Licenciatura em Gestão de Sistemas e Computação

Implementação de um sistema de autenticação e orquestração de máquinas virtuais no paradigma de Computação Nuvem

Trabalho Final de Licenciatura

Elaborado por Gonçalo Roldão

Aluno nº 20172128

Orientadora: Professora Doutora Virgínia Araújo

Barcarena

dezembro 2020

Atlântica - Instituto Universitário

Licenciatura em Gestão de Sistemas e Computação

Implementação de um sistema de autenticação e orquestração de máquinas virtuais no paradigma de Computação Nuvem

Trabalho Final de Licenciatura

Elaborado por Gonçalo Roldão

Aluno nº 20172128

Orientadora: Professora Doutora Virgínia Araújo

Barcarena

dezembro 2020

O autor é o único responsável pelas ideias expressas neste relatório

AGRADECIMENTOS

Antes de apresentar este trabalho gostaria de dar um agradecimento especial a todos os membros da turma e aos professores desta instituição que me ajudaram a realizá-lo e que partilharam comigo os seus conhecimentos e orientação indispensáveis.

Gostaria também de agradecer à empresa que participou e incentivou o desenvolvimento deste trabalho, auxiliando paralelamente o crescimento profissional futuro.

Um agradecimento especial para todos os membros do curso que me apoiaram e ajudaram com especial destaque os seguintes membros: Joana Bernardo e Davidson Sousa que estiveram sempre postos a ajudar mesmo fora do horário escolar e profissional.

RESUMO

Implementação de um sistema de autenticação e orquestração de máquinas virtuais no paradigma de Computação Nuvem

A necessidade que os negócios têm em obter ferramentas cada vez mais eficientes para suportarem o seu negócio tem crescido exponencialmente. A presença online das pequenas e médias empresas tornou-se quase obrigatório de forma a obterem visibilidade ao publico alvo que pretendem atingir.

Este trabalho tem como um dos objetivos principais, a criação de um artefacto que permite a empresas de pequena e média escala, investirem numa solução tecnológica eficiente e de baixo custo para determinadas necessidades, sejam elas configurações de servidores, hospedagem de sites ou armazenamentos de ficheiros sem necessitarem de gastar recursos em manutenção dos mesmos, sendo esse papel a responsabilidade dos fornecedores do sistema.

A metodologia de investigação utilizada neste trabalho DSR (*Design Science Research)* sendo a mais apropriada para uma solução focada e eficiente dos problemas.

Através de um laboratório construído em pequena escala, é possível demonstrar que é possível criar uma infraestrutura essencial para uma empresa sem grandes custos associados. Tornado esta infraestrutura tecnológica muito mais rápida, eficiente e autónoma, transportando a responsabilidade de manter as máquinas operacionais para os fornecedores da nuvem, permitindo às empresas focarem-se totalmente na sua área de negócio.

Com a conclusão deste artefacto é possível satisfazer muitas das necessidades tecnológicas que são transversais no âmbito das pequenas e médias empresas

Palavras-chave: Nuvem, Virtualização, VPN, RemoteApps, Redundância, Segurança

ABSTRACT

Implementation of an authentication and orchestration system for virtual machines in the cloud Computing paradigm

The need that businesses have to obtain increasingly efficient tools to support their business has grown exponentially. The online presence of small and medium-sized companies has become almost mandatory in order to gain visibility to the target audience they want to reach.

This project has as one of the main objectives, the creation of an artifact that allows small and medium scale companies to invest in an efficient and low-cost technological solution for certain needs, be it server configurations, website hosting or file storage without needing to spend resources on maintaining them, this role being the responsibility of the system suppliers.

The research methodology used in this work DSR (Design Science Research) being the most appropriate for a focused and efficient solution of problems.

Through a laboratory built on a small scale, it is possible to demonstrate that it is possible to create an essential infrastructure for a company without great associated costs. Making processes much faster, more efficient and autonomous, carrying the responsibility of keeping the machines operational for cloud suppliers, allowing companies to fully focus on their business area.

With the completion of this artifact it is possible to satisfy many of the technological needs that are transversal in the scope of small and medium enterprises.

Keywords: Cloud, Virtualization, VPN, RemoteApps, Redundancy, Security

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

DNS- Domain Name System

DHCP- Dynamic Host Configuration Protocol

AD- Active Directory

GPO- Group Policy Object

VPN- Virtual Private Network

IAAS- Infrastructure as a Service

PAAS- Platform as a Service

SAAS- Software as a Service

DFS- Distributed File System

DC- Domain Controller

SSD- Solid-Stade Drive

HDD- Hard Disk Drive

RAM- Random Access Memory

HTTP- Hypertext Transfer Protocol

HTTPS- Hypertext Transfer Protocol Secure

IP adress- Internet Protocol address

RDS- Remote Desktop Services

FQDN- Fully Qualified Domain Name

LAN- Local Area Network

WAN- Wide Area Network

VSS- Volume Shadow Copy Service

1 INTRODUÇÃO

1.1. Contexto e Motivação

Observando o mercado, constata-se que atualmente assiste-se a uma época em que o conceito de nuvem, é cada vez mais utilizado pelas empresas.

Mais de 90% das empresas a nível mundial (Roberts, 2019), operam em ambientes híbridos com uma mistura de nuvem pública, nuvem privada, TI tradicional e inúmeros aplicativos *SaaS (Software as a Service)*, como por exemplo *Microsoft Office 365*.

Diversas empresas utilizam um conjunto de vários fornecedores de serviços baseados na nuvem, oferecendo ferramentas e sistemas de gestão próprios.

Segundo um estudo da *McKinsey & Company* (Roberts, 2019), a *multicloud* híbrida é uma tendência emergente atualmente. De acordo com este estudo, a *multicloud* híbrida irá produzir efeitos no mercado. Em concreto, será uma oportunidade para as empresas dependerem menos de fornecedores e deste modo usufruírem do potencial das tecnologias baseadas na nuvem.

Este trabalho irá impulsionar o conhecimento sobre as tecnologias baseadas em *cloud Computing*, auxiliando na realização profissional assim como pessoal.

Ao construir um laboratório é possível observar as diversas opções de customização desde replicação de informação entre servidores a adicionar funcionalidades especificas aos mesmos, necessárias para uma infraestrutura empresarial, existentes no mercado neste momento.

1.2 Descrição do Problema

Muitas das pequenas e médias empresas existentes, possuem diversas necessidades tecnológicas relativas à gestão dos utilizadores, segurança, acessos, partilha de informações e equipamentos informáticos presentes na empresa.

A empresa Company é uma pequena empresa com fundos reduzidos para acesso a sistemas e tecnologias de informação complexos.

Foi efetuada uma reunião com o CEO da empresa *Company* que uma vez que a sua empresa estava a crescer em número de funcionários e parque informático, surgiram diversas necessidades.

As necessidades apresentadas foram:

- Gestão centralizada de utilizadores e equipamentos informáticos;
- Autenticação segura dos utilizadores da empresa;
- Aprovisionar Software e apenas prestar acesso ao mesmo consoante permissões dos utilizadores;
- Partilha de informação de forma segura com redundância e acessos condicionados conforme permissões;
- Automatizar processos de instalação de software, impressoras e mapeamento da partilha de informação;
- Segurança no acesso à rede empresarial de forma remota;
- Minimizar os custos de manutenção mantendo os equipamentos que suportam a infraestrutura tecnológica fora das instalações físicas da empresa.

Estas necessidades advêm dos recursos limitados que estas empresas podem despender para investir numa infraestrutura tecnológica que possa dar uma resposta eficiente.

Este trabalho propõe uma das várias soluções existentes no mercado para responder a estas necessidades.

1.3 Objetivos de Investigação

Após análise de várias soluções existentes no mercado, o objetivo do autor foca-se na resolução de todos os problemas identificados no ponto 1.2 deste relatório que oferece uma forma centralizada para a solução dos mesmos.

Considerando o problema identificado no ponto 1.2 desde relatório, foram definidos os seguintes *Research Goals* (RG) para dissipar o problema:

- RG 1 – Realizar o levantamento dos requisitos que satisfazem as necessidades de empresas com défice nas áreas tecnológicas;
- RG 2 – Descrever toda a arquitetura que inclui o desenho lógico, assim como a infraestrutura e o software utilizado;
- RG 3 – Desenvolver e testar todo o sistema referente ao domínio (domínio permite agrupar de forma centralizada todos os objetos presentes numa determinada rede empresarial), como demonstração, neste trabalho irá chamar-se *company.local.*

1.4 Metodologia de Investigação

O método de Investigação utilizado no desenvolvimento deste trabalho foi o DSR (*Design Science Research*), uma vez que se trata de uma metodologia objetiva e focada na resolução eficiente de problemas.

A metodologia método DSR, foi desenvolvido como um modelo que fosse consistente com a literatura anterior, um modelo padrão para informação científica, um modelo intuitivo mentalmente para pesquisa cientifica em sistemas de informação. (Peffers, et al., The Design Science Research Process, 2006)

Para a adoção apropriada deste método, este trabalho foi desenvolvido seguindo o processo de 6 fases propostas por *Ken Peffers e Tuure Tuunanen* (Peffers, et al., The Design Science Research Process, 2006):

1. Identificação do problema - Definir e identificar o problema, justificando e solucionando e, por associação, desenvolver com eficiência uma solução que capture a complexidade do problema resolvendo-o de 2 maneiras: motivando o investigador pelo trabalho realizado e auxiliando o leitor nas investigações futuras;

2. Objetivos da solução – Os objetivos da solução podem ser quantitativos ou qualitativos no contexto da solução desejada. As soluções deverão ser racionalmente especificadas, para que os requisitos para que o conhecimento do problema e da solução sejam implementados com eficiência;

3. Desenho e desenvolvimento – Para desenhar uma solução será necessária a construção de um modelo, a criação de um método ou a configuração de uma implementação. Esta atividade inclui pontos determinantes para a funcionalidade e arquitetura de recursos para o desenvolvimento e conhecimento teórico das soluções;

4. Demonstração – A eficiência para a solução de um problema consiste na tentativa, simulação e demonstração do sucesso;

5. Avaliação – Através do estudo do problema e da solução é possível comparar os objetivos da solução e os seus resultados numa demonstração. Dependendo da natureza do problema, a avaliação pode incluir itens de comparação de funcionalidade qualitativa, quantitativa, de forma a obter o feedback dos clientes, investigadores e comunidade.

6. Comunicação – A transmissão das soluções pode ser efetuada através de artigos, trabalhos ou outros meios. Sendo que estas soluções são baseadas no conjunto dos pontos anteriores.

1.5 Estrutura do Documento

Como referido anteriormente, este trabalho segue o método DSR. Assim, o primeiro capítulo, identifica o âmbito e a motivação para o desenvolvimento do presente trabalho, os objetivos de investigação, método de investigação, referindo problemas identificados no ambiente profissional do autor.

No segundo capítulo é possível verificar a revisão da literatura de todos os conceitos utilizados na investigação e desenvolvimento do trabalho no contexto atual

O terceiro capítulo apresenta os requisitos funcionais e não funcionais para a solução a desenvolver.

No quarto capítulo é apresentado uma visão geral da arquitetura do sistema e com detalhe para a arquitetura física.

O quinto capítulo apresenta várias ilustrações e suas descrições sobre os processos de instalação e validação do sistema.

O sexto capítulo, apresenta a conclusão do trabalho desenvolvido referindo também possíveis melhorias complementares.

2 REVISÃO DE LITERATURA

2.1 Conceito Nuvem

Nuvem é um conceito de virtualização que vai permitir às empresas grandes, médias ou pequenas, a oportunidade de criar uma infraestrutura tecnologia que pode conter servidores a executarem sistemas operativos como Windows ou Unix a partir de qualquer ponto geográfico sem existir a necessidade de possuir qualquer tipo de hardware ou ocupar espaço físico. (Rand Morimoto, Windows Server 2016 Unleashed, 2017).

Tendo isto presente, a nuvem define uma rede de servidores virtuais baseados em arquitetura distribuída assentes em *datacenters* (Centros de Dados) com presença global, com funções especificas, que podem ou não comunicar entre si dependendo da solução implementada para o cliente.

A Nuvem possui como grandes vantagens a inexistência de custos de manutenção dos equipamentos internos do Cliente, um sistema de custo *pay as you go* que auxilia a que pequenas empresas possam ter a sua infraestrutura na nuvem com baixo custo de investimento.

De acordo com (Simmon, 2018), existem 4 tipos de implementações possíveis de nuvem: nuvem privada, nuvem pública, nuvem híbrida e nuvem partilhada. Cada um destes modelos, difere na maneira como os acessos aos recursos da nuvem são efetuados e qual o outorgante responsável por cada recurso.

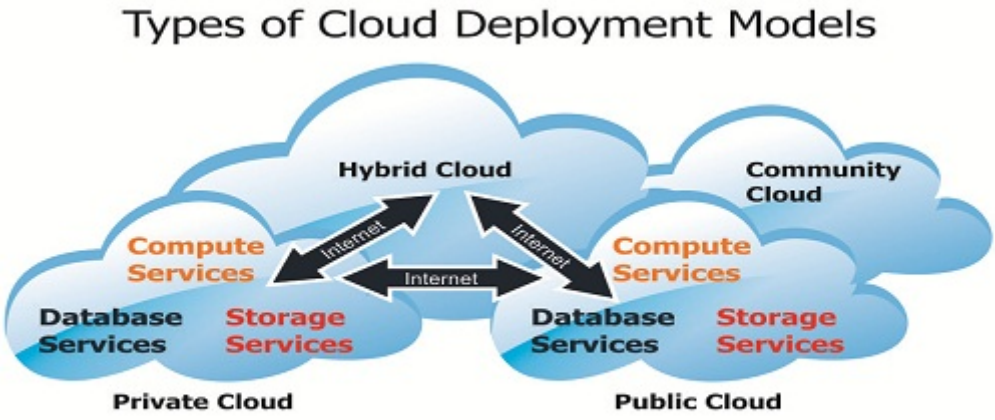

Figura 1 Tipos de Cloud, retirado de (Selby, 2016)

2.1.1 Nuvem Pública

A nuvem pública é constituída por um conjunto de serviços (PaaS, IaaS, SaaS) tecnológicos, disponibilizados para o publico geral, através do qual grandes organizações que têm a possibilidade de possuírem inúmeros *datacenters* por todo o mundo com grande poder computacional. Este tipo de serviços é vendido conforme as necessidades reveladas pelo cliente e são normalmente cobrados conforme tempo de utilização, componentes utilizados e largura de banda consumida. (Attaran, 2017).

Num ambiente de nuvem publica, os servidores são baseiam-se numa arquitetura distribuída, assentes em diversos *datacenters* espalhados pelo mundo, permitem ao cliente criar uma rede dedicada constituída por diversos servidores com comunicação entre si num plano de pagamento *pay as you go*.

A nuvem pública auxilia a gestão de IT a ser mais dinâmica e flexível às necessidades de cada empresa.

Figura 2 Nuvem pública retirado de (Hybrid ICT, 2018)

2.1.2 Nuvem Privada

A infraestrutura de uma nuvem privada, oferece muitas das vantagens da nuvem publica, com a adição que o controlo sobre a própria infraestrutura pelos fornecedores é efetuado de forma direta (Attaran, 2017).

A nuvem privada consiste em redes de servidores normalmente assentes num *datacenter* privado, que podem ser propriedade de uma única organização e geridos pela mesma ou por terceiros (Simmon, 2018).

Esta solução é ideal para empresas que prestam serviços de *Manage Services* proporcionando desta forma um serviço adaptável ao cliente.

Tem como grande vantagem, o facto de a entidade responsável pelo *datacenter* possuir um controlo e resposta mais eficiente no tratamento de problemas e pedidos de novas implementações que possam ocorrer.

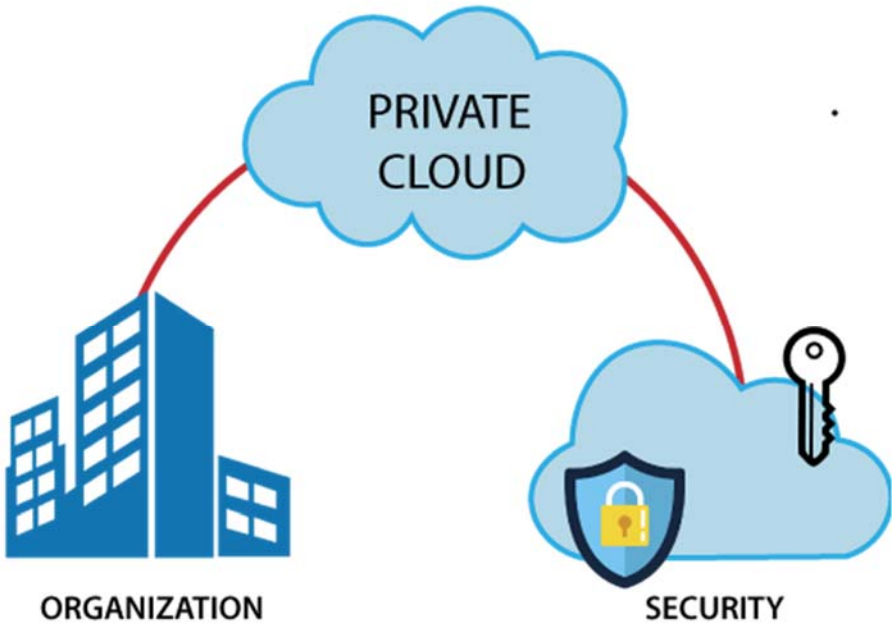

Figura 3 Nuvem Privada retirado de (javatpoint, 2018)

2.1.3 Nuvem Híbrida

A nuvem híbrida é uma junção de pelo menos 2 tipos de nuvem, podendo conter processos de automatização entre ambas. Este tipo de tecnologia permite aos clientes capitalizarem ao máximo as vantagens de uma nuvem pública com os valores de uma nuvem privada ou infraestrutura local tradicional (Simmon, 2018).

Numa nuvem híbrida, os dados e as aplicações podem mover-se entre nuvem privadas e públicas para uma maior flexibilidade e existirem mais opções de implementação. Por exemplo, pode-se utilizar a nuvem pública para necessidades com grande volume e baixa segurança, como e-mail baseado na web e a nuvem privada (ou outra infraestrutura no local) para operações confidenciais e críticas para a empresa, como relatórios financeiros que por vezes devido a questões legais têm que estar presentes em solo nacional.

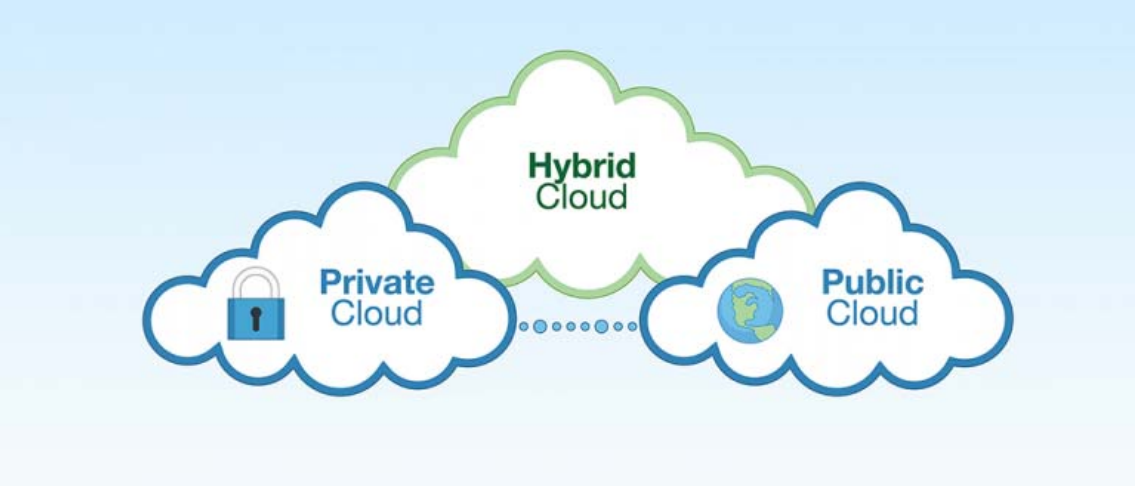

Figura 4 Nuvem Híbrida retirado de (Girijala, 2018)

2.1.4 Nuvem Comunitária

A nuvem comunitária, trata-se de uma implementação efetuada por diversas organizações que partilham interesses em comum.

Esta solução, pode ser gerida pelas próprias organizações que a desenvolveram ou por organizações de terceiros especializadas.

A infraestrutura pode estar presente localmente nas organizações, fora das mesmas ou ambos, tornando-se assim numa solução multicloud (Neto, 2015).

Temos como alguns exemplos que utilizam esta solução, os serviços públicos de saúde e de energia.

2.2 Serviços Nuvem

Os vários modelos apresentados ao longo do capítulo 2.1 deste trabalho, prestam essencialmente 3 tipos de serviços (IaaS, PaaS, SaaS) em que cada um possui características especificas com o objetivo de satisfazer qualquer necessidade dos clientes.

Cada um dos serviços tem um publico alvo a atingir. Enquanto Infrastructure as a Service, refere-se aos recursos de hardware de máquinas virtuais disponibilizados pelos fornecedores de serviços Nuvem consoante as necessidades do cliente, *Plataform as a Service*, tem como público alvo principal, proporcionar um ambiente de desenvolvimento e de testes, em que os programadores realizarem os testes necessários para desenvolver uma determinada aplicação. *Software as a Service*, proporciona um ambiente altamente abstrato desenvolvido especificamente para utilizadores finais sem necessidade de possuir conhecimentos técnicos para usufruírem das ferramentas e serviços oferecidos.

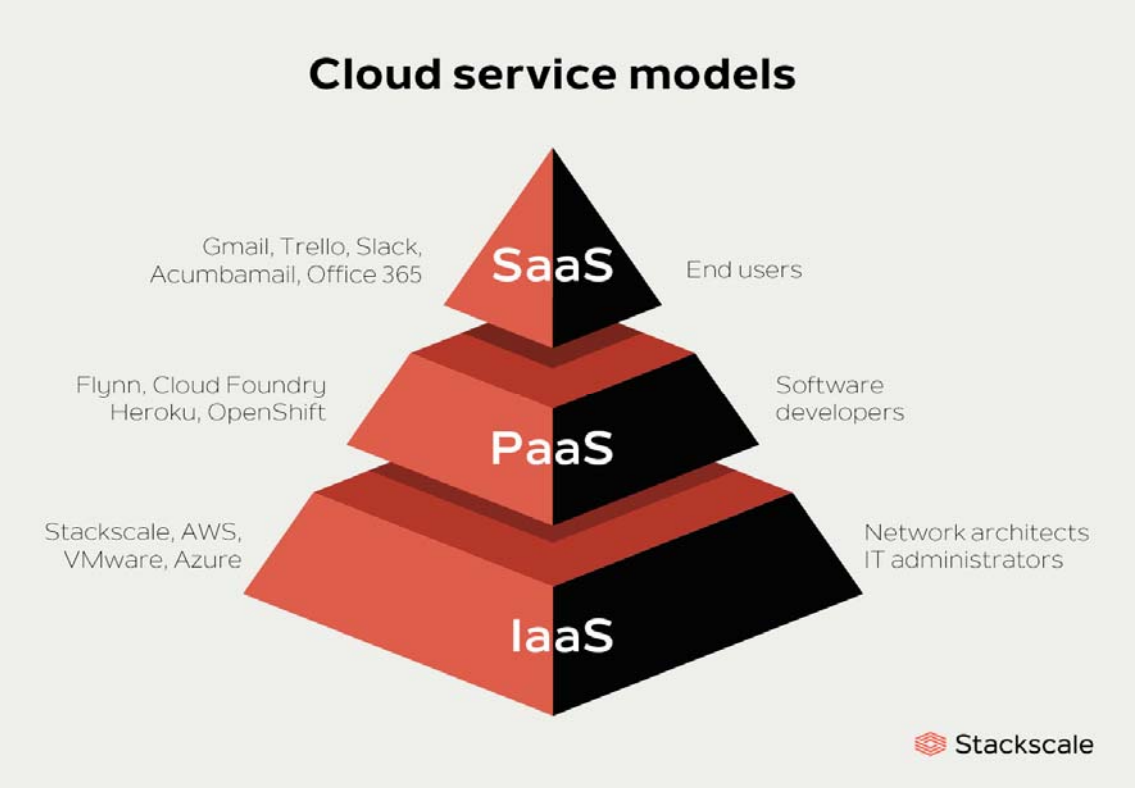

Figura 5 tipos de serviços nuvem retirado de (Stackscale, 2020)

2.2.1Infrastructure as a Service (IaaS)

IaaS tem como grande vantagem, o alugar de hardware, possibilitando aos clientes terem controlo do equipamento, e caso seja necessário alocar mais recursos em tempo real ou quase em tempo real. Este tipo de serviço é aprovisionado e gerido através da Internet (Microsoft, 2020).

Este tipo de serviço possibilita então que os clientes instalarem o que for necessário para satisfazer as suas necessidades. O fornecedor tem apenas que garantir o acesso à gestão das máquinas e dos recursos alocados. O cliente por outro lado tem à sua responsabilidade, toda a gestão das aplicações e serviços nela instalados, desde o Sistema Operativo à gestão da base de dados e das aplicações.

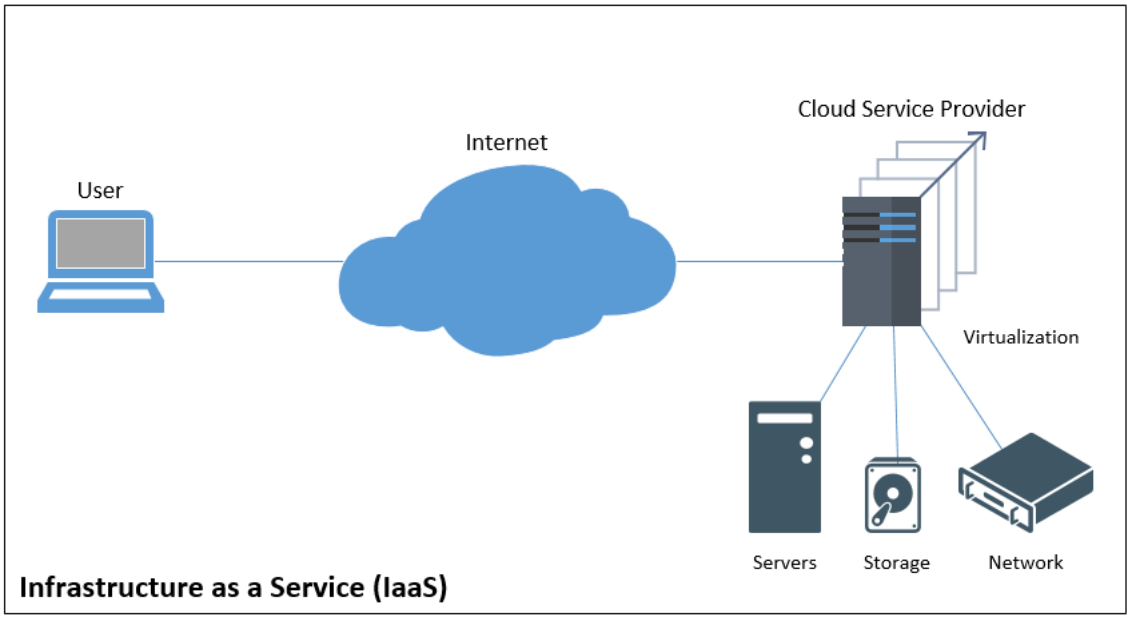

Figura 6 Infrastructure as a Service retirado de (Death, 2017)

2.2.2 Platformas a Service (PaaS)

Paa permite o alugar de um sistema totalmente funcional, pronto para o cliente instalar e testar qualquer tipo de aplicação ou serviço desde software tradicional a configuração de *Web Servers* (Microsoft, 2020).

Este conceito é ideal seja para testar algum tipo de implementação numa empresa, seja para realizar um *lift and Shift* que significa a passagem dos serviços presentes em *datacenters* locais para gestão centralizada na nuvem.

O fornecedor de serviços de nuvem tem a responsabilidade da gestão das aplicações prestadoras de serviços e da infraestrutura base.

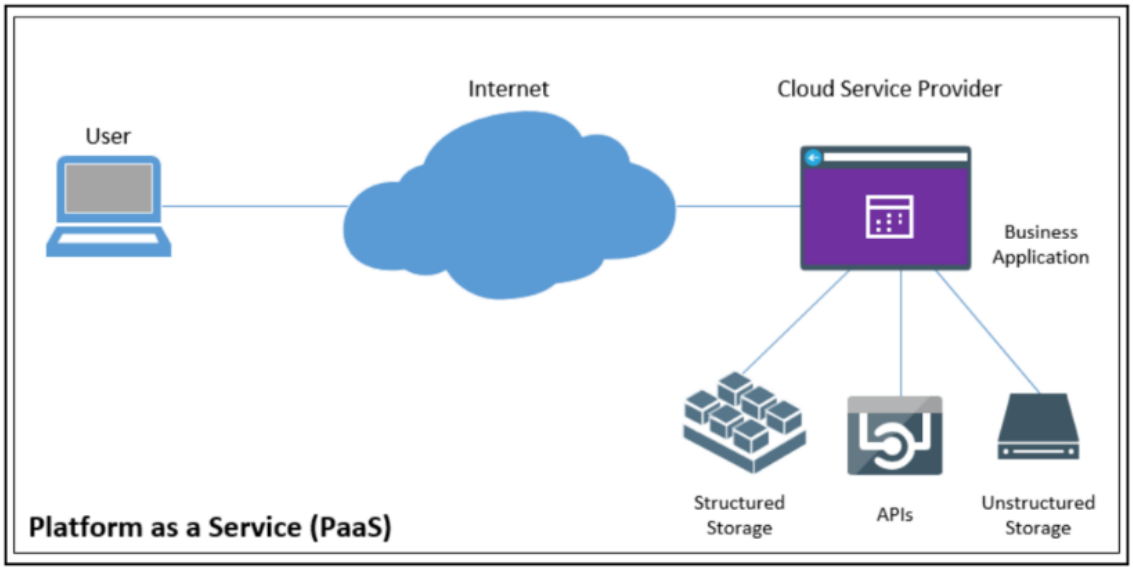

Figura 7 Plataform as a Service retirado de (Death, 2017)

2.2.3 Software as a Service (SaaS)

O fornecedor de serviços nuvem tem a capacidade de disponibilizar *software* baseado em computação distribuída, como por exemplo Microsoft *office 365* que contém serviço de *email* e aplicações *web* (Microsoft, 2020).

Os custos são baseados no modelo *pay as you go* cuja principal vantagem reside no facto de os custos crescerem conforme as funcionalidades acrescidas desejadas pelos clientes.

A gestão deste tipo de serviço é inteiramente feita pelo fornecedor de serviços na nuvem (Microsoft, 2020).

De acordo com (Araujo, 2013) exitem 2 categorias principais de *software as a service*:

- *Line of business services:* serviço fornecido a todo o tipo de empresas, soluções customizáveis e de grande calibre de forma a tornar simples os processos financeiros e a relação entre o cliente e a instituição. Estes serviços são cobrados em forma de subscrições.
- *Consumer-oriented services offered to the general users,* este tipo de serviços é também por vezes cobrado em forma de subscrição ao consumidor final, ou fornecido de forma gratuita e financiado através de publicidade.

A Figura 8, apresenta diversas plataformas que possuem uma implementação na nuvem como o email, Wordpress entre outros.

Figura 8 Software as a Service retirado de (juridoc, 2020)

2.3 Conceito *Firewall*

O conceito de Firewall refere-se a um dispositivo de segurança de rede que filtra através de políticas de segurança previamente configuradas, o tipo de informação autorizada entre redes externas (*Internet*) e redes internas (Watchguard, 2020).

Pode tratar-se de um equipamento físico ou virtual essencial numa rede empresarial que oferece uma gama alargada de serviços.

Se for colocada no topo da infraestrutura, ligada em modo *bridge* com o equipamento do operador de comunicações, tem a capacidade de filtrar conteúdo de e para a *Internet* e criação de regras personalizadas de segurança.

Possui também a capacidade de atribuir endereços de IP aos equipamentos localizados na rede (*DHCP*) e resolução de nomes (*DNS*).

É possível ainda configurar este equipamento para estabelecer ligações *VPN, site-to-site* encriptadas expandido desta forma a mesma rede e acessos em todos os locais geográficos da empresa.

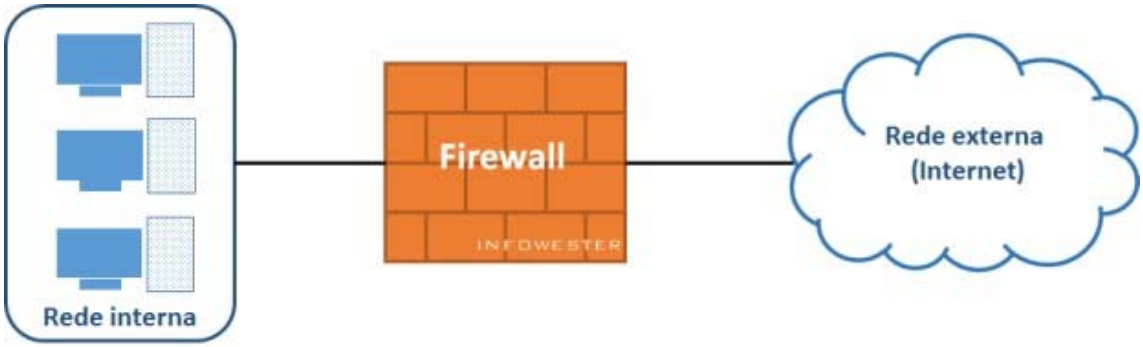

Figura 9 Conceito Firewall retirado de (Alecrim, 2013)

2.4 Dynamic Host Configuration Protocol (DHCP)

DHCP é um protocolo cliente servidor que fornece um identificador único a cada dispositivo presente na rede interna. Este identificador único transmite-se num endereço *IP* que fica alocado ao dispositivo durante um determinado período temporal e pode ser ou não renovado ao final desse tempo.

Para além de ser alocado um endereço *IP* ao dispositivo, é ainda transmitida informação adicional como a máscara *subnet* que representa um determinado intervalo de endereços *IP* aos quais o dispositivo pode efetuar comunicações e o qual o *default gateway,* endereço *IP* por omissão que os dispositivos clientes devem redirecionar o seu trafego (Microsoft, 2020).

Esta função pode estar presente em firewall, servidores ou routers, onde através da configuração do Protocolo *DHCP* é possível definir a/as gamas de endereços *IP* numa determinada mascara de *sub-net* e *default gateway*.

Tecnicamente, o protocolo *DHCP* é uma comunicação que inicia quando um dispositivo se conecta a uma rede, efetuando um pedido em *Broadcast* para a rede inteira com o objetivo de localizar o servidor *DHCP,* este ultimo por sua vez responde com uma mensagem em que se identifica responsável por essa funcionalidade na rede (caso exista mais do que um servidor *DHCP* na rede, o cliente escolhe o que tiver menos latência). O dispositivo cliente envia uma mensagem em *unicast* para o endereço que respondeu ser responsável pelo *DHCP* requisitando um endereço *IP* para si próprio. O servidor *DHCP* caso existam endereços *IP* disponíveis irá responder, alocando assim um endereço *IP* ao dispositivo (T. Mrugalski, 2018).

As principais mensagens incluídas no protocolo *DHCP* são as seguintes (T. Mrugalski, 2018):

1 ***SOLICIT –*** Mensagem enviada pelo dispositivo cliente com o objetivo de localizar o/os servidores *DHCP* presentes na rede.

2 ***ADVERTISE –*** Mensagem enviada pelo servidor *DHCP* indicando que é responsável pelo serviço *DHCP,* reposta direta à mensagem *SOLICIT.*

3 ***REQUEST –*** Mensagem enviada pelo dispositivo cliente requisitando as configurações *DHCP* presentes incluindo endereço *IP* que irá ser alocado ao próprio, a subnet a que pertence e o *Default Gateway.*

4 ***CONFIRM –*** O dispositivo cliente, envia uma mensagem ao servidor com o objetivo de determinar se o endereço alocado ainda se encontra atualizado para efetuar comunicações na rede que se encontra.

5 ***RENEW –*** O dispositivo cliente envia uma mensagem para o servidor DHCP anteriormente contactado para renovar o *DHCP Lease* assignado ao próprio.

6 ***REBIND –*** O dispositivo cliente envia uma mensagem ao servidor *DHCP* para expandir o *DHCP Lease* e atualizar configurações que possam ter sido alteradas.

7 ***REPLY –*** O servidor envia uma mensagem de resposta contendo o endereço *IP* e configurações ao cliente, trata-se de uma resposta a uma mensagem de caracter *Solicit, Request, Renew* ou *Rebind*.

8 ***RELEASE –*** O dispositivo cliente, envia uma mensagem ao servidor com o objetivo de informar que não irá usar mais as configurações fornecidas.

9 ***DECLINE –*** O dispositivo cliente envia uma mensagem ao servidor indicando que o endereço *IP* disponibilizado já se encontra em utilização na rede em que o dispositivo cliente está inserido.

10 ***RECONFIGURE –*** O servidor envia uma mensagem ao dispositivo cliente para informar que as configurações *DHCP* sofreram alterações e como consequência o dispositivo cliente irá ter que enviar ter que efetuar uma comunicação *Renew/Reply*, *Rebind/Reply* ou *Information-Request/Reply* com o servidor para receber as novas configurações

11 ***INFORMATION-REQUEST –*** O dispositivo cliente envia uma mensagem ao servidor *DHCP* de caracter meramente informativo, requisitando as configurações *DHCP* sem lhe ser atribuído nenhum *DHCP Lease*

2.5 Domain Name System (DNS)

Domain Name System, trata-se de um serviço hospedado em servidores localizados na Internet ou numa rede privada que contém uma base de dados que apresenta um mapeamento de endereços *IP* ao *hostname* associado. Estes servidores auxiliam os dispositivos clientes na resolução de nomes para os endereços *IP*.

Uma vez que os humanos memorizam mais facilmente nomes que números e sabendo que os dispositivos cliente utilizam o protocolo *TCP/IP* para comunicarem com um determinado destino na Internet e este protocolo utiliza apenas endereços IP, é necessário que exista esta resolução de nomes, caso contrário, os utilizadores iriam necessitar de memorizar os endereços *IP* que desejam comunicar.

Este sistema foi implementado durante a década de 80, anterior a esta altura, existia um sistema central que possuía um ficheiro de texto denominado "HOSTS" que armazenava todos os *hostnames* e os endereços *IP* correspondentes a todas as máquinas na Internet (Sanjay, 2018).

A figura 10, ilustra um pedido efetuado por um computador para visualizar a página *foobar.com*, o pedido é feito inicialmente ao servidor *DNS* que responde com o endereço *IP* correspondente ao nome *foobar.com*, com esta informação, o computador já pode efetuar o pedido diretamente ao servidor onde está alojado a página uma vez que já tem conhecimento do seu endereço *IP*.

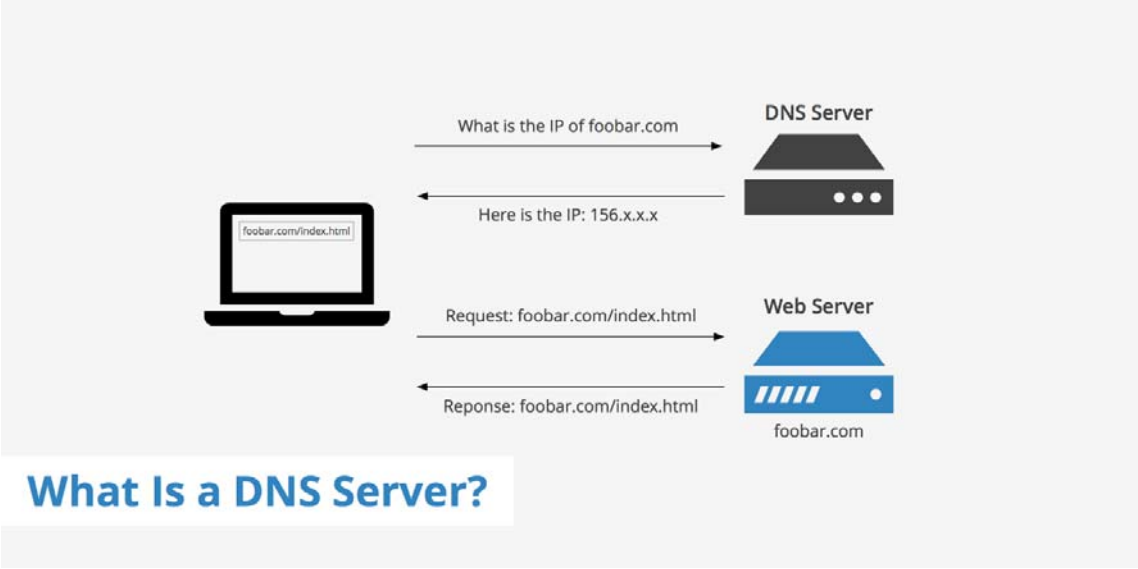

Figura 10 DNS Server retirado de (Coelho, 2019)

2.6 Domain Controller e Active Directory

Domain Controller é um conceito que se aplica quando existe uma máquina com o *Windows Server* instalado e que esteja a correr o serviço de *Active Directory* e por associação DNS, tornando-se desta forma responsável pelo domínio criado e pela resolução de nomes internamente. (Microsoft, 2020)

Os servidores que têm este tipo de *roles*, são responsáveis por armazenar numa base de dados, todos os objetos existentes num determinado domínio, como computadores, utilizadores, grupos e os atributos associados assim como autenticar todos os utilizadores de domínio (Microsoft, 2020).

Existe também a possibilidade de replicar automaticamente configurando um determinado intervalo de tempo, a base de dados para outro servidor, tornando assim o *role* de *Domain Controller* redundante numa determinada infraestrutura tecnológica empresarial.

Através do *Active Directory*, é permitido gerir o conteúdo da base dados (computadores, utilizadores e grupos), podendo estabelecer determinadas regras como por exemplo complexidade de *password* dos utilizadores ou mandar executar determinados scripts e tarefas durante o login. É a partir desta ferramenta que são configurados os acessos a determinada informação relativos aos utilizadores.

Todos as máquinas inseridas no domínio (caso utilizadores tenham permissões), podem consultar a base de dados presentes num *Domain Controller* através do protocolo LDAP, sendo desta forma possível configurar acessos a partir de uma plataforma centralizada.

2.7 Conceito Domínio

O domínio refere-se a um conjunto de objetos em que podem estar inseridos milhares de máquinas, utilizadores e grupos. (Microsoft, 2020)

Através da implementação de um domínio é possível agrupar de forma centralizada todos os objetos presentes numa determinada rede.

Dependendo do tipo de solução, uma empresa pode ter diversos domínios ou apenas um único, mesmo tendo diversas localizações físicas geograficamente.

2.8 Replicação *DFS*

A replicação DFS, é caracterizada pela replicação de informação entre 2 ou mais servidores, em que qualquer alteração efetuada, é replicada para os restantes membros inseridos no grupo de replicação (Microsoft, 2019).

Este tipo de replicação, utiliza um algoritmo *remote differential compression*, capaz de identificar as alterações efetuadas ao nível de blocos de ficheiros, e apenas sincroniza essa mesma informação quando o ficheiro não estiver a ser utilizado. (Microsoft, 2019)

É ainda possível limitar a velocidade de sincronização de forma a não causar constrangimentos na rede e causar *downtime* para os utilizadores.

2.9 Remote Desktop Services (RDS)

Remote Desktop Services é a plataforma de virtualização que permite aos utilizadores utilizarem software necessário para o seu trabalho no dia a dia instalado em máquinas na nuvem (Microsoft, 2017).

Esta plataforma abrange várias possíveis soluções, desde virtualização de um ambiente remoto na sua totalidade a apenas a aplicação em si, a primeira opção é extremamente viável para empresas que tenham *thin clients* (computadores simples sem sistema operativo e sem grande poder de computação), a segunda opção permite a utilizadores executarem aplicações remotas de forma semelhante a aplicações locais, de forma transparente para os utilizadores.

A figura 11 representa diversas máquinas clientes conectadas a um único servidor.

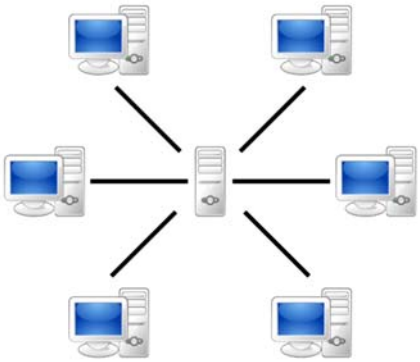

Figura 11 clientes conectados a um servidor retirado de (Wikipedia, 2020)

2.9 Lightweight Directory Access Protocol (LDAP)

Este protocolo é baseado no modelo cliente-servidor em que a comunicação é efetuada por TCP/IP que tem como principal função, realizar *querys* e modificar serviços de diretório.

Um diretório LDAP é uma série de objetos que possuem identificadores únicos e atributos similares organizados de forma lógica e hierárquica (Hristov, 2016).

O identificador único de cada objeto possui um *distinguished name (DN)* constituído pelo *Relative distiguished name (RDN)* construído a partir de alguns atributos do objeto seguido pelo *DN* do nível superior.

A máquina cliente inicia a sessão LDAP quando contacta o servidor LDAP. Após estabelecer esta conexão, o cliente envia pedidos seja para consultar a base de dados de diretório ou para alterar conteúdos.

A pesquisa LDAP, permite o acesso a uma parte da base dados que corresponde ao critério utilizado.

A autenticação de uma máquina cliente inserida num domínio é realizada através deste método, a máquina ao receber as credenciais de domínio, realiza uma comunicação com o *Domain Controller* de forma a verificar a veracidade das credenciais utilizadas.

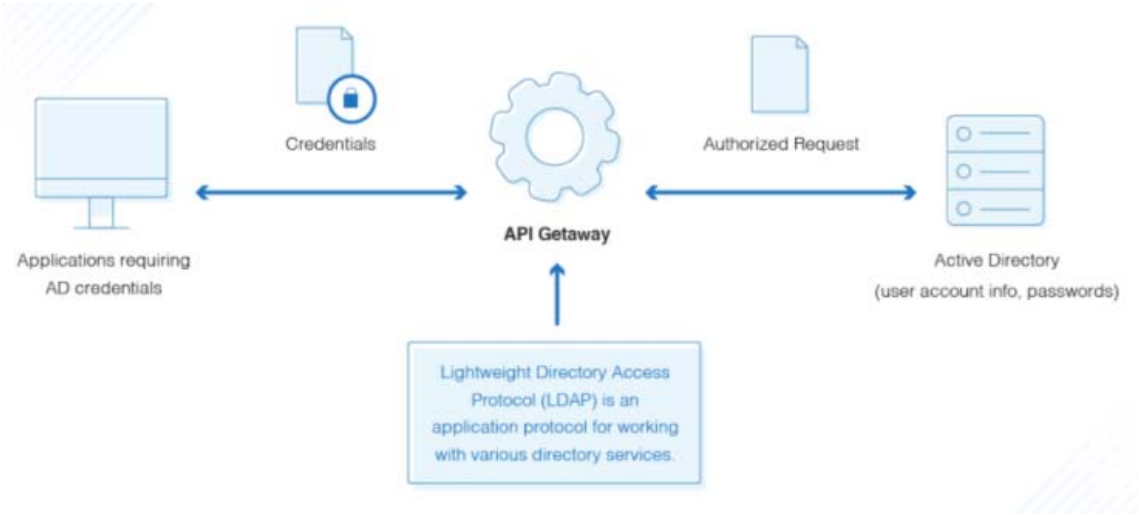

Figura 12 autenticação LDAP retirado de (dnsstuff, 2020)

2.11 Virtual Private Network (VPN)

Uma *Virtual Private Network,* permite que um dispositivo se conecte a uma *LAN* através de uma comunicação encriptada, também conhecido por túnel utilizando a Internet *(WAN)* como linha de transporte.

A comunicação encriptada permite garantir a integridade dos dados transmitidos entre o dispositivo e a rede a que o mesmo se conecta. Utilizando uma chave que apenas o dispositivo autorizado e o equipamento ao qual se conecta conhece, previne desta forma que equipamentos ou utilizadores maliciosos possam "escutar" a comunicação.

Esta ligação permite também que os utilizadores possam trabalhar de forma segura e remotamente, acedendo aos recursos locais da empresa (Cisco, 2020).

Os equipamentos que fornecem o serviço VPN, obrigam a que os utilizadores/dispositivos conectados obedeçam a uma série de requisitos previamente definidos para ser possível estabelecer um túnel entre ambos.

Existem 2 tipos de VPN:

- ***Remote Access-*** permite que dispositivos como computadores e telemóveis fora da rede empresarial, se conectem à mesma, acedendo desta forma aos recursos necessários permitindo assim ao utilizador trabalhar a partir de casa.
- ***Site-to-Site-*** Este tipo de VPN, permite expandir a rede de uma determinada empresa entre vários escritórios, com posições geográficas diferentes, são utilizados equipamentos que permitem estabelecer uma rota física ou virtual de forma dinâmica ou estática.

A figura 12 representa uma ligação *VPN* encriptada para aceder de forma privada à Internet.

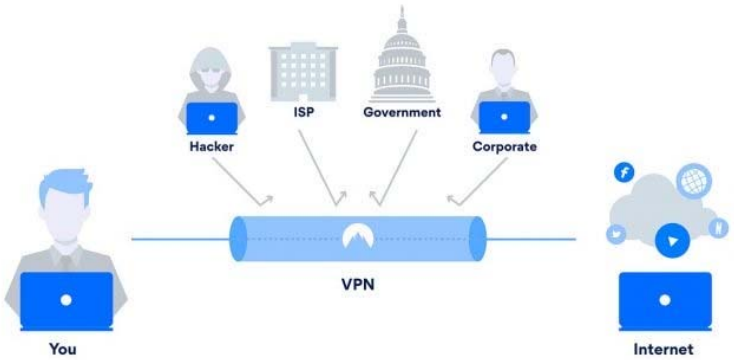

Figura 13 Ligação VPN retirado de (Gogoni, n.d.)

2.12 Shadow Copy

Usando o serviço de *Shadow copy* fornecido pelo Windows, pode-se efetuar uma cópia de ficheiros partilhados em rede em determinadas alturas do dia, possibilitando os próprios utilizadores recuperarem informação eliminada equivocamente, aumentando assim a produtividade reduzindo em paralelo os custos de administração do sistema (Microsoft, 2019).

A cópia efetuada e armazenada temporariamente, tem apenas permissões de leitura, negando assim a possibilidade de prejudicar a integridade do *backup* efetuado naquela altura.

O máximo de informação permitida através deste serviço é de 64TB.

Uma solução completa de VSS necessita dos seguintes componentes:

- ***VSS Service-*** Serviço do sistema operativo responsável pela intercomunicação entre os componentes necessários;
- ***VSS Requester-*** Este serviço refere-se ao *software* que efetua o pedido para a criação das *shadow copies*, pode-se referir ao *software* incluindo no *Windows* ou desenvolvido por terceiros;
- ***VSS Writer-*** Componente que garante a integridade dos dados que irão ser armazenados, incluídos no *Windows* ou desenvolvidos por terceiros;
- ***VSS Provider-*** Componente que cria e administra as *shadow copies* pode ser executado no *hardware* de forma a não sobrecarregar os recursos alocados a outras tarefas ou a nível de *software* sendo que o sistema operativo *Windows* já inclui este componente.

O *VSS Provider* pode executar a cópia de um dos 3 métodos descritos:

- ***Complete copy-*** Este método é uma cópia completa ou clone da localização original no ponto escolhido;
- ***Copy-on-write-*** Este método efetua uma cópia diferencial apenas dos ficheiros que foram alterados;
- ***Redirect-on-write-*** Este método efetua uma cópia diferencial da localização original para uma drive numa localização externa.

2.13 Internet Protocol v4 e v6

Os endereços IP, têm a principal função de identificar um dispositivo numa rede, como uma morada identifica uma casa. A nomenclatura deste endereço necessita de ser interpretado pelos equipamentos como tal, é constituído por 4 octetos totalizando 32 bits no caso do *IPv4* ou 8 grupos de 4 dígitos hexadecimais totalizando 128 em *IPv6.*

Cada equipamento conectado a uma determinada rede, seja em *LAN* ou *WAN*, necessita de possuir um endereço único que irá permitir que os dispositivos consigam localizar e comunicar entre si.

Os endereços *IP,* podem ser divididos em 3 classes, normalmente designadas por A, B e C que tem as seguintes configurações (Banzal, 2007):

- **Classe A**- O primeiro octeto é utilizado para identificar a *network ID* enquanto os restantes 3 octetos são identificadores do *host ID;*
  Mascara *Subnet*: 255.0.0.0
- **Classe B**- Os dois primeiros octetos são utilizados para identificar a *network ID* enquanto os restantes 2 octetos são identificadores do *host ID*
  Mascara *Subnet*: 255.255.0.0
- **Classe C**- Os 3 primeiros octetos são utilizados para identificar a *network ID* enquanto o restante octeto é utilizado para identificar o *host ID.*
  Mascara *Subnet*: 255.255.255.0

2.14 Local Area Network

A *Local Area Network,* é constituída por dispositivos conectados entre si numa rede que pode ser doméstica onde normalmente trata-se de uma localização geográfica pequena ou empresarial que pode estender-se a vários países ou escritórios separados fisicamente.

As grandes vantagens deste tipo de rede é que permite a partilha de ficheiros, impressoras, e podem inclusive obter controlo sobre outros equipamentos dentro da mesma rede (Cisco, n.d.).

2.15 Wide Area Network

A *Wide Area Network,* refere-se a um conjunto de redes onde a comunicação é efetuada através de routers que reencaminham as mensagens para os dispositivos inseridos dentro de cada rede.

Um exemplo de uma *WAN* é a própria Internet (Cisco, n.d.).

2.16 *Open System Interconnection Model* (Modelo *OSI)*

O modelo OSI, serve como referência mais básica e essencial de *networking* desde que foi idealizado em 1984. Este modelo tem como principal objetivo, definir regras padrão para os diferentes produtores de equipamentos de *networking* para que estes possam comunicar entre si.

O modelo OSI, representa uma arquitetura hierárquica que compartimenta logicamente as funcionalidades necessárias para existir uma comunicação entre sistemas (Miller, 2020).

O modelo de OSI possui 7 camadas, cada camada possui um nível de abstração e uma função bem definida. Os princípios que foram aplicados para definir cada uma das camadas foram os seguintes (Miller, 2020):

- Cada camada deve ser criada quando um nível diferente de abstração for necessário;
- Cada camada deve possuir uma função bem definida e estruturada;
- A função de cada camada, deve ser idealizada tendo sempre em consideração os protocolos utilizados como padrão internacionalmente;
- As fronteiras de cada camada devem ser idealizadas com o objetivo de minimizar a quantidade de informação transportada pelas interfaces;
- O número de camadas deve ser em número suficiente para distinguir as funções das restantes camadas e não deve ser muito extenso ao ponto de se tornar confuso.

A divisão em camadas, permite separar as funções de *networking* em partes lógicas e simples e permite ainda escalabilidade, novos protocolos ou serviços são mais fáceis de adicionar numa arquitetura em camadas.

As 7 camadas de OSI são descritas como (Miller, 2020):

1. ***Physical Layer-*** A camada física está encarregue de transmitir dados em bruto (bits) através de um canal de comunicação. Esta camada tem o objetivo de que quando o emissor envia 1 bit de informação, o mesmo bit deve ser recebido como 1 bit no recetor e não como 0 bit.

2. ***Data Link Layer-*** A principal função desta camada e transformar os dados brutos em transmissões livres de erros na camada de rede. Esta tarefa é realizada através do emissor que divide os dados em *data frames*, sendo estes transmitidos de forma sequencial. O recetor tem por sua vez que confirmar que recebeu estes pacotes ao recetor.

3. ***Network Layer-*** Esta camada permite controlar o tráfego presente numa *sub-net*, efetuando o roteamento dos pacotes e controlo de congestionamento da própria rede. Esta camada suporta transmissões *connectionless* e *connection-oriented.* Os equipamentos (switches) presentes nesta camada, determinam através de tabelas estáticas qual a maneira mais eficiente de transmitir o tráfego.

4. ***Transport Layer-*** A função principal desta camada é transformar os dados provenientes da *session layer,* dividindo-os em unidades mais pequenas e encaminhar para a *network layer.* Esta camada tem ainda que garantir que os bits enviados são os mesmos que foram transmitidos, sem modificações, perca ou duplicação. Caso ocorra algum erro na transmissão, a *transport layer* é responsável por corrigi-lo. Existem uma série de regras para correção de erros, pode ser necessário transmitir apenas os dados que ficaram corrompidos ou reiniciar toda a transmissão. Estas correções apenas são possíveis através da confirmação de Receção do pacote, caso não exista esta confirmação, a *transport layer* pode retransmitir o pacote ou despoletar um erro de *time-out.*

5. ***Session Layer-*** Esta camada permite que 2 entidades troquem comunicações através de uma rede. As aplicações em ambas as entidades, podem trocar dados entre si enquanto a sessão estiver ativa. Esta camada é responsável pela preparação da sessão, troca de mensagens e terminar a sessão quando estiver concluída. Esta sessão pode ser usada para realizar login num sistema ou transferir ficheiros entre 2 máquinas. A *session layer* tem ainda a opção de controlar a comunicação entre as 2 entidades, esta comunicação pode ser feita apenas numa direção de cada vez ou em ambas as direções simultaneamente. A atribuição de *tokens* permite controlar quem efetua a comunicação no canal, impedindo assim que o transmissor e o recetor efetuem a mesma tarefa simultaneamente. Um dos requisitos para a comunicação nesta camada é a sincronização entre ambas as máquinas, caso ocorra algum problema na transmissão de dados, é possível transmitir a partir do último momento em que ambos tinham conectividade, não sendo necessário a transmissão desde o início.

6. ***Presentation Layer-*** Esta camada é responsável pelo formato, sintaxe e semântica dos dados transferidos. Para mensagens transmitidas, converte os dados num formato genérico. Para mensagens recebidas converte os dados que estão num formato genérico num formato que seja possível interpretar pela aplicação que espera a transmissão. Diferentes máquinas possuem diferentes códigos para representar os mesmos dados. Esta camada possibilita que a comunicação entre os sistemas seja efetuada numa linguagem comum através da encriptação por exemplo.

7. ***Application Layer***- Esta camada permite que as aplicações acedam aos serviços de *networking* que suportam aplicações diretamente. Esta camada permite ainda que as aplicações passem por uma validação de segurança e autenticação. Esta aplicação permite as seguintes funcionalidades:
    - *File transfer, Access and Management (FTAM)*- Habilita serviços numa rede como por exemplo, mover ficheiros entre diferentes sistemas, leitura, escrita, remoção e gestão de ficheiros localizados remotamente;
    - *Virtual Terminal (VT)*- Fornece serviços que possibilita o acesso a aplicações em diferentes sistemas computacionais.
    - *Electronic Mail and Messaging Handling (MHS)*- Facilita a troca de mensagens eletrónicas e documentos.
    - *Directory Services (DS)*- Fornece serviços cuja função é associar nomes a endereços.
    - *Common management Information Protocol (CMIP)*- Fornece serviços para gerir redes.

A figura 13 representa a arquitetura e interações entre as diferentes camadas do.

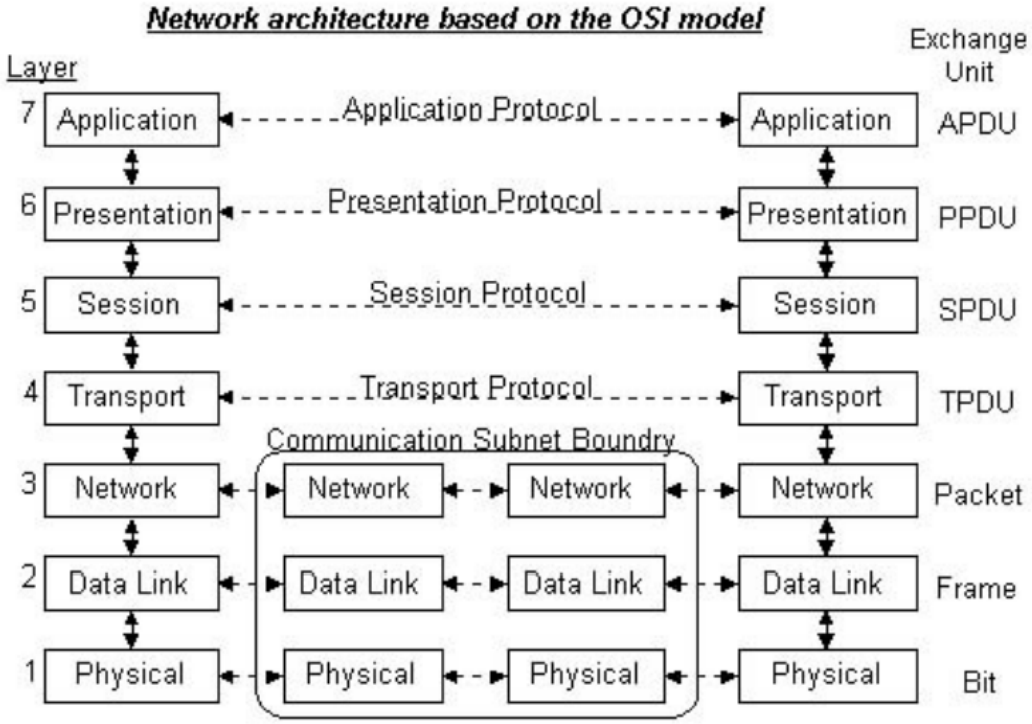

Figura 14 Arquitetura do modelo OSI retirado de (Miller, 2020)

2.17 Virtualização

Com o crescimento natural das empresas, os departamentos de informática são confrontados com desafios novos e complexos para acompanhar este crescimento. À medida que os colaboradores, parceiros empresariais e clientes exigem uma resposta mais rápida, eficiente e aplicações sofisticadas, a infraestrutura IT tem de expandir e inovar, colocando mais pressão no departamento de IT (VMWARE).

A tecnologia de virtualização ajuda a responder a estas necessidades e desafios. Onde era necessário gastar cerca de 70% do orçamento alocado ao departamento de informática para a manutenção dos equipamentos e renovação, com a adição que um servidor físico com apenas um sistema operativo possui cerca de 12% de eficiência. (VMWARE).

A virtualização de máquinas, responde a estas necessidades permitindo que múltiplos sistemas operativos e aplicações sejam executados a partir de uma única máquina física ou "*host"*.

O conceito de virtualização tem como característica principal a possibilidade de criar máquinas virtuais que podem possuir um sistema operativo e aplicações associadas. Uma vez que cada máquina virtual é completamente independente, podem ser executadas múltiplas instâncias utilizando apenas uma máquina física.

O software denominado por "*hypervisor"* desassocia a máquina virtual do "*host"* permitindo assim alocar dinamicamente recursos conforme necessidade.

Este tipo de tecnologia, redefina o conceito de computação e possui as seguintes vantagens (VMWARE):

- **Múltiplas aplicações em cada servidor:** Uma vez que cada máquina virtual encapsula e simula uma máquina física, é possível executar múltiplas aplicações e sistemas operativos a partir de um único servidor físico.
- **Máxima utilização dos recursos do servidor, minimizando quantidade de servidores:** Cada máquina física é aproveitada ao máximo da sua capacidade, permitindo assim reduzir custos uma vez que é minimizado o número de servidores fisicos.
- **Facilidade e rapidez em alocar Aplicações e recursos:** Através da utilização de máquinas virtuais, que contém ficheiros de software em que é possível manipular as mesmas e efetuar processos de migração, apenas copiando e colando os ficheiros. Esta característica, permite ao IT rapidez, facilidade e flexibilidade na gestão da infraestrutura. É possível ainda efetuar o processo de "*live migration"* que se caracteriza pela transferência de máquinas virtuais que estão ativas entre servidores físicos.

2.18 Engenharia de Requisitos

Engenharia de requisitos refere-se a uma comunicação intensiva entre o analista e o cliente sobre o propósito da construção de um determinado *software*, quais as funções que o mesmo irá realizar e qual o contexto em que se insere (Kotonya & Sommerville, 1998).

Esta atividade realizada pelo analista denomina-se por levantamento de requisitos, sendo que um requisito retrata uma necessidade que uma determinada entidade necessita de satisfazer através da implementação de uma solução tecnológica (IEEE, 1996).

(IEEE, 1998) define o conceito de requisitos a partir de três declarações:

1- Uma condição que necessita de ser atingida de forma a resolver uma necessidade ou um objetivo para uma entidade.
2- Uma condição que necessita de ser satisfeita para cumprir um contrato ou especificação de um determinado sistema desenvolvido.
3- Uma representação documentada das condições descritas no ponto 1 e 2

2.18.1 Requisitos Funcionais

De acordo com (Bourque & Fairley, 2014) os requisitos funcionais, representam as funções que o *software* desenhado necessita de executar, cada requisito funcional pode ainda ser descrito como um dos passos necessários para validar o comportamento desejado por parte da aplicação desenhada.

(Fernandes & Machado, 2015) descreve um requisito funcional como uma função que pode ser executada pelos utilizadores do sistema despoletando uma resposta a um determinado estímulo imposto pelos utilizadores. Os requisitos funcionais devem ainda estar inseridos nas fases de conceção e implementação do sistema.

2.18.2 Requisitos Não Funcionais

Requisitos não funcionais como aqueles que limitam a solução apresentada, podem ainda ser descritos como requisitos de qualidade que adicionam valor a solução (Bourque & Fairley, 2014).

Fernandes e Machado, retratam os requisitos não funcionais como um conjunto de complementos, que tornam a solução mais atrativa, por exemplo rapidez, utilidade e confiabilidade da mesma (Fernandes & Machado, 2015).

3 Desenho da solução Atual

Conforme descrito no capítulo 1.2 deste relatório, é então possível verificar que a empresa descrita possui uma infraestrutura rudimentar que necessita de melhorias de forma a melhorar e tornar eficiente os processos de admissão e configuração de utilizadores/máquinas.

Durante análise localmente na empresa, foi possível realizar o desenho de rede descrito na figura 15.

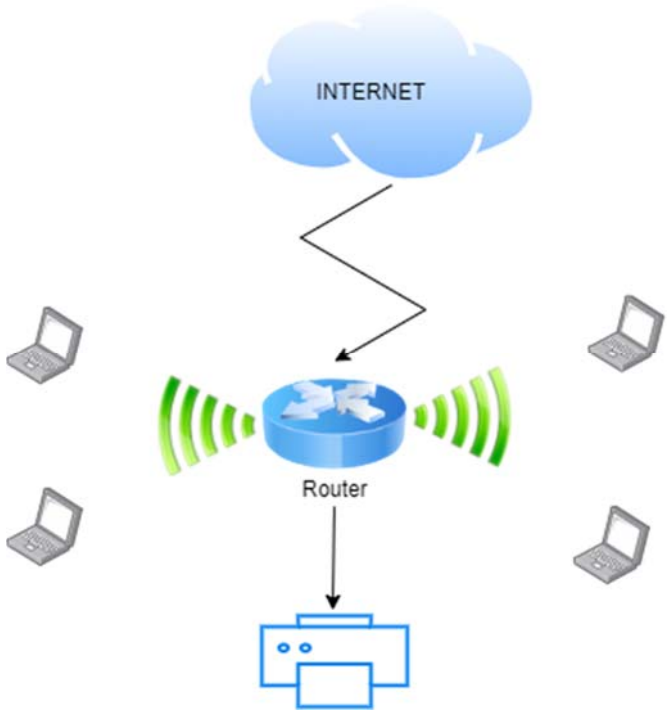

Figura 15 Diagrama de rede inicial

Após esta análise foi então possível efetuar o levantamento de requisitos funcionais e não funcionais descritos no capítulo 4 deste relatório.

4 ESPECIFICAÇÃO DE REQUISITOS

Neste capítulo são especificados os requisitos funcionais e não funcionais do sistema, com base num diagrama de casos de uso.

Casos de uso

Os casos de uso descrevem as funções que os atores podem realizar no sistema, apresentando uma visão geral da funcionalidade do sistema.
A figura 18 descreve os casos de uso com a implementação realizada.

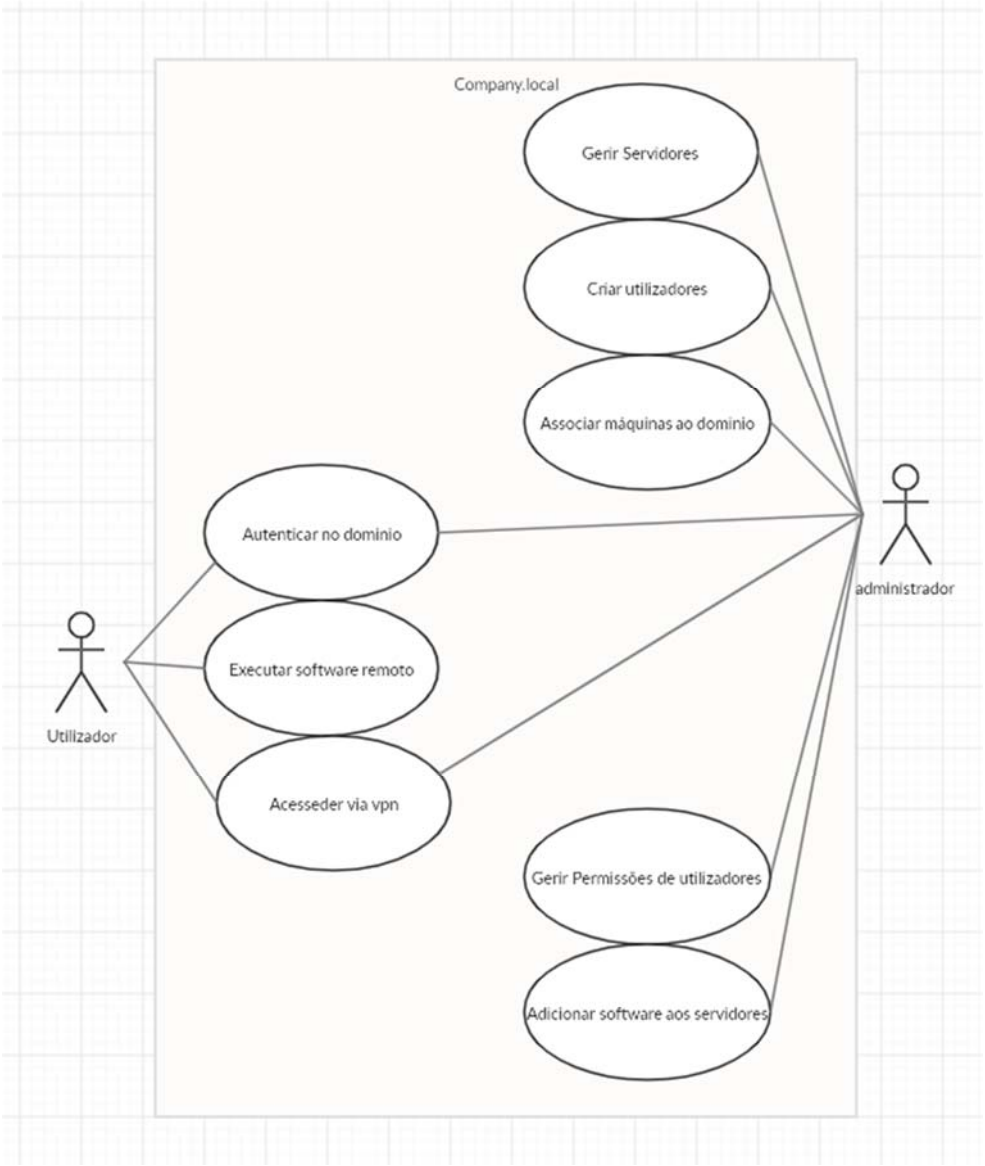

Figura 16 Diagrama de Casos de Uso

Neste diagrama são identificados os atores presentes no sistema, que são:

- Utilizador: É qualquer utilizador humano que pertence aos colaboradores da empresa e que possui permissões limitadas;
- Administrador: É uma generalização de Utilizador que tem permissões totais sobre toda a infraestrutura de domínio, é a partir deste utilizador que os serviços críticos são executados.

Ao nível das relações dos atores com o sistema implementado, as relações identificadas no sistema são:

- Autenticar Utilizador no Domínio: O utilizador tem permissões para fazer login nos computadores inseridos no domínio, mediante permissões;
- Executar Software Remoto: O utilizador autenticado poderá executar software que esteja a ser partilhado pelo servidor aplicacional desde que tenha permissões para tal;
- Aceder via VPN, caso o utilizador esteja criado na *firewall* com permissões, é possível aceder aos recursos de forma remota;
- Gerir servidores: O administrador tem permissões totais sobre os mesmos, logo pode instalar/modificar qualquer aplicação inerente aos mesmos;
- Criar utilizadores: O administrador tem permissões para criar e modificar utilizadores de domínio através da *Active Directory;*
- Associar máquinas ao domínio: O administrador, possui permissões para associar máquinas ao domínio;
- Gerir permissões de utilizadores: Através da Active Directory, o administrador tem a possibilidade de manipular as permissões dos utilizadores inseridos no domínio;
- Adicionar Software aos servidores: Uma vez que o administrador possui total controle sobre os servidores, este pode adicionar ou remover software dos servidores;

4.1 Requisitos Funcionais

Do Diagrama de Casos de Uso e de acordo com as necessidades da empresa tipo, resulta a especificação de requisitos funcionais apresentada na tabela apresentada na tabela 1. A experiência profissional em Administração de sistemas do autor deste trabalho e o feedback do CEO da empresa tipo, foi possível analisar um padrão de necessidades identificadas em pequenas e médias empresas. O levantamento de requisitos é sempre um fator essencial quando se efetua uma implementação ou alteração a uma infraestrutura que pode afetar o workflow de uma empresa.

Cada código referencia a descrição de um requisito e ao mesmo tempo a sua prioridade referente à funcionalidade do sistrema. As prioridades estão classificadas em alta, média ou baixa. Para a coluna das prioridades entende-se: Alta- Serviços críticos indispensável para a infraestrutura, Média- Completa a infraestrutura, mas não se trata de um serviço critico, Baixa- Implementação/configuração facultativa.

Código	Prioridade	Descrição do requisito
RF01	Alta	Pretende-se gerir os utilizadores e computadores associados a um domínio.
RF02	Média	Pretende-se gerir os acessos de cada utilizador.
RF03	Alta	Permitir a disponibilização de *software* mediante permissões.
RF04	Alta	Desenvolver a pasta partilhada em rede com 5 GB e com replicação para outro servidor.
RF05	Alta	Possibilidade de criar utilizadores.
RF06	Alta	O sistema deve permitir a criação de tarefas automatizadas sem interação humana.
RF07	Alta	O sistema deve permitir acesso remoto via VPN aos recursos company.local.
RF08	Alta	Pretende-se gerir a informação através de permissões aplicadas a cada utilizador.
RF09	Alta	Configurar replicação do *Fileshare* para outro servidor.
RF10	Média	Deconvolver *Secondary Domain Controler* com replicação.
RF11	Alta	Permitir autenticação em qualquer máquina registada no domínio.
RF12	Média	Pretende-se que os utilizadores acedam a *software* fornecido pelo servidor aplicacional.

Tabela 1 Requisitos Funcionais: Sistema

4.2 Requisitos não funcionais

A revisão da literatura e as necessidades identificadas pela empresa tipo em estudo, permitem identificar os requisitos não funcionais indicados na tabela 2 em baixo.

Cada código referencia a descrição de um requisito e ao mesmo tempo a sua prioridade referente à funcionalidade do sistrema. As prioridades estão classificadas em alta, média ou baixa. Para a coluna das prioridades entende-se: Alta- Serviços críticos indispensável para a infraestrutura, Média- Completa a infraestrutura, mas não se trata de um serviço critico, Baixa- Implementação/configuração facultativa.

Código	Prioridade	Descrição do requisito
RF01	Alta	O sistema deve ser desenvolvido recorrendo às ferramentas nativas da *Microsoft*
RF02	Média	Pretende-se que os utilizadores acedam a *software* fornecido pelo servidor aplicacional
RF03	Alta	O sistema deve estar disponível 99.9% do tempo em horário 24/7
RF04	Baixa	Os servidores devem demorar no máximo 10 minutos a reiniciar
RF05	Alta	A autenticação efetuada pelos utilizadores deve ser garantida pelas ferramentas de segurança da Microsoft
RF06	Baixa	Os servidores devem estar configurados em linguagem simples e universal (Inglês).
RF7	Média	A utilização deve ser transparente para os utilizadores.
RF8	Alta	O sistema deve ser escalável.
RF9	Baixa	A necessidade de instalar *software* de terceiros deve ser inexistente.
RF10	Baixo	O sistema deve ser intuitivo de implementar.
RF11	Média	O sistema deve possibilitar a integração com sistemas baseados na Nuvem como *Azure Active Directory* ou *Office 365.*
RF12	Alta	O sistema deve possuir uma camada adicional de segurança através da autenticação dos utilizadores.

Tabela 2 Requisitos não funcionais: Sistema

5 Desenho da solução implementada

5.1 Arquitetura do sistema

O autor propõe que a solução seja constituída por uma máquina *Linux com* que tem o *software* de *firewall PFSense* instalado e que serve toda a infraestrutura incluindo a máquina física em que está hospedado todas as máquinas virtuais necessárias ao trabalho.

O trabalho descrito ao longo deste relatório, é caracterizado por um sistema físico de máquinas que inicia com o router da Operadora que comunica diretamente com a *Internet*, este equipamento está configurado em modo *Bridge* com a Firewall que por sua vez está conectado a um *switch* que transmite o sinal para a restante infraestrutura conforme no diagrama de rede.

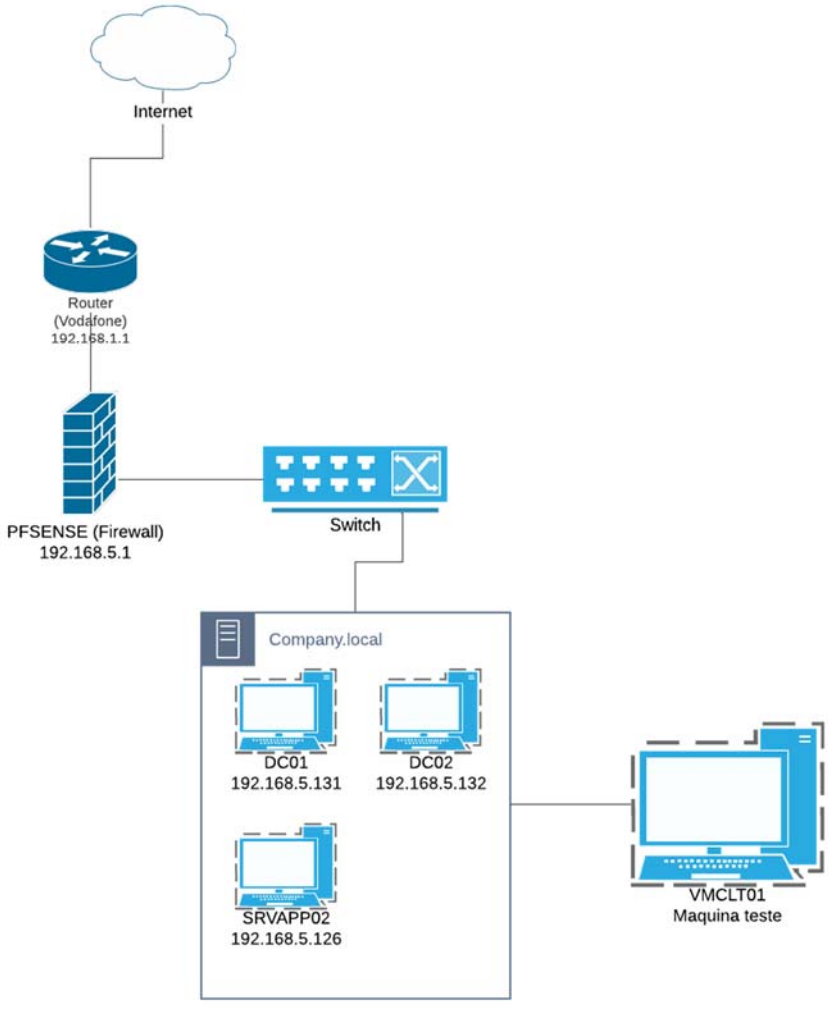

Figura 17 Desenho Fisico

As 3 máquinas virtuais (*guests*) estão configuradas a partir do Software *VMware Workstation 15 Player*, foi escolhido este software, uma vez que permite configurar manualmente as placas de rede emuladas, simulando assim uma infraestrutura empresarial.

A figura 15 ilustra o desenho lógico da infraestrutura onde é possível ter uma visão geral sobre como o sistema de virtualização está implementado.

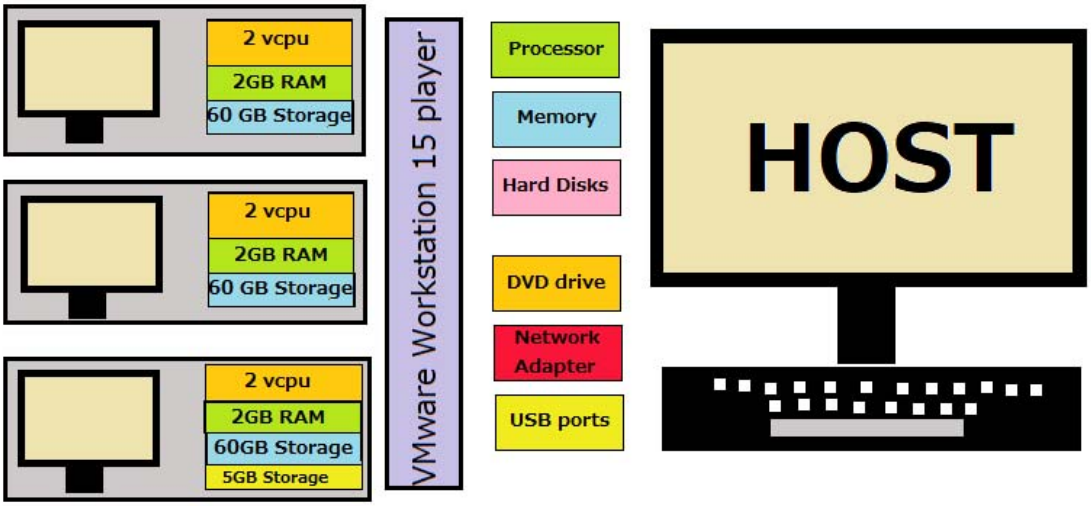

Figura 18 Desenho lógico

5.2 Arquitetura *Firewall*

A máquina *Linux* que tem o *software* da *firewall* (*PFSense*) instalado tem os seguintes componentes: Processador *Intel* (R) *Celeron* (R) CPU N3150 @ 1.60GHZ, 8GB de *RAM*, 65GB SSD, possui a versão *Linux FreeBSD* 11.3 *Stable* e a versão da *PFSense* 2.4.5.

Figura 19 *Firewall*

Foi também criado o aceso *VPN* que possibilita o acesso a partir de qualquer dispositivo desde sistemas operativos *android* e *IOS* a *Windows* e *Mac OS* mesmo fora da rede em que está inserido a infraestrutura do trabalho como demonstrado na figura 3.

A ligação é efetuada através do *OpenVPN Client* que é possível fazer o *download* diretamente da página de gestão da *Firewall*.

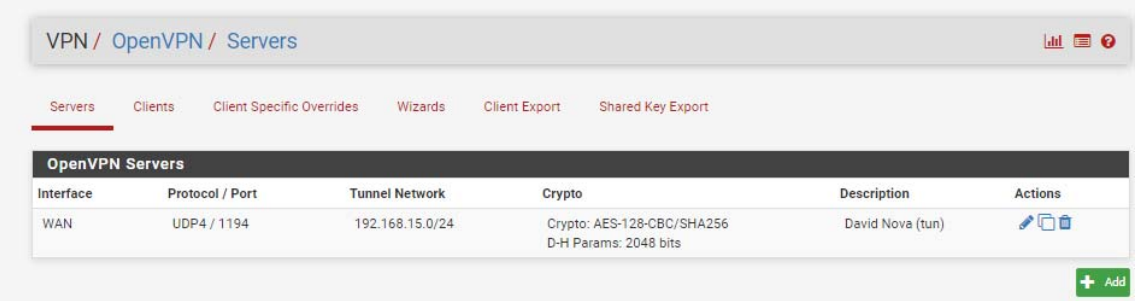

Figura 20 Configuração VPN

5.3 Arquitetura da máquina *host*

A máquina que contém os componentes abaixo, contém todas as máquinas virtuais essenciais para a infraestrutura do domínio *company.local.* As máquinas virtuais (*guests*) foram desenvolvidas a partir do *software VMware Workstation 15 player* e assentam no disco HDD, pois apesar de ser mais lento, é o que tem mais espaço para armazenar as máquinas.

Os componentes desta máquina são: Processador *Intel Core* i7-7700k @4.20GHZ, *motherboard Asus Prime* Z270-K, 16GB *RAM* DDR4 3200MHZ, possui dois discos de armazenamento, M.2 2280 *Samsung* 970 *Evo Plus* 250 GB SSD e 3,5" *Seagate* Barracuda 2 TB 7200RPM 2TB HDD, possui ainda o *Windows 10 PRO* como sistema Operativo e uma placa Gráfica MSI *Geforce* GTX 1080 TI 11GB GDDR5.

5.4 Arquitetura das máquinas *Guest*

As máquinas virtuais que constituem este sistema, possuem uma lista de componentes padrão salvo o *Secondary Domain Controller* que tem a adição de possuir um *fileshare*.

O sistema é constituído por 3 servidores virtuais, DC01 (*Domain Controller),* DC02 (*Secondary Domain* Controller*)* e SRVAPP02 (Servidor aplicacional) e uma máquina também ela virtual para testar as implementações.

Cada Máquina virtual tem 2 processadores lógicos, 2GB *RAM* e 60GB de armazenamento, sendo que o DC02 tem a adição de um disco adicional de 5GB. Os servidores possuem um sistema operativo *Windows Server 2016 Standard Evaluation* enquanto a máquina de testes possui um *Windows 10 PRO.*

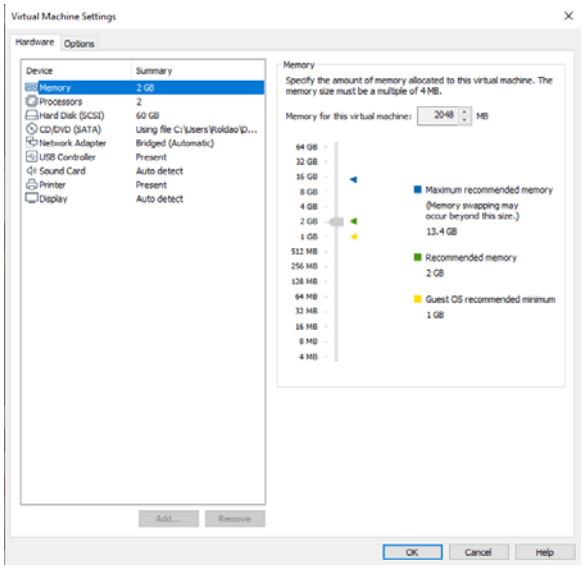

Figura 21 Configuração máquinas virtuais

5.5 Componentes de *Software*

A presente secção demonstra a grande vantagem deste trabalho. Na máquina *host* apenas será necessário instalar qualquer versão do Windows 10 e o software *VMware Workstation 15 Player* onde será possível configurar e criar todas as máquinas virtuais necessárias para a implementação.

Por outro lado, nas máquinas virtuais, será necessário instalar o *Windows Server stantard 2016* e associar as roles necessárias através do *Server Manager* (já incluído na versão do Windows). Em concreto:

1) ***Primary Domain Controller – Hostname DC01***

- Active Directory Domain Services (AD DS)
- Domain Name System
- File and Storage Services

2) ***Secondary Domain Controller – Hostname DC02***

- Active Directory Domain Services (AD DS)
- Domain Name System
- File and Storage Services
- DFS Management

3) ***Remote APP Server – Hostname SRVAPP02***

- File and Storage Services
- Internet Information Services (IIS) Manager
- Remote Desktop Services

6 IMPLEMENTAÇAO DO SISTEMA

O presente capítulo, irá demonstrar a interação e comunicação dos vários *roles* associados a cada servidor, esta demonstração irá ser efetuada através de ilustrações e descrições associada.

Cada função presente nos servidores, pode ser associada a um tipo de serviço de nuvem, para além das máquinas virtuais em si serem *Infrastructure as a service* (IAAS) tem-se:

- ***Domain Controller-*** *Platform as a service.*
- ***Secondary Domain Controller-*** *Platform as a service.*
- ***Remote Desktop Services-*** *Software as a service.*
- ***Fileshare-*** *Platform as a service.*
- ***Shadow copy-*** *Platform as a service.*
- ***DFS Replication-*** *Platform as a service.*

6.1 Primary Domain Controller and Secondary Domain Controller

O servidor que desempenha a função de *Primary Domain Controller (DC01),* onde está apenas configurado a *role* de *Active Directory* e *DNS,* comunica e replica a informação presente na *Active Directory* com o *Secondary Domain Controller (DC02).* O servidor *Secondary Domain Controller*, possui ainda uma *Drive* adicional (*Fileshare*) que simula a informação partilhada entre os utilizadores numa empresa, esta *drive* partilhada, possui acessos limitados consoante as permissões de cada utilizador, e replica a informação através da tecnologia *DFS* para o servidor *DC01.*

A figura 19 ilustra a comunicação e replicação entre os servidores.

Figura 22 DC01 e DC02 interaction

6.2 Servidor Aplicacional

O servidor aplicacional (SRVAPP02), possui a *role* de *Remote Desktop Services* o que permite instalar uma determinada aplicação e partilhar a mesma com os utilizadores que foram previamente autorizadas a utilizar a mesma. Este servidor aplicacional, possui também a *role* de *IIS (Internet Information Services)* que permite hospedar um portal onde é possível descarregar o atalho para aceder ao software partilhado.

Se ocorrer uma tentativa de executar a aplicação por um utilizador que não esteja autorizado a tal, a ligação irá ser negada.

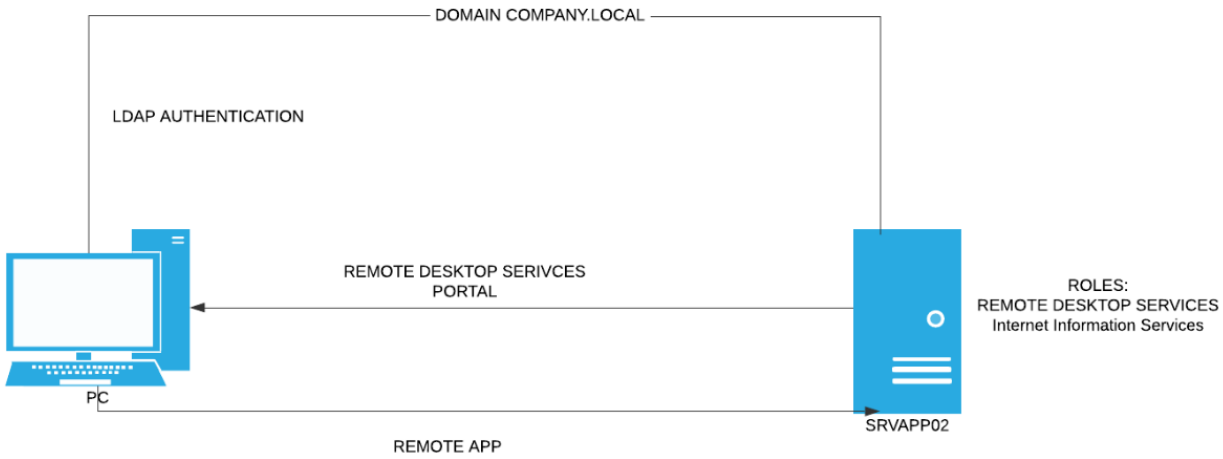

Figura 23 interação entre PC cliente e SRVAPP02

6.3 Reflexão de Custos

Na reflexão de custos de uma empresa são analisados serviços e orçamentos de maneira a efetuar uma simulação para minimizar custos, uma vez que os custos da infraestrutura tecnológica seja uma implementação híbrida, local ou nuvem, possuem um fator critico no orçamento de uma empresa.

Esta reflexão de custos ira representar uma comparação entre nuvem privada e nuvem publica assim como o custo de todo o hardware incluído na nuvem privada e os custos de optar por uma implementação em nuvem publica.

Os custos das soluções apresentadas, nomeadamente da nuvem privada, inclui as despesas variáveis como por exemplo a energia elétrica consumida pelo hardware.

A solução de nuvem privada ira apresentar também custos de *Manage Services* que se irá adaptar ao modelo de negócios do cliente, implementando assim trabalhos personalizáveis e customizáveis à medida.

A tabela 3 irá evidenciar os custos de hardware da implementação de nuvem privada onde assenta toda a infraestrutura descrita neste trabalho.

Hardware	**Descrição**	**Preço**
CPU	*Intel Core i7-7700K*	394,00€
Motherboard	*ASUS PRIME Z270-K*	119,85€
Fonte de Alimentação	*Nox Hummer 80+ Bronze 650W Semi Modular*	69,90€
GPU	*GeForce GTX 1080Ti Gaming X Trio 11GB GDDR5X*	940,00€
RAM	*G.SKILL Trident Z 16GB (2x8GB) DDR4-3600MHz*	129,00€
CPU Cooler	*Water Cooler CPU Corsair Hydro Series H100x 240mm*	91,90€
Caixa	*Extended-ATX Cooler Master MasterCase MC500M*	149,90€
SSD	*M.2 2280 Samsung 970 Evo Plus 250GB*	79,90€
HDD	*3.5" Seagate Barracuda 2TB 7200RPM 256MB SATA III*	62,90€
		2,037.35€

Tabela 3 *hardware cloud* privada

Os servidores descritos neste trabalho irão ter ainda um custo de operabilidade mensal para o cliente conforme descrito na tabela 4.

Hardware	**Descrição**	**Preço**
DC01	*Domain Controller*	80,00€
DC02	*Secondary Domain Controller e File Server*	90,00€
SRVAPP02	*Servidor aplicacional*	130,00€
		300,00€

Tabela 4 Custos de subscrição dos servidores

O autor deste trabalho irá ser responsável por realizar a manutenção dos servidores, garantir que os mesmos se encontram disponíveis para acesso por parte dos clientes e implementações novas a nível de infraestrutura solicitado pelo cliente.

De forma a prestar um serviço completo para os clientes, irá existir uma empresa parceira prestadora de *Manage Services* que irá realizar todas as implementações necessárias localmente e suporte técnico local, garantindo assim um serviço personalizado.

A tabela apresenta os custos destes serviços, sendo que estes podem ser alterados consoante as necessidades do cliente, garantindo assim um serviço justo para os clientes que realizam menos pedidos.

Os serviços prestados, estão divididos em avença de suporte técnico que implica um custo mensal ou bolsa de horas, em que o cliente pode comprar um determinado número de horas de suporte técnico.

Cenários	Descrição	Preço
Avença	Valor mensal	500,00€
Bolsa de horas	Valor unitário por hora	40,00€

Tabela 5 *Manage Services*

Uma vez que a implementação descrita neste trabalho assenta maioritariamente em plataformas e *software* fornecido pela própria *Microsoft*, o fornecedor de nuvem pública que irá ser alvo de comparação, será a *Microsoft Azure.*

Consultando a calculadora de preços fornecida pela *Microsoft Azure* em (Microsoft, 2020), é possível observarmos uma estimativa de quanto irá ser o custo mensal de uma infraestrutura semelhante (a funcionar 24/7), apenas com o Sistema Operativo e devida licença ativa sem estar configurado e personalizado para uma empresa ou necessidade especifica.

Assim sendo, a figura 21, ilustra os custos calculados, num ambiente *pay as you go*, sendo possível alterar posteriormente os recursos alocados às máquinas virtuais consoante necessidades, aumentando assim os custos mensais.

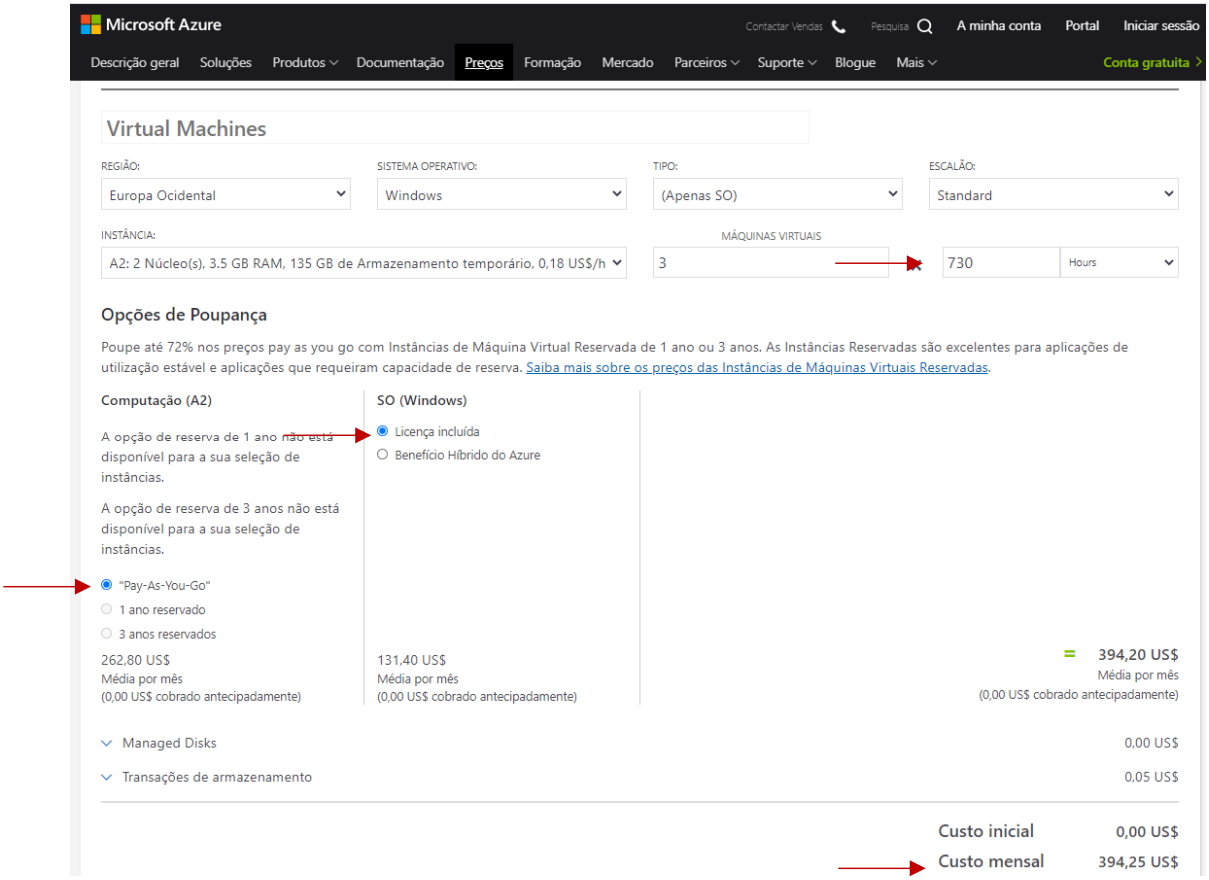

Figura 21 *Microsoft Azure Calculator* retirado de (Microsoft, 2020)

7 VALIDAÇÃO E DEMONSTRAÇÃO DE RESULTADOS

A prova de validação das funcionalidades de gestão de autenticação, gestão de acessos e segurança da informação, irá ser descrito nos pontos deste capítulo, juntamente com os fluxogramas associados.

7.1 Autenticação no domínio

Sendo que o sistema implementado foca-se principalmente em estabelecer um ponto central onde é possível gerir utilizadores e computadores, é necessário salientar que a autenticação é feita através do protocolo Kerberos.

Assumindo que a máquina encontra-se no domínio *company.local*, qualquer utilizador de domínio desde que tenha permissões para tal pode realizar login no computador sendo aplicadas as politicas referentes ao utilizador e/ou máquina.

O fluxograma deste tipo de autenticação está ilustrado na figura 24.

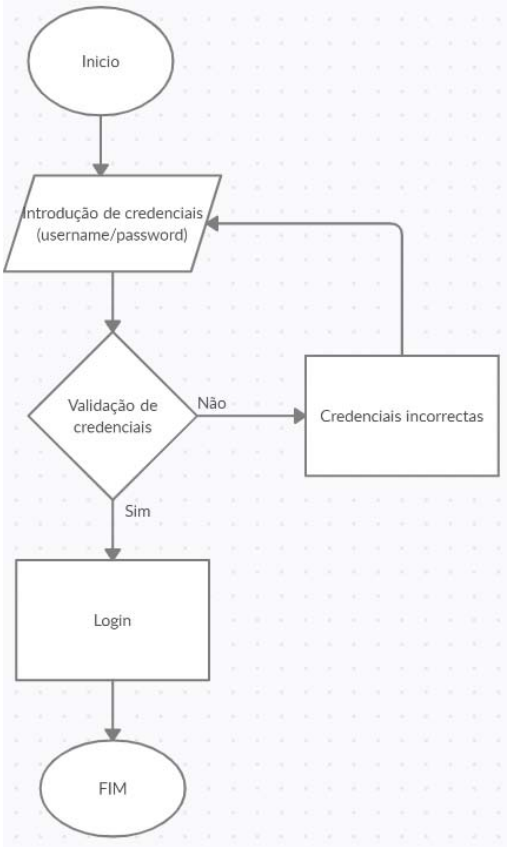

Figura 24 Fluxograma Autenticação

7.2 Gestão de acessos

Os acessos dos utilizadores são geridos através de grupos presentes na *Active Directory*, desde acessos a servidores, partilha de ficheiros ou aceder a *software* instalado no servidor aplicacional.

As permissões são validadas consoante as credenciais que são introduzidas. Numa infraestrutura de domínio, primeiro são validadas as permissões das credenciais em que o login é feito, caso o utilizador não tenha permissões para aceder ao recurso, irá surgir uma mensagem de acesso negado.

A figura 26, representa o fluxograma do processo de acesso à informação.

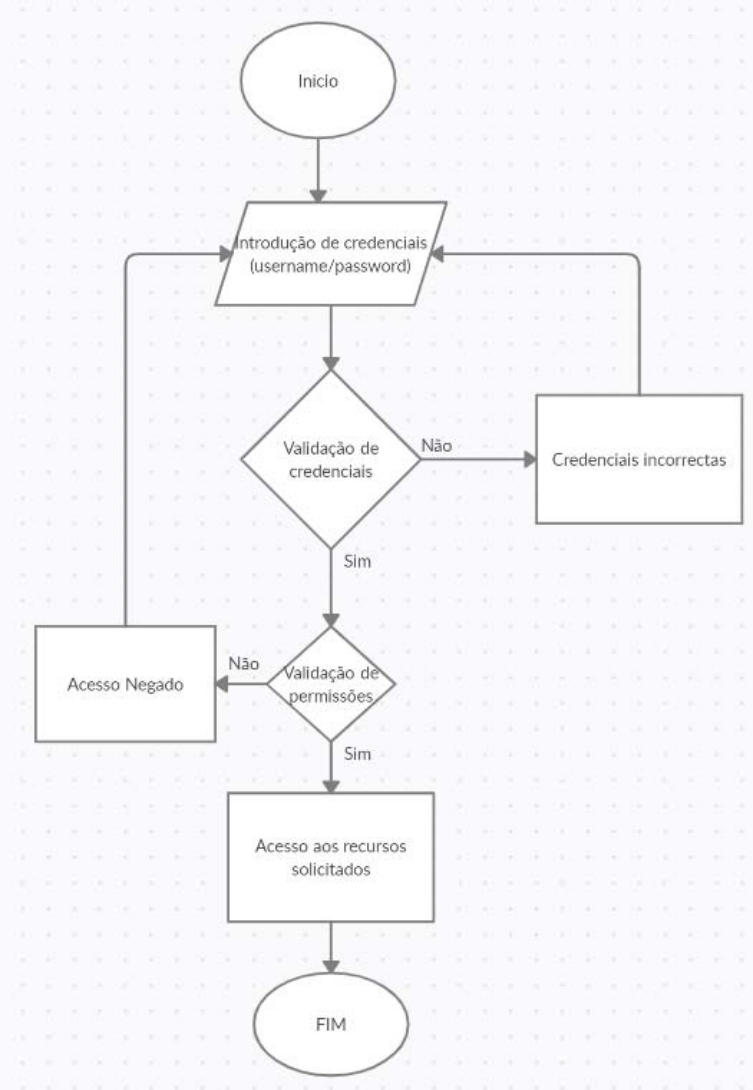

Figura 25 Fluxograma de permissões

7.3 Segurança da informação

A segurança da informação presente na infraestrutura do domínio *company.local*, é garantida através do protocolo *Kerberos.* Por outro lado, para aceder ao *software* presente no servidor aplicacional, é necessário possuírem um certificado digital instalado na máquina, para além de possuírem credenciais de dominio.

Quanto mais complexa e aleatória for a password dos utilizadores, mais resistente será a ataques de *password spraying* e *brute force*.

A infraestrutura do domínio, está salvaguardada pela firewall *PFSense*, a qual permite a criação de regras personalizadas sobre o tráfego que vai e vem da Internet. Até a data, não foram identificadas falhas de segurança na versão utilizada.

A maior falha de segurança identificada neste tipo de infraestrutura, são *malwares* que muitas vezes são instalados inadvertidamente pelos utilizadores, como forma de mitigar estes casos, os utilizadores padrão não possuem permissões para realizar login nos servidores nem são administradores locais com permissões para instalar software de forma autónoma.

A segurança no *software* partilhado através do servidor aplicacional, reside no facto de o mesmo ser apenas acessível quando a máquina cliente possui um certificado digital emitido pelo próprio servidor.

A figura 26 ilustra o certificado *self-signed* que necessita de estar instalado. Os processos de instalação e configuração do certificado estão descritos no capítulo 1.5 e 1.6 do Anexo I.

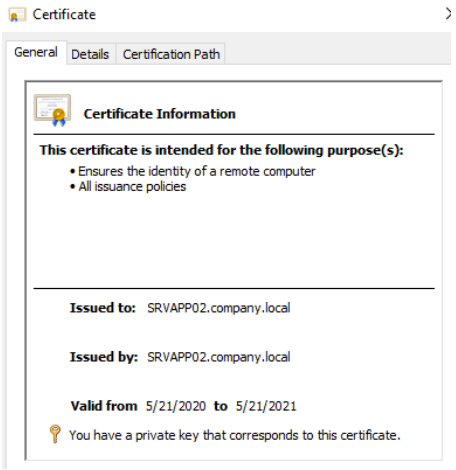

Figura 26 Certificado RemoteApp

7.4 Replicação Active Directory

A replicação entre os *Domain Controllers*, é configurada através do *Active Directory Sites and Services* e está a replicar informação de 10 em 10 minutos.

A figura 22 foi retirada do servidor *DC01* que comprova esta replicação

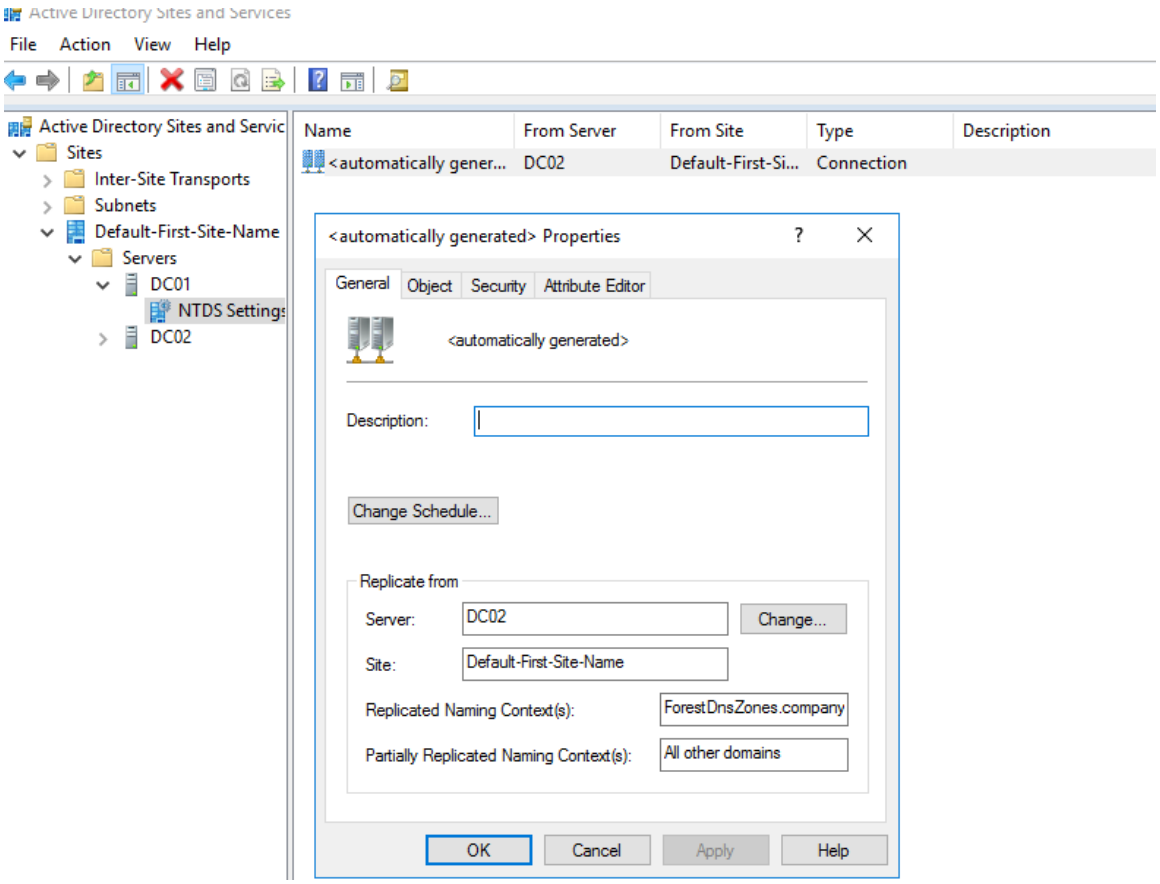

Figura 22 Active Directory Sites and Services

7.5 Replicação *DFS*

O servidor *Secondary Domain Controller* tem replicação DFS Configurada para tudo o que estiver na *drive* E:\ que contém o *fileshare*, ser replicada para o DC01 na localização C:\DFS_REP.

A figura 23 representa a validação deste processo.

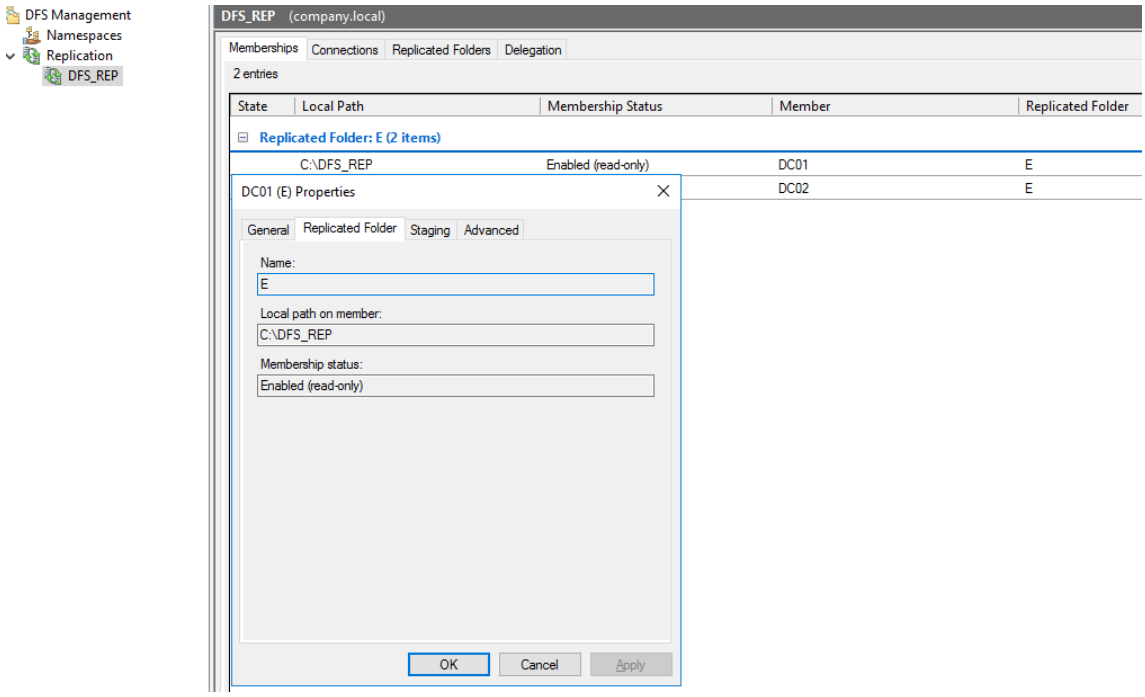

Figura 23 Replicação DFS

7.6 Validação configuração domínio, DNS, Fileshare e RemoteAPP

Foi criada uma máquina virtual que apenas contém a versão do *Windows 10 PRO* para comprovar as funcionalidades, uma vez que apenas podem ser comprovadas com uma máquina de testes.

Na figura 24, conseguimos confirmar que de facto quem atribui os IP's (DHCP Server) é a Firewall que tem o IP 192.168.5.1, o DNS primário refere-se ao DC01 que irá permitir resolver nomes internamente

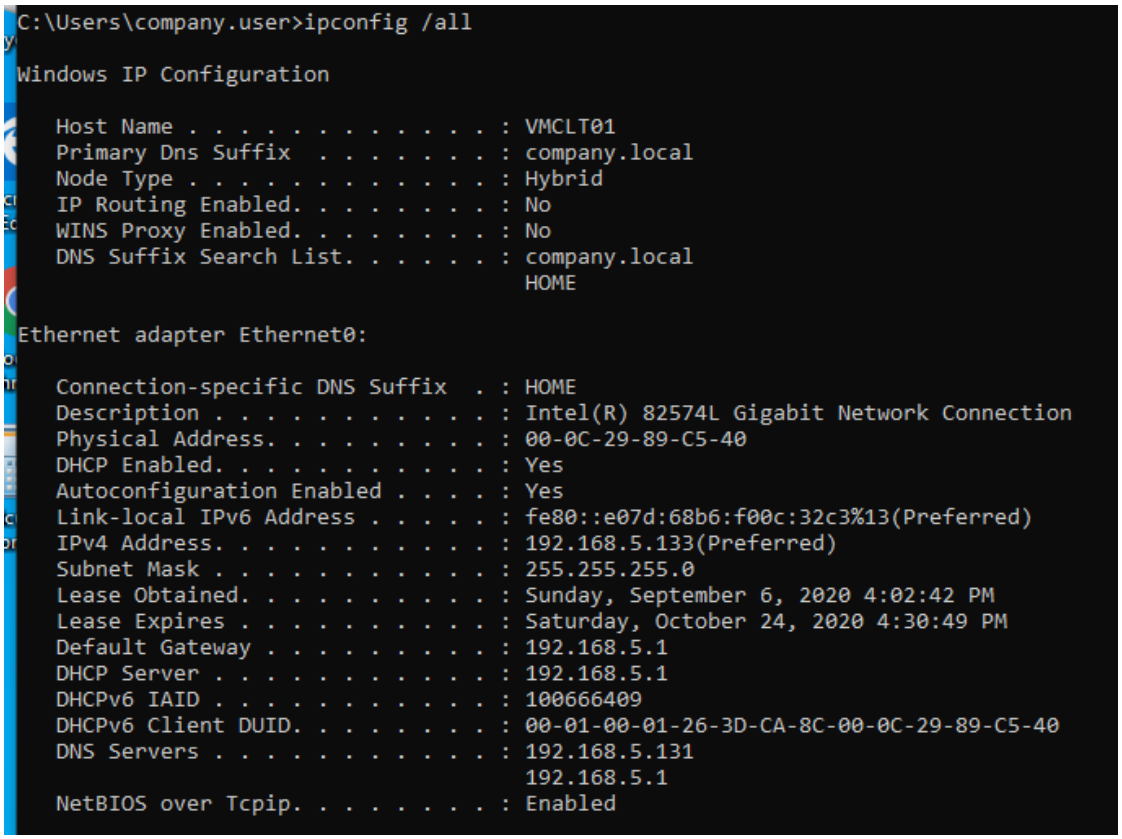

Figura 24 Informações de rede a partir da máquina cliente

A figura 25 comprova ainda que é possível resolver nomes internos e que ao efetuarmos uma pesquisa pelo nome do domínio (company.local), é-nos apresentado os endereços IP do DC01 e DC02, o que significa que caso um destes falhe, é possível continuar a resolver os nomes internos.

```
C:\Users\company.user>ping company.local

Pinging company.local [192.168.5.131] with 32 bytes of data:
Reply from 192.168.5.131: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.5.131:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\company.user>nslookup company.local
Server:  UnKnown
Address:  192.168.5.131

Name:    company.local
Addresses:  192.168.5.131
          192.168.5.132
```

Figura 27 Resolução de nomes internos

Na imagem 26 conseguimos ainda verificar que o utilizador que se encontra autenticado na máquina é o *company.local\company.user*, significando que se trata de um utilizador de domínio.

```
C:\Users\company.user>whoami
company\company.user
```

Figura 28 Utilizador autenticado na máquina cliente

A figura 27 comprova que na máquina cliente, existe o mapeamento do *fileshare* e o mesmo é efetuado via GPO conforme descrito no anexo deste trabalho.

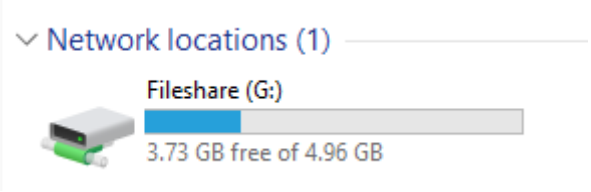

Figura 27 Mapeamento Fileshare máquina cliente

A Figura 28, comprova que o *Remote Desktop Services* instalado no servidor aplicacional está configurado de forma correta, uma vez que é possível adicionar a ligação por *Remote APP* ao mesmo a partir da máquina cliente e abrir a aplicação que o utilizador autenticado tem autorização.

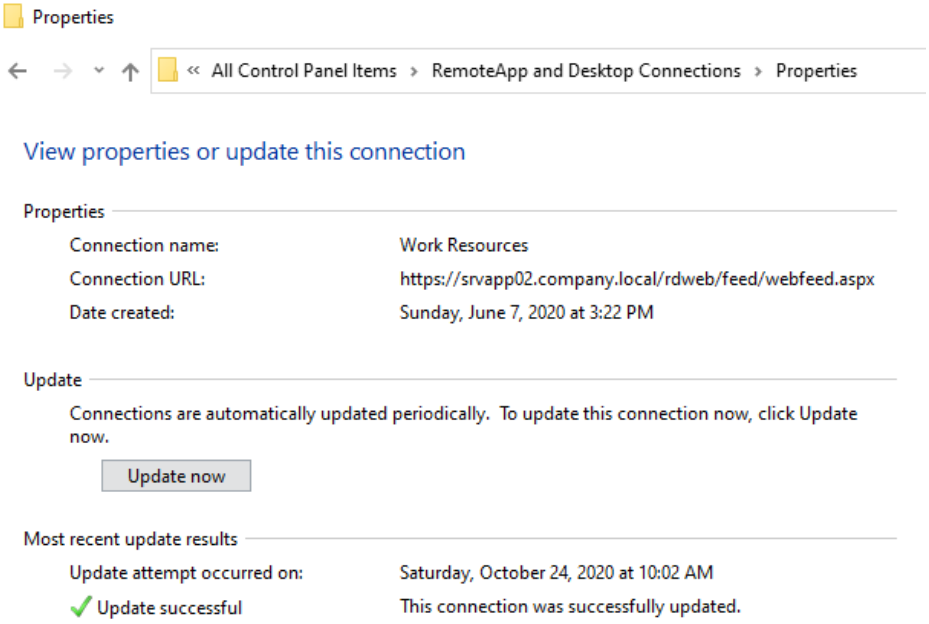

Figura 28 Configuração Remote APP

7.7 Validação de requisitos funcionais

Na tabela 6 é possível verificar que todos os requisitos funcionais foram cumpridos, obedecendo às soluções apresentadas.

Código	Prioridade	Descrição do requisito
RF01	Alta	Pretende-se gerir os utilizadores e computadores associados a um domínio.
Solução		Implementação de Active Directory.
RF02	Média	Pretende-se gerir os acessos de cada utilizador.
Solução		Criados grupos de utilizadores para aceder a diferentes acessos no sistema.
RF03	Alta	Permitir a disponibilização de *software* mediante permissões.
Solução		Implementação de Remote Desktop Services cujos acessos são controlados por grupos.
RF04	Alta	Desenvolver a pasta partilhada em rede com 5 GB e com replicação para outro servidor.
Solução		Adição de um disco virtual de 5GB e implementação da replicação DFS de todo o conteúdo.
RF05	Alta	Possibilidade de criar utilizadores.
Solução		Implementação de Active Directory.
RF06	Alta	O sistema deve permitir a criação de tarefas automatizadas sem interação humana.
Solução		Implementação de GPO através do group policy management.
RF07	Alta	O sistema deve permitir acesso remoto via VPN aos recursos company.local.
Solução		Criado perfil *VPN* na *Firewall* pfsense.
RF08	Alta	Pretende-se gerir a informação através de permissões aplicadas a cada utilizador.
Solução		Criados diversos grupos com acessos condicionados ao fileshare.
RF09	Alta	Configurar replicação do *Fileshare* para outro servidor.
Solução		Implementação de replicação DFS.

RF10	Média	Deconvolver *Secondary Domain Controler* com replicação.
Solução		Implementação de Secondary Domain Controller num servidor independente com replicação.
RF11	Alta	Permitir autenticação em qualquer máquina registada no domínio.
Solução		Implementação do domínio, registado máquinas no mesmo e criados utilizadores para o efeito.
RF12	Média	Pretende-se que os utilizadores acedam a *software* fornecido pelo servidor aplicacional.
Solução		Implementação de Remote Desktop Services.

Tabela 6 Validação de requisitos funcionais

7.8 Validação de requisitos Não funcionais

Na tabela 6 é possível verificar que todos os requisitos não funcionais foram cumpridos, obedecendo às soluções apresentadas.

Código	Prioridade	Descrição do requisito
RF01	Alta	O sistema deve ser desenvolvido recorrendo às ferramentas nativas da *Microsoft*
Solução		Todas as ferramentas utilizadas no trabalho são da Microsoft exceto a Firewall.
RF02	Média	Pretende-se que os utilizadores acedam a *software* fornecido pelo servidor aplicacional
Solução		Implementação de Remote Desktop Services e criados utilizadores para acesso.
RF03	Alta	O sistema deve estar disponível 99.9% do tempo em horário 24/7
Solução		Trabalho assente em máquinas virtuais de fácil transposição (caso seja necessário) e existe ainda uma UPS que alimenta o *host* e os equipamentos de comunicação.
RF04	Baixa	Os servidores devem demorar no máximo 10 minutos a reiniciar
Solução		Máquinas virtuais com performance para o efeito.

Código	Prioridade	Descrição do requisito
RF05	Alta	A autenticação efetuada pelos utilizadores deve ser garantida pelas ferramentas de segurança da Microsoft
Solução		Através da implementação de Active Directory, os utilizadores são autenticados através do protocolo LDAP
RF06	Baixa	Os servidores devem estar configurados em linguagem simples e universal (Inglês).
Solução		Os servidores e suas funcionalidades encontram-se todas em Inglês
RF7	Média	A utilização deve ser transparente para os utilizadores.
Solução		Os utilizadores não necessitam de saber como o sistema está implementado para conseguirem aceder.
RF8	Alta	O sistema deve ser escalável.
Solução		Trabalho assente em máquinas virtuais, que por definição são escaláveis.
RF9	Baixa	A necessidade de instalar *software* de terceiros deve ser inexistente.
Solução		Todos as ferramentas utilizadas são da Microsoft.
RF10	Baixo	O sistema deve ser intuitivo de implementar.
Solução		Consistência na linguagem utilizada no trabalho prático e utilizadas ferramentas conhecidas pelo público geral com informação disponível.
RF11	Média	O sistema deve possibilitar a integração com sistemas baseados na Nuvem como *Azure Active Directory* ou *Office 365.*
Solução		Implementação de Windows Server 2012 e Active Directory que suporta esta funcionalidade.
RF12	Alta	O sistema deve possuir uma camada adicional de segurança através da autenticação dos utilizadores.
Solução		Efetuado através do protocolo LDAP incluído na Active Directory.

Tabela 7 Validação requisitos não funcionais

8 CONCLUSÃO

O trabalho descrito neste relatório, permite demonstrar a facilidade e as vantagens da implementação de uma infraestrutura tecnológica, seja *on-premise* ou através de serviços na nuvem, como um meio de permitir às empresas gerir utilizadores, computadores e informação associados à mesma.

Com base na definição inicial do problema:

"Muitas das pequenas e médias empresas existentes, possuem diversas necessidades tecnológicas relativas à gestão dos utilizadores, segurança, acessos, partilha de informações e equipamentos informáticos presentes na empresa.

A empresa Company é uma pequena empresa com fundos reduzidos para acesso a sistemas e tecnologias de informação complexos.

Foi efetuada uma reunião com o CEO da empresa Company que uma vez que a sua empresa estava a crescer em número de funcionários e parque informático, surgiram diversas necessidades.

Foram definidos os seguintes objetivos de investigação (RGs):

- RG 1 – Realizar o levantamento dos requisitos que satisfazem as necessidades de empresas com défice nas áreas tecnológicas;

- RG 2 – Descrever toda a arquitetura física que inclui o trabalho, assim como o software utilizado para o mesmo;

- RG 3 – Desenvolver e testar todo o sistema referente ao domínio *company.local.*

Deste modo, relativamente a:

- RG 1, foi efetuado o levantamento dos requisitos funcionais e não funcionais de uma empresa fictícia conforme demonstrado no capítulo 3,

- RG 2, no capítulo 4 foram descritas todas as especificações das máquinas utilizadas durante a implementação, seja a nível de hardware como a nível de software,

- RG 3, após a configuração dos 3 servidores presentes, foi também criada uma máquina virtual para demonstração e testes de todas as funcionalidades do sistema.

Neste sistema, sendo maioritariamente intuitivo é possível realizar uma aprendizagem do sistema através de processos de instalação ilustrados neste relatório.

Para uma mais fácil compreensão é possível verificar que os menus encontram-se em inglês, sendo que esta é a linguagem universal utilizada no mundo tecnológico permitindo assim uma partilha de experiencias e resolução de problemas entre administradores de sistemas.

O sistema idealizado inicialmente, depois de um processo extenso de investigação e desenvolvimento, foi implementado e testado com sucesso com o auxílio de uma máquina virtual cliente em que é possível observar o correto funcionamento do sistema.

Na parte prática do trabalho, é possível demonstrar os serviços descritos no relatório a executar em tempo real, constituído por 3 servidores e 1 máquina cliente, todos eles utilizando tecnologia de virtualização.

Uma vez que as tecnologias utilizadas ao longo deste trabalho fazem parte da experiência diária profissional do autor, não foram detetados impedimentos ou limitações durante o desenvolvimento.

Como sugestão de melhoria, num trabalho complementar, seria ideal realizar um *lift-and-shift,* estratégia de mover aplicações ou um conjunto de sistemas de um ambiente para outro sem ser necessário parar para redesenhar a aplicação ou o workflow dos processos, ao mover estes serviços para a *cloud service* seja ela publica ou privada, é possível diminuir os custos de manutenção e *downtime* dos serviços.

Outro trabalho futuro, seria implementar o serviço PaaS *Azure Active Directory,* que permite uma gestão ainda mais detalhada dos utilizadores e computadores, como por exemplo implementar sistemas de *conditional access,* aumentando assim exponencialmente a segurança dos dados relativos ao cliente.

BIBLIOGRAFIA

Alecrim, E. (19 de Fevereiro de 2013). *Firewall*. Obtido de Redes e Historia: https://sites.google.com/site/redesehistoria/mecanismos-de-proteccion/firewalls-y-proxies/-que-es-un-firewall

Araujo, V. &. (2013). Business and Technical Requirements of Software-as-a-Service: Implications in Portuguese Enterprise Business Context. *International Journal in Foundations of Computer Science & Technology, 3*, 1-14. doi:10.5121/ijfcst.2013.3601

Araújo, V. &. (2016). SaaS impact assessment in business contexts. *2016 11th Iberian Conference on Information Systems and Technologies (CISTI).* doi:10.1109/CISTI.2016.7521463

Araújo, V. &. (2016). Software como um Serviço: uma visão holística. *Revista lbérica de Sistemas e Tecnologias de Informação.*, 145-157. doi:10.17013/risti.19.145-157Corpus ID: 59347966

Attaran, M. (2017). Journal of International Technology and Information Management. *Cloud Computing Technology: Leveraging the Power of The Internet to Improve Business Performance*, pp. 116-120.

Banzal, S. (2007). *Data and Computer Network Communication* (1 ed.). Laxmi Publications Pvt Ltd. Obtido de Coursera.

Bourque, P., & Fairley, R. E. (2014). Guide to the Software Engineering Body of Knowledge. (IEEE, Ed.)

Cisco. (01 de Abril de 2020). *What Is a VPN? - Virtual Private Network*. Obtido de Cisco: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html?dtid=osscdc000283

Cisco. (s.d.). *What is a LAN? Local Area Network* . Obtido de Cisco: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

Cisco. (s.d.). *What is a wan wide area network*. Obtido de Cisco: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html

Coelho, M. (13 de Junho de 2019). *Vamos configurar um servidor de DNS no CentOS 7 através do Webmin*. Obtido de Medium:

https://medium.com/@miguel.migas.coelho/vamos-configurar-um-servidor-de-dns-no-centos-7-atrav%C3%A9s-do-webmin-763512f53362

Death, D. (2017). *Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework.* (P. Publishing, Ed.) Obtido de Information Security Handbook.

dnsstuff. (21 de Maio de 2020). *Active Directory and LDAP Authentication Guide*. Obtido de DNSstuff: https://www.dnsstuff.com/active-directory-ldap-authentication

Fernandes, J. M., & Machado, R. J. (2015). *Requirements in Engineering Projects.* Springer.

Girijala, R. (13 de Julho de 2018). *Hybrid Cloud For Entrepreneurs* . Obtido de Karmel Soft: https://www.karmelsoft.com/hybrid-cloud-for-entrepreneurs/

Gogoni, R. (s.d.). *O que é VPN?* Obtido de Tecnoblog: https://tecnoblog.net/283693/o-que-e-vpn/

Hristov, V. (2016). Using Lightweight Directory acess protocol for service level specifications administration. pp. 1-5.

Hybrid ICT. (2018). *Cloud Computing - Public Cloud*. Obtido de Hybrid ICT: https://www.hybridict.com.au/corporate-cloud-services/cloud-computing/public-cloud/

IEEE. (22 de Dezembro de 1996). Guide for Developing System Requirements Specifications. *IEEE*, 1-30. doi:10.1109/IEEESTD.1996.81000

IEEE. (22 de Dezembro de 1998). IEEE Guide for Developing System. *Requirements Specifications*.

javatpoint. (2018). *Private Cloud* . Obtido de javatpoint: https://www.javatpoint.com/private-cloud

juridoc. (11 de Abril de 2020). *O que é um sistema SaaS para gestão de contratos?* Obtido de juridoc: https://www.juridoc.com.br/blog/tecnologia/10948-o-que-e-um-sistema-saas-para-gestao-de-contratos/

Kotonya, G., & Sommerville, I. (1998). *Requirements Engineering: Processes and Techniques.* Wiley.

Microsoft. (22 de Fevereiro de 2017). *Welcome to Remote Desktop Services in Windows Server 2016*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

Microsoft. (8 de Março de 2019). *DFS Replication overview*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/dfsr-overview

Microsoft. (30 de Janeiro de 2019). *Volume Shadow Copy Service*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service

Microsoft. (2020). *Active Directory Technical Specification.* Microsoft.

Microsoft. (2020). *Calculadora de Preços*. Obtido de Microsoft Azure: https://azure.microsoft.com/pt-pt/pricing/calculator/

Microsoft. (2020). *Domain Controller Roles: Active Directory* . Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc786438(v=ws.10)?redirectedfrom=MSDN

Microsoft. (2020). *Domain Name System (DNS)*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/networking/dns/dns-top

Microsoft. (2020). *Dynamic Host Configuration Protocol (DHCP)*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

Microsoft. (2020). *O que é IaaS? Infraestrutura como Serviço*. Obtido de Microsoft Azure: https://azure.microsoft.com/pt-pt/overview/what-is-iaas/

Microsoft. (2020). *O que é PaaS? Plataforma como Serviço*. Obtido de Microsoft Azure: https://azure.microsoft.com/pt-pt/overview/what-is-paas/

Microsoft. (2020). *O que é SaaS? Software como Serviço*. Obtido de Microsoft Azure: https://azure.microsoft.com/pt-pt/overview/what-is-saas/

Microsoft. (2020). *Tipos de serviços cloud - Learn* . Obtido de Microsoft Docs: https://docs.microsoft.com/pt-pt/learn/modules/principles-cloud-computing/5-types-of-cloud-services

Microsoft. (2020). *Understanding Domains*. Obtido de Microsoft Docs: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd861323(v%3dws.11)

Miller, R. (2020). The OSI Model: An Overview. *Information Security Reading Room*.

Neto, M. V. (2015). *Computação em Nuvem: Nova Arquitetura de TI.* Brasport, 2015.

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2006). *The Design Science Research Process.*

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (Fevereiro de 2006). The design science research process: A model for producing and presenting information systems research.

Rand Morimoto, J. S. (2017). *Windows Server 2016 Unleashed.* Sams.

Rand Morimoto, J. S. (2017). *Windows Server 2016: Unleashed.* Sams.

Roberts, A. E. (05 de Agosto de 2019). *Unlocking business acceleration in a hybrid cloud world*. Obtido de McKinsey: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/unlocking-business-acceleration-in-a-hybrid-cloud-world

Sanjay, B. R. (2018). *Domain Name System (DNS) Security: Attacks Identification and Protection Methods.*

Selby, B. (21 de Maio de 2016). *What is Cloud Storage and What are is Advantages?* Obtido de Cloud Storage Advice: https://cloudstorageadvice.com/what-is-cloud-storage/cloud-3/

Simmon, E. (Fevereiro de 2018). Evaluation of Cloud Computing. *NIST Special Publication 500-322*.

Sotiris Ioannidis, A. D. (2019). *Implementing a Distributed Firewall.*

Stackscale. (14 de Abril de 2020). *SaaS, PaaS and IaaS: the main cloud service models*. Obtido de Stackscale: https://www.stackscale.com/blog/cloud-service-models/

T. Mrugalski, M. S.-I. (2018). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* Internet Engineering Task Force.

VMWARE. (s.d.). *VMware, Inc.* Obtido de Virtualization Essentials: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ebook/gated-vmw-ebook-virtualization-essentials.pdf

Watchguard. (2020). *About Firewalls*. Obtido de Watchguard: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/overview/networksecurity/firewals_about_c.html

Wikipedia. (11 de Junho de 2020). *Client-server*. Obtido de Simple English Wikipedia, the free encyclopedia: https://simple.wikipedia.org/wiki/Client-server

ANEXO I – Processos de instalação

1.1 Processo de instalação do *Domain Controler*

Após instalação do *Windows server*, é necessário adicionar as funções que o servidor irá executar.

Para adicionar a função de *Domain Controler*, abrir o *Server Manager*, pressionar o botão *Manage* e clicar na opção *Add Roles and Features*.

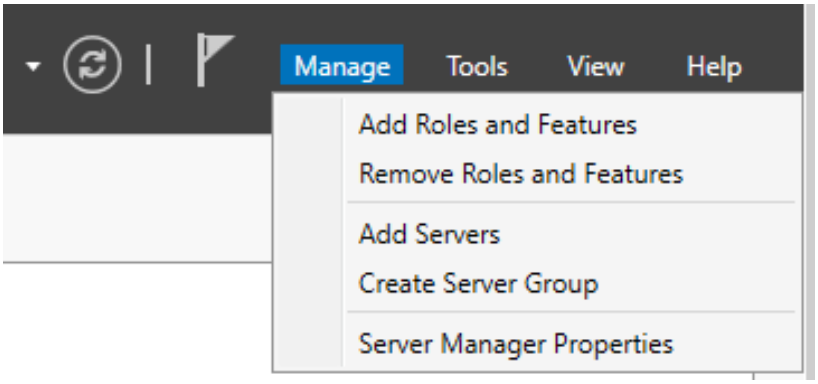

Figura 29 Adicionar funções ao *Windows Server*

O menu seguinte irá conter alguns requisitos e sugestões de boas práticas sobre o que deve ser feito como password complexa do utilizador, configuração de endereços IP estáticos para servidores e a versão do *Windows* deve estar atualizada.

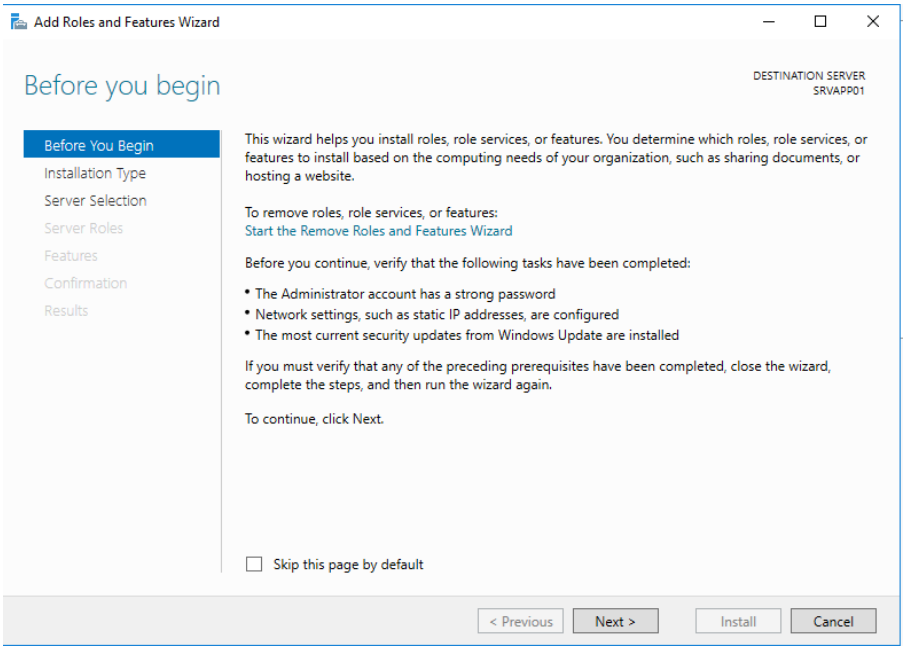

Figura 30 Mensagem informativa

A janela apresentada na figura 31, refere-se ao tipo de instalação que se deseja realizar, a primeira opção refere-se à instalação das funções num servidor específico enquanto a segunda opção estabelece automaticamente um ambiente de acesso remoto para aplicações definidas.

Como o pretendido é "promover" o servidor para *Domain Controler*, selecionar a primeira opção e continuar.

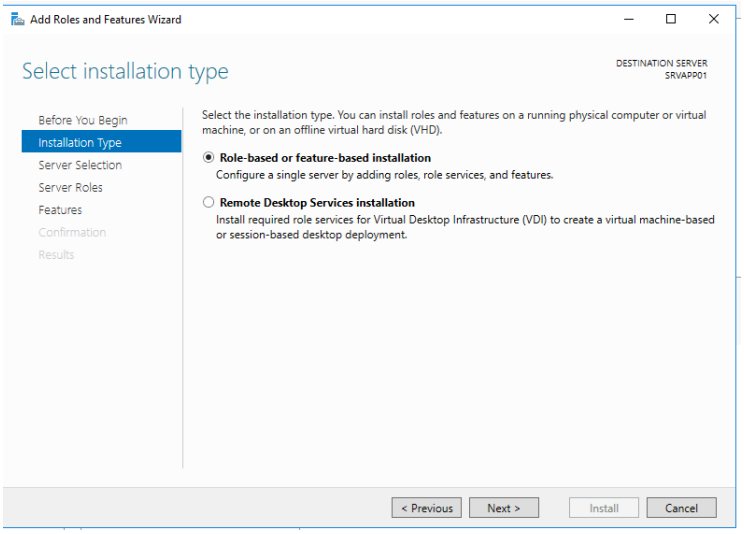

Figura 31 Tipo de instalação

A figura 32 ilustra a seleção do servidor ou disco virtual em que irá ser instalado a função. Uma vez que o servidor em que iremos instalar a função é ele próprio, carregar em seguinte.

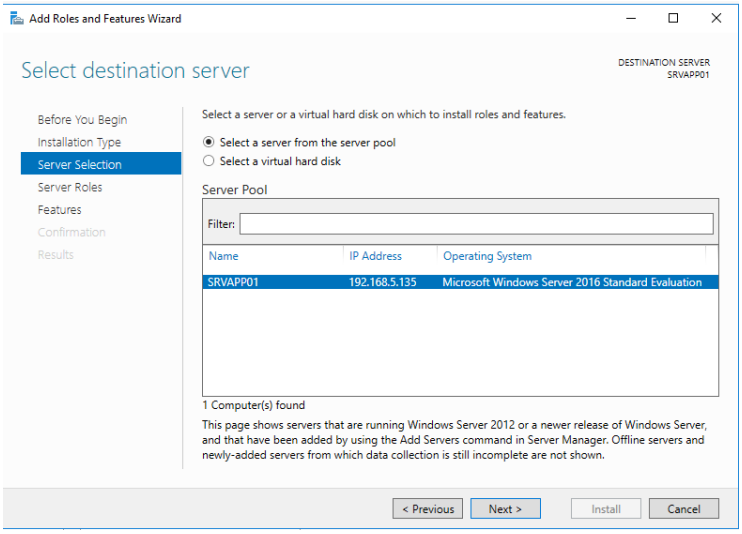

Figura 32 Seleção do servidor

No menu ilustrado na figura 33, pode-se selecionar quais as funções suportadas pelo *Windows Server*, neste caso selecionar *Active Directory Domain Services*.

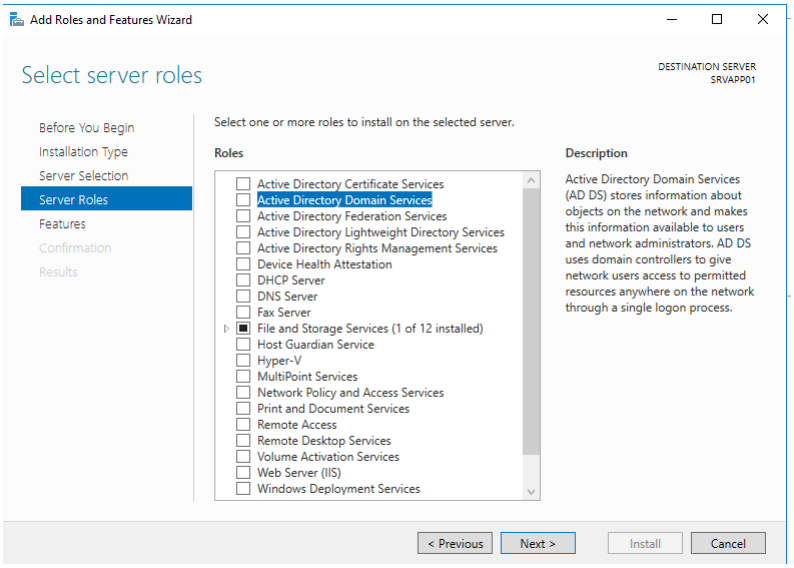

Figura 33 Selecionar quais as funções a instalar

Após seleção da função desejada, é apresentado um segundo menu, indicando quais os pré-requisitos obrigatórios, pressionar botão *Add Features*.

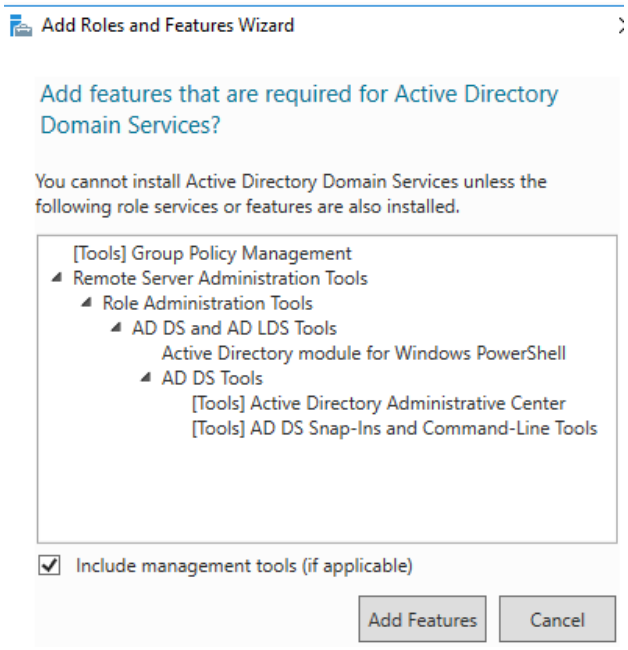

Figura 34 Componentes adicionais

No menu seguinte, são apresentados componentes essenciais para o correto funcionamento dos serviços.

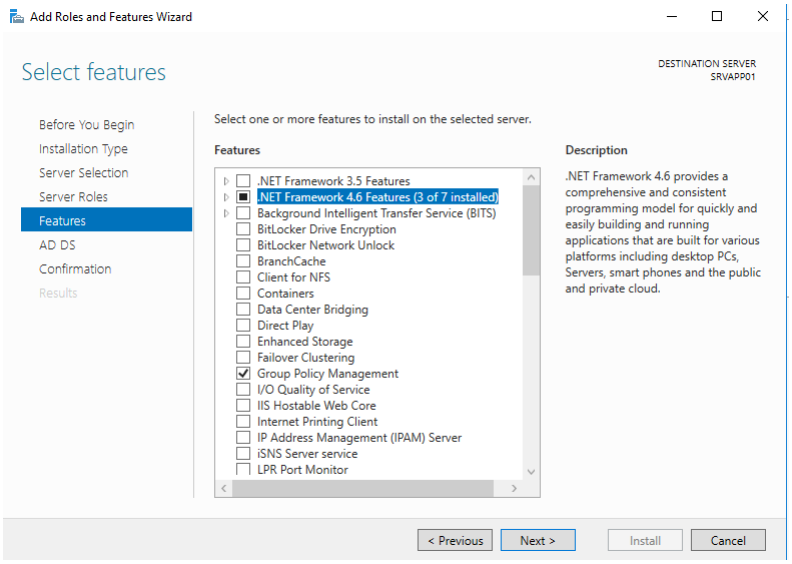

Figura 35 Componentes adicionais

Caso o cliente possua uma subscrição de *Azure Active directory*, é possível sincronizar a mesma com a *Active Directory* local, proporcionando uma gestão dos utilizadores e dispositivos pertencentes ao domínio a partir de qualquer sítio desde que exista ligação à Internet.

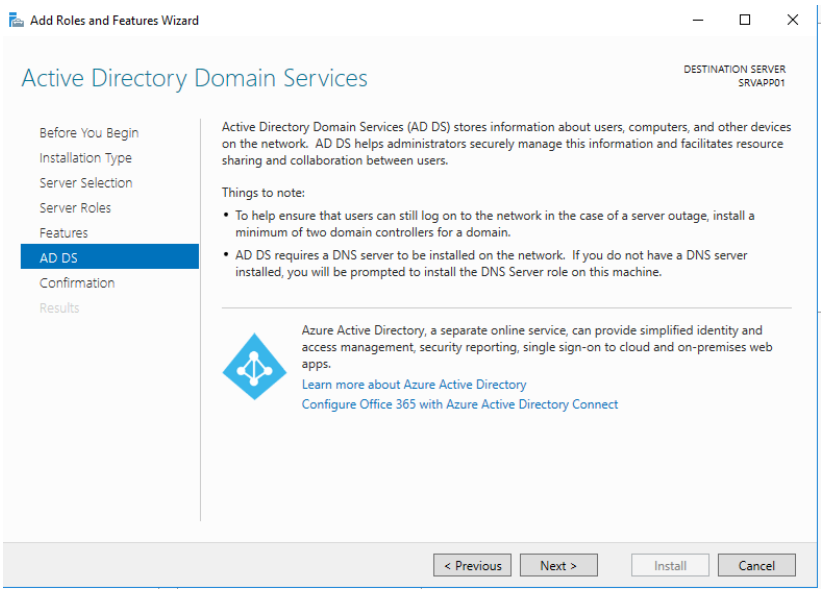

Figura 36 Azure Active Directory

O menu seguinte, é apresentado um resumo de todos os componentes escolhidos que irão ser instalados.

Caso o servidor em que esta operação esteja a ser realizada não esteja a disponibilizar um serviço critico, podemos ainda selecionar a caixa para fazer *restart* automático caso seja necessário para terminar as configurações com sucesso.

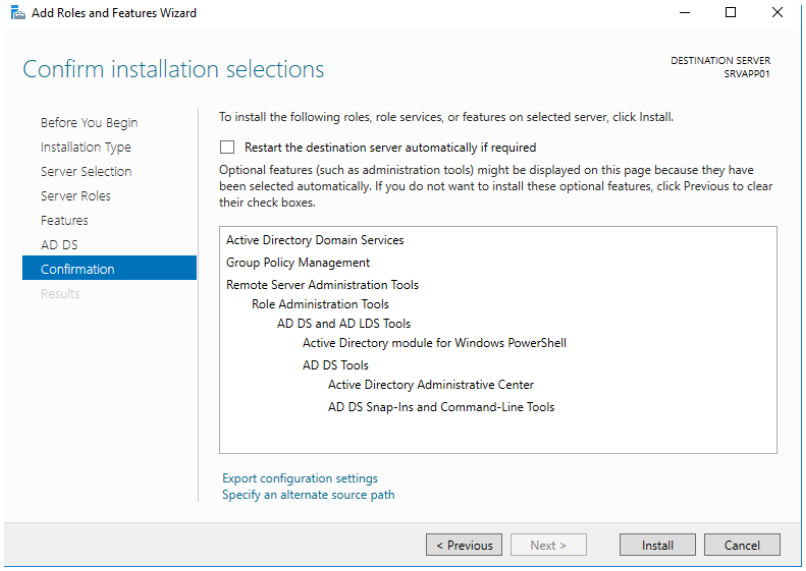

Figura 37 Resumo das funções a instalar

Após instalação dos componentes, é necessário "promover" o servidor para *Domain Controller*. Para efetuar este procedimento, é necessário clicar na frase *Promote this server do a domain Controller.*

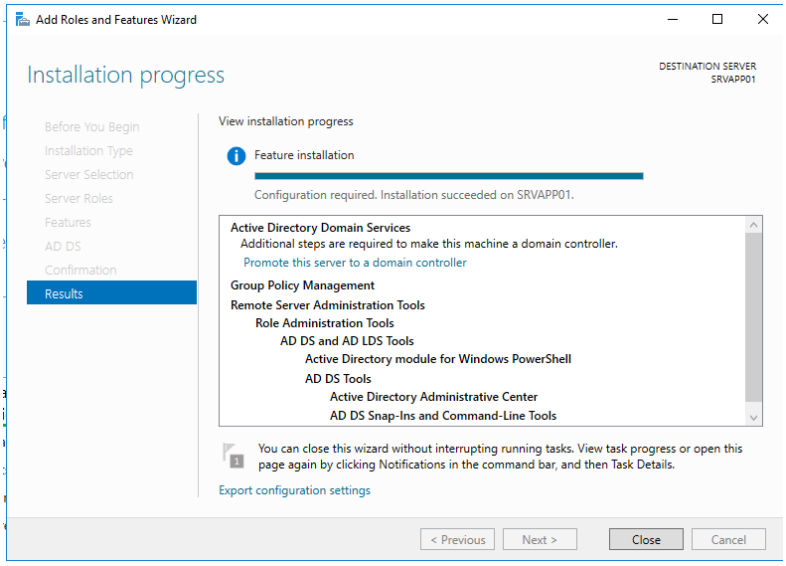

Figura 38 Progresso de instalação

Sendo que esta demonstração será para o *Primary Domain Controller,* selecionar *Add a new forest.*

No campo *Root domain name,* é necessário escrever o nome desejado para o domínio, neste caso *company.local.*

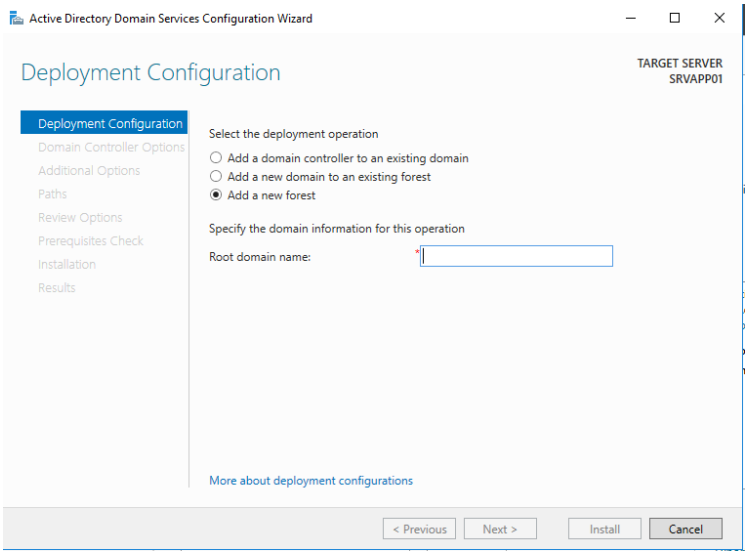

Figura 39 Configuração de new forest

Os campos *Forest functional Level* e *Domain Functional Level*, retrata o ambiente em que os mesmos serão instalados, neste caso *Windows Server* 2016.

O menu seguinte (*Specify domain controller capabilities),* apresenta opções complementares essenciais para a solução apresentada como instalar a funcionalidade de DNS de forma às máquinas clientes efetuarem resolução de nomes internamente.

O *Primary Domain Controller* por motivos de boas práticas, também deve ser um *Global Catalog Server*, tendo a possibilidade de disponibilizar informação de atributos presentes na *Active Directory* às máquinas presentes na rede.

A opção *Read only domain controller,* como o nome indica não permite que sejam efetuadas alterações na *Active Directory,* servindo apenas para consulta.

Por segurança, é necessário ainda introduzir uma password para *Directory Services Restore Mode,* permitindo que caso a base dados da *active directory* ou o próprio servidor ficar com alguma funcionalidade corrompida, através desta *password* é possível aceder à base de dados e restaurar/reparar a mesma.

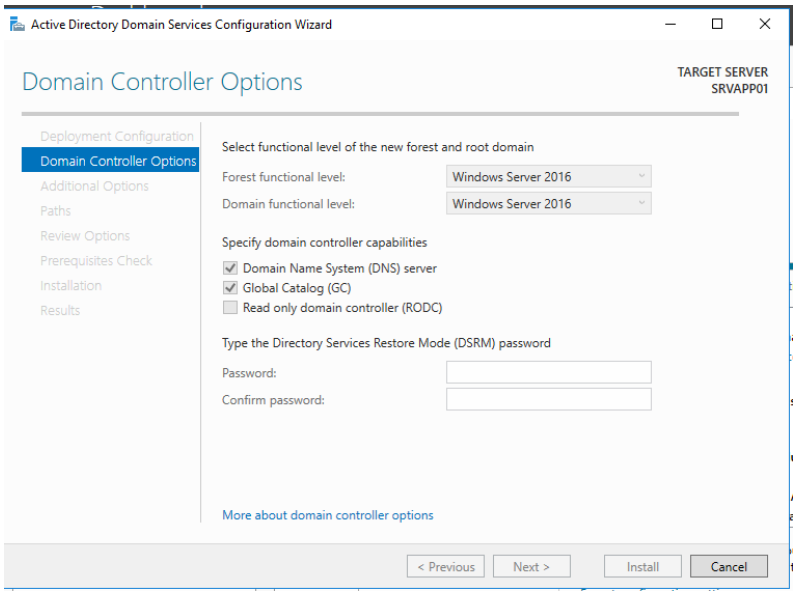

Figura 40 Opções *Domain Controller*

O aviso apresentado na figura 41, significa apenas que não foi possível detetar um DNS numa hierarquia mais elevada, este aviso é normal uma vez que ainda não é suposto este domínio ser acessível a partir da Internet.

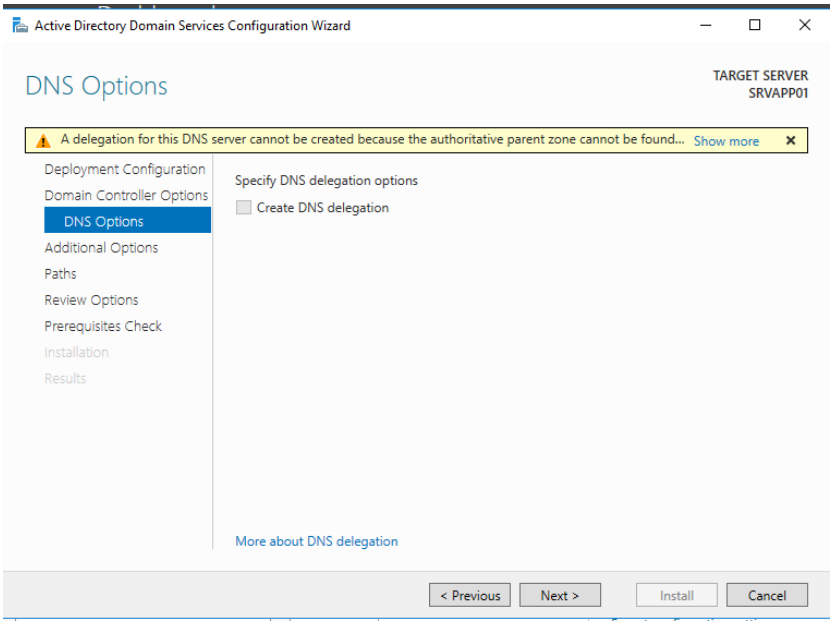

Figura 41 Opções DNS

No menu apresentado na figura 42, é possível configurar o *NetBios domain name*, que é um subdomínio do domínio principal. Sendo normalmente uma abreviatura, simplifica o processo de adicionar máquinas ao domínio.

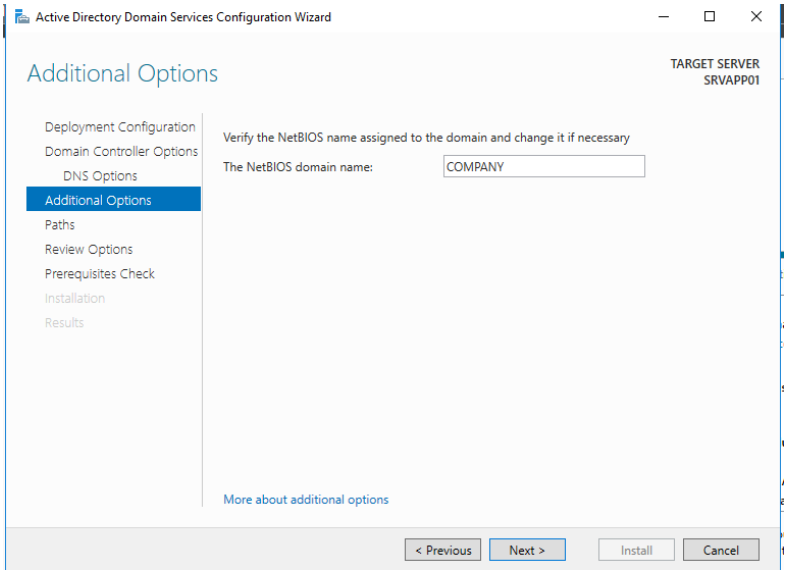

Figura 42 Configurar NetBios domain name

É necessário configurar a localização das 3 pastas que contêm os ficheiros essenciais para o correto funcionamento do *Domain Controler*, a pasta que contém a base de dados, *logs* do sistema e *SysVol* que contém as *Group Policy templates* e *scripts* que podem ser utilizados em *GPO*.

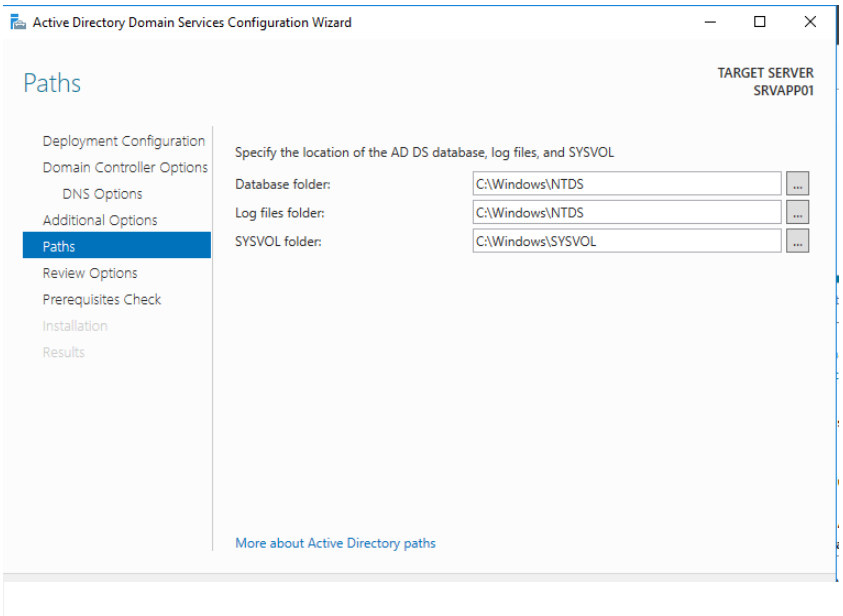

Figura 43 Diretorias essenciais para o sistema

Na figura 44, é demonstrado o menu que resume todas as opções escolhidas durante o processo de forma a validar as mesmas antes da implementação.

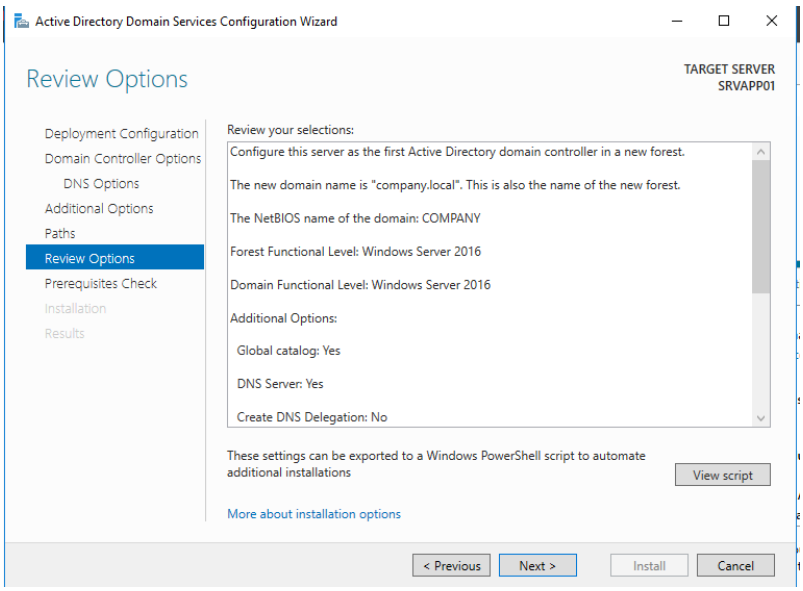

Figura 44 Resumo das configurações

O menu ilustrado na figura 45, representa uma verificação do sistema de forma a verificar se os pré-requisitos estão instalados e em conformidade.

É também apresentado avisos ou erros que possam surgir também nesta análise.

Nenhum dos avisos apresentados é impeditivo para instalação do sistema.

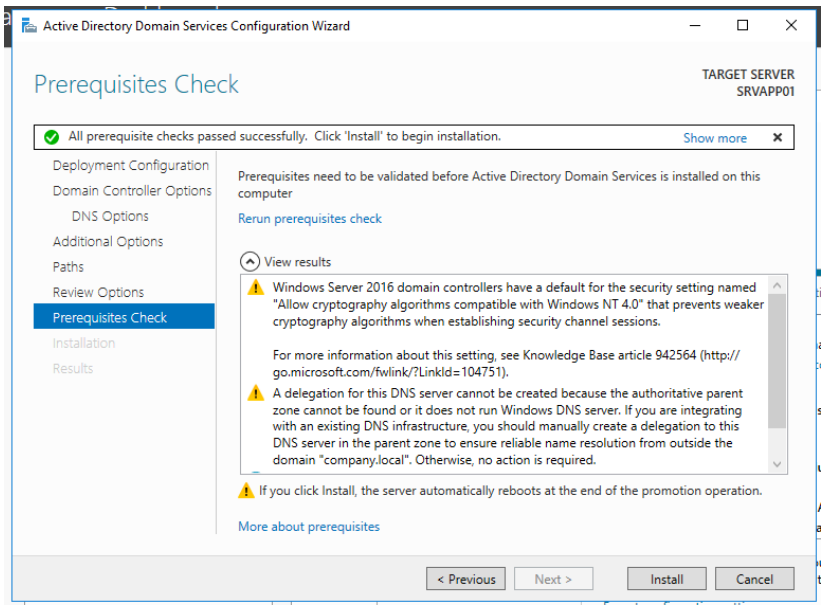

Figura 45 Revisão de pré-requesitos

Após o sistema reiniciar para implementar as funcionalidades acabadas de instalar, ao aceder ao *Server Manager*, no menu *Tools*, verifica-se que existe uma opção denominada de *Active Directory Users and Computers.*

Ao executar esta funcionalidade, pode-se verificar a *Forest* criada juntamente com algumas *organizational units* por defeito que incluem a localização das máquinas adicionadas ao domínio *(Computers),* os servidores que possuem o *role de Domain Controller (Domain Controllers),* os utilizadores e grupos automaticamente criados *(Users).*

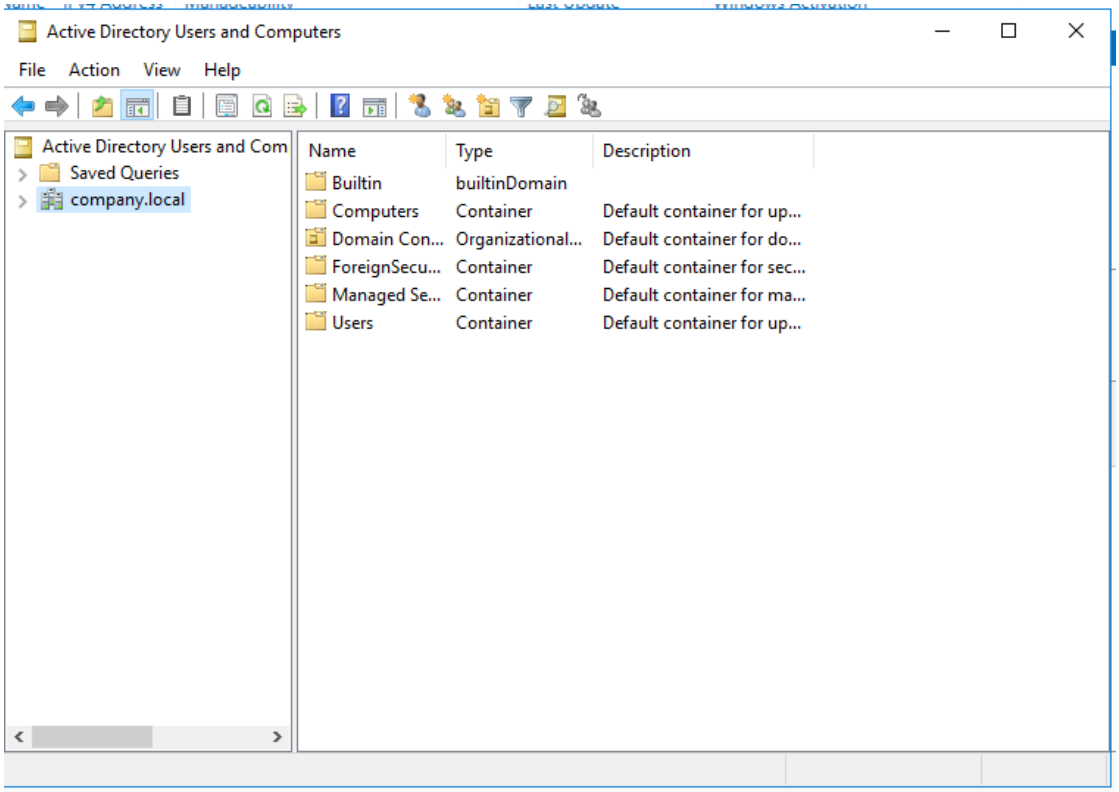

Figura 46 Active Directory

1.2 Processo de instalação do Secondary Domain Controller

De forma a ser possível configurar o *Secondary Domain Controller*, é necessário que a máquina tenha como *DNS server* o *IP* do *Primary Domain Controller*.

No caso da solução apresentada, o *IP* da máquina DC02 é 192.168.5.132 com a máscara 255.255.255.0 e cujo *default gateway* contém o ip 192.168.5.1 (endereço *IP* da *firewall*).

O servidor *DNS* que irá consultar será o DC01 (*Primary Domain Controller*) que tem o *IP* 192.168.5.131, e como *alternate DNS server* está o endereço *IP* da Firewall.

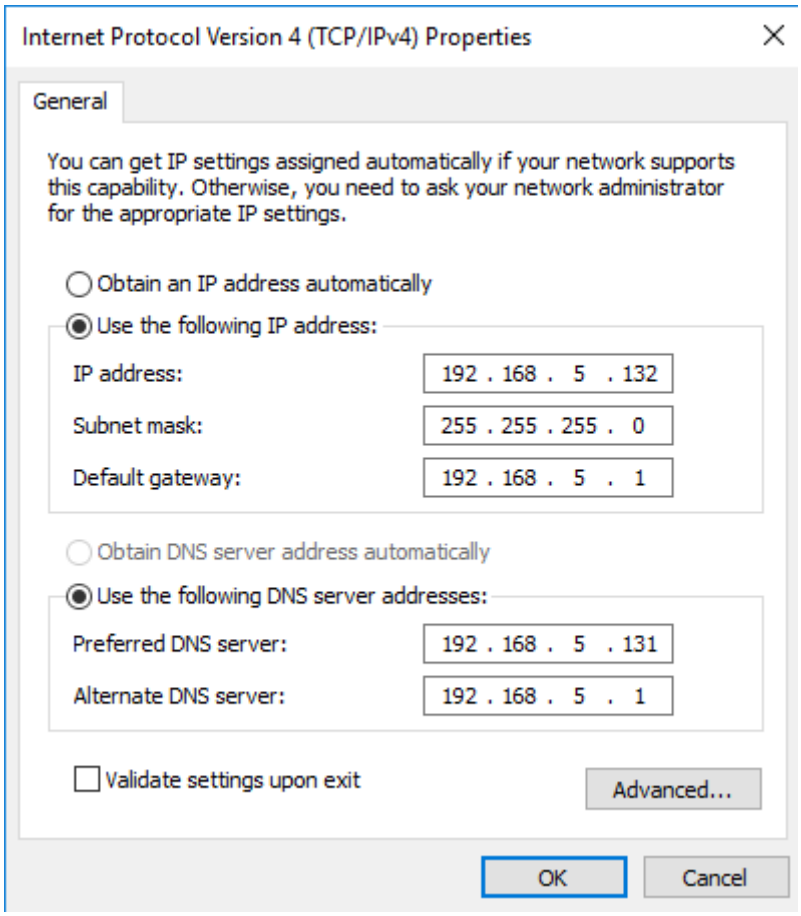

Figura 47 Configuração IP “DC02”

Para adicionar um *secondary domain controller*, é necessário efetuar os passos descritos no ponto 1.1 deste relatório com as seguintes alterações:

No menu *Deployment Configuration* é necessário selecionar a opção *Add a domain controller to an existing domain.* É necessário também colocar credenciais de um utilizador com acesso de administração (neste caso *company.local\administrator* e respetiva *password*) que o servidor irá utilizar para se registar no domínio e efetuar os procedimentos necessários.

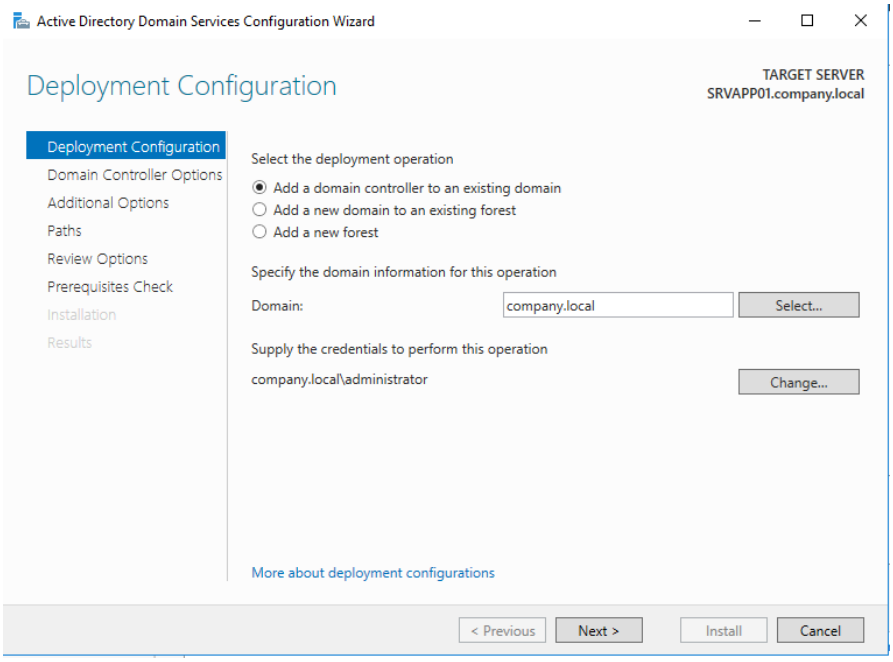

Figura 48 Adicionar secondary domain controller

Uma vez que o servidor DC02, irá possuir as mesmas funções do DC01 de forma a prevenir um ponto único de falha, o mesmo irá possuir a função de DNS e *Global Catalog*. Existir redundância de serviços é uma boa prática, logo foi criado o *Secondary Domain Controller* com o objetivo que caso o principal tenha algum tipo de problema que impeça o normal funcionamento, a transição permite diminuir o *downtime* para os utilizadores.

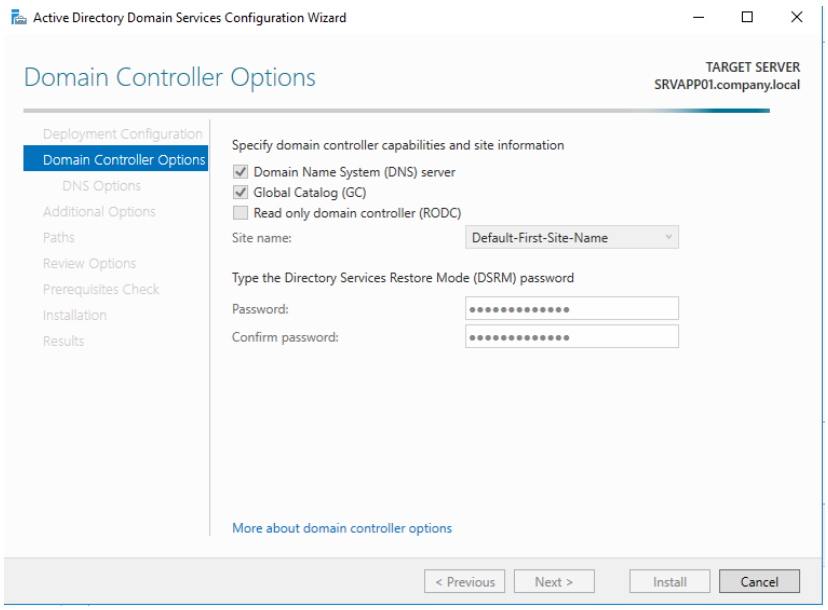

Figura 49 Duplicar Funcionalidades para DC02

Uma vez que ambos os servidores encontram-se na mesma rede, é possível selecionar qual o servidor para replicar.

Caso os servidores não coexistam dentro da mesma rede, pode-se efetuar a instalação através de um dispositivo externo, este método possui diversas desvantagens sendo a principal que as alterações efetuadas só serão atualizadas de forma manual.

Os restantes passos estão descritos no ponto 1.1 uma vez que a *role* instalada é a mesma.

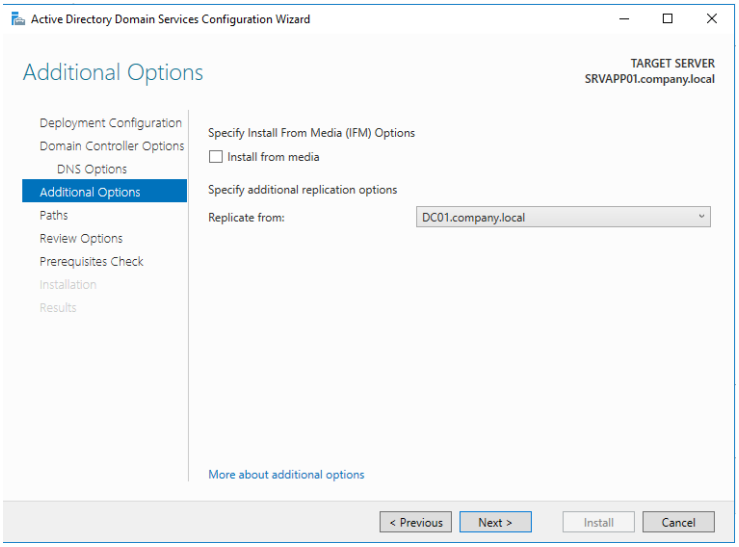

Figura 50 Servidor de destino da replicação AD DS

1.3 Processo de criação de utilizador de domínio

Conforme referido no capítulo 1.1 em 1.2, a gestão de utilizadores e computadores de domínio, é efetuado no *Domain Controller*. Sendo assim, para ser criado o utilizador que irá aceder aos recursos e às máquinas adicionadas ao domínio, é necessário através do *Active Directory Users and Computers,* selecionar a *Organizacional Unit* pretendida e criar um novo objeto (*user*) conforme descrito na figura 51.

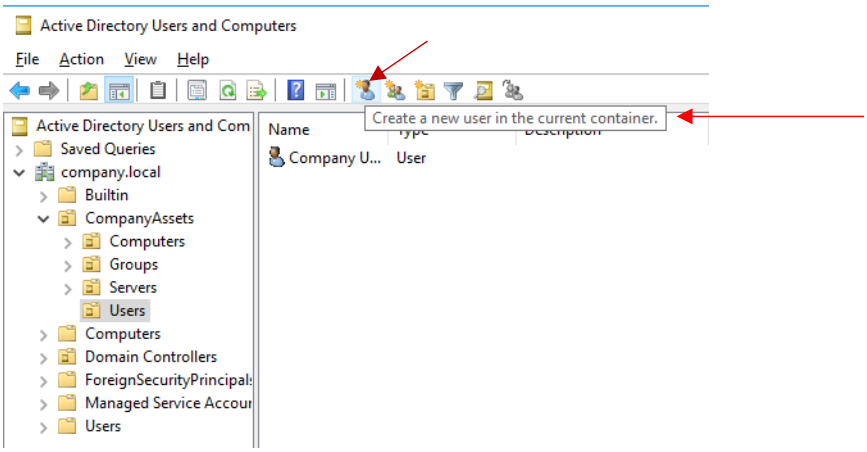

Figura 51 Criar um utilizador

No menu da criação do utilizador, existem diversos campos a preencher com informação como o nome e o *username* utilizado para se autenticar no domínio.

No menu posterior, é possível configurar uma password que esteja de acordo com as regras de complexidade, pode-se ainda configurar para o utilizador mudar a *password* na próxima vez que fizer login, não seja permitido ao próprio utilizador mudar a *password*, a *password* nunca expira e a conta ficar interdita de efetuar login.

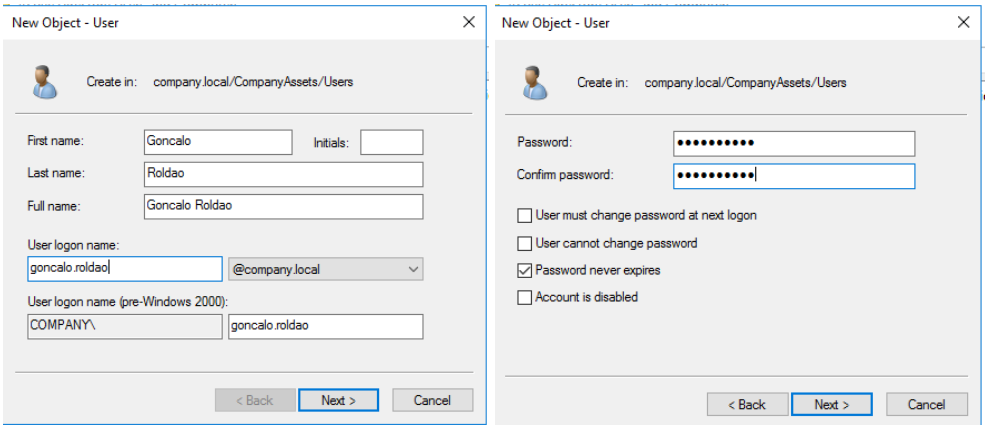

Figura 52 Informação sobre o utilizador

Uma vez que o *fileshare* está dividido em permissões especificas para cada pasta, foram criados grupos de acesso às mesmas.

Estas permissões estão em forma de grupos o que significa que para aceder a uma determinada pasta com determinadas permissões, os utilizadores terão de fazer parte do grupo. Neste caso os grupos criados possuem uma nomenclatura "FSA_nome_da_pasta", esta nomenclatura intuitiva serve para aquando a consulta dos grupos, apenas pelo nome é possível verificar qual o grupo responsável por atribuir permissões a cada pasta.

A figura 53 ilustra a atribuição do grupo ao utilizador Goncalo Roldao.

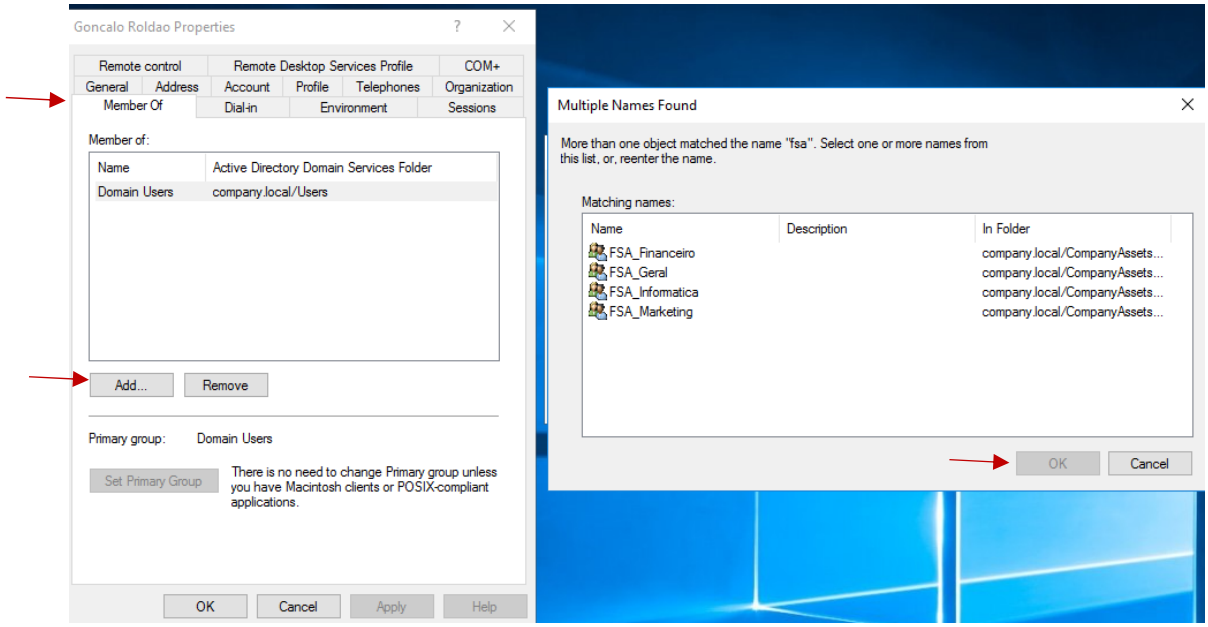

Figura 53 Atribuição de grupos a utilizadores

1.4 Processo de configuração das permissões do *Fileshare*

De forma a garantir que apenas certos utilizadores podem aceder a determinada informação, é necessário configurar uma hierarquia de pastas.

Através da hierarquização de pastas, garante-se que todas os ficheiros criados à posteriori dentro das pastas pelos próprios utilizadores herdam as permissões da pasta no nível imediatamente acima.

Os utilizadores inseridos nos grupos, apenas têm o tipo de acesso indicado na tabela 6 que representa o mapa de permissões do *Fileshare.*

Pasta	Grupos	Tipo de acesso	Herança	Aplicado a:
E:\dados	*Administrators*	*Full control*	*None*	*This folder, subfolders and files*
	Domain Users	*Read & Execute*	*None*	*This folder only*
E:\dados\Fileshare	*Administrators*	*Full control*	*E:*	*This folder, subfolders and files*
	FSA_Geral	*Special*	*None*	*This folder only*
	FSA_Informatica	*Special*	*None*	*This folder only*
	FSA_Marketing	*Special*	*None*	*This folder only*
	FSA_Financeiro	*Special*	*None*	*This folder only*
E:\dados\Fileshare\ 01-Financeiro	*Administrators*	*Full control*	*E:*	*This folder, subfolders and files*
	FSA_Financeiro	*Modify*	*None*	*This folder, subfolders and files*
E:\dados\Fileshare\ 02-Geral	*Administrators*	*Full control*	*E:*	*This folder, subfolders and files*
	FSA_Geral	*Modify*	*None*	*This folder, subfolders and files*
E:\dados\Fileshare\ 03-Marketing	*Administrators*	*Full control*	*E:*	*This folder, subfolders and files*
	FSA_Marketing	Modify	None	This folder, subfolders and files
E:\dados\Fileshare\ 04-Informática	Administrators	Full control	E:	This folder, subfolders and files
	FSA_informatica	Modify	None	This folder, subfolders and files

Tabela 8 Mapa permissões *Fileshare*

1.5 Processo de instalação do *Remote Desktop App Server*

Para configurar o *remote server app*, é necessário instalar as funções:

***Web server* (IIS):** irá permitir neste caso a possibilidade de hospedar uma página *web* interna capaz de autenticar os utilizadores e disponibilizar as aplicações a que os mesmos têm acesso.

***Remote desktop services* (RDS):** esta funcionalidade contém um pacote de serviços que é necessário adicionar ao servidor para ser possível disponibilizar as aplicações para as máquinas clientes acederem.

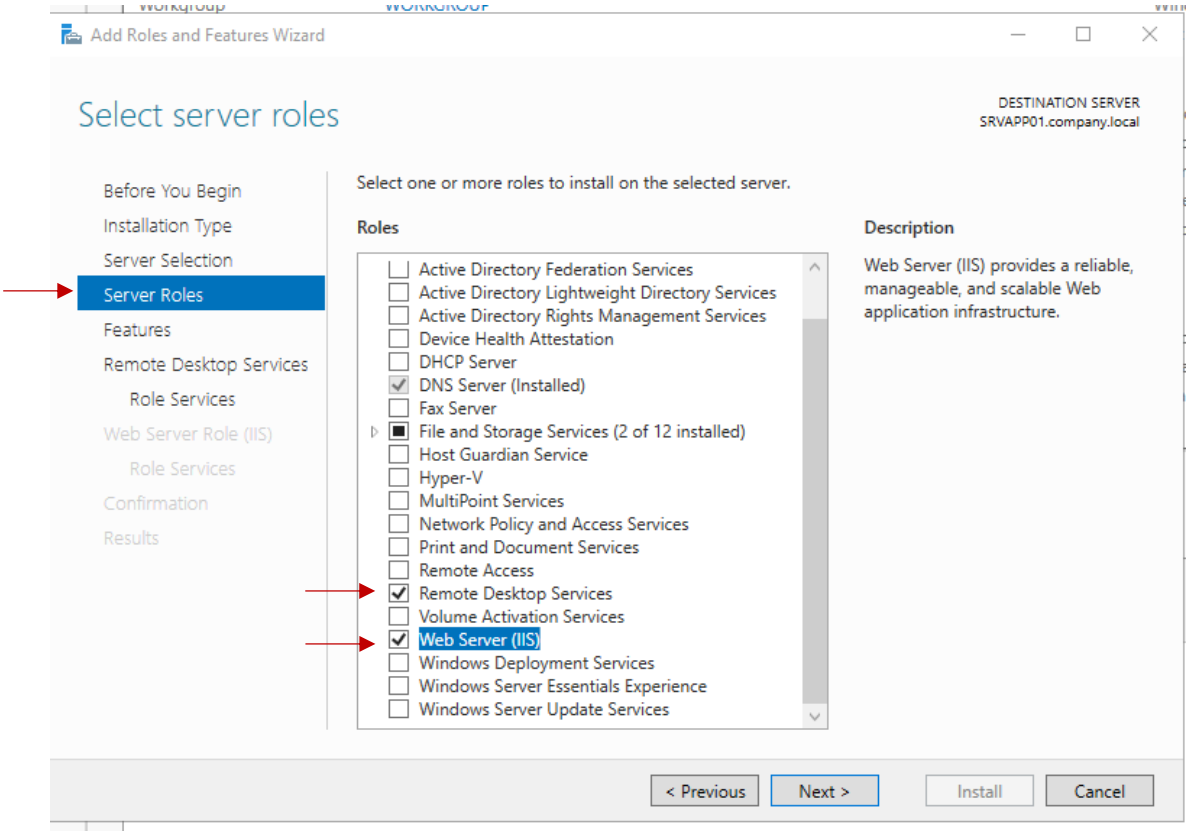

Figura 54 Instalar Remote Desktop Services e Web Server

Uma vez que o pretendido é que os utilizadores executem as aplicações num ambiente controlado, é necessário instalar as seguintes funcionalidades:

***Remote Desktop Connection Broker*:** permite que os utilizadores se conectem ao servidor executando apenas as aplicações ao qual os mesmos têm acesso, diminuindo assim o consumo de recursos.

***Remote Desktop Session Host*:** permite ao servidor, hospedar aplicações numa "coleção" de aplicações que os utilizadores têm acesso. Permite também a utilização de alguns recursos públicos do servidor.

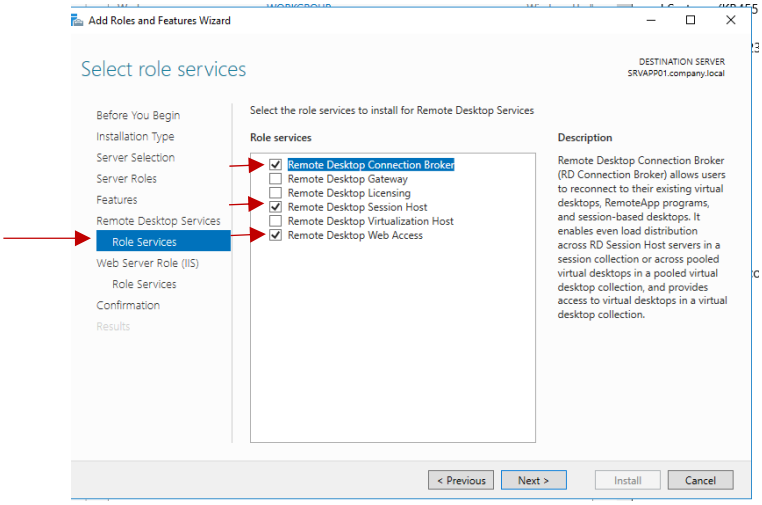

Figura 55 *Remote Desktop Services Roles*

O menu ilustrado na figura 56, trata-se de informação meramente informativa, descrevendo vantagens da utilização do *web server da Microsoft*.

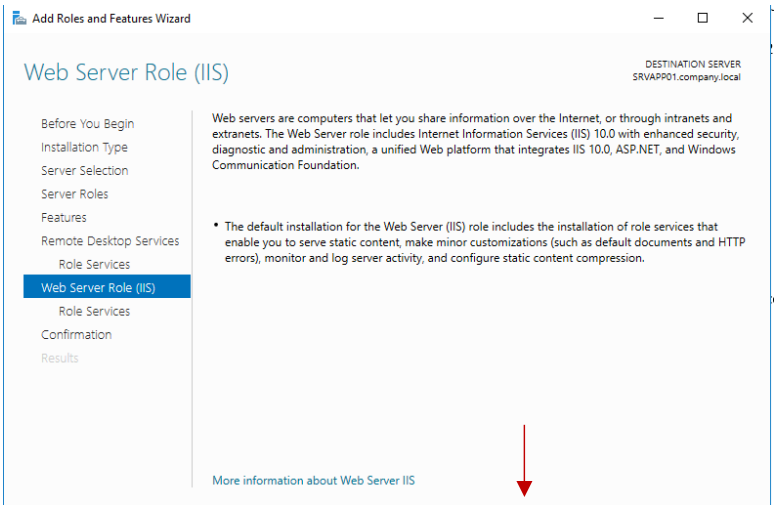

Figura 56 Web Server descrição

O *web server (IIS)* permite não só hospedar páginas internamente num ambiente de Intranet, mas também externamente para a Internet, por isso torna-se um sistema com muitas opções para selecionar.

Uma vez que para o trabalho apresentado, não são necessárias todas as funcionalidades descritas, basta apenas selecionar as opções indicadas por defeito.

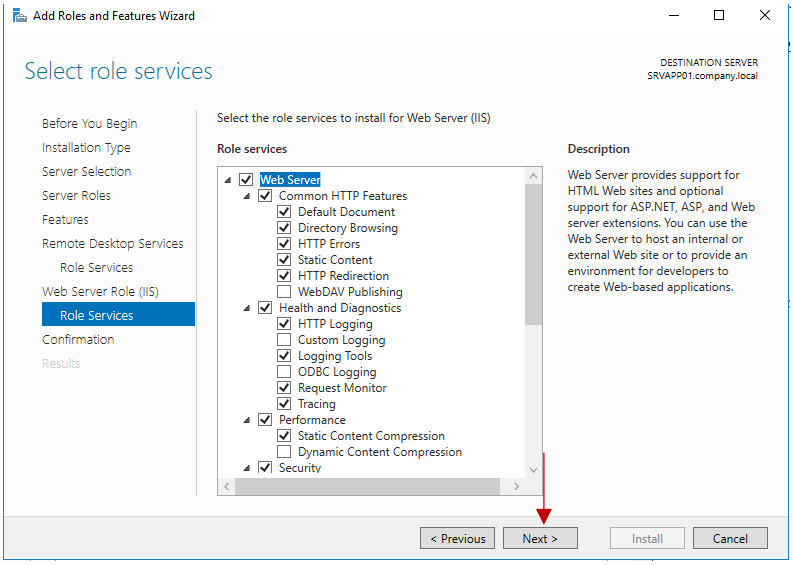

Figura 57 Serviços incluídos no Web Server

Após o servidor ter feito todas as configurações necessárias e ter reiniciado, é possível verificar que existe um novo separador no *Server Manager* denominado *Remote Desktop Services,* é possível adicionar uma nova *collection* que irá incluir todos os programas que é pretendido partilhar com os utilizadores.

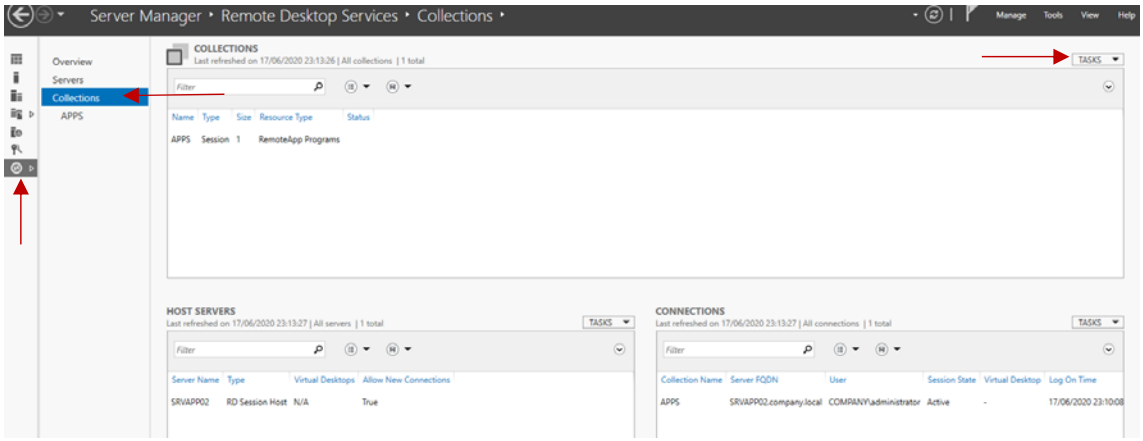

Figura 58 Remote Desktop Services – Collections

Para adicionar uma *collection* basta pressionar o botão *tasks* no canto superior direito e clicar em *Create Session Collection"*.

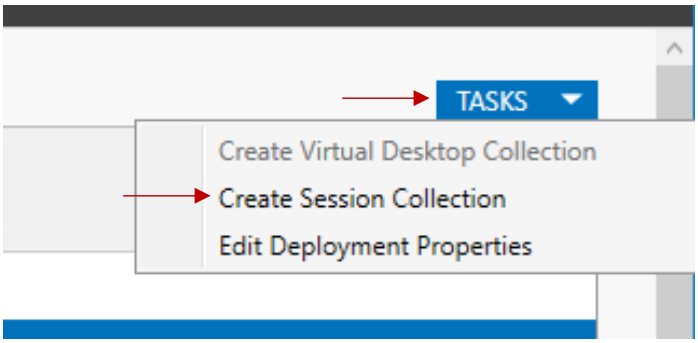

Figura 59 Create Session Collection

O primeiro passo para adicionar uma *collection* é atribuir o nome à mesma que deve ser intuitivo consoante as aplicações inseridas.

É possível ainda preencher o campo *Description* com informação sobre as aplicações.

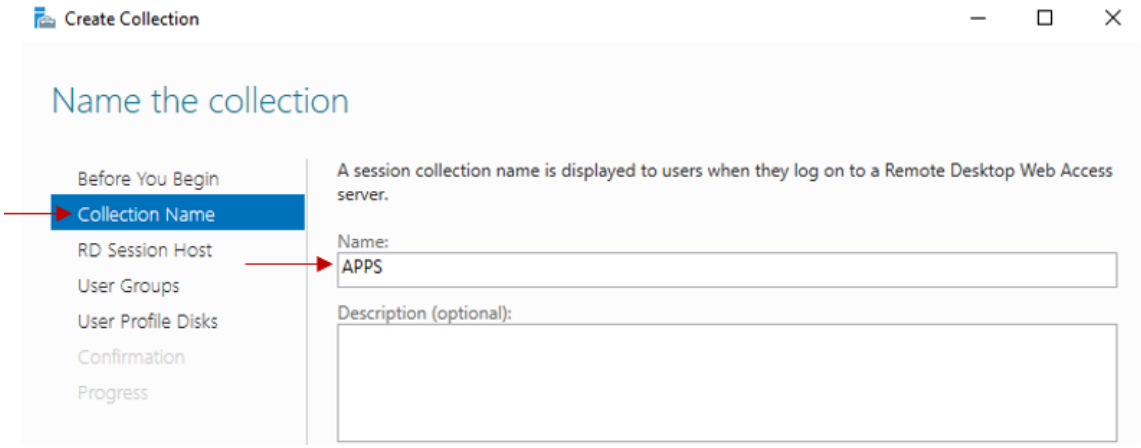

Figura 60 Atribuir o Nome da Collection

Como demonstrado na figura 61, é necessário selecionar o servidor desejado para hospedar as sessões dos utilizadores.

De notar que caso existam mais servidores no domínio com a *role* de *Remote Desktop Services* no domínio *company.local*, irão aparecer neste menu.

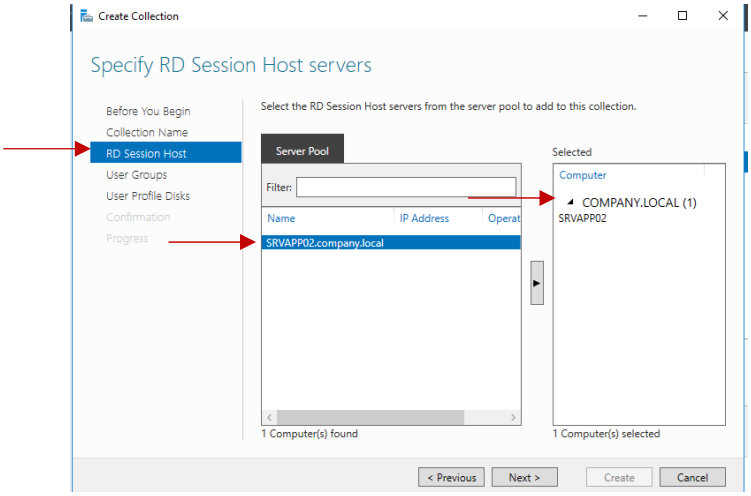

Figura 61 Selecionar servidor para remoteapp

No menu demonstrado na figura 62, é possível definir quais os utilizadores que irão ter acesso a esta *collection* de aplicações.

As boas práticas mencionam que qualquer permissão fornecida aos utilizadores deve ser aplicada a grupos e não a utilizadores individuais.

Neste caso, os utilizadores inseridos no grupo *remote_desktop_users* irão ter as permissões necessárias para aceder aos aplicativos.

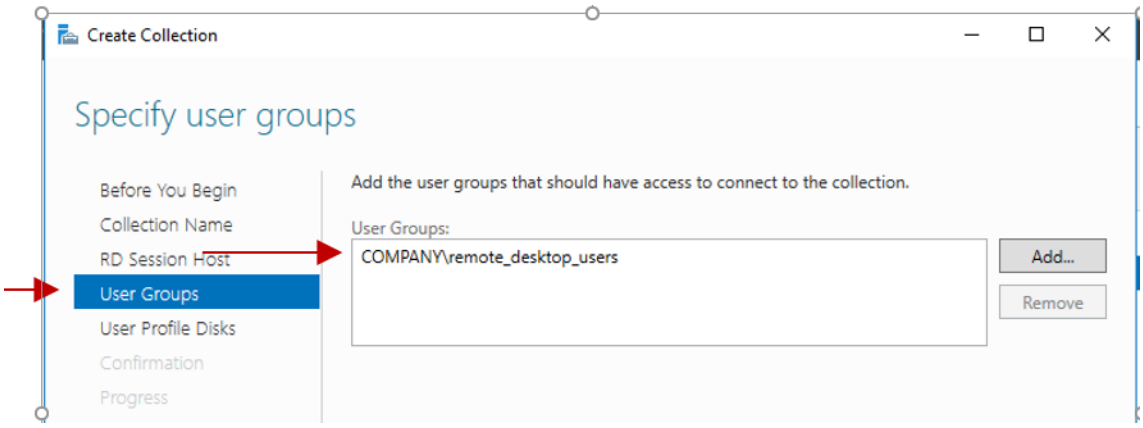

Figura 62 Permissões para aceder às Remote Apps

Existe a possibilidade de configurar determinado espaço em disco para armazenar os dados resultantes das sessões dos utilizadores.

Uma vez que as aplicações partilhadas no trabalho desenvolvido, são padrões do *Windows*, não é necessário armazenar estes dados.

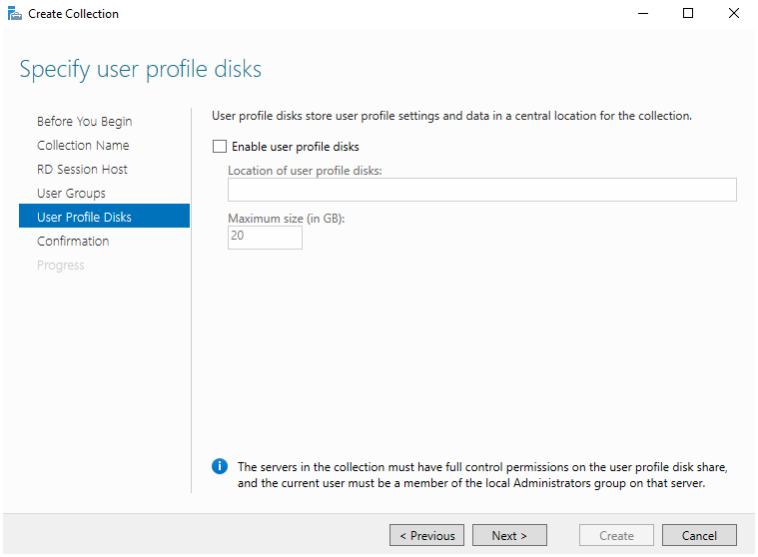

Figura 63 Especificar armazenamento de dados de utilizadores

O último passo na configuração é um resumo das opções escolhidas.

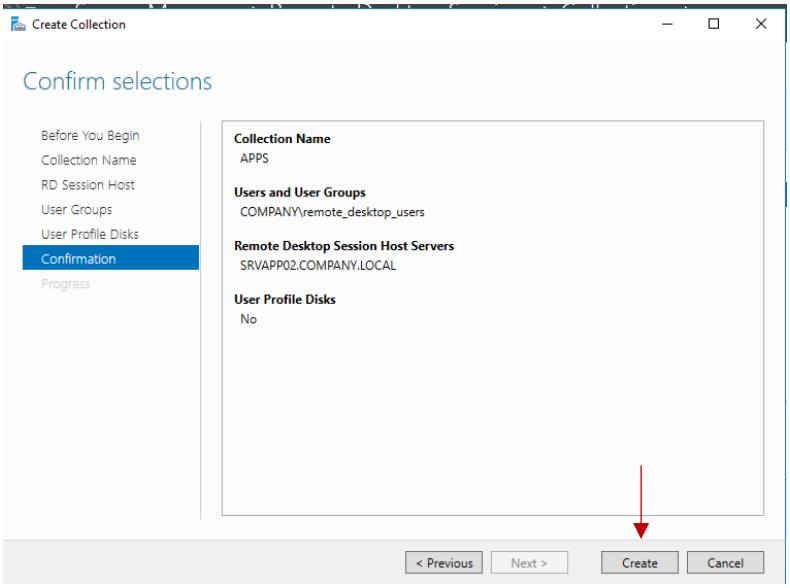

Figura 64 Resumo configurações Collection

Após a criação da *collection*, é necessário publicar as aplicações desejadas. Para o efeito, no *server manager*, irá surgir a *collection* criada, neste caso *APPS*, ao selecionar a mesma, no menu *REMOTEAPP PROGRAMS*, existe um botão denominado *tasks* que expande demonstrando a possibilidade de adicionar ou remover aplicações.

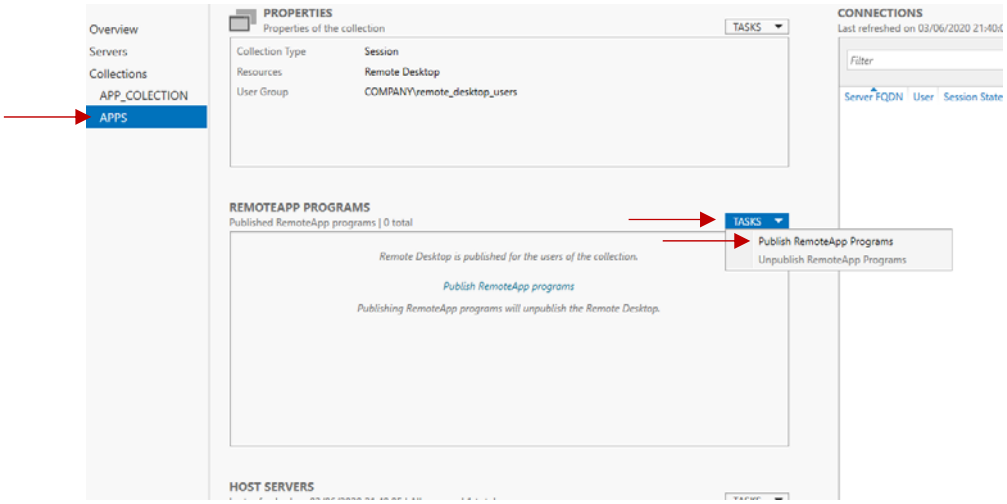

Figura 65 Publicar aplicações

Conforme demonstrado na figura 66, existem por defeito algumas aplicações nativas do *Windows* que é possível adicionar, no entanto é permitido selecionar uma aplicação instalada anteriormente numa localização especifica manualmente através do botão Add.

Como o objetivo deste trabalho é demonstrar o correto funcionamento deste serviço, apenas a aplicação *Calculator* irá ser partilhada.

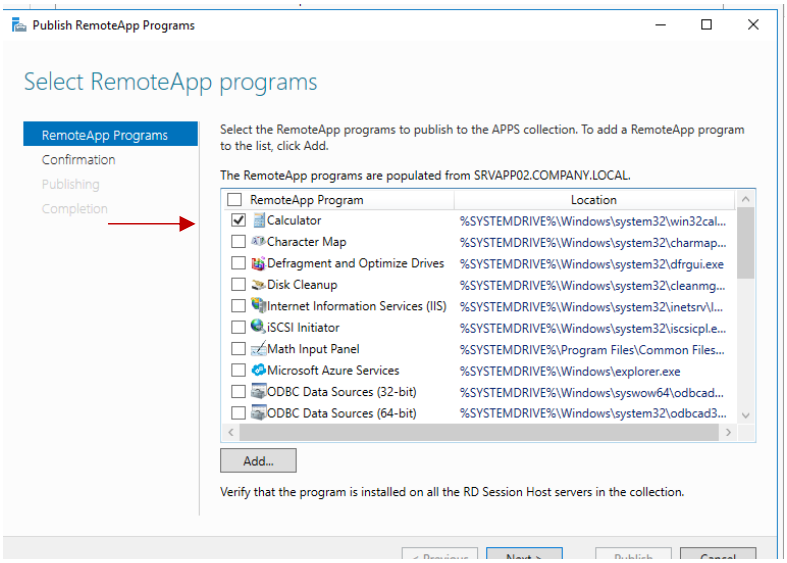

Figura 66 Selecionar aplicações a partilhar

O menu ilustrado na figura 67, resume as aplicações adicionas no passo anterior à *collection*, assim como a sua localização no servidor.

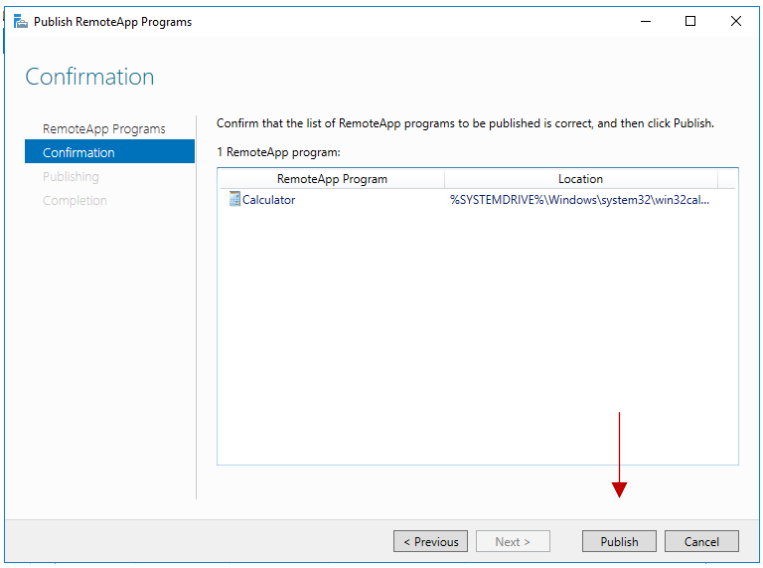

Figura 67 Confirmação de apps publicadas

Para tornar a *collection* fidedigna para as máquinas (clientes) que as consultam, é necessário criar e associar um certificado à *collection* e ao site hospedado no próprio servidor que contém a autenticação dos utilizadores e as aplicações remotas às quais têm acesso.

O ideal no âmbito empresarial seria associar um certificado SSL, obtido através de empresas certificadoras, no entanto neste trabalho, irá ser criado um certificado *self-sign* por parte do servidor aplicacional através do *IIS*.

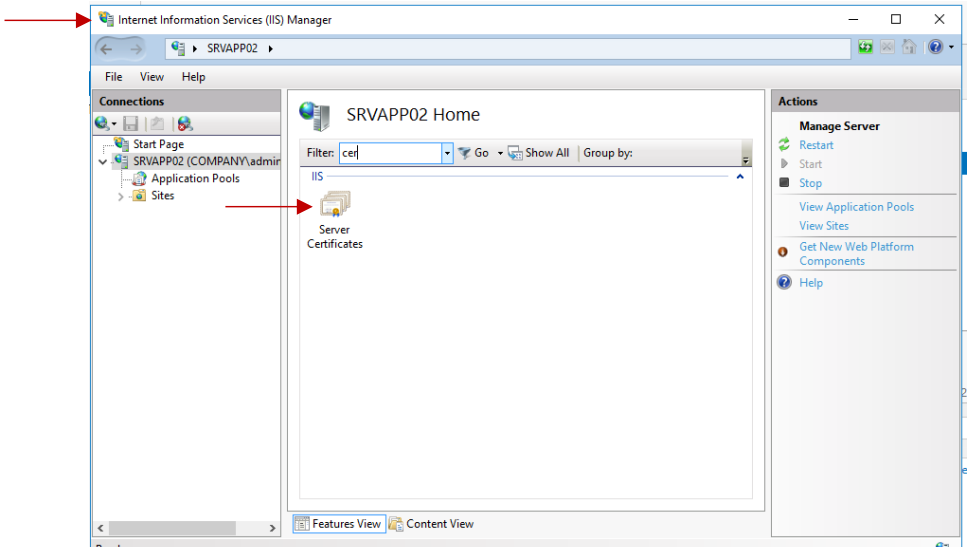

Figura 68 Internet Information Services

No menu ilustrado na figura 69, é possível consultar os certificados que existem no servidor assim como adicionar novos.

Para iniciar o processo de criação do certificado, é necessário clicar no botão *Create Self-Signed Certeficate.*

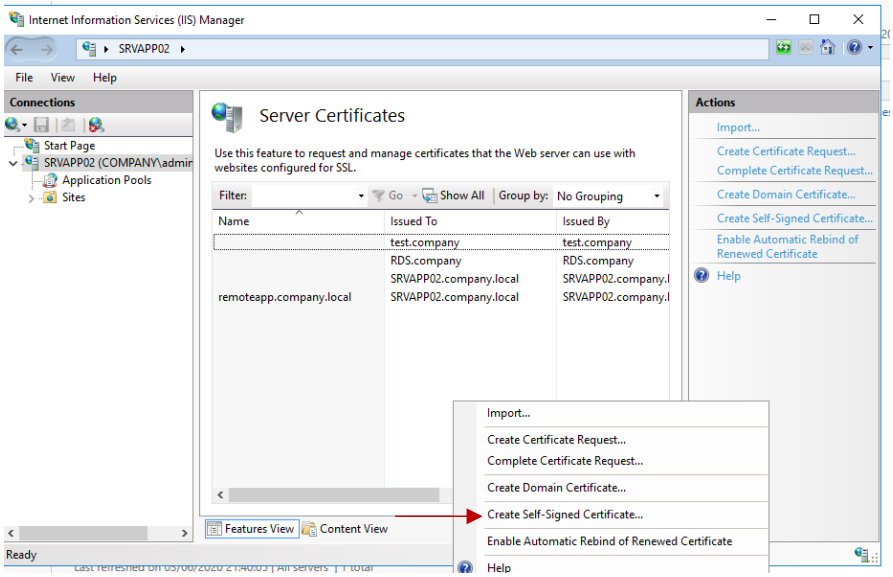

Figura 69 Certificados instalados no servidor

Como indicado na descrição da caixa de texto a preencher, na figura 70, as boas práticas indicam que o nome do certificado deve ser intuitivo para a função que o mesmo vai realizar.

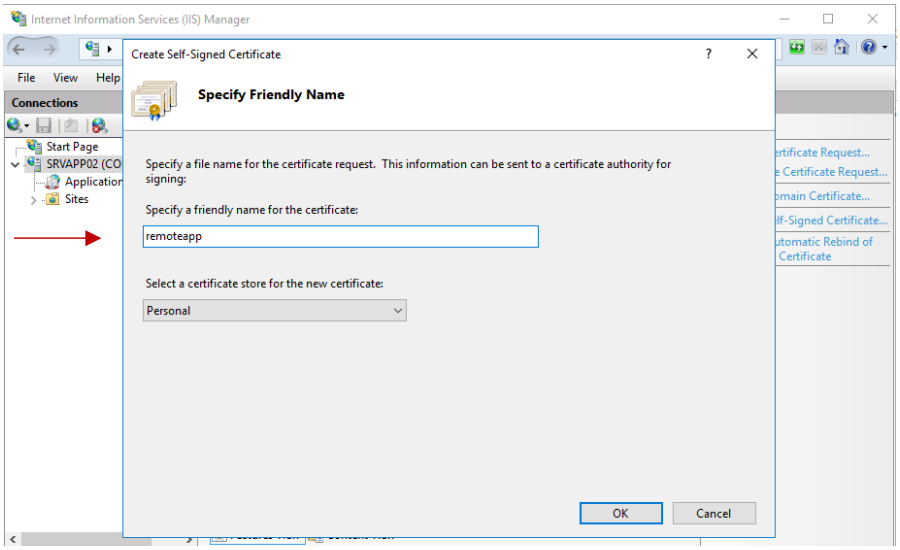

Figura 70 Nomear Certificado

De maneira a tornar o site fidedigno, é necessário associar o certificado previamente criado ao site. Para realizar este processo, clicar em *Bindings*, selecionar *https*, clicar em *edit* e adicionar o certificado previamente criado ao menu *SSL certificate*.

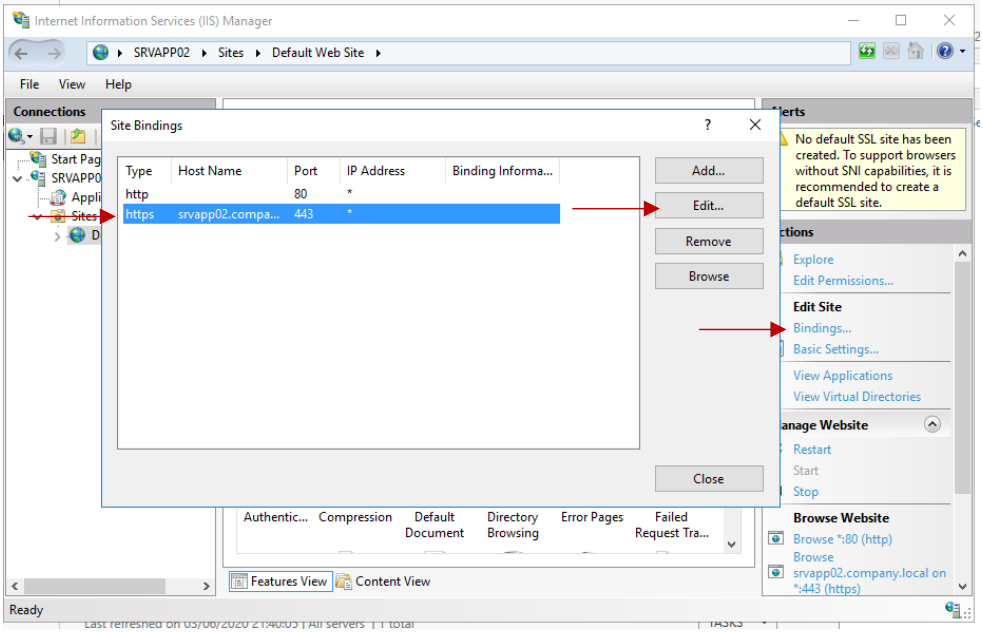

Figura 71 Associar certificado a site

Para ser associado o certificado à *collection* previamente criada (APPS), no menu com o mesmo nome no *server manager*, após clicar em *tasks*, surge um submenu, clicando na aba *Certificates*, pode-se adicionar o certificado criado a *RD Connection Broker – Enable Single Sign ON* e *RD Connection Broker – Publishing*.

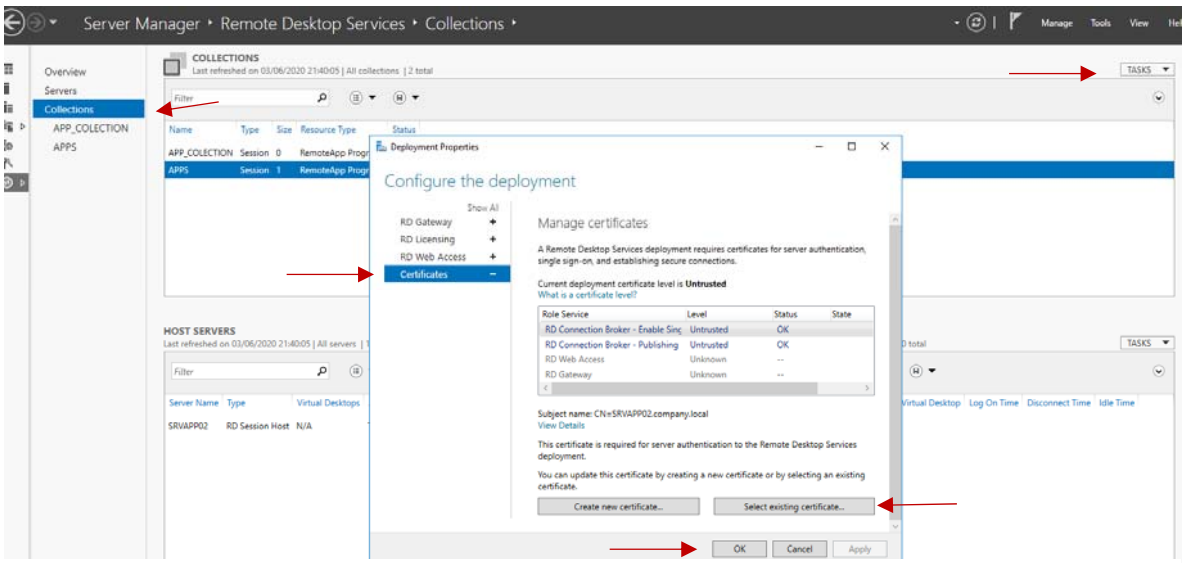

Figura 72 Associar certificado a collection

No menu ilustrado na figura 73, na opção *Choose a different Certeficate,* pode-se selecionar o certificado previamente criado e assim tornarmos fidedigna e segura a ligação.

Todos os certificados possuem uma data de validade, obrigando assim a uma renovação ao longo do tempo de forma a tornar o sistema seguro e atualizado.

O certificado em questão expira no dia 4 de junho de 2021, pelo que caso este trabalho fosse uma implementação num ambiente real, o certificado teria de ser renovado por volta dessa altura.

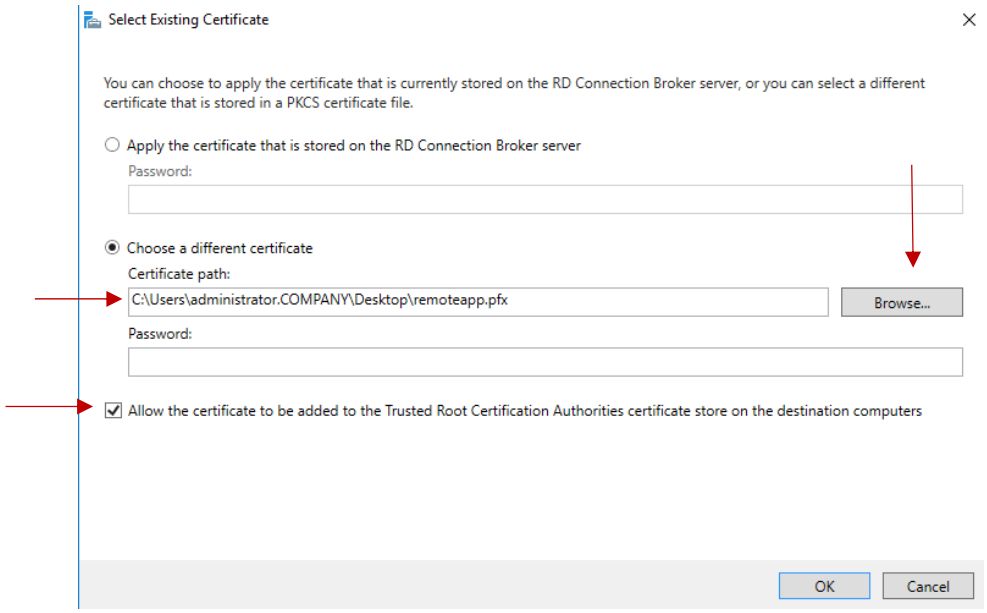

Figura 73 Selecionar certificado

1.6 Processo de adicionar *remote app* a uma máquina cliente

Com o objetivo de aceder de forma segura ao servidor, apenas as máquinas clientes que tenham o certificado instalado conseguirão aceder às aplicações partilhadas.

Para o efeito, é necessário instalar o certificado, caso a máquina seja utilizada por diversos utilizadores, é possível instalar o certificado no registo do utilizador, caso contrário pode-se instalar na máquina e fica disponível para todos os utilizadores que entrarem na mesma.

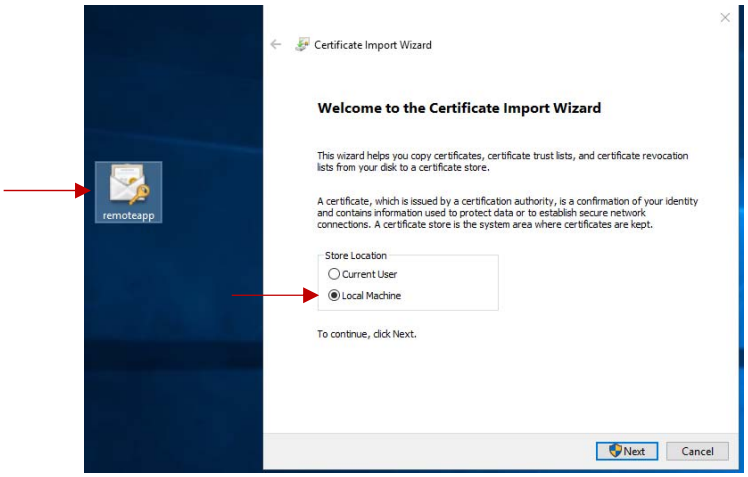

Figura 74 Instalar certificado

Este tipo de certificados, deve ser instalado sempre na *store Trusted Root Certification Authorities* uma vez que irá ficar associado a um tipo de serviço ou software. É aconselhado instalação manual em detrimento da instalação automática de forma a garantir o correto funcionamento.

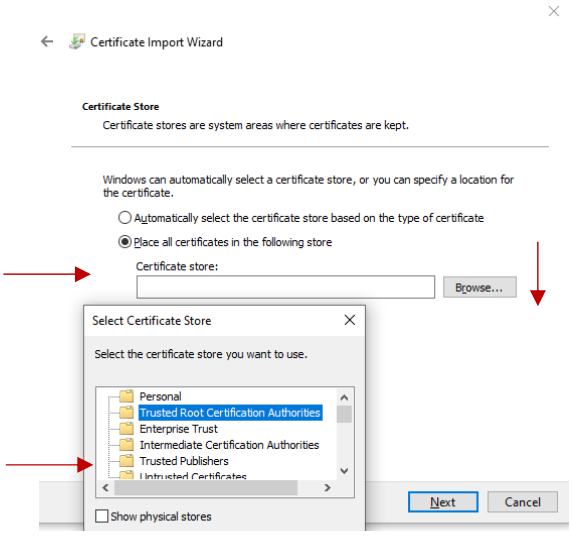

Figura 75 Localização da instalação do certificado

É possível estabelecer ligação com o servidor que fornece o serviço de *remoteapp* diretamente a partir do Windows eliminando a necessidade de instalar programas terceiros.

No painel de controlo do Windows existe uma opção *RemoteApp and desktop connections*, pressionando o botão *Acess RemoteAPP and desktops*, irá surgir a janela apresentada na figura 76.

No campo disponível é necessário inserir o URL onde está disponível o serviço de *RemoteApp*, neste caso, o FQDN (*fully qualified domain name)* do servidor aplicacional e os restantes parâmetros.

O endereço da localização deste serviço que terá que ser introduzido na caixa de texto será: https://srvapp02.company.local/rdweb/feed/webfeed.aspx

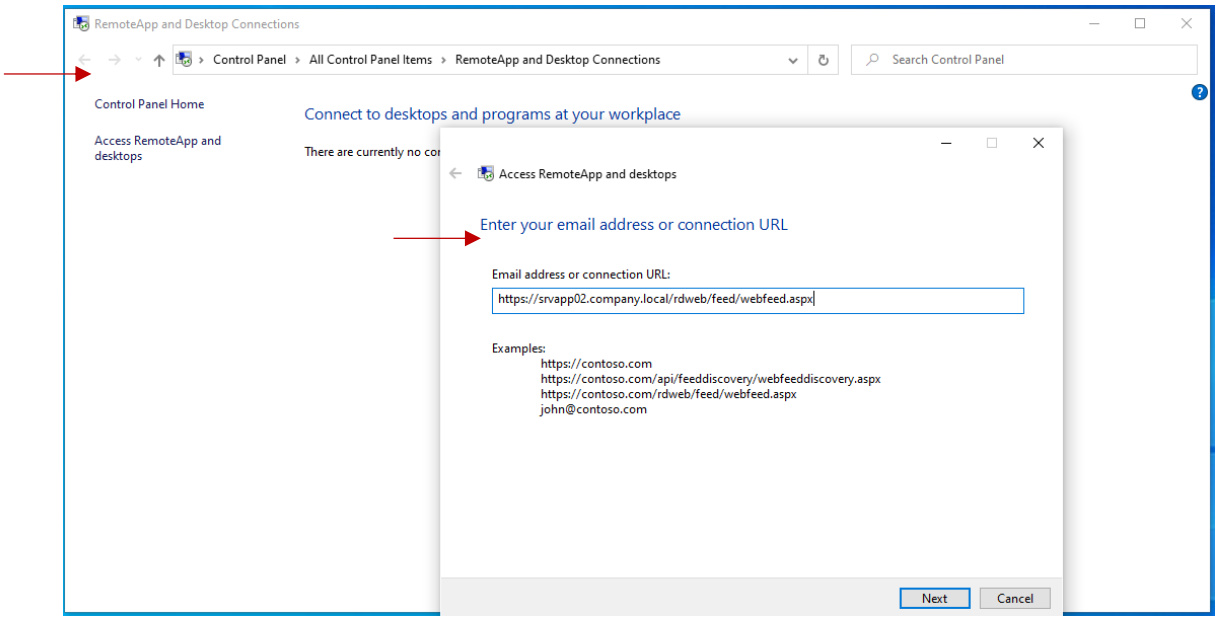

Figura 76 Adicionar RemoteAPP ao Windows

Esta ligação é apenas possível efetuar dentro da infraestrutura do domínio *company.local* cujos DNS configurados sejam o DNS 192.168.5.131 (DC01) ou 192.168.5.132 (DC02), após validação do certificado surge uma breve mensagem de confirmação das alterações que irão ser efetuadas ao computador. No menu ilustrado na figura 65, é necessário introduzir o *username* e *password* de domínio do utilizador que irá validar o acesso às *remoteapps* configuradas no servidor SRVAPP02.

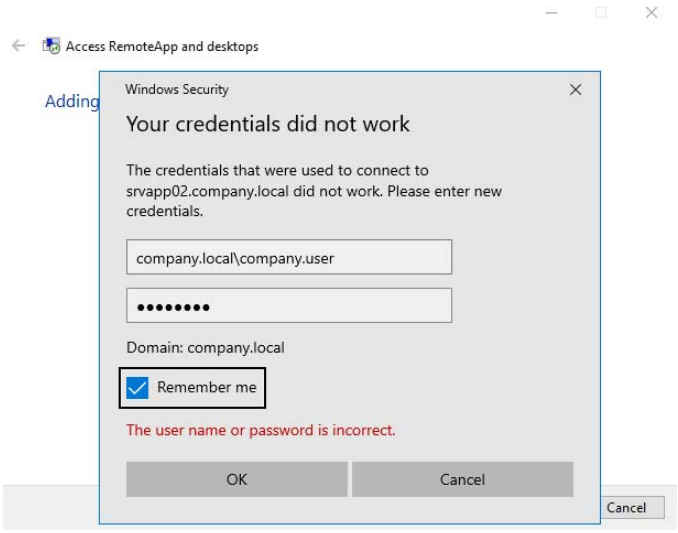

Figura 77 Introduzir credenciais de acesso

Após a ligação ser estabelecida com sucesso, é apresentado o menu ilustrado na figura 78, representando um pequeno resumo da ligação, a data mais recente em que foi atualizado, quantos recursos a conta tem permissões para aceder, a data em que foi adicionada e se a conexão está ativa. Ao clicar no botão *view resources* é possível verificar as aplicações que a conta tem acesso, neste caso a única aplicação que irá surgir será a calculadora adicionada previamente à *collection.*

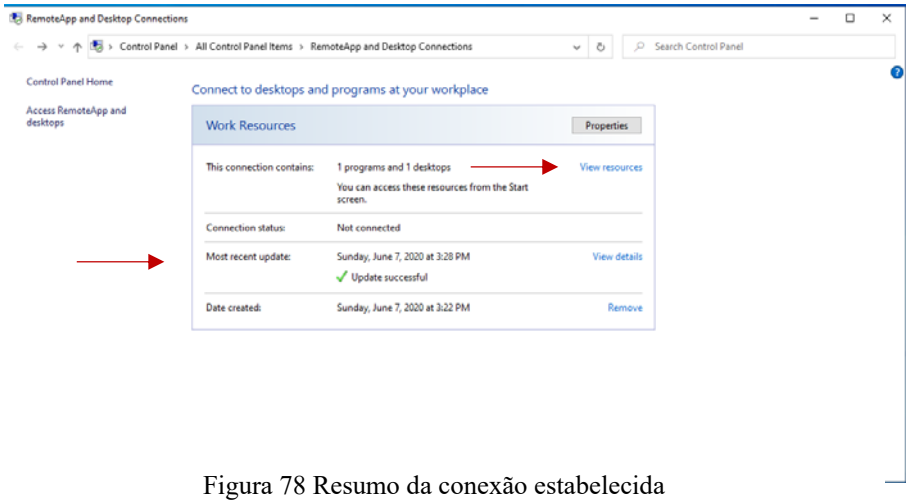

Figura 78 Resumo da conexão estabelecida

1.7 Processo de criação e replicação de drive partilhada

Após adicionar um disco adicional à máquina virtual, é possível partilhar o mesmo em rede, de forma a ficar disponível para as máquinas clientes acederem via *network drive.*

Ao abrir o menu das propriedades do disco, conforme ilustrado na figura 80, existe um separador *Sharing* que permite efetuar a partilha através de um nome escolhido para o efeito.

É possível também gerir as permissões que controlam o tipo de acesso que determinados utilizadores têm a determinadas diretorias dentro da pasta partilhada assim como o número de utilizadores que acedem em simultâneo.

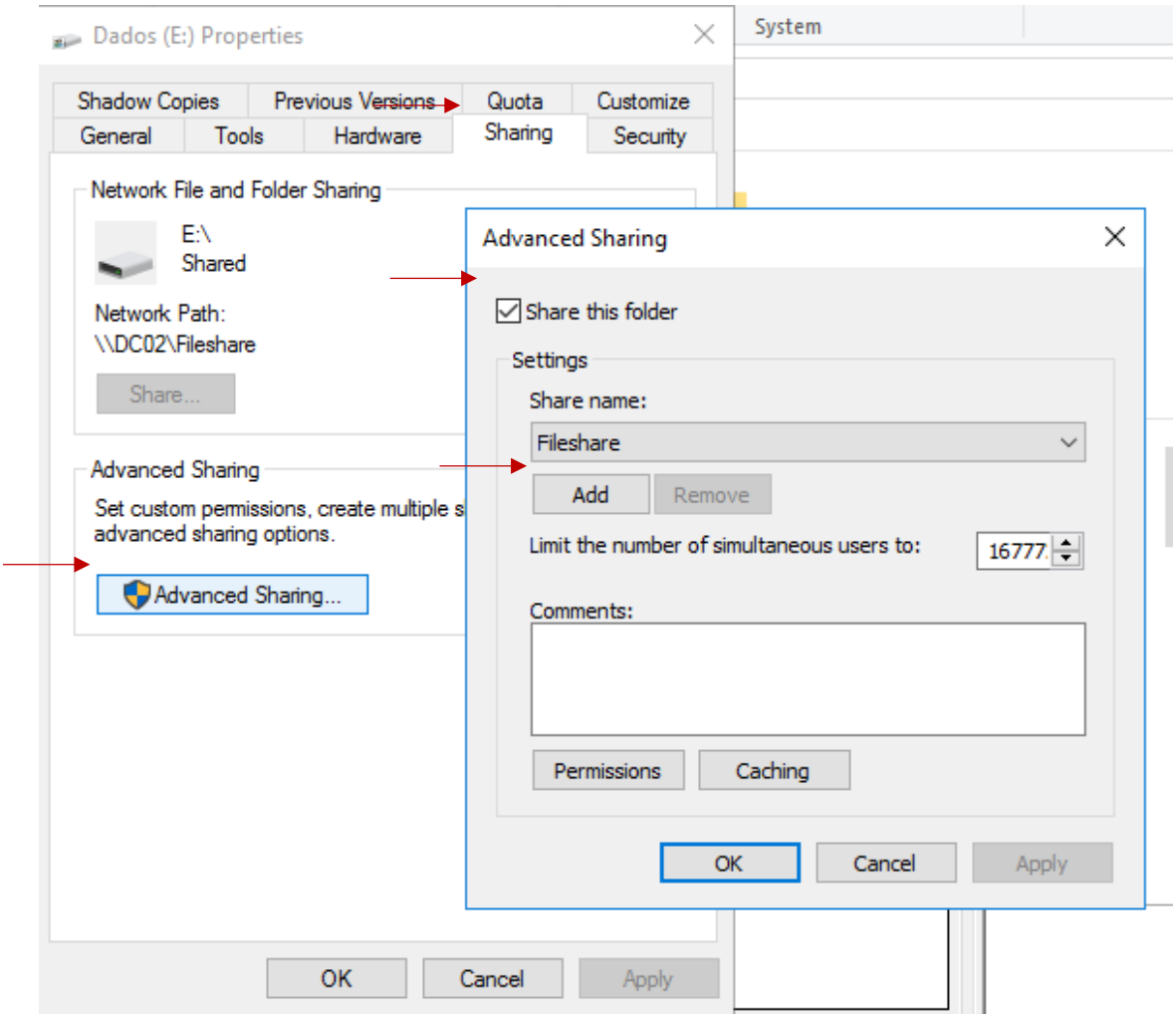

Figura 79 Partilhar partição

A estrutura demonstrada na figura 80 trata-se apenas de um exemplo, no entanto pode ser alterada conforme as preferências do cliente. De notar que cada pasta tem um grupo associado de permissões de forma a facilitar gerir os acessos dos utilizadores, estrutura que novamente pode ser alterado conforme escolha do cliente.

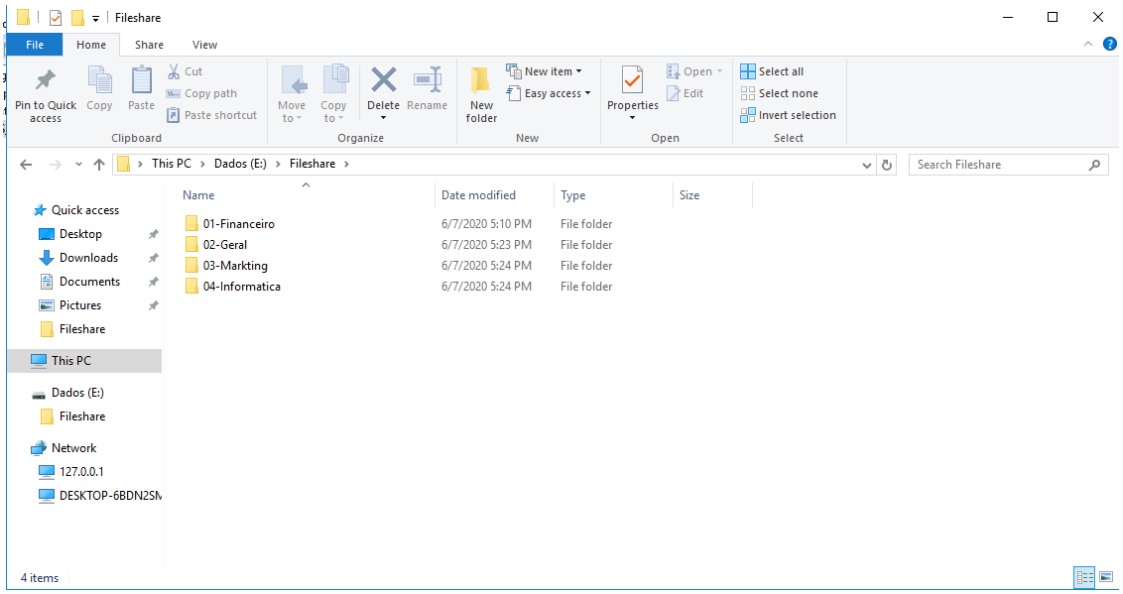

Figura 80 Estrutura Fileshare

É possível incutir determinadas regras a utilizadores e a computadores adicionados ao domínio. A figura 59 mostra um exemplo deste método, foi criado uma regra (GPO) que afeta todos os utilizadores do domínio em que irá ser mapeada uma *network drive*, oriunda do servidor DC02 (192.168.5.132) que também possui o *role* de *file server*.

A *network drive* irá possuir a *label Fileshare* e irá ficar associada à letra G: da máquina em que o utilizador se autêntica. De notar que esta regra apenas é implementada em utilizadores existentes no domínio que efetuam autenticação numa máquina também adicionada ao domínio.

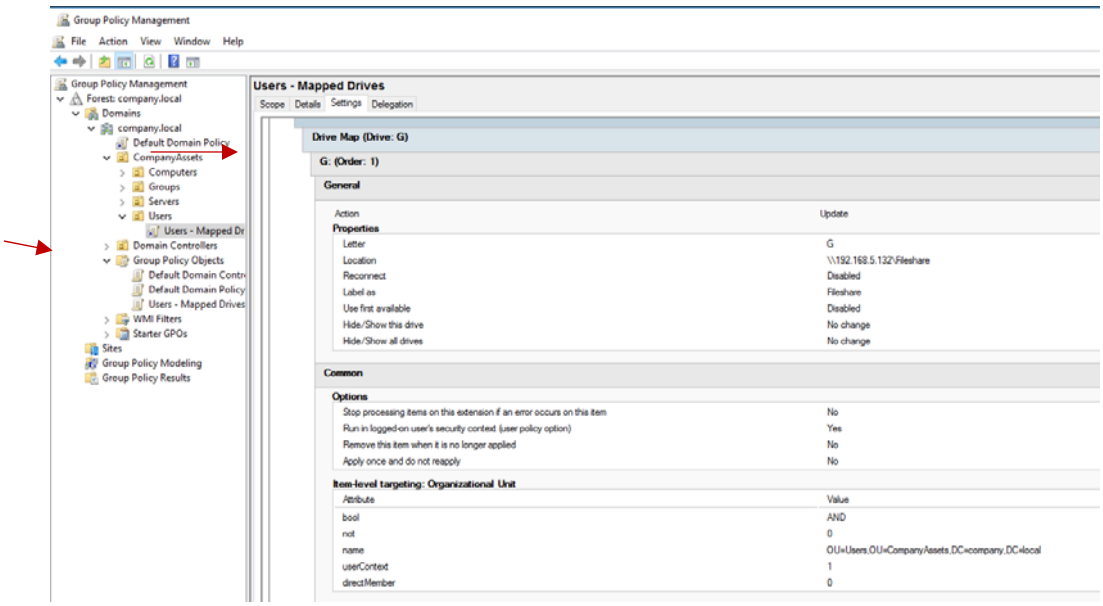

Figura 81 Mapeamento automático através de GPO

1.8 Processo de configuração *Shadow Copy*

Shadow copy é uma ferramenta importante que deve ser implementada, principalmente em discos que têm muitas alterações em ficheiros como pastas partilhadas em rede acessíveis por diversos utilizadores. Esta funcionalidade permite armazenar temporariamente ficheiros existentes na localização à altura do agendamento efetuado.

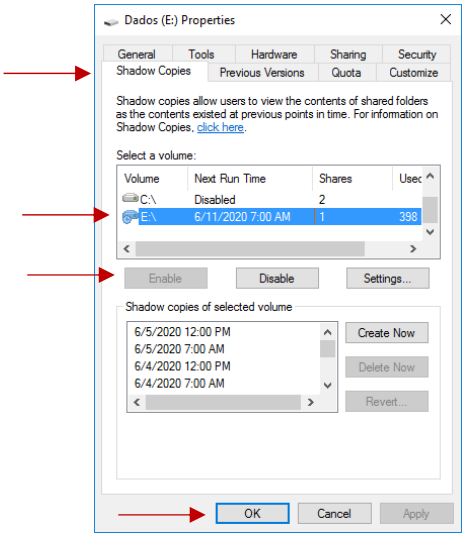

Figura 82 Shadow copy menu

Depois de habilitarmos o *Shadow Copy* presente no menu ilustrado na figura 83, é possível configurar qual o espaço reservado ao armazenamento dos ficheiros (evita ocupar espaço de forma desnecessária e indesejada).
É igualmente possível definir quais os dias da semana que irá ser armazenado os ficheiros e a que horas, as boas práticas indicam que deve ser efetuado não mais que 2 vezes por dia, de preferência em alturas com pouco movimento e evitar cópias com intervalos inferiores a 1 hora.

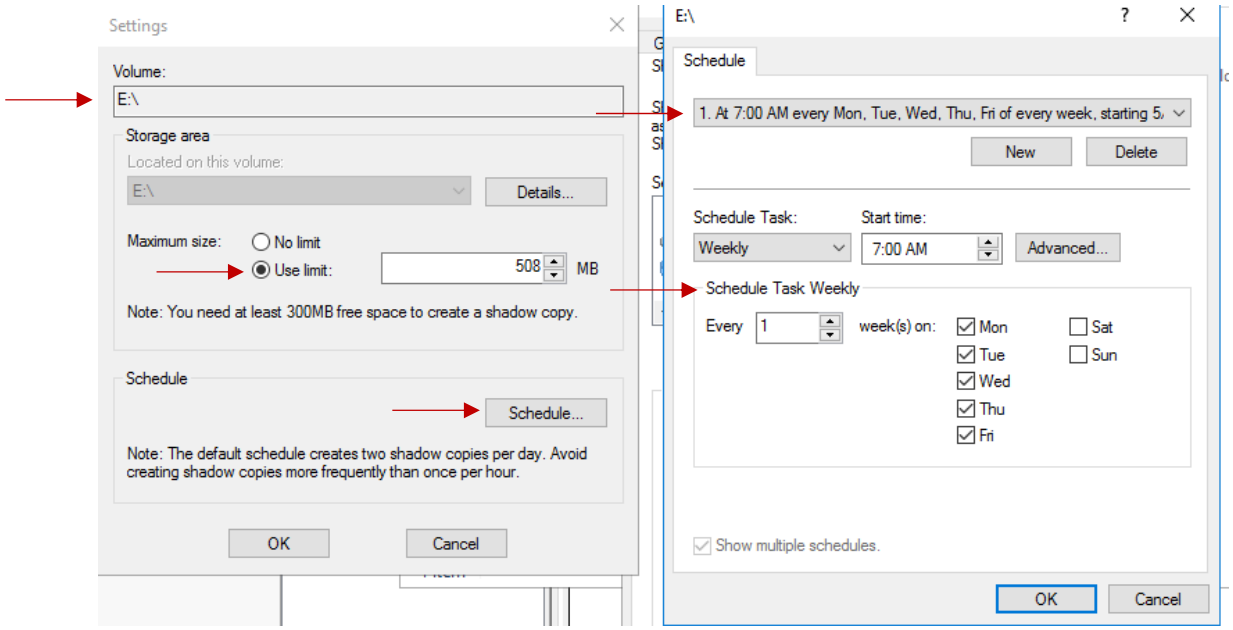

Figura 83 Configurações do Shadow Copy

1.9 Processo de configuração *DFS Replication*

Ao adicionar a *role* de *DFS Replication* ao servidor que tem o *fileshare* hospedado, neste caso o DC02, é possível replicar os dados para outro servidor garantindo desta forma a redundância dos mesmos.

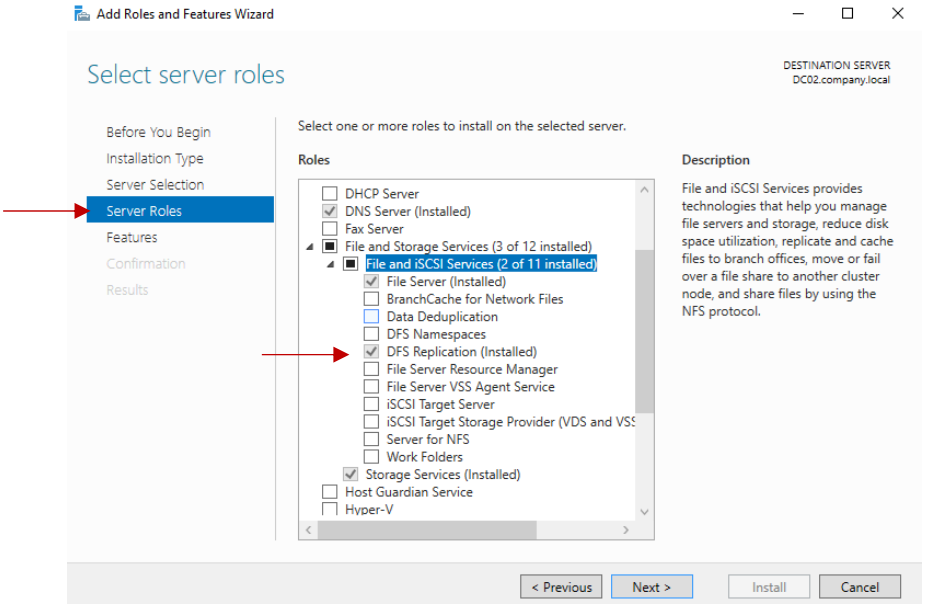

Figura 84 Adicionar role DFS Replication

Após a instalação do *role DFS Replication*, é possível aceder ao menu de gestão DFS dando assim inicio à configuração do mesmo.

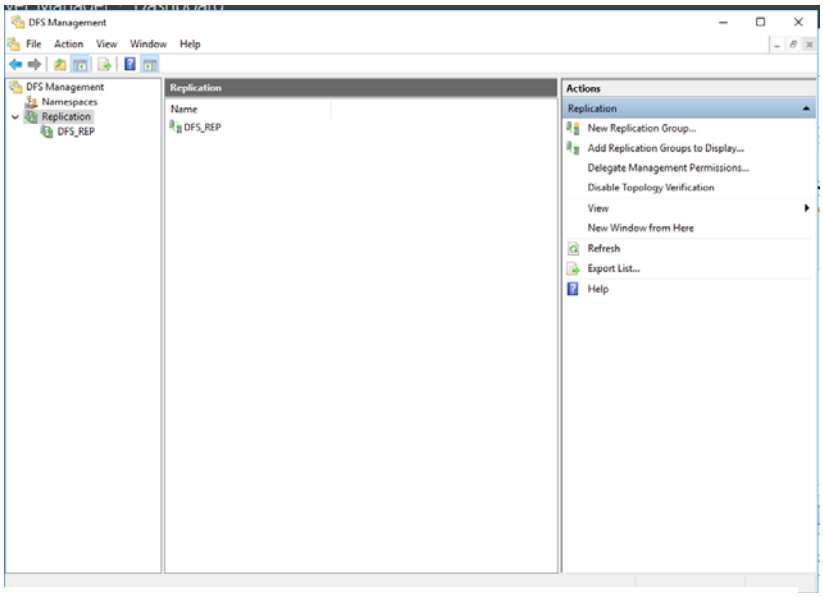

Figura 85 DFS Management menu

Para configurar esta ferramenta, é necessário executar diversos passos para garantir o correto funcionamento da mesma.

Replication Group type- É possível optar por implementar uma replicação através de diversos servidores (*Multipurpose replication group*) ou apenas entre dois servidores (*Replication group for data collection*). Para este trabalho foi selecionada a primeira opção uma vez que um dos objetivos principais é o sistema ser escalável e customizável consoante necessidades do cliente

Name and Domain- Surge a opção de nomearmos o *replication group* que deve ser intuitivo e claro sobre a sua funcionalidade.

Existe ainda a opção de selecionar o domínio dentro do qual a replicação irá ser feita, neste caso será *company.local* uma vez que as máquinas que irão efetuar a replicação, pertencem a este domínio.

Para o efeito do trabalho, uma vez que o objetivo é apenas demonstrar a funcionalidade desta ferramenta, foi dado o nome de *DFS_REP*.

Replication Group Members- É necessário adicionar todas as máquinas que irão participar nesta replicação, no caso deste trabalho, a máquina DC01 e DC02.

Topology Selection- O objetivo deste menu é selecionar a melhor topologia para as necessidades do cliente, a opção *Hub and Spoke* necessita que exista 3 ou mais membros em que a informação contida no principal, é replicado para os restantes.

A opção *Full mesh*, a replicação é realizada entre todos os membros não existindo nenhuma hierarquia.

No topology, permite criar uma topologia customizável, tem como alvo alguma necessidade especifica do cliente.

Neste trabalho, a opção selecionada foi a *Full mesh*, que na prática será também a mais utilizada em ambientes reais.

Replication Group Schedule and Bandwidth- Essencial em qualquer ferramenta de replicação de ficheiros, existe a opção de usar toda a largura de banda para efetuar uma replicação instantânea ou limitar a mesma caso exista constrangimentos em termos de velocidade de internet.

Existe também a opção de realizar a replicação em dias específicos ou horas especificas que causem menos impacto para os utilizadores.

No âmbito deste trabalho, foi selecionada a opção da replicação instantâneas usando toda a largura de banda disponível, uma vez que serve apenas para demonstração, no entanto as boas práticas dizem que tal deve ser feito em horas com menos interações por parte dos utilizadores.

Primary Member- Neste menu, é necessário definir qual o servidor que tem primazia caso exista informação previamente replicada.

No caso do trabalho, o servidor que contém a estrutura da informação e é acessível pelos utilizadores é o DC02 logo este será o servidor principal quando a replicação for efetuada.

Folders to Replicate- Este menu é composto por uma tabela onde é possível adicionar quais as pastas presentes no servidor de (DC02) origem que se deseja replicar.

Local Path of DFSReports on other members- Neste menu, é apresentada uma tabela com os membros previamente definidos que fazem parte da replicação. É possível definir qual a localização em que irá ser realizada a replicação no destino.

No trabalho, foi criada uma pasta na localização DC01\c$\DFS_REP que irá estar sempre sincronizada com a informação presente na pasta partilhada presente no DC02.

É possível ainda definir se a informação replicada, tem permissões apenas de leitura, impedindo desta forma que informação seja eliminada de forma equivoca.

Os restantes menus (*Review Settings and Create Replication Group* e *Confirmation),* apresentam apenas informação informativa das configurações efetuadas nos menus anteriores.

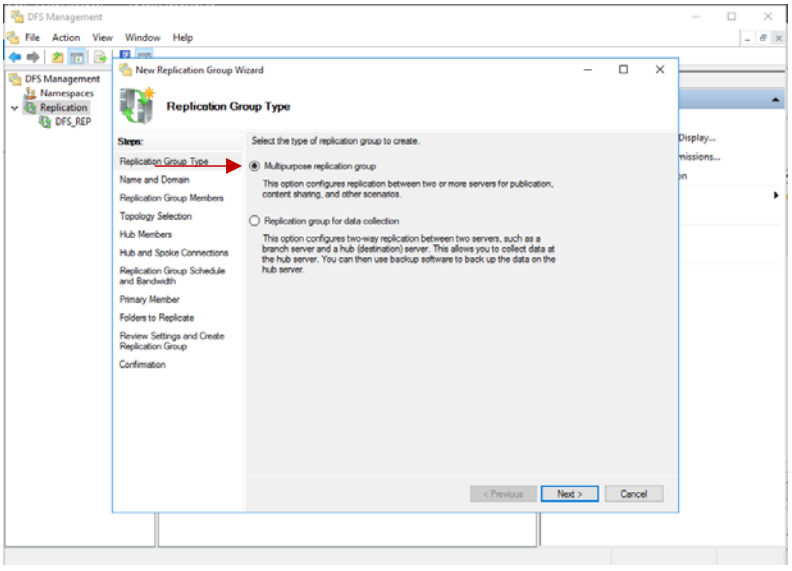

Figura 86 Criar Replication Group

Na figura ilustrada abaixo, é possível verificar o funcionamento da replicação DFS.

O conteúdo presente em dc01\c$\DFS_REP\Fileshare é exatamente o mesmo que em dc02\Fileshare.

Uma vez que a replicação foi configurada com acesso apenas de leitura, previne desta forma a eliminação dos ficheiros de forma equivoca, criando assim um ambiente seguro para a replicação de ficheiros.

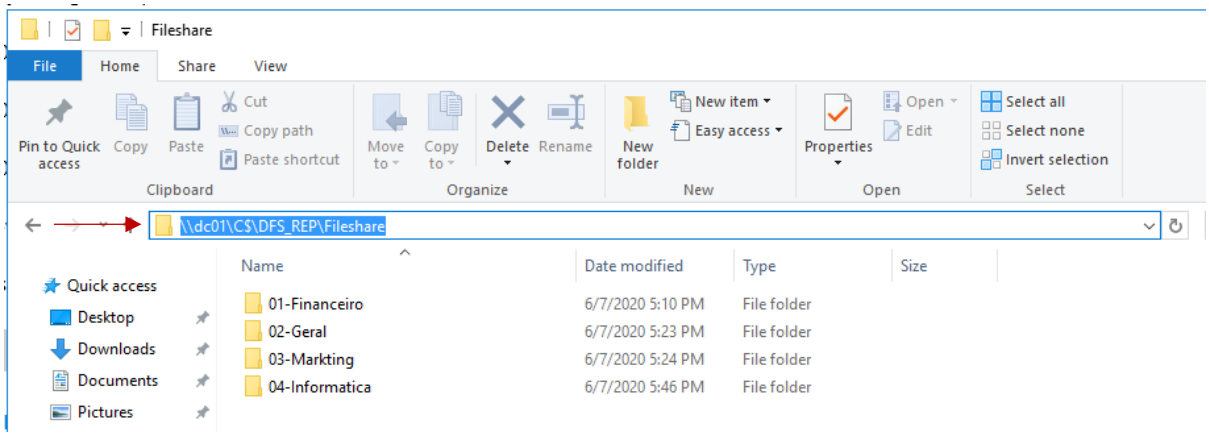

Figura 87 Replicação DFS no servidor DC01