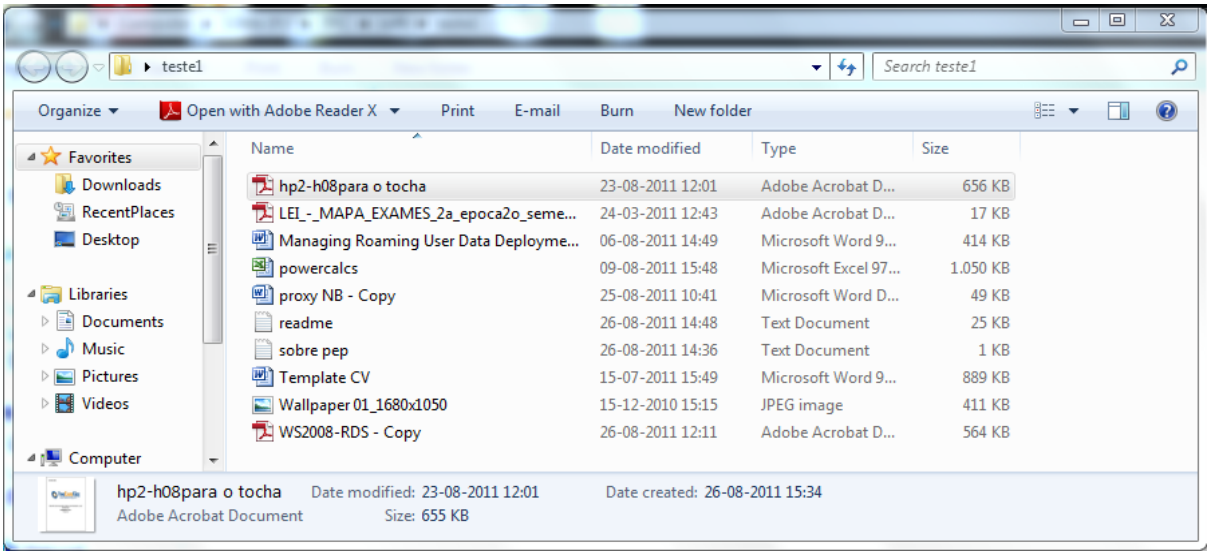
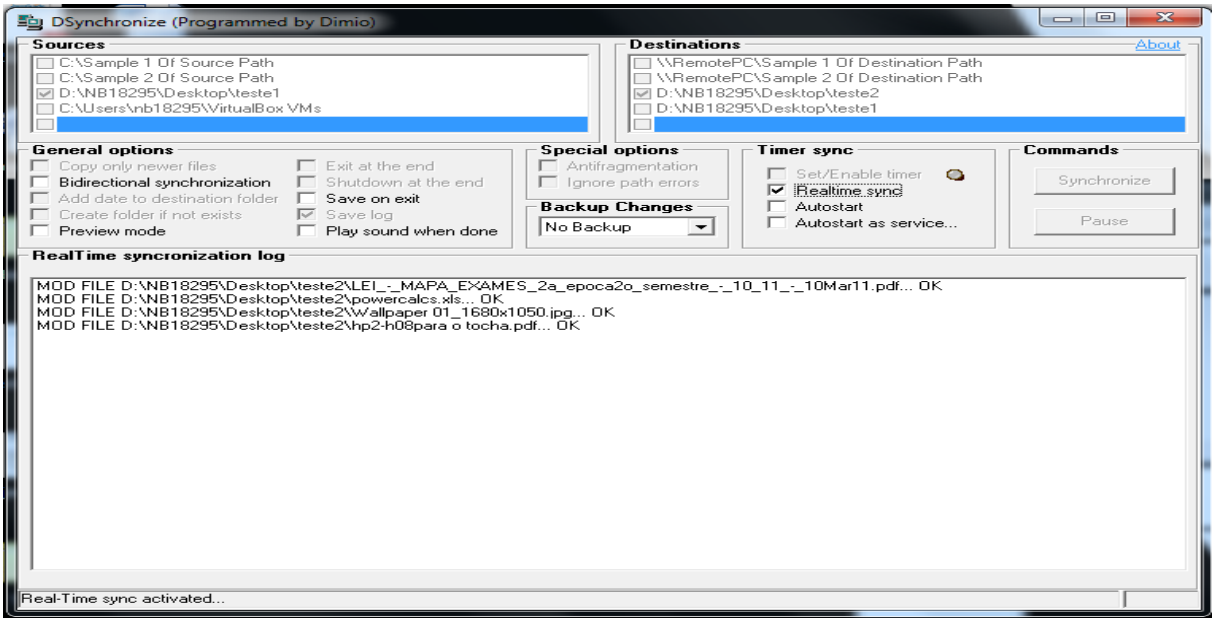


Fig.6 resultado da sincronização com utilização da ferramenta Desynchronize



7-Conclusão

Este Projecto veio de uma forma alargar os meus conhecimentos e dar uma maior visão acerca de sistema virtualizado.

Após vários testes e comparação de varias ferramentas que fazem backup e sincronização de dados, com base neste testes pude obter resultados significativo acerca das ferramentas testadas.

Posso concluir após um longo período e diversas fases de testes, a aplicação esta preparada para poder executar o que me foi proposto.

8-Referencias

http://www.microsoft.com/windowsserver2008/en/us/rds-product-home.aspx

http://technet.microsoft.com/en-us/windowsserver/ee236407.aspx

http://blogs.technet.com/b/yungchou/archive/2010/01/04/remote-desktop-services-rds-architecture-explained.aspx

http://technet.microsoft.com/pt-br/library/ee216791.aspx

http://msdn.microsoft.com/en-us/library/ms995347

http://technet.microsoft.com/pt-pt/library/cc730864.aspx

http://www.windowsecurity.com/articles/Securing-Remote-Desktop-Services-Windows-Server-2008-R2.html

http://aaronwalrath.wordpress.com/2010/05/23/installing-and-configuring-remote-desktop-services-terminal-services-on-windows-server-2008%c2%a0r2/3/

http://technet.microsoft.com/pt-br/library/cc730763(WS.10).aspx

http://groups.google.com/group/microsoft.public.windows.server.security/browse_thread/thread/74481d3a971f4536

http://www.mcsesolution.com/Windows-Server-2008-R2/remote-desktop-services-aplicacao-remota-remoteapp.html

http://www.microsoft.com/Windowsserver2008/en/us/wss08.aspx

http://technet.microsoft.com/en-us/library/cc753479(WS.10).aspx

http://technet.microsoft.com/en-us/library/cc738596(WS.10).aspx

http://blogs.msdn.com/b/rds/archive/2009/06/02/user-profiles-on-windows-server-2008-r2-remote-desktop-services.aspx

https://cmg.vlabcenter.com/console.aspx?sessionID=a6eb7907-de2b-4c0a-8a0a-1c808fec3afc&moduleID=4fde280e-46b1-4256-a27b-e032e01d79a2

http://www.vivaolinux.com.br/artigo/Backup-com-Rsync

http://serverfault.com/questions/tagged/rsync

http://www.itefix.no/i2/node/10650

http://fabienduchene.blogspot.com/2010/01/rsync-for-windows-cwrsync.html

http://en.wikipedia.org/wiki/Rsync

http://serverfault.com/questions/tagged/rsync

http://www.4d.com/pt/downloads/trial.html

http://technet.microsoft.com/pt-br/library/ms151763.aspx

http://pt.software-free-download.net/archives/188

http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp

http://www.ghacks.net/2008/10/02/windows-backup-software-deltacopy/

http://www.4reackt.com/conselhos-informaticos/2564-o-que-%E9-o-md5-message-digest-algorithm-5-a.html

Anexos

Fig.1 Instalação do Active Directory Domain Service

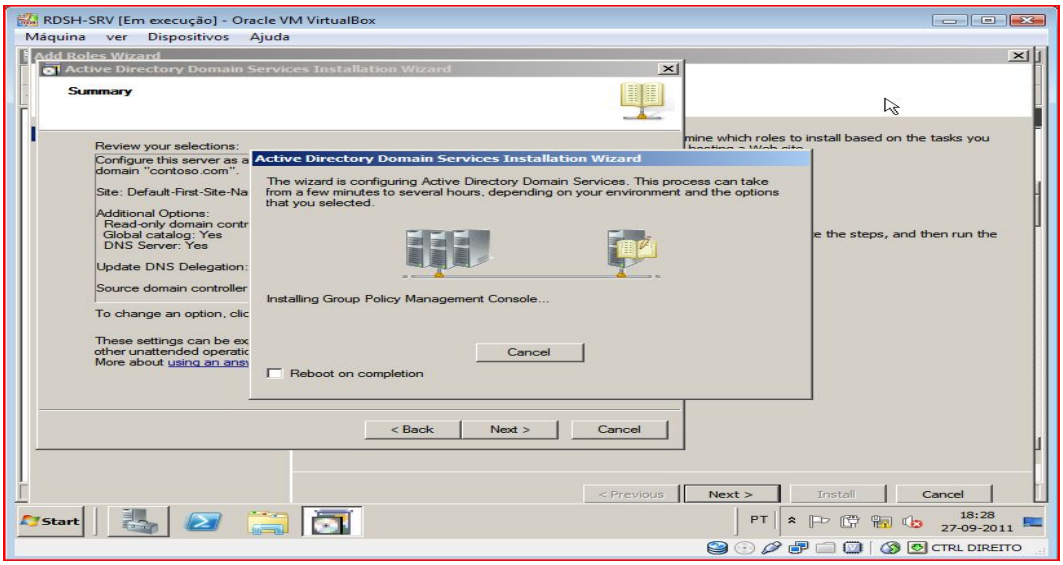


Fig.2Instalação de roles “DNS, ADDS”

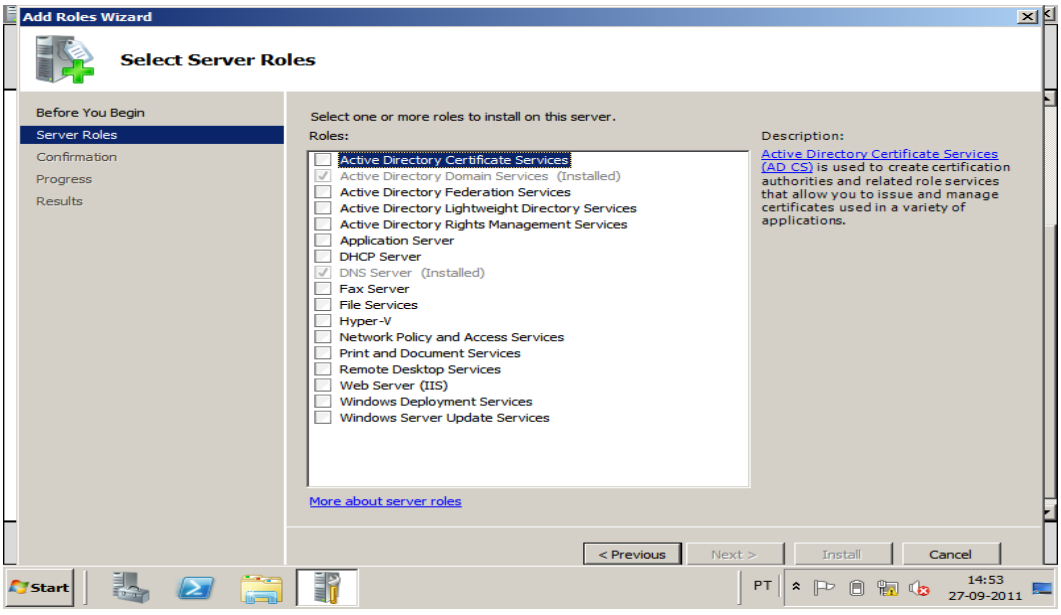


Fig.3 Configuração do CA

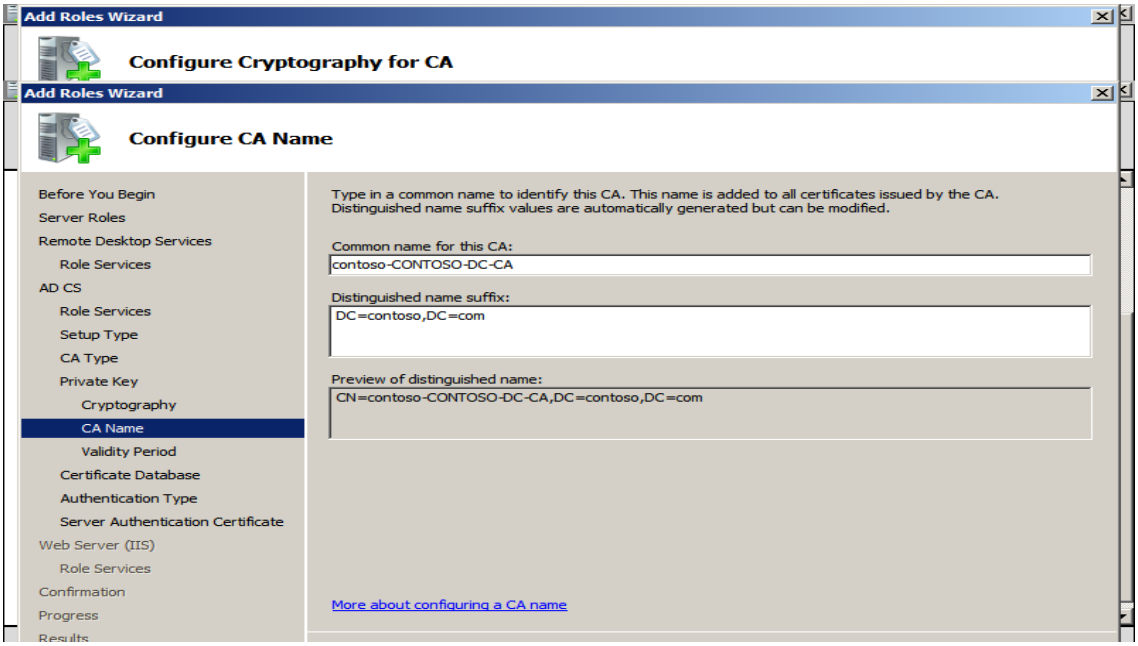


Fig.4 Configuração do cryptography

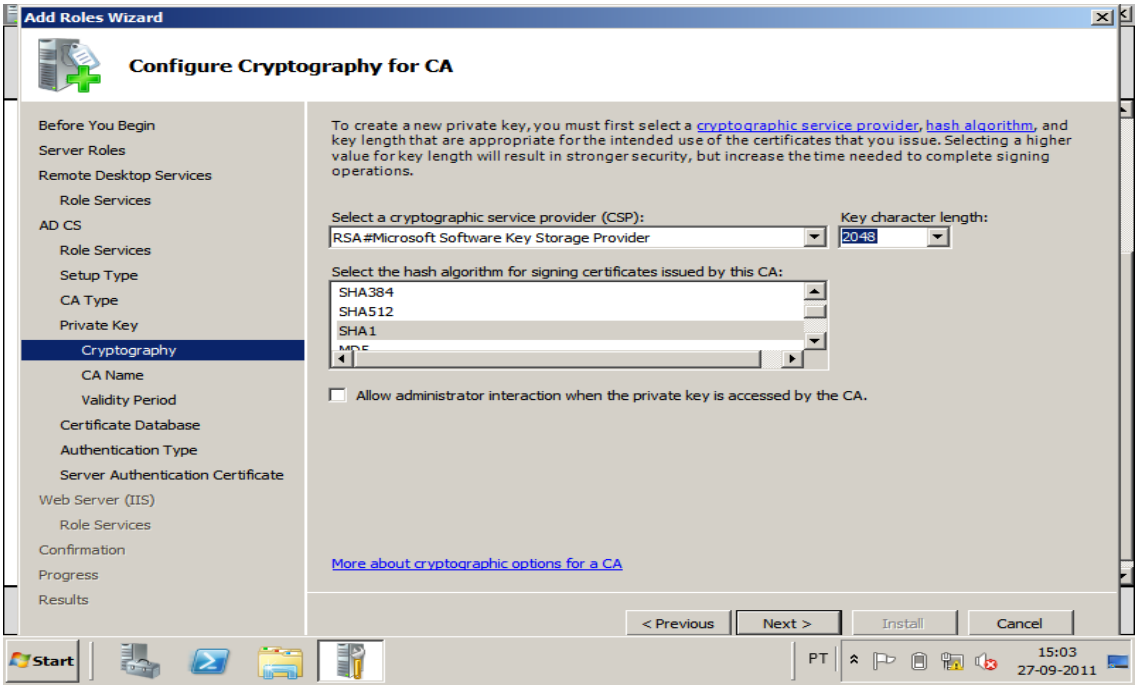


Fig.5 pedido de password “Acesso Remote Desktop”