Instituto Superior de Tecnologias Avançadas

Licenciatura em Informática

Disaster Recover para Azure

Solução para Autenticação na Cloud

Realizado por: Paulo Alexandre Alcântara da Costa Moreira – 30259

Coordenador – Professor Dr. Pedro Brandão

Orientadora - Professora Dra. Dulce Mourato

Lisboa, Ano Letivo 2022/2023

Instituto Superior de Tecnologias Avançadas

Licenciatura em Informática

Disaster Recover para Azure

Solução para Autenticação na Cloud

Realizado por: Paulo Alexandre Alcântara da Costa Moreira – 30259

Coordenador – Professor Dr. Pedro Brandão

Orientadora - Professora Dra. Dulce Mourato

Lisboa, Ano Letivo 2022/202

Resumo

O objetivo deste trabalho foi demonstrar o conceito de Disaster Recovery as a Service (DRaaS) simulando e demonstrando a recuperação de um controlador de domínio através do Azure, nomeadamente procurou demonstrar a recuperação de um controlador de domínio por meio do Azure, bem como a centralização da administração de AD pela web.

Na revisão da literatura foram abordados conceitos como a virtualização, o Azure e as suas ofertas no mercado, a computação na nuvem incluindo os diferentes modelos em que esta pode ser entregue e algumas das vantagens e desvantagens da mesma e estabelecendo pontos de convergência sobre o hipervisor e o seu papel na virtualização.

Foi seguida uma metodologia de investigação de cariz qualitativo, quanto aos objetivos exploratória e descritiva e no que diz respeito aos procedimentos foi escolhida a pesquisa de estudo de caso, onde se detalharam o todos os procedimentos no caso de uma falha na infraestrutura e como através da Cloud foi possível autenticar o cliente e o funcionamento dos laboratórios os laboratórios e a descrição do que foi implementado. No capítulo dos resultados, são detalhados as escolhas que foram feitas e como elas cumprem os objetivos que foram estabelecidos. Também são descritos os testes que foram realizados para avaliar a eficácia da solução.

O presente trabalho demonstrou a viabilidade e a eficácia do conceito de Disaster Recovery as a Service (DRaaS) através da simulação e demonstração da recuperação de um controlador de domínio através do Azure.

Palavras-Chave: Hyper-V, Virtualização, DRaaS, Azure.

Abstract

The objective of this work was to demonstrate the concept of Disaster Recovery as a Service (DRaaS) by simulating and demonstrating the recovery of a domain controller through Azure. Specifically, it sought to demonstrate the recovery of a domain controller through Azure, as well as the centralization of AD administration through the web.

In the literature review, concepts such as virtualization, Azure and its market offerings, cloud computing including the different models in which it can be delivered and some of its advantages and disadvantages were addressed, establishing points of convergence on the hypervisor and its role in virtualization.

A qualitative research methodology was followed, with exploratory and descriptive objectives, and with regard to procedures, case study research was chosen, where all the procedures in the event of an infrastructure failure were detailed and how through the Cloud it was possible to authenticate the client and the functioning of the laboratories and the description of what was implemented. In the chapter on results, the choices that were made are detailed and how they meet the objectives that were established. The tests that were carried out to evaluate the effectiveness of the solution are also described.

This work demonstrated the viability and effectiveness of the Disaster Recovery as a Service (DRaaS) concept through the simulation and demonstration of the recovery of a domain controller through Azure.

Keywords: Hyper-V, Virtualization, DRaaS, Azure.

Índice

Introdução vi
Revisão da Literatura 12
Materiais e Métodos de Desenvolvimento 29
Resultados 34
Discusão de resultados 41
Conclusão 43
Referências Bibliográficas … 44

Índice de Tabelas

Tabela 1- Cronograma da criação do artefacto digital e etapas da investigação 30
Tabela 2 - Dados para Criação de Máquinas 39
Tabela 3 - Dados para Contas 39
Tabela 4 - Chaves Sistema Operativo 40

Índice das Figuras

Figura 1- Comparação entre os Diferentes Modelos de Cloud 16
Figura 2 - Diferenças entre os vários tipos de Cloud Disponíveis..... 17
Figura 3 - Edição do Windows Server 2016..... 22
Figura 4 -Árvores e Florestas num Domínio 23
Figura 5 - Replicação Entre Sites..... 23
Figura 6 - Esquema de Funcionamento dos Hipervisores 24
Figura 7 - Virtualização de Dados. 25
Figura 8 -Virtualização de Servidores. 25
Figura 9 - Hipervisor Tipo 1. 27
Figura 10 - Hipervisor Tipo 2. 28
Figura 11 - Diagrama infraestrutura. 31
Figura 12 - Prepare Infrastructure. 35
Figura 13 - Deployment. 36
Figura 14 - Source 36
Figura 15 - Targe. 37
Figura 16 - Prepare..... 37
Figura 17 - Policy 38

Abreviaturas

AD - Active Directory

ADFS - Active Directory Federation Services

ADLDS - Active Directory Lightweight Directory Services

ADRMS - Active Directory Rights Management Services

AWS - Amazon Web Service

BIOS - Basic Input/Output System

BSD - Berkeley Software Distribution

CMS - Cambridge Monitor System

CP - Control Program

CPU - Central Process Unit

CRM - Customer Relationship Management

DARPA - Defense Advanced Research Projects Agency

DC – Domain Controller

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DoS - Denial of Service

DRaaS - Disaster Recovery as a Service

GC - Global Catalog

GE - General Eletrics

GPT - Guided Partition Table

IA - Inteligência Artificial

IaaS - Infra-Structure as a Service

IBM - International Bussiness Machines

IIS - Internet Information Services

IP - Internet Protocol

IT - Information Techonology

KVM - Kernel Virtualization Module

LDAP - Lightweight Directory Access Protocol

MAC - Mathematics and Computation

MIT - Massachusetts Institute of Technology

PaaS - Platform as a Service

RAM - Random Access Memory

SaaS - Software as a Service

SQL - Structured Query Language

SSD - Solid State Drive

TB - TeraBytes

UEFI - Unified Extensible Firmware Interface

VDI - Virtual Desktop Interface

Introdução

A virtualização é uma tecnologia que se tem vindo a falar e tem mudado a forma como usamos os computadores, hoje em dia o mercado está a optar por soluções virtualizadas, desde um simples servidor até um desktop, todos os sistemas começam a tirar partido desta tecnologia para rentabilizar custos e aumentar flexibilidade.

O objetivo deste estudo foi explorar o uso da recuperação de sites através do Azure, um conceito cada vez mais adotado pelas empresas, como uma solução passível de investimento. O estudo visou demonstrar a recuperação de um controlador de domínio por meio do Azure, bem como a centralização. Foram ainda efetuados testes de soluções de virtualização e de nuvem para encontrar a melhor maneira de aplicá-las no ambiente pretendido.

Na revisão da literatura apresentaram-se alguns dos conceitos como a virtualização, uma das opções: o Azure e suas ofertas de mercado, modelos de computação em nuvem e o papel do hipervisor na virtualização. Também discutiu as vantagens e desvantagens da computação em nuvem, os critérios éticos cumpridos, incluindo os procedimentos adotados para garantir a segurança e privacidade dos dados.

No capítulo do resultados descreveram-se os dois laboratórios que foram montados para testar o conceito de recuperação de sites através do Azure. O primeiro laboratório consistiu num controlador de domínio e um cliente, enquanto o segundo laboratório foi montado para mostrar a compatibilidade do Azure com qualquer sistema operativo e demonstrar uma alternativa de código aberto às soluções da Microsoft.Foram também explicadas as diversas etapas para ‘carregar’ a máquina para o Azure e realizar o teste de autenticação, para confirmar como funciona e do. foi implementado no projeto.

Na discussão dos resultados aprofundaram-se as questões que podem ser melhoradas na infraestrutura de rede, como por exemplo: incluir informações sobre como os dados, como foram armazenados e protegidos, e como a infraestrutura de rede foi gerida e monitorizada. Também se destacaram os critérios éticos presentes em termos de procedimentos adotados para garantir a segurança e privacidade dos dados.

Foi possível concretizar conceito de Disaster Recovery as a Service (DRaaS) e a recuperação de um controlador de domínio por meio do Azure. Também foi abordada a centralização da administração de AD por meio da web e o teste de prova de conceito, que demonstrou a capacidade de recuperar todas as informações e configurações, num curto período de tempo.

O desenvolvimento deste estudo abordou as soluções apresentadas para os objetivos secundários propostos que foram:

- Recuperação do Controlador de Domínio via Azure (Cloud)
- Centralização de Gestão da AD via Web

Foi também feito um teste como prova de conceito, para provar que funcionou e demonstrou-se que em pouco tempo se consegue recuperar a informação toda, assim como a respetiva configuração.

Revisão da Literatura

A recuperação em caso de desastre explora a possibilidade de algum tipo de catástrofe. Neste capítulo de revisão da literatura, foram abordadas situações de calamidade e como costumam aparecer aos utilizadores, o mesmo vai servir de ponto de partida para responder à motivação subjacente à implementação prática: Qual é a inspiração por trás da criação de um cenário de recuperação de desastres?

Snedaker (2013. p.1) procura responder de forma simples, considerando a natureza imprevisível dos desastres e seu potencial impacto nas operações críticas, por que é crucial desenvolver cenários e planos de preparação para recuperação de desastres?

> The inspiration behind creating a disaster recovery scenario is often rooted in the understanding that disasters can strike at any time and can have serious consequences. Forecasting and preparation are motivated by the need to protect critical assets and ensure the continuity of operations (Snedaker, 2013. p.1),

No livro "Disaster Recovery Planning: Preparing for the Unthinkable", de Jon William Toigo (2013), identificou-se que a inspiração para a importância da recuperação de desastres foi impulsionada por custos elevados por não haver uma alternativa. Conforme Toigo (2013, p.55) argumenta:

> History is filled with examples of organizations that learned the hard way about the importance of disaster recovery. The motivation for creating recovery scenarios often comes from painful lessons of the past, where lack of preparation resulted in significant losses (Toigo, 2013. p.55),

Dado o grande número de organizações que sofreram grandes perdas devido à falta de preparação para recuperação de desastres, por que é importante aprender com seus erros e desenvolver planos de recuperação eficazes?

As estratégias que podem ser adotadas para evitar cenários complicados em termos empresariais e que nortearam esta pesquisa, em termos de potenciais respostas a questões de investigação foram:

• Virtualização e computação em nuvem oferecem flexibilidade na recuperação do sistema. Essas tecnologias permitem que as organizações implementem rapidamente ambientes alternativos em caso de desastre.

• A resiliência nas infraestruturas é essencial para proteger os dados. A conformidade regulamentar, a necessidade de proteger dados críticos e o reconhecimento de que a resiliência organizacional é essencial para a sobrevivência a longo prazo também podem motivar a recuperação de desastres.

É necessário ter políticas de segurança e recuperação definidas. Elas são fundamentais para saber orientar as ações que podem acontecer em caso de um desastre. Um plano robusto faz toda a diferença, quando se encontra uma situação de recuperação de dados, sendo que o conhecimento de diretrizes claras e bem definidas, ajuda a uma melhor ação e organização durante todo o evento. Ideias reforçadas por alguns autores como Toigo (2013. p.14) que refere, a propósito "virtualization and Cloud computing offer flexibility in system recovery. These technologies enable organizations to quickly implement alternate environments in case of a disaster".

No livro "Business Continuity and Disaster Recovery Planning for IT Professionals", de Susan Snedaker (2013), abordam-se estas questões e dá-se relevância à importância de uma equipa preparada para proteger os dados e saber como os restaurar. A autora fornece informações importantes sobre a continuidade de negócio e como as recuperações de desastres beneficiam as empresas de TI.

A proteção de dados é crítica e fundamental para qualquer organização nos dias que correm, são muitas as vantagens a adotar nas empresas que têm em conta um plano contra desastres que podem ocorrer e prejudicar o negócio.

> The motivation behind disaster recovery is often a combination of regulatory compliance, the need to protect critical data, and the recognition that organizational resilience is essential for long-term survival (Gregory, 2011. p.32).

É necessário ter politicas de segurança e recuperação definidas, elas são fundamentais para saber orientar as ações que pode acontecer em caso de um desastre, é um plano robusto que faz toda a diferença quando se encontra uma situação de recuperação de dados, o conhecimento de diretrizes claras e bem definidas ajudam a uma melhor ação e organização durante todo o evento, encontramos no livro 'Business Continuity and Disaster Recovery Planning for IT Professionals' por Susan Snedaker (2013) que aborda estas questões e dá relevância á importância de uma equipa preparada para proteger os dados e saber como os restaurar.

A autora Susan Snedaker (2013) fornece informações importantes sobre a continuidade de negócio e, como a recuperações de desastres beneficiam as empresas de TI, a proteção de dados que são críticos e fundamentais para qualquer organização nos dias que correm.

São muitas as vantagens a adotar nas empresas que tem em conta um plano contra desastres que podem ocorrer e prejudicar o negócio.

Virtualização e Segurança - ao falarmos de virtualização ligada a uma rede global que é a internet, também devemos abordar o tema da segurança e o que podemos fazer para salvaguardar ao máximo os nossos dados que são confidenciais. Deve-se ter em conta que aos dias de hoje qualquer computador seja Windows ou Linux é equipado com uma primeira barreira ao mundo exterior, ou seja uma firewall que é onde é feito o controlo do tráfego que entra e sai através de regras criadas por nós, ou por aplicações instaladas. No caso do Windows a firewall que vem integrada no sistema é o Windows Firewall e no caso do Linux a firewall que vem instalada por defeito em distribuições Debian/Ubuntu é o Iptables. Qualquer função que adicionamos no nosso servidor ou computador este abre automaticamente a porta do nosso serviço para permitir tráfego.

Algo importante a reter e que internamente as portas são abertas e o tráfego é permitido dentro da nossa rede local, mas quando estamos a falar da internet, então o cenário é outro, porque cada porta que a gente abra ou crie uma exceção para ela deixar tráfego é uma porta que pode estar sujeita a ataques externos como DoS, IP Spoofing e Session Hijacking. São ataques que se tratam de ganhar acesso não autorizado ás máquinas á exceção do DoS que é um ataque apenas para impedir acesso á máquina, um exemplo deste ataque é um e o excesso de pings até chegar ao ponto de a máquina não conseguir responder. Existem, no entanto, para além das firewall's algumas regras abaixo descritas que podem ajudar a prevenir ataques e a aumentar a segurança.

1 – Controlo de acesso dos utilizadores á rede, deve ser restrito o acesso aos utilizadores por zonas de acordo com as suas funções;

2 – Educar os utilizadores acerca de comportamentos a adotar na rede corporativa (downloads, utilização e orientações sobre ataques virtuais);

3 – Ter uma política de segurança clara e divulgada internamente englobando qualquer dispositivo que se ligue a rede.

Um dos principais objetivos deste projeto que é a Replicação da Máquina Virtual para o Azure possibilitou aprender a realizar um *backup* da nossa máquina virtual, que contém todas as definições do nosso domínio para a Cloud do Azure e recuperar em caso de desastre.

Nos capítulos dos resultados e discussão de resultados foi mostrado todo o processo de replicação de uma máquina para Azure, passo a passo, incluindo depois uma prova de conceito, onde é realizado um teste de uma falha planeada no controlador de domínio e depois é simulada uma falha de DC para demonstrar como funciona, não só o planeamento todo de um processo de uma solução destas, mas como pode ser recuperado um controlador de domínio, após falha via Azure.

Em suma Cloud Computing é o fornecimento de serviços informáticos, incluindo armazenamento, bases de dados, rede, software, servidores, análises e inteligência, através da Internet da internet (‘Cloud’), para disponibilizar mais rapidamente recursos e poupanças no dimensionamento. Os serviços Cloud são entregues através de 3 modelos estandardizados: IaaS, SaaS e PaaS.

Cloud computing é mais do que aceder a ficheiros em múltiplos dispositivos. Graças a serviços de computação na nuvem, os utilizadores podem ver o seu e-mail em qualquer computador e ainda guardar ficheiros usando serviços como o DropBox ou o Google Drive. Permite aos utilizadores que façam backup das suas músicas, ficheiros, e fotos e estes estejam disponíveis na eventual falha de um disco rígido.

Oferece também ás grandes empresas uma enorme redução de custos. Antes da nuvem se tornar uma alternativa viável, as empresas precisavam de comprar, construir e manter infraestruturas e pessoal para a gerir. As empresas podem agora trocar infraestruturas e departamentos de pessoal para as gerir por ligações de internet mais rápida, onde os empregados interagem com a Cloud online para completar as suas tarefas.

A estrutura da nuvem permite também aos utilizadores salvar espaço no seu computador. Permite que as empresas de software possam passar a disponibilizar os seus produtos via Web e não por métodos tradicionais, como DVDs e ou PEN drives.

Quanto às vantagens de Cloud Computing: o software baseado na Cloud oferece às empresas de todos os setores uma série de benefícios incluindo a habilidade de usar software de qualquer dispositivo via uma aplicação nativa ou um explorador da internet, como resultado os utilizadores podem levar os seus ficheiros e definições para outros dispositivos de uma maneira perfeita.

No que diz respeito às desvantagens de Cloud Computing: a segurança sempre foi uma das maiores preocupações com a nuvem, especialmente no que toca a registos médicos sensíveis e

informação financeira. Os regulamentos forçam os serviços de computação na nuvem para reforçar as medidas de segurança e conformidade, mas este continua sendo um problema contínuo. A encriptação protege informação vital, mas se a chave de encriptação for perdida, os dados desaparecem.

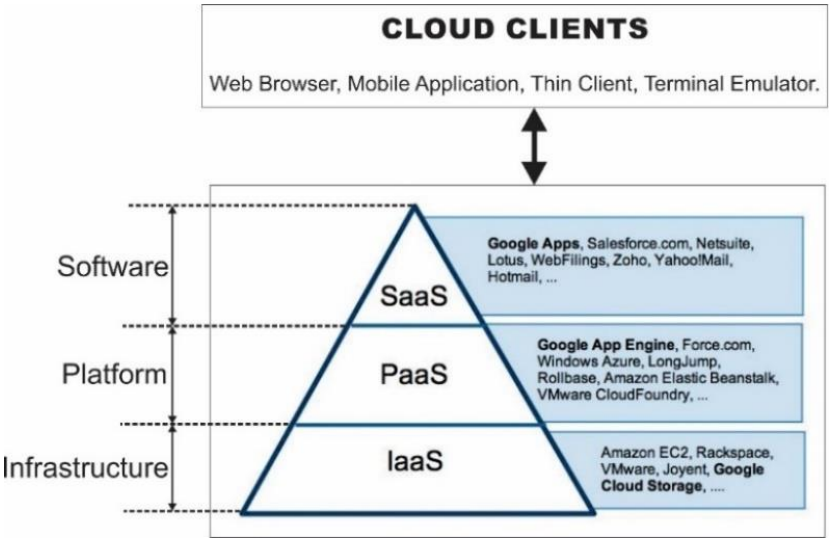

Figura 1- Comparação entre os Diferentes Modelos de Cloud (Sheenobi, 2018, p.1.)

IaaS – A primeira camada está relacionada com hardware, os produtos aqui estão associados a serviços como processamento, servidores, dispositivos de armazenamento e gestão de bases de dados e todos os outros serviços relacionados com hardware que são oferecidos ao utilizador final.

PaaS – A segunda camada é aquela onde os programadores podem construir e testar as suas aplicações que correm no IaaS, ou na camada acima SaaS.

SaaS – A última camada está relacionada exclusivamente com as aplicações para o utilizador final.

Existem 3 tipos de computação na Cloud: Private Clouds, Community Clouds e Public Clouds ou Hybrid Clouds.

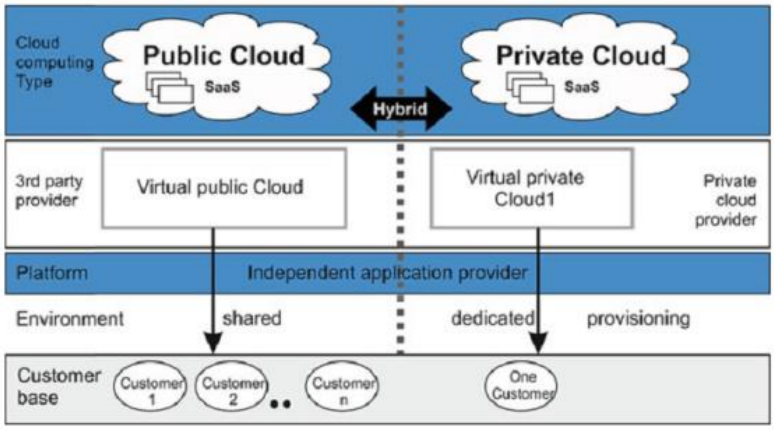

Figura 2 - Diferenças entre os vários tipos de Cloud Disponíveis (Boshlee, 2020, p.1.

Private Cloud – É uma infraestrutura aprovisionada para uso exclusivo de uma pessoa ou uma organização que tenha múltiplos utilizadores.

Community Cloud – Aprovisionado exclusivamente para ser usado por uma comunidade de consumidores de organizações que partilham as mesmas preocupações.

Public Cloud - São as Clouds usadas pelo público em geral.

Hybrid Cloud –As Cloud's híbridas são infraestruturas que combinam os dois tipos de Cloud e estão vinculadas através de uma tecnologia que permite que os dados e as aplicações sejam partilhadas entre elas.

Os servidores mantidos pelas companhias de computação na nuvem podem ser vítimas de desastres naturais, falhas internas e falhas de energia. O alcance geográfico da computação na nuvem pode ter dois lados: um apagão na Califórnia, pode parar utilizadores noutro canto do mundo e uma empresa em Lisboa pode perder os seus dados se houvesse um colapso no seu fornecedor principal.

Assim como na tecnologia, existe uma curva de aprendizagem para ambos os empregados e gestores, mas com muitos utilizadores acedendo e manipulando informação através de um único portal, erros inadvertidos podem acontecer e ser transferidos através de um sistema inteiro.

Como vimos acima, a computação em nuvem ou Cloud Computing pode ser implementando de várias maneiras. Alguns utilizadores todos os dados e aplicações na Cloud, enquanto outros optam por um modelo híbrido mantendo as aplicações e dados em servidores privados e os restantes na nuvem.

As maiores empresas no ramo empresarial de computação em nuvem incluem:

•Google Cloud

•Amazon Web Services (AWS)

•Microsoft Azure

•IBM Cloud

•Aliyun

Amazon Web Services é 100 por cento público e incluem um modelo de pagamento consoante os serviços subscritos. O microsoft Azure permite aos clientes manter alguns dados nos seus sites enquanto que a Aliyun é uma subsidiária do grupo Alibaba.

Microsoft Azure é uma plataforma que foi lançada pela Microsoft em Fevereiro de 2010 com o nome de Windows Azure e assumiu o nome de Microsoft Azure em 2014. É destinada a disponibilizar um conjunto de serviços Cloud onde é permitida a liberdade para criar, gerir e implementar aplicações numa rede global.

O Microsoft Azure nasceu em meados do ano 2000 como uma iniciativa interna com o nome de Código Project Red-Dog, nesta altura a Microsoft tentava apanhar a Amazon que já tinha lançado o seu serviço de Cloud Computing. Dois anos depois da Amazon ter lançado a AWS como um simples Sistema de armazenamento, a Microsoft anuncia que vai lançar o seu próprio serviço de Cloud Computing Service chamado de Windows Azure.

O plano da Microsoft era oferecer cinco categorias chave de serviços na nuvem: Windows Azure para computação (Virtualização de Máquinas), Armazenamento e Rede, Serviços para Bases de Dados SQL, Serviços .NET para programadores; Serviços Live para partilha de ficheiros e Serviços Sharepoint e Microsoft Dynamics CRM para ofertas SaaS.

A Microsoft começou a lançar versões dos seus serviços Cloud e em Fevereiro de 2010, a plataforma Azure ficou disponível comercialmente. As primeiras críticas a esta plataforma eram mistas, com muitos dos analistas a dar preferência a AWS. Contudo a Microsoft tem vindo a desenvolver e a melhorar o Azure, adicionando suporte a várias linguagens de programação, *frameworks* e sistemas operativos, incluindo Linux. Em abril de 2014 Windows Azure passou a ser chamado de Microsoft Azure.

A Microsoft continuou a expandir as suas capacidades na nuvem, aumentou o suporte para software open-source e aos dias de hoje tornou-se uma solução para empresas que não possuem servidores físicos. O Azure é uma plataforma de computação em nuvem, que oferece uma gama completa de serviços para empresas de todos os tamanhos. Estes serviços podem ser utilizados

para apoiar uma variedade de objetivos empresariais, ajudando as empresas a serem mais eficientes, produtivas e competitivas.

Pode ajudar no negócio de várias maneiras, dependendo dos objetivos específicos. Por exemplo, se o negócio está a desenvolver uma nova aplicação, o Azure pode fornecer a infraestrutura e as ferramentas necessárias para o fazer, permitindo que os engenheiros se concentrem na criação de aplicações inovadoras. Recolher dados para melhorar a sua compreensão dos clientes, o Azure pode fornecer-lhe as ferramentas necessárias para analisar esses dados, permitindo-lhe tomar decisões mais informadas.

O Azure funciona em dois modelos: Pré-pago e Pós-pago. No modelo pré-pago apenas se paga os os serviços que precisamos baseados na necessidade e na capacidade de investimento na altura. No Modelo Pós-pago, torna-se possível pedir mais recursos consoante a necessidade. O Microsoft Azure disponibiliza alguns dos seguintes serviços:

- Máquinas Virtuais – Torna-se possível no Azure fornecer máquinas virtuais que funcionam como computadores completos. É possível para uma empresa adquirir quantas máquinas forem necessárias para gerir o negócio com a flexibilidade de configuração e ferramentas especificas para cada caso
- Gestão de Rede – É possível gerir a rede interna dentro do próprio painel de controlo incluído no Azure, é possível monitorizar, diagnosticar e obter informações sobre o desempenho e integridade do sistema
- Armazenamento e Backup – O Backup dos dados na nuvem permite que toda a informação crítica seja recuperada em minutos e não haja prejuízos para a empresa
- Aplicações na Nuvem – Além da possibilidade de o Azure simular um computador inteiro na nuvem, torna-se também possível usar como uma plataforma de software virtualizado
- Containers – Tratam-se de pacotes de Código e ferramentas isoladas do Sistema em que estão funcionando, são umas das soluções mais populares do Mercado para dar portabilidade e flexibilidade ao desenvolvimento de produtos digitais. Para empresas que trabalham com SaaS, existe a vantagem de permitir testes em várias plataformas distintas e facilitar o trabalho aos programadores.
- Databases – Disponibiliza um dos melhores serviços de bases de dados do Mercado, é uma Plataforma inteligente e altamente compatível que permite migrar bases de dados sem alterar aplicações

- Análise de dados com IA e Machine Learning – O azure oferece recursos de Inteligência Artificial para uma análise de dados muito mais complexa que os relatórios normais
- Internet of Things – Através de um Hub fornecido pelo Azure são conectados e geridos os dispositivos num único sistema de gestão na nuvem.
- Streaming – Disponibiliza streaming de vídeos simplificados através de uma ferramenta nativa, com grande qualidade para maior contacto com o público ou para comunicação interna.

Usar o Microsoft Azure não é só uma questão de economia em recursos tecnológicos, pode inclusive trazer vantagens na parte da Administração, Operação e Otimização:

- Processos Ágeis – Um sistema integrado e centralizado na Cloud torna os processos do dia a dia mais ágeis e automatiza algumas tarefas, o que economiza o tempo dos funcionários.
- Apoios a novas estratégias – A recolha e análise de dados é um fator de motivação na procura de novas maneiras para reformular processo, conquistar novos sectores e aumentar a qualidade de entrega ao cliente. São dados confiáveis e mais detalhados para decisões com menos riscos e mais retorno
- Segurança – Sendo o Azure produto de uma das empresas de tecnologia do mundo o torna mais confiável, o suporte é ágil e eficiente e qualquer tipo de ameaça pode ser combatida a curto prazo sem se ter de preocupar com atualizações de hardware ou patches de segurança.
- Estratégia na TI – Ajudar as TI a se tornar parte fundamental das novas estratégias para negócio. O foco da transformação digital é precisamente trazer a tecnologia para o centro da discussão e encontrar novas maneiras de encantar e conquistar o público.

Ao longo do tempo também foram apontadas algumas desvantagens do Azure:

- Segurança e Disponibilidade – Este é sempre um fator a ter conta quando se subscreve a este tipo de serviços na nuvem. A maior parte das violações de segurança serem causadas por erro humano, no entanto é preciso ter em conta que os sistemas nas instalações de uma organização podem nem sempre trabalhar na perfeição e esta pode não ter os membros necessários na sua equipa de TI. Do lado da Nuvem a segurança e a gestão estão nas mãos dos especialistas
- Possibilidade do Fornecedor de Serviços entrar em Falência – Existe sempre a possibilidade de uma empresa que seja fornecedora deste tipo de serviços falir, quando se

avalia os fornecedores deve-se ter em conta como se poderá obter os dados de volta em caso de descontinuação da utilização de um serviço

- Necessidade de Internet mais fiável – Para se poder usufruir das ferramentas na nuvem é necessário um internet mais fiável e maioríssimo largura de banda.

O Windows Server 2016 é um Sistema Operativo para Servidores desenvolvido pela Microsoft como parte da família de sistemas do Windows NT, foi desenvolvido juntamente com o Windows 10 e é o Sucessor do Windows server 2012 R2. Algumas das funções que este disponibiliza são:

- Serviços de Certificados do Active Directory (AD)
- Active Directory Domain Services (AD): Serviços de controle de domínio do AD
- Serviços de Federação do Active Directory Federação (ADFS)
- Active Directory Lightweight Directory Services (ADLDS)
- Active Directory Rights Management Services (ADRMS)
- Atestado de integridade do dispositivo (Device Health Attestation Service)
- Servidor DHCP (DHCP)
- Servidor Domain Name Server (DNS)
- Serviços de Arquivo e Armazenamento de Serviços (File And Storage Service)
- Serviço Guardião de Host(Host Guardian Service Role)
- Hyper-V (virtualização de máquinas virtuais)
- Serviços de impressão e documentos
- Acesso remoto
- Serviços de Área de Trabalho Remota
- Serviços de ativação de volume
- Servidor Web IIS
- Experiência do Windows Server Essentials (Server Essentials Role)
- Windows Server Update Services (WSUS)

O Windows Server 2016 disponibiliza as seguintes edições:

- Windows Server 2016 Nano Server
- Windows Server 2016 Datacenter
- Windows Server 2016 Standard
- Windows Server 2016 Essentials.

Service/role	Datacenter	Standard	Essentials
Active Directory Certificate Services	●	●	■[1]
Active Directory Domain Services	●	●	■[2]
Active Directory Federation Services	●	●	●
Active Directory Lightweight Directory Services	●	●	●
Active Directory Rights Management Service[6]	●	●	●
Device Health Attestation	●	●	
DHCP Server	●	●	●
Domain Name System (DNS) Server	●	●	■
Fax Server	●	●	●
File Services	●	●	■[3]
Host Guardian Service	●	●	
Hyper-V	●	●	●
Network Controller	●		

Figura 3 - Edição do Windows Server 2016 (Vandhossos, 2020, p.1).

Uma das *roles* mais importantes do Windows Server é o Active Directory. O Active Directory é um serviço de diretório que é usado em ambiente Windows. É distribuído por uma base de dados hierárquica, que partilha informação sobre a localização, segurança, gestão e organização de computadores e recursos de rede incluindo ficheiros, utilizadores, grupos, periféricos e equipamentos de rede.

Active Directory é um serviço de diretório exclusivo da Microsoft para ser usados em redes com Domino Windows. Fornece autenticação e funções de autorização assim como uma framework para os outros serviços. O Active Directory usa LDAP versões 2 e 3, a versão Microsoft do Kerberos e DNS. Domain Controllers e Global Catalogs

Controlador de Domínio é uma peça central do Active Directory. É um servidor que responde as autenticações de segurança dentro de um domínio de computadores e é responsável por permitir aos computadores o acesso a recursos do Domínio. Este servidor autentica utilizadores, armazena informação sobre as suas respetivas contas e impõe politicas de segurança dentro do domínio. Nos sistemas que não sejam Microsoft, os controladores de domínio podem ser estabelecidos via software como o Samba ou RedHat FreelPA.

Global Catalog é uma base de dados distribuída que é armazenada nos controladores de Domínio e é usada para uma pesquisa mais rápida. Fornece um catálogo pesquisável de todos os objetos em um ou mais domínios Active Directory.

Um Domínio é um conceito introduzido no Windows NT, em que o utilizador pode ter acesso a uma série de recursos com o uso único de uma combinação e senha.

Quando começamos a falar de Domínios é importante perceber a diferença entre uma Tree uma Forest, informação útil para quando se configura um controlador de domínio. Tree ou ávores é composto por domínios com o mesmo espaço de nome. Um pequeno exemplo abaixo:

desenvolvimento.microsoft.pt / comercial.microsoft.pt

Os domínios desenvolvimento e comercial são subdomínios do domínio microsoft.pt

Forest ou floresta é o topo da estrutura, trata-se de um conjunto de uma ou mais árvores (trees) que partilham uma configuração típica, GC (Global Catalog), estrutura lógica, configuração de diretório e um esquema de diretório.

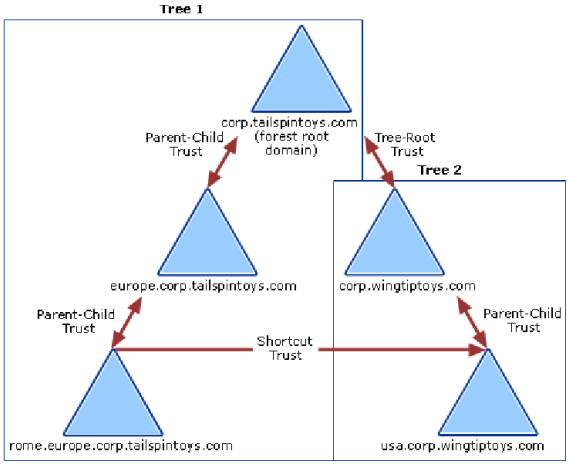

Figura 4 -Árvores e Florestas num Domínio (Hanapakova, 2015, p.2).

A replicação de Sites é um processo onde cópias dos dados do diretório são criados e mantidos em vários controladores de Domínio.

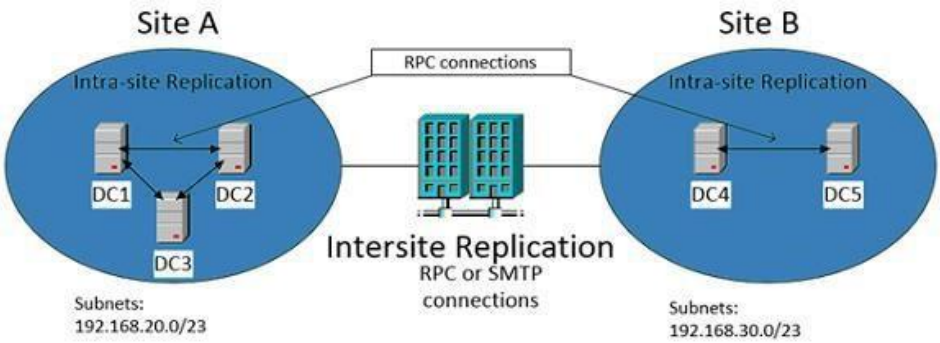

Figura 5 - Replicação Entre Sites (Sergayau, 2018, p.2).

Como funcionam estas operações? - Softwares chamados de Hypervisors separam os recursos físicos dos ambientes virtuais que precisam de recursos. Hypervisors podem ser utilizados em cima de um sistema operativo (ex: Portátil) ou instalado diretamente no hardware (ex: Servidor). Hipervisores utilizam os recursos físicos e vão repartir-los entre as máquinas virtuais, para as que as possam usar.

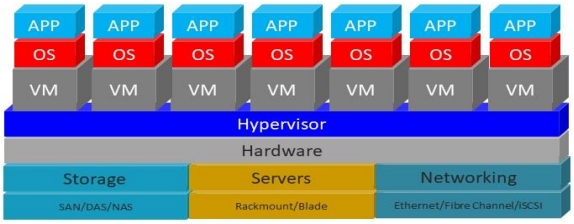

Figura 6 - Esquema de Funcionamento dos Hipervisores (Conan, 2016, p.2).

Recursos são particionados consoante o necessário a partir do ambiente físico para os diversos ambientes virtuais. Os utilizadores interagem e correm aplicações dentro do ambiente virtual (Tipicamente chamado Máquina Virtual). A máquina virtual funciona como um único ficheiro de dados que pode ser movido de um computador para o outro e funcionar da mesma maneira.

Quando o ambiente virtual está a correr e o utilizador ou um programa requerem recursos adicionais do ambiente físico, o hipervisor comunica com o sistema físicos e armazena em cache as definições. Os dados que estão espalhados em vários sítios podem ser consolidados numa única fonte. A virtualização de dados permite as empresas tratarem dados como um fornecimento dinâmico, fornecendo capacidades de processamento que podem trazer dados de várias fontes, acomodando novas fontes de dados e transformação de dados de acordo com as necessidades do utilizador. As ferramentas de virtualização de dados ficam na frente de várias fontes de dados e permitem que elas sejam tratadas como fonte única, fornecendo os dados necessários no momento certo para qualquer aplicação ou utilizador.

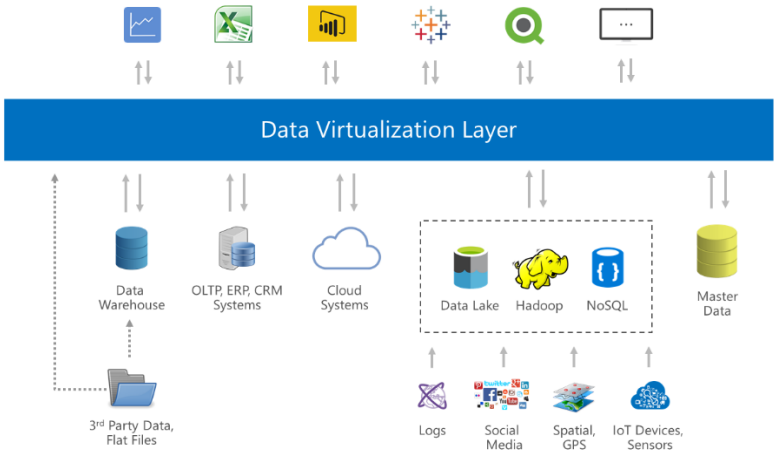

Figura 7 - Virtualização de Dados (Fotemi, 2014, p.3).

Servidores são computadores concebidos para processar volumes altos de tarefas especificas para que outros computadores possam realizar as outras tarefas. Virtualizar um servidor permite que ele execute mais dessas funções especificas e envolve particioná-lo para que os componentes possam servir múltiplas funções.

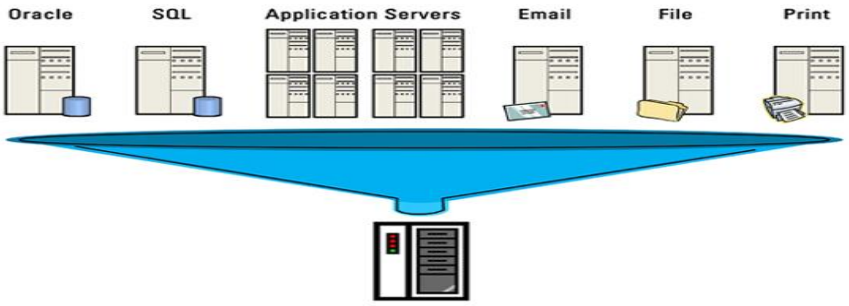

Figura 8 -Virtualização de Servidores (Torbart, 2020, p.3).

A virtualização de sistemas operativos ocorre no Kernel (o gestor de tarefas centrais dos sistemas operativos). É uma maneira útil de correr Windows e Linux lado a lado. Empresas podem também carregar sistemas virtuais para computadores, o que pode:

- Reduzir em massa custos de hardware, uma vez que os computadores não requerem grandes recursos para o uso
- Aumenta a segurança visto que todas as instâncias virtuais podem ser monitorizadas e isoladas
- Reduz o tempo perdido em serviços de IT, como update de software

A virtualização de funções de rede, separa as funções chaves de uma rede (como serviços de diretório, partilha de ficheiros, e configuração de IP), para que possam ser distribuídas por vários ambientes. Uma vez que as funções de software são independentes das máquinas físicas onde vivem, funções específicas podem ser empacotadas numa nova rede e atribuídas a um ambiente. A virtualização de redes reduz o acesso de equipamentos físicos como switchs, routers, cabos e *hubs* que são necessários para criar várias redes independentes e são particularmente populares no sector das telecomunicações.

Antes dos hipervisores, muitos dos computadores apenas podiam correr um sistema operativo de cada vez, isto fazia com que fossem estáveis uma vez que o hardware apenas lidava com solicitações de um sistema operativo. A desvantagem e que esta abordagem desperdiçava recursos uma vez que o sistema operativo não podia usar todos os recursos do computador.

Um Hipervisor resolve o problema. Trata-se de um pequeno software que permite correr múltiplos sistemas operativos lado a lado, partilhando os mesmos recursos físicos do computador. Estes sistemas operativos veem como máquinas virtuais, ficheiros que simulam um computador completo em software.

O hipervisor é também conhecido como gestor de máquinas virtuais, gere estas máquinas assim que vão correndo lado a lado. Separa as máquinas virtuais da camada lógica, assignando a cada uma parte dos recursos físicos do computador. Isto previne que as máquinas virtuais interfiram umas com as outras, se por exemplo alguma das máquinas falhar as outras não comprometidas.

Um hipervisor do tipo 1 corre diretamente sobre o hardware físico do computador, interagindo diretamente com o CPU, memória, e armazenamento físico. Por esta razão estes hipervisors são também conhecidos como bare-metal Hipervisores. Um Hipervisor toma o lugar do sistema operativo.

- Prós: São altamente eficientes porque têm acesso direto ao hardware físico. Isto aumenta também a segurança, isto porque não há nada entre a maquina virtual e o CPU que possa estar comprometido em caso de ataque
- Cons: Normalmente precisa de uma máquina separada para administrar e gerir as máquinas virtuais e controlar o hardware físico.

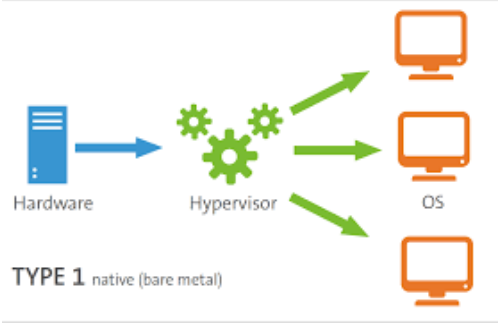

Figura 9 - Hipervisor Tipo 1 (Hommer, 2016, p.3).

Hyper-V é o produto de virtualização da Microsoft que nasceu em 2005 com o nome de Virtual Server 2005. Em 4 de Fevereiro de 2008 foi lançado o Windows Server 2008 e com ele introduzido o Hyper-V. Permite criar e correr uma máquina virtual. Uma máquina virtual atua como um computador completo, correndo um sistema operativo e programas. Quando são necessários recursos, as máquinas virtuais dão maior flexibilidade, ajuda a poupar tempo e dinheiro e tornam-se numa maneira mais eficiente de usar o hardware em vez de correr apenas um sistema operativo. Cada máquina corre no seu espaço isolado, o que na prática quer dizer que o utilizador pode correr mais que uma máquina virtual ao mesmo tempo.

A KVM é uma tecnologia de virtualização *open source* baseada em Linux. Isto quer dizer que o Linux pode ser transformado em um hipervisor, permitindo que uma máquina corra vários ambientes virtuais isolados, os quais são chamados de Máquinas Virtuais. O KVM foi anunciado pela primeira vez em 2006 e um ano depois foi inserida à versão Kernel do Linux da linha principal, isto foi feito com o intuito de tornar o KVM parte do código atual de Linux para que aproveitasse todos os recursos, correções e avanços do novo Linux.

Um hipervisor do tipo 2 não corre diretamente em cima do *hardware*. Em vez disso corre numa aplicação dentro de um Sistema Operativo. Hipervisors do tipo 2 raramente aparecem em servidores, sendo mais usados para utilizadores individuais que têm necessidade de correr múltiplos sistemas operativos (Ex: Engenheiros, profissionais de segurança que analisam malware e utilizadores que precisam de acesso a aplicações que apenas estão disponíveis noutras plataformas).

Tradicionalmente oferecem ferramentas para instalar no sistema operativo virtualizado. Estas ferramentas oferecem melhorias nas conexões entre a máquina virtual e o sistema operativo

físico, permitindo ao utilizador que copie ficheiros entre o sistema operativo fisico e a máquina virtual.

- Prós: Ativa o acesso fácil e rápido a um sistema operativo alternativo lado a lado com o sistema operativo principal.
- Cons: O hypervisor tipo 2 precisa de aceder aos recursos físicos do computador através do sistema operativo que tem o acesso primário aos componentes. Isto introduz alguma latência, afetando a performance, isto introduz também riscos potenciais de segurança uma vez que se o sistema operativo principal for comprometido, as máquinas virtuais podem ser comprometidas.

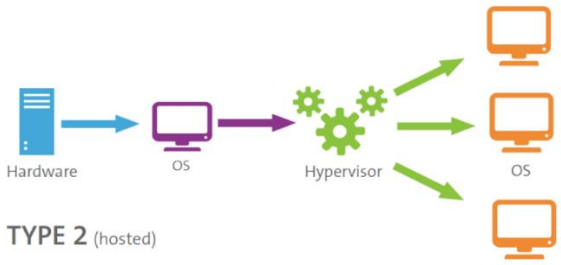

Figura 10 - Hipervisor Tipo 2 (Hommer, 2016, p.3).

A Vmware Workstation é um hipervisor que é executado em versões x64 dos sistemas operativos Windows e Linux (anteriormente existiam versões para sistemas x86). Permite que sejam criadas várias máquinas virtuais que podem correr seus próprios sistemas operacionais. Esta operação ocorre aquando da sua execução sobre o sistema operativo principal.

A Virtualbox é outro exemplo de um hipervisor tipo 2, é um hipervisor em código aberto livre para virtualização de sistemas x86, desenvolvido pela Oracle e Adquirido pela Sun MicroSystems em 2008, que voltou a ser adquirido pela Oracle em 2010. O Virtualbox pode ser instalado em Windows, MacOS, Linux, Solaris, OpenSolaris e também pode ser instalado em FreeBSD e Genode. Suporta a criação e gestão de máquinas virtuais que corram Windows, BSD, OS/2, Solaris, Haiku e Osx86 e também versões limitadas de sistemas operativos Apple.

Materiais e Métodos de Desenvolvimento

O artefacto digital produzido apresentou uma situação real de recuperação de desastres, num ambiente de Cloud Computing. Para isso, foi seguida uma metodologia de investigação de cariz qualitativo, quanto aos objetivos exploratória e descritiva e no que diz respeito aos procedimentos foi escolhida a pesquisa de estudo de caso, A investigação qualitativa é um tipo de investigação, compreensão de significados, crenças, valores e experiências.

Uma estratégia de investigação qualitativa que se concentra na análise aprofundada de um caso ou unidade singular. O caso pode ser uma pessoa um evento ou um fenómeno

Os laboratórios de investigação são espaços onde se realizam investigações científicas. A investigação qualitativa pode ser utilizada em laboratórios para compreender melhor os fenómenos que estão a ser estudados.

No início da proposta deste projeto, foram estabelecidos os seguintes objetivos para a proteção dos dados em uma infraestrutura de pequena ou grande dimensão:

- Simplicidade: a solução deve ser fácil de implementar e de usar.
- Inovação: a solução deve ser diferente das soluções existentes, oferecendo novas funcionalidades ou melhorias significativas.
- Objetividade: a solução deve ser baseada em princípios sólidos e deve ser eficaz na proteção dos dados.
- Funcionalidade: a solução deve atender às necessidades específicas da infraestrutura.
- Atratividade: a solução deve ser atraente para os utilizadores e deve motivá-los a utilizá-la.

Para atingir estes objetivos, foram realizadas várias etapas minuciosas, incluindo:

Análise de literatura existente: foram analisados livros, artigos e websites oficiais sobre disaster recovery.

Realização de experiências: Foram realizados testes para avaliar diferentes soluções e tecnologias.

Consulta de vídeos e documentos relevantes: Foram consultados vídeos e documentos que continham informações relevantes para o projeto.

Estas etapas foram cruciais para a inspiração e para a definição das escolhas que foram feitas. Elas permitiram compreender os desafios envolvidos na proteção de dados e identificar as soluções mais adequadas para o caso.

Em resumo, as etapas que foram realizadas foram essenciais para o sucesso do projeto. Elas permitiram desenvolver uma solução eficaz, simples, inovadora, objetiva, funcional e atraente para a proteção dos dados, são apresentados alguns exemplos específicos de como as etapas que foram realizadas contribuíram para o sucesso do projeto:

A análise de literatura existente permitiu identificar as principais ameaças aos dados e as melhores práticas para a sua proteção a realização de experiências diferentes soluções e tecnologias e selecionar as que melhor se adequavam às necessidades, consulta de vídeos e documentos relevantes permitiu obter informações sobre soluções e tecnologias que não eram conhecidas.

Estas etapas permitiram desenvolver uma solução que é eficaz na proteção dos dados e que atende às necessidades específicas. Foi possível realizar, desta forma, pesquisas exploratórias porque são importantes para o desenvolvimento do conhecimento, pois possibilitam a exploração de novos tópicos ou problemas, que obtenham uma compreensão mais profunda do assunto e que possam gerar novas ideias. As pesquisas exploratórias foram importantes para o desenvolvimento de uma solução eficaz, simples, inovadora, objetiva, funcional e atraente para a proteção de dados.

Foi também criado um cronograma da investigação e com datas definidas para as atividades.

Tabela 1- Cronograma da criação do artefacto digital e etapas da investigação (Moreira, 2023, p.4).

Datas	**Atividades/ Trabalhos a desenvolver**
Outubro 2022 - Março 2023	Apresentação e aceitação do tema. Desenvolvimento do pré-projeto. Desenvolvimento e apresentação do Pitch.
Março 2023 – Setembro 2023	Entrega do trabalho final: parte prática e parte teórica baseada no anexo do Projeto Académico.

No diagrama seguinte (Figura 11) explicado de seguida é possível ter uma noção de como tudo funcionou.

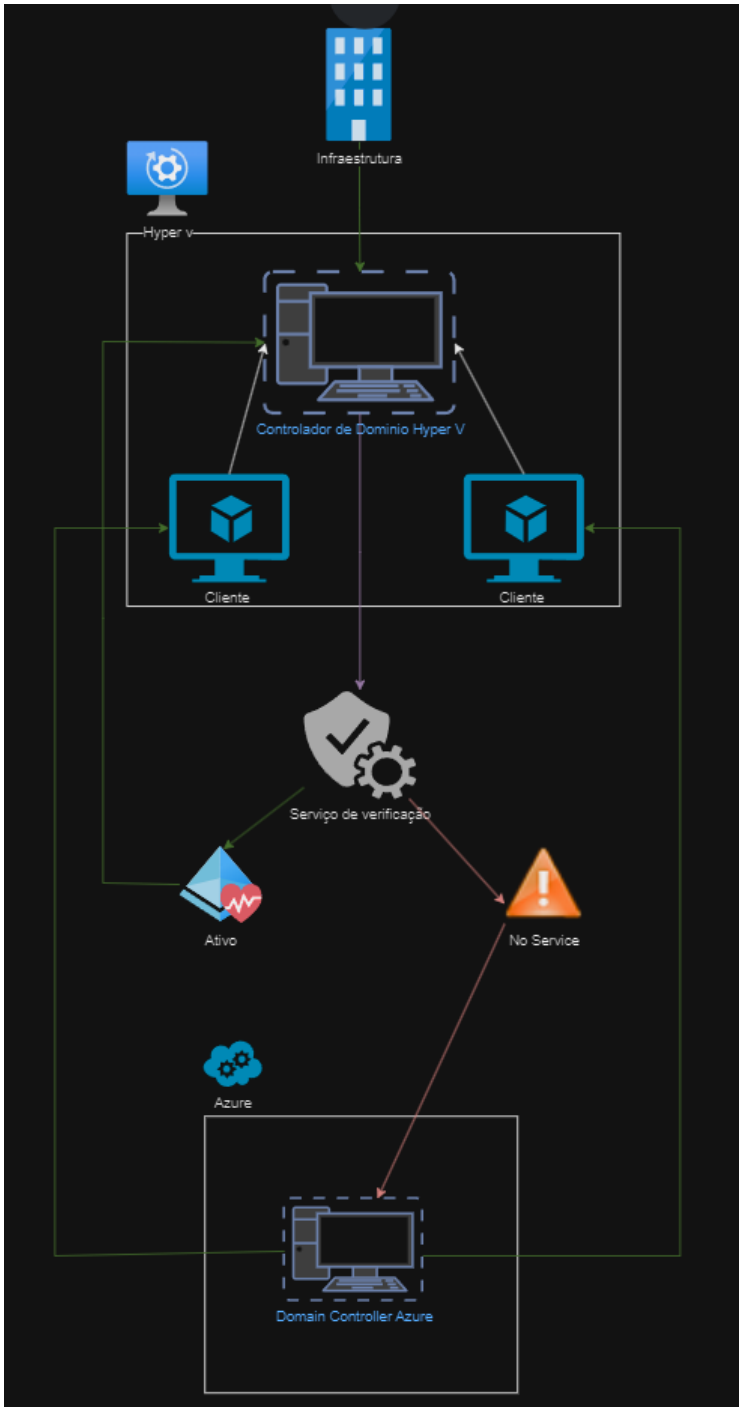

Figura 11 - Diagrama infraestrutura (Moreira, 2023, p.4).

No diagrama (Figura 11) podemos ver uma infraestrutura de rede composta por dois domínios: um domínio local (on-premises) e um domínio na nuvem (Azure). O domínio local

consiste em um servidor Hyper-V, que é responsável por executar os serviços de virtualização, e dois clientes, que são os computadores que acedem aos serviços do domínio. O servidor Hyper-V é um software que permite a criação de máquinas virtuais, que são computadores que funcionam dentro de um computador físico. As máquinas virtuais são uma forma eficiente de usar os recursos de um computador físico, pois permitem que vários sistemas operacionais sejam executados simultaneamente.

Os dois clientes são computadores que acedem aos serviços do domínio local. Esses serviços podem incluir, por exemplo, serviços de impressão, serviços de arquivos e serviços de rede. O domínio na nuvem consiste em um controlador de domínio do Azure, que é responsável por gerenciar os utilizadores e computadores do domínio. O controlador de domínio do Azure é um serviço fornecido pela Microsoft que permite a criação de um domínio na nuvem. Os domínios na nuvem oferecem uma variedade de vantagens, incluindo escalabilidade, disponibilidade e segurança.

Os dois domínios estão conectados por uma rede VPN. A VPN permite que os computadores dos dois domínios se comuniquem de forma segura. O diagrama também mostra que o serviço de verificação está ativo no domínio local. O serviço de verificação é responsável por monitorar a infraestrutura de rede e alertar os administradores sobre possíveis problemas.

O serviço de verificação é uma ferramenta importante para garantir a disponibilidade e a segurança da infraestrutura de rede.

Para chegar a essas conclusões, utilizei uma combinação de métodos, incluindo:

- Observação: observei o diagrama cuidadosamente e tentei entender como os diferentes componentes estão conectados.
- Levantamento de requisitos: tentei identificar os requisitos da infraestrutura de rede, como o que ela deve fazer e como ela deve funcionar.
- Fatores indispensáveis: considerei fatores indispensáveis para uma infraestrutura de rede segura e confiável, como o uso de criptografia e o monitoramento da rede.

O diagrama (Figura 11) mostra uma infraestrutura de rede composta por componentes e tecnologias modernos e eficazes. O uso de um domínio na nuvem, uma VPN e um serviço de verificação ajuda a garantir a disponibilidade, a segurança e a confiabilidade da infraestrutura de rede.

No entanto, existem algumas questões que podem ser melhoradas, como a inclusão de informações sobre como os dados são armazenados e protegidos e como a infraestrutura de rede é gerenciada e monitorada. Essas questões devem ser consideradas para melhorar ainda mais a segurança e a confiabilidade da infraestrutura de rede.

Em termos de segurança e privacidade, foram reunidos os seguintes critérios éticos:

- Segurança: o software foi usado de forma segura, sem colocar em risco os dados ou a infraestrutura.
- Privacidade: os dados foram tratados de forma privada, sem serem divulgados a terceiros sem autorização.
- Especificamente, os seguintes procedimentos foram adotados para garantir a segurança e a privacidade dos dados:
- O software foi instalado em um ambiente seguro, protegido por firewalls e outros mecanismos de segurança.

Os dados foram criptografados antes de serem enviados para o software.

O acesso aos dados foi restrito a utilizadores autorizados.

Além disso, foram tomadas as seguintes medidas para garantir a privacidade dos dados:

Os dados foram anonimizados antes de serem enviados para o software.

Os resultados da análise foram divulgados de forma agregada, sem identificar indivíduos.

Estes procedimentos foram suficientes para garantir a segurança e a privacidade dos dados durante a análise do diagrama (Figura 11) apresentado anteriormente.

Resultados

A recuperação de desastres é um processo essencial para garantir a continuidade operacional de uma organização. Em caso de desastre, uma solução de recuperação de desastres eficaz pode ajudar a restaurar os sistemas e dados rapidamente, minimizando o impacto financeiro e operacional.

Os principais desafios da recuperação de desastres no Azure incluem:

Configuração de máquinas virtuais e alocação de redes e serviços: Este é um processo complexo que requer atenção aos detalhes e uma compreensão da otimização de recursos.

É importante garantir recursos suficientes para evitar perda de dados e interrupções de comunicação: Isso exige uma estimativa precisa dos requisitos e da disponibilidade de recursos.

A busca por um serviço de nuvem seguro, confiável e econômico: Este é um processo que exige uma avaliação completa e uma tomada de decisão estratégica.

Oportunidades da recuperação de desastres no Azure oferece para implementar uma solução de recuperação de desastres eficaz, incluindo:

Uma variedade de serviços e recursos, que podem ser usados para implementar uma solução de recuperação de desastres, incluindo máquinas virtuais, redes, armazenamento, segurança, e serviços de backup e recuperação.

O Azure é uma plataforma confiável e segura, que oferece uma variedade de recursos para proteger os dados, sistemas e econômica, que pode ser dimensionada para atender às necessidades de uma organização.

A implementação da solução de recuperação de desastres foi um desafio, tive que enfrentar uma série de desafios, incluindo:

- A configuração de máquinas virtuais e a alocação de redes e serviços: Este foi um processo complexo que requeria atenção aos detalhes e uma compreensão da otimização de recursos.
- A necessidade de garantir recursos suficientes para evitar perda de dados e interrupções de comunicação: Isso exigiu uma estimativa precisa dos requisitos e da disponibilidade de recursos.

A busca por um serviço de nuvem seguro, confiável e econômico, este foi um processo que exigiu uma avaliação completa e uma tomada de decisão estratégica.

Ajustes e adaptações após a implementação inicial da solução de recuperação de desastres, fiz uma série de ajustes e adaptações para melhorar seu desempenho e confiabilidade.

Essas alterações incluíram:

- Otimização de recursos: Ajustei a alocação de recursos para garantir o desempenho ideal e mitigar o risco de escassez de recursos.
- Integração de serviços em nuvem: Revi a estratégia de integração para garantir a integração e interoperabilidade sem problemas.
- Contingências operacionais: Ajustei a solução para mitigar riscos e aprimorar a continuidade operacional.

A implementação da solução de recuperação de desastres no Azure foi um processo desafiador, mas recompensador. Ao enfrentar os desafios e aproveitar as oportunidades, pude desenvolver uma solução eficaz que ajudou a proteger os dados e sistemas críticos.

1. Criar a infraestrutura no Azure configurada On-Premises.

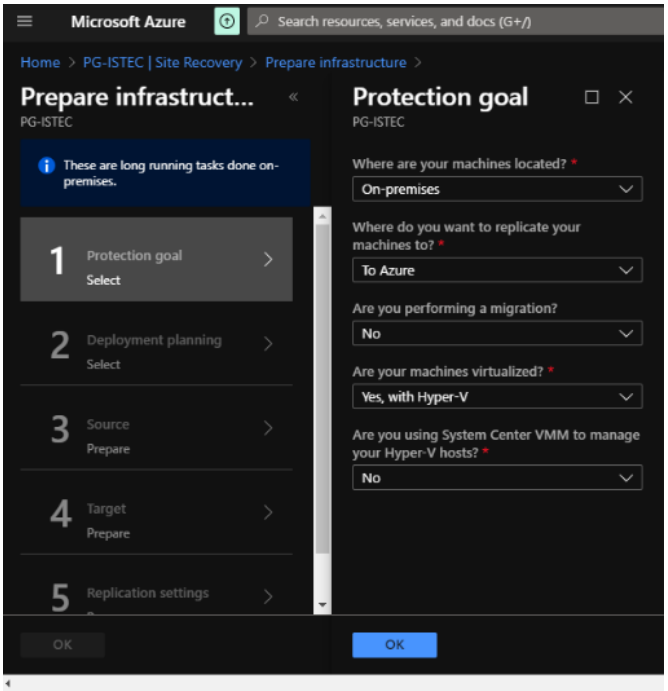

Figura 12 - Prepare Infrastructure (Moreira, 2023, p.5).

Na imagem estão várias opções, quando escolhi on-premises quer dizer que as nossas máquinas estão alojadas no servidor fisicamente e se pretendo fazer o backup para Azure.

2. Depois disso, é apresentado um ecrã com a seguinte pergunta: "Deseja descarregar um ficheiro Excel para planear a largura de banda, armazenamento e outros dados necessários para visualizar a melhor opção para proteger o seu controlador de domínio?".

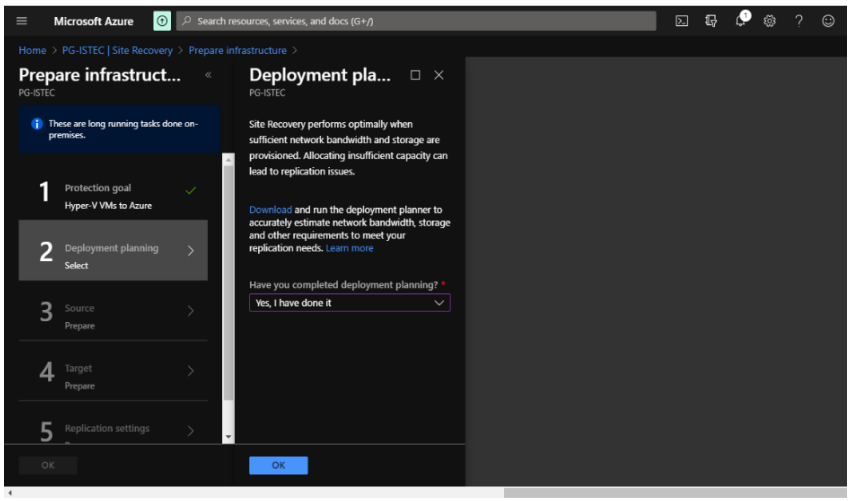

Figura 13 - Deployment (Moreira, 2023, p.5).

3. Após a preparação e o planeamento, é apresentado o seguinte ecrã para começar a preparar a integração da nossa máquina na Azure.

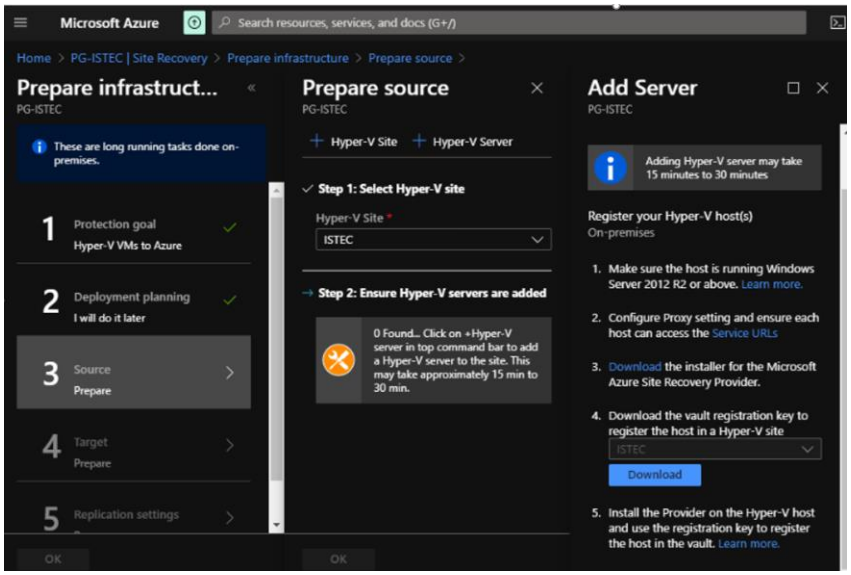

Figura 14 - Source (Moreira, 2023, p.5).

4. Create New e depois chegamos ao seguinte ecrã:

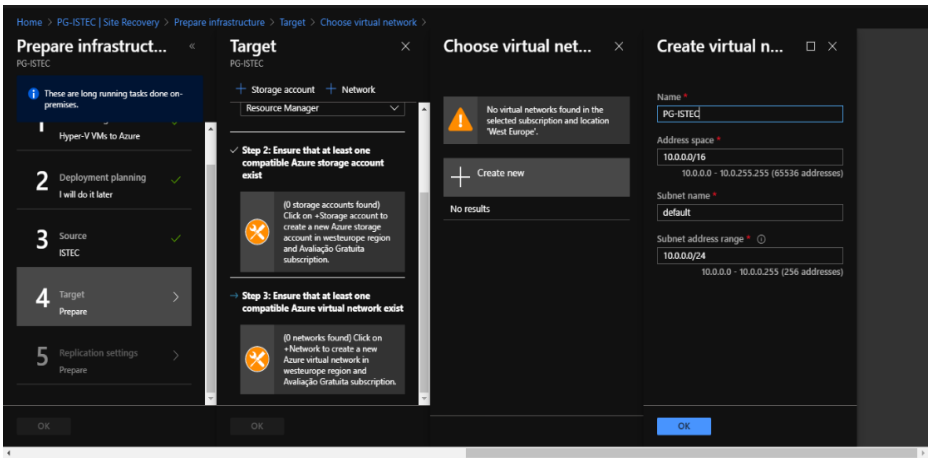

Figura 15 - Target (Moreira, 2023, p.6).

Neste passo é pedido o nome e a Subnet que estamos a usar na nossa máquina, e os dados da mesma para serem guardados na Azure. No nosso caso será:

Name: PG-ISTEC

Address Space: 192.168.1.0/24

Subnet Name: PG-CLUSTER1

Subnet Address Range: 192.168.1.0/24

5. Após a preparação da nossa Infraestrutura, podemos prosseguir com o nosso passo que será criar uma política de replicação, chegando a este ponto temos o seguinte ecrã:

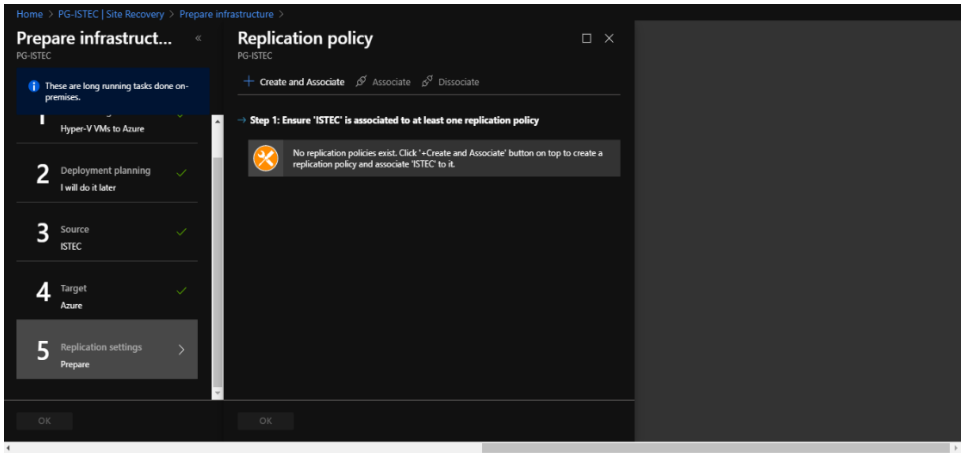

Figura 16 - Prepare (Moreira, 2023, p.6).

Clicamos no Create and Associate e é nos apresentada as seguintes opções:

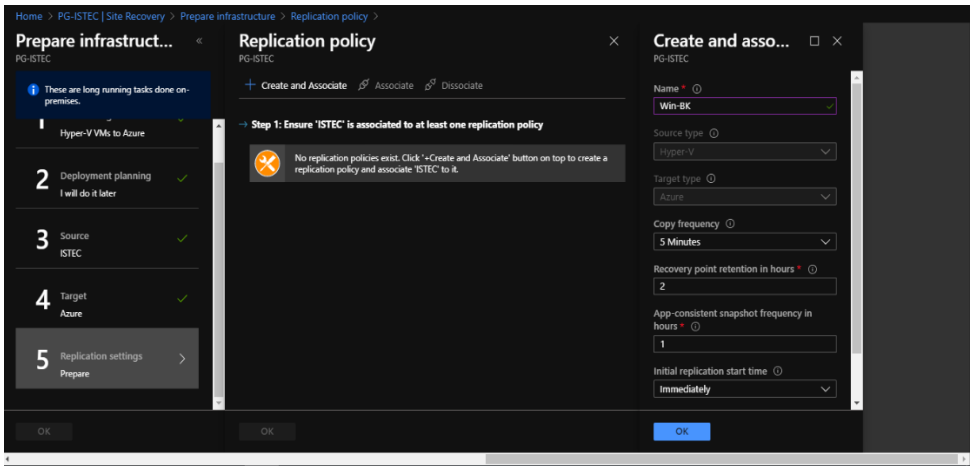

Figura 17 - Policy (Moreira, 2023, p.6).

Para a execução deste projeto foram criadas 2 máquinas virtuais. É composto por um Controlador de Domínio, um Cliente. Os recursos físicos usados para a implementação destes laboratórios foram um processador i3 7100 2.4Ghz, com um SSD de 512Gb, 20Gb de Memória RAM, com o sistema operativo Windows Server 2016 e Windows 10 Pro.

Para configuração do Hyper-V é necessário configurar o hypervisor de maneira a este poder estar preparado para a criação de todas as máquinas virtuais. Após instalação do Sistema Operativo deve-se por boa prática alterar sempre o nome da máquina. O nome da máquina pode ser alterado via PowerShell, para isso devem abrir o Powershell como administrador (botão direito do rato sobre o poweshell e clicar em Run as Administrator) e depois devem inserir o novo comando:

Rename-Computer -NewName PC1 -Restart

Após o reinício da máquina podemos efetuar a instalação novamente em powershell do hyper-v, para isso basta em seguida introduzirmos o seguinte comando:

Enable-WindowsOptionalFeature -Online -FeatureName Microsof-Hyper-V -All

Após a execução deste comando o Hyper-V é instalado com todos os seus extras, para confirmar basta clicar no iniciar e procurar o Hyper-V Manager.

Depois de ter a role de Hyper-V instalada, é necessário proceder a criação das máquinas virtuais. No gestor do Hyper-V, clicar Actions -> New -> Virtual Machine, adicionar um nome á maquina virtual (EX: DC1), escolher Geração 2, especificar a memória pretendida que neste caso vamos escolher 3096MB e deixar a opção de memória dinâmica ativa, deve-se ter conta que a memoria tambem deve ser alterada mediante o sistema que pretendemos instalar, no passo a seguir

devemos escolher o espaço de disco pretendido e por fim selecionar o ISO para poder iniciar a instalação do sistema na Máquina Virtual. De notar que é importante perceber a diferença entre escolher Geração 1 e Geração 2 afim de se perceber o motivo desta escolha.

Generation 1 – São máquinas que suportam a arquitetura legacy baseada em BIOS e são carregadas a partir do MBR dos discos virtuais. Uma BIOS com hardware virtual é emulada pelo Hyper-V

Generation 2 – Estas máquinas virtuais suportam UEFI que é similar a BIOS e que tem a vantagem de estender o suporte de dispositivos e recursos, alguns exemplos são o suporte a GPT que permite superar o limite de 2TB e Secure Boot que oferece proteção contra discos de arranque modificados.

Tabela 2 - Dados para Criação de Máquinas (Moreira, 2023, p.6).

VM's	SISTEMA OPERATIVO	RAM	DISCO	LIGAÇÃO DE REDE	IP'S
DC1	Windows Server 2016	3096	40GB	NET	10.0.0.1
SRV1	Windows Server 2016	3096	40GB	LAB1	192.168.1.58

Tabela 3 - Dados para Contas (Moreira, 2023, p8).

Contas	Acessos	
VM	USER	PASSWORD
DC1	Administrator	P@ssw0rd
Client	Administrator	P@ssw0rd

Tabela 4 - Chaves sistema operativo (Moreira, 2023, p8).

Sistema Operativo	Chave
Windows Server 2016	2NQGF-B8FM7-3YY3J-26BTF-F62G4
Windows Server 2016	2NQGF-B8FM7-3YY3J-26BTF-F62G4
Windows 10	
	7V9JN-WVMCF-YRGMK-JWJ2B-XBRXB

De destacar que o Windows Server Standard 2016 não é o aconselhável para esta solução que vamos montar, visto que se encontra limitado a nível de licenciamento a 2 máquinas virtuais, sendo que passará a uma máquina se o nosso *host* ou máquina física tiver um serviço de DNS ou DHCP configurado. Para soluções Azure on-premisse a Microsoft recomenda o uso da versão Datacenter do Server 2016.

Discussão de resultados

Os resultados obtidos foram positivos e demonstraram que a recuperação de sites através do Azure foi uma solução eficaz para garantir a continuidade operacional. O processo de recuperação foi rápido e eficiente, levando menos de 10 minutos para ativar um controlador de domínio replicado no Azure.

O processo de recuperação de sites através do Azure consistiu em duas etapas:

- Replicação do controlador de domínio para o Azure: Essa etapa é realizada usando o serviço Azure Site Recovery. A replicação pode ser feita de forma contínua ou incremental.
- Failover do controlador de domínio replicado: Essa etapa é realizada usando o serviço Azure Active Directory Domain Services.

O Azure é uma solução confiável para a recuperação de sites, oferece uma série de recursos que ajudam a proteger os dados e aplicativos críticos contra desastres.

Esses recursos incluem:

- Redundância e disponibilidade: O Azure oferece uma infraestrutura redundante e disponível para proteger os dados e aplicativos críticos contra falhas de hardware ou software.
- Segurança: O Azure oferece uma série de recursos de segurança para proteger os dados e aplicativos críticos contra ataques cibernéticos.
- Escalabilidade: O Azure pode ser facilmente escalado para atender às necessidades de qualquer organização.

A opção pela recuperação de sites através do Azure foi baseada nos seguintes fatores:

Eficácia: O resultado demonstrou que o processo de recuperação através do Azure é rápido e eficiente, levando menos de 15 minutos para ativar um controlador de domínio replicado no Azure.

- Confiabilidade: O Azure oferece uma série de recursos que ajudam a proteger os dados e aplicativos críticos contra desastres.
- Abrangência: O Azure oferece uma ampla gama de recursos que podem ser usados para proteger sites de diferentes tamanhos e complexidades.

- A recuperação de sites através do Azure é uma solução eficaz e confiável que pode ajudar as organizações a proteger seus dados e aplicativos críticos contra desastres.

O Azure é uma solução de recuperação de sites completa e abrangente que pode atender às necessidades de organizações de todos os tamanhos e complexidades.

Conclusão

A implementação de uma solução de virtualização deve ser estudada para cada cenário e avaliados os transtornos que possa ser gerado. Desta maneira, deve ser avaliado os custos e os recursos necessários como a largura de banda necessária e o armazenamento para o pretendido.

Com este trabalho pretendeu-se demonstrar um conceito que já está presente no mercado atualmente e continua a ser cada vez mais uma aposta das empresas, que é a virtualização das suas infraestruturas no Azure. Foi apresentado o processo que procurou replicar uma máquina virtual até à recuperação de um controlador de domínio em caso de falha, a este processo todo dá-se o nome de DRaaS, a isto acrescentou-se uma amostra de como se pode gerir uma Ative Directory a partir de uma página de internet. O Azure permite aos dias de hoje replicar toda a informação de um controlador de domínio para a nuvem e recuperar o mesmo em caso de desastre em pouco tempo, reduzindo assim a necessidade de haver um grande investimento em infraestruturas e dando mais cash-flow a uma empresa.

O projeto permitiu-me consolidar os meus conhecimentos na área e ampliar a pesquisa realizada sobre o mesmo. Para dar continuidade ao projeto, seria interessante aprofundar o desenvolvimento do tema e das suas mecânicas, avançando assim o meu conhecimento e aprendizagem para possíveis futuros projetos na área, que poderão beneficiar da pesquisa e desenvolvimento realizados no presente.

Referências Bibliográficas

Bose, M. (2018, August 15). *The Differences Between Hyper-V Generation 1 vs. 2 VMs*. Official NAKIVO Blog. https://www.nakivo.com/blog/hyper-v-generation-1-vs-2/

Computer Hope. (2019, March 9). *What is VirtualBox?* Computerhope.com. https://www.computerhope.com/jargon/v/virtualbox.htm

Conroy, S. (2018, January 25). *History of Virtualization*. I Don't Know, Read the Manual; I Don't Know, Read The Manual. https://www.idkrtm.com/history-of-virtualization/December 11, J. V. in N. on, 2017, & Pst, 5:09 A. (2017, December 11). *Windows Server 2016: A cheat sheet*. TechRepublic. https://www.techrepublic.com/article/windows-server-2016-the-smart-persons-guide/

Frankenfield, J. (2023, April 5). *Cloud Computing*. Investopedia. https://www.investopedia.com/terms/c/Cloud-computing.asp

IBM Cloud Education. (2019, May 8). *us-en_Cloud_learnhub_hypervisors_a_complete_guide*. Ibm.com. https://www.ibm.com/Cloud/learn/hypervisors

Microsoft. (2019). *What is ASP.NET? | .NET*. Microsoft. https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet

Oludele, A., C. Ogu, E., Shade, K., & Chinecherem, U. (2014). On the Evolution of Virtualization and Cloud Computing: A Review. *Journal of Computer Sciences and Applications*, *2*(3), 40–43. https://doi.org/10.12691/jcsa-2-3-1

Redhat. (2018, March 2). *What is virtualization?* Redhat.com. https://www.redhat.com/en/topics/virtualization/what-is-virtualization

What is VMware? - Definition from WhatIs.com. (2019). *What is VMware? - Definition from WhatIs.com*. SearchVMware. https://searchvmware.techtarget.com/definition/VMware