Publicação e Administração Web

Bruno Faria A20610

Luís Leandro A20615

Marco Oliveira A20608

Miguel Pinto A18606

IPCA, 21 junho 2021

Índice

[Índice de Abreviaturas 1](#_Toc75303414)

[Introdução 2](#_Toc75303415)

[Virtualização 3](#_Toc75303416)

[Vantagens da Virtualização de Servidores 3](#_Toc75303417)

[Oracle VM VirtualBox 4](#_Toc75303418)

[Vantagens do VirtualBox 4](#_Toc75303419)

[Máquinas Virtuais 5](#_Toc75303420)

[Criação de uma Máquina Virtual 5](#_Toc75303421)

[Instalação Windows Server 8](#_Toc75303422)

[Instalação Debian 12](#_Toc75303423)

[Windows Server 17](#_Toc75303424)

[Configuração do Windows Server 17](#_Toc75303425)

[Active Directory 19](#_Toc75303426)

[O que é? 19](#_Toc75303427)

[DNS 19](#_Toc75303428)

[DHCP 19](#_Toc75303429)

[IP 20](#_Toc75303430)

[Configuração do AD DS 21](#_Toc75303431)

[Domínio vs. Grupo de Trabalho 23](#_Toc75303432)

[Unidades Organizacionais e Utilizadores 25](#_Toc75303433)

[Políticas de Grupo (GPO) 27](#_Toc75303434)

[Criação de Grupos de Utilizadores 28](#_Toc75303435)

[Quotas de Armazenamento 29](#_Toc75303436)

[Quotas em Disco 29](#_Toc75303437)

[Quotas em Pasta 31](#_Toc75303438)

[Backup e Restauro Windows Server 34](#_Toc75303439)

[Backup Agendado 34](#_Toc75303440)

[IIS (Internet Information Services) 38](#_Toc75303441)

[DHCP 41](#_Toc75303442)

[Configuração do Servidor DHCP 41](#_Toc75303443)

[Políticas de Auditoria 46](#_Toc75303444)

[Permissões 49](#_Toc75303445)

[Permissões Explicitas e Herdadas 49](#_Toc75303446)

[Linux 50](#_Toc75303447)

[Debian 50](#_Toc75303448)

[SSH 51](#_Toc75303449)

[Configuração SSH 51](#_Toc75303450)

[Servidor Wordpress 54](#_Toc75303451)

[Configuração de Servidor Wordpress 54](#_Toc75303452)

[Servidor Email 57](#_Toc75303453)

[Configuração do Servidor Email 57](#_Toc75303454)

[Firewall 62](#_Toc75303455)

[Instalação da UFW 62](#_Toc75303456)

[Backup no Debian 64](#_Toc75303457)

# Índice de Abreviaturas

CLI – Command Line Interface

AD – Active Directory

DHCP – Dynamic Host Configuration Protocol

FTP – File Transfer Protocol

DNS – Domain Name System

VB – Oracle VM Virtual Box

ISO – Optical Disk Image

OS – Operating System

VM – Virtual Machine

AD DS – Active Directory Domain Services

IP – Internet Protocol

DC – Domain Controller

OU – Unidade Organizacional

GPO – Group Policy

IIS – Internet Information Services

SSH – Secure Shell

GUI – Graphical User Interface

# Introdução

No âmbito da disciplina de Publicação e Administração Web, foi-nos proposto elaborar este relatório com base em todos os conteúdos lecionados durante o semestre.

Inicialmente é abordada a criação de máquinas virtuais e a instalação e configuração de sistemas operativos nas mesmas, neste caso, o Windows Server, o Windows e o Debian.

Posteriormente é tratada a instalação e configuração do Active Directory, a criação e gestão de domínios, unidades organizacionais, políticas de grupo, grupos de utilizadores e utilizadores, o servidor de ficheiros, quotas em pasta e em disco e o backup e restauro.

Por último são referidos os servidores web, email e DHCP, a publicação de páginas web estáticas e dinâmicas, a administração de servidores, acesso por FTP, as Firewall e os clientes de email.

# Virtualização

Durante este semestre, trabalhamos com máquinas virtualizadas através do software da Oracle VirtualBox.

A virtualização cria um ambiente informático simulado, em vez de um ambiente físico. Isto permite às organizações a divisão de um único computador ou servidor físico em várias máquinas virtuais.

## Vantagens da Virtualização de Servidores

*1 – Gestão centralizada de recursos*

Uma vez que as máquinas virtuais criadas podem ser modificadas ou removidas rapidamente conforme é necessário, a virtualização permite que as empresas economizem tempo para realizar a sua manutenção.

*2 – Economia*

Através da virtualização, é possível reduzir diversos gastos, como o “cooling” e a eletricidade utilizada, assim como poupar no espaço físico utilizado na empresa.

*3 – Backups mais ágeis*

Como os dados dos dispositivos de armazenamento se encontram no mesmo lugar em que o sistema está localizado, as políticas de cópias de segurança da empresa podem ser executadas mais agilmente e com maior precisão.

*4 – Otimização da recuperação de desastres*

Uma vez que a virtualização fornece a capacidade de abstração do hardware, assim como a consolidação dos servidores e a redução de danos, torna-se possível criar rapidamente cópias dos servidores atuais em caso de paragem do sistema.

Para além disso, a virtualização disponibiliza recursos de redução de danos, o que permite que a empresa teste o seu plano de “Disaster Recovery “previamente.

*5 – Maior segurança*

Ao utilizar servidores virtuais, as empresas podem definir vários níveis de acesso para cada tipo de utilizadores. Além disso, é possível isolar equipamentos de determinados grupos de acesso, facilitando a gestão de utilizadores e aumentando o nível de segurança dos dados.

# Oracle VM VirtualBox

O software de virtualização VirtualBox permite a instalação e utilização de um sistema operacional dentro de outro, assim como os seus respetivos softwares, como dois ou mais computadores independentes, mas compartilhando fisicamente o mesmo hardware.

Existem diversos softwares de virtualização no mercado, no entanto, o VirtualBox destaca-se em alguns aspetos.

## Vantagens do VirtualBox

*1 – Open Source*

O VB é um software Open Source, o que, para além de transmitir mais confiabilidade que softwares proprietários, no que diz respeito ao nível de segurança da aplicação e dos dados dos utilizadores, uma vez que o código é acessível a qualquer pessoa, apresenta também uma maior fonte de suporte, uma vez que existe uma extensa comunidade de fãs da filosofia Open Source que estão constantemente a debater e a sugerir melhorias no código.

*2 – Facilidade de utilização*

É um software leve, o que torna a instalação e a utilização fáceis, sem comprometer a potência e rapidez da virtualização. Para além disso, o assistente de criação de novas máquinas virtuais é bastante intuitivo, o que faz com que qualquer pessoa o consiga utilizar sem ser necessário conhecimento prévio.

*3 – Snapshots*

O VB possibilita a criação de Snapshots, o que, no caso de algum problema na máquina, facilita o “rollback” para um estado anterior da mesma.

No fundo, apesar de um Snapshot não ser uma cópia de segurança, o fundamento é o mesmo, para além de serem de mais rápido restauro e não exigirem muito espaço de armazenamento.

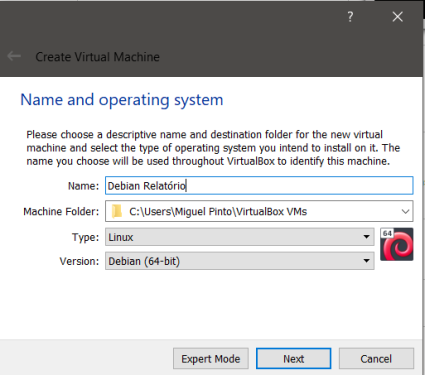
# Máquinas Virtuais

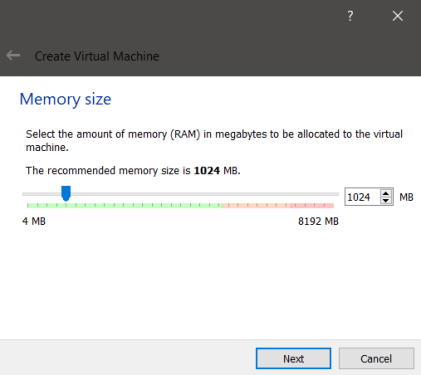
Para iniciar a configuração do nosso sistema virtual, iremos configurar e instalar 3 máquinas virtuais, usando o Oracle VirtualBox. Serão estas uma máquina Windows Server, uma máquina Windows 10 e uma máquina Debian sem ambiente gráfico.

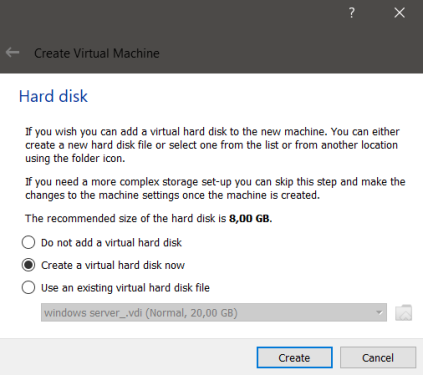
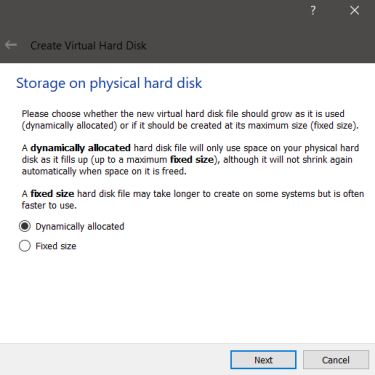
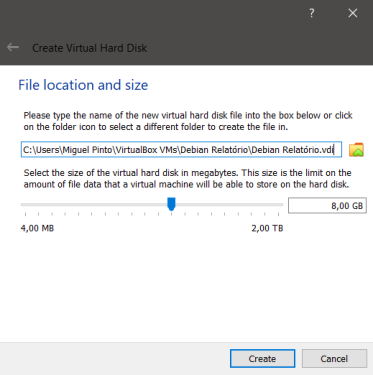
Iremos começar por instalar a nossa máquina Windows Server.

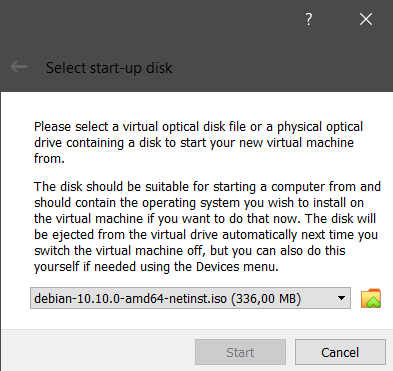
## Criação de uma Máquina Virtual

Apesar do VirtualBox possuir um assistente de criação de máquinas virtuais bastante intuitivo, achamos por bem demonstrar como criar uma máquina virtual.

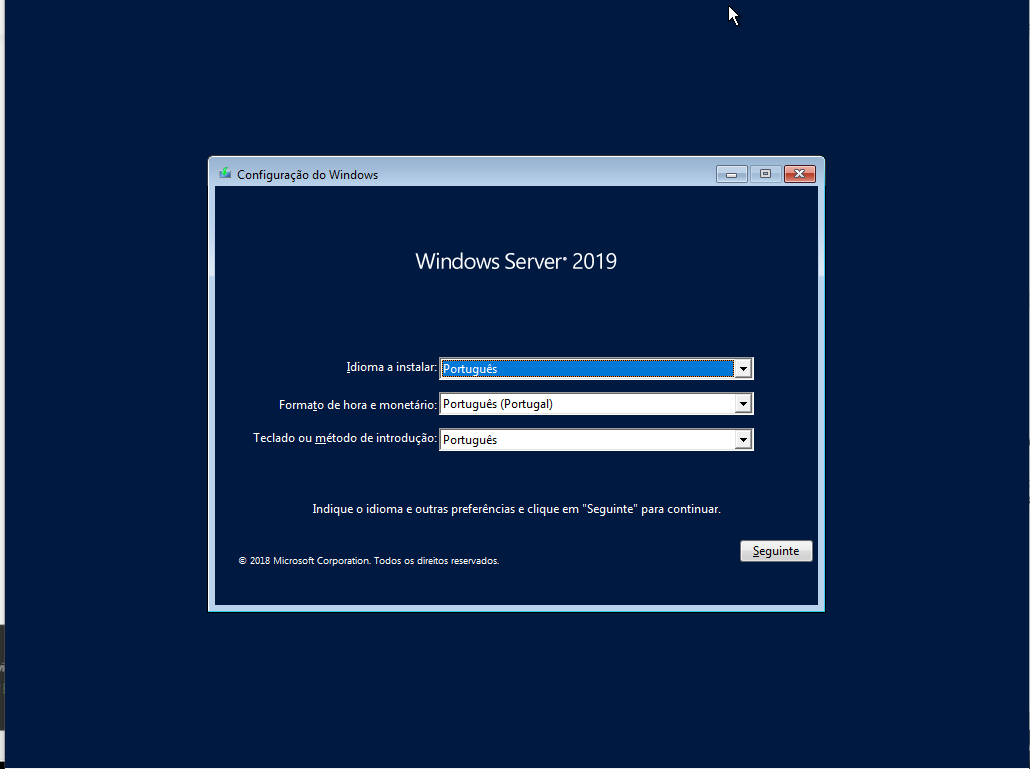
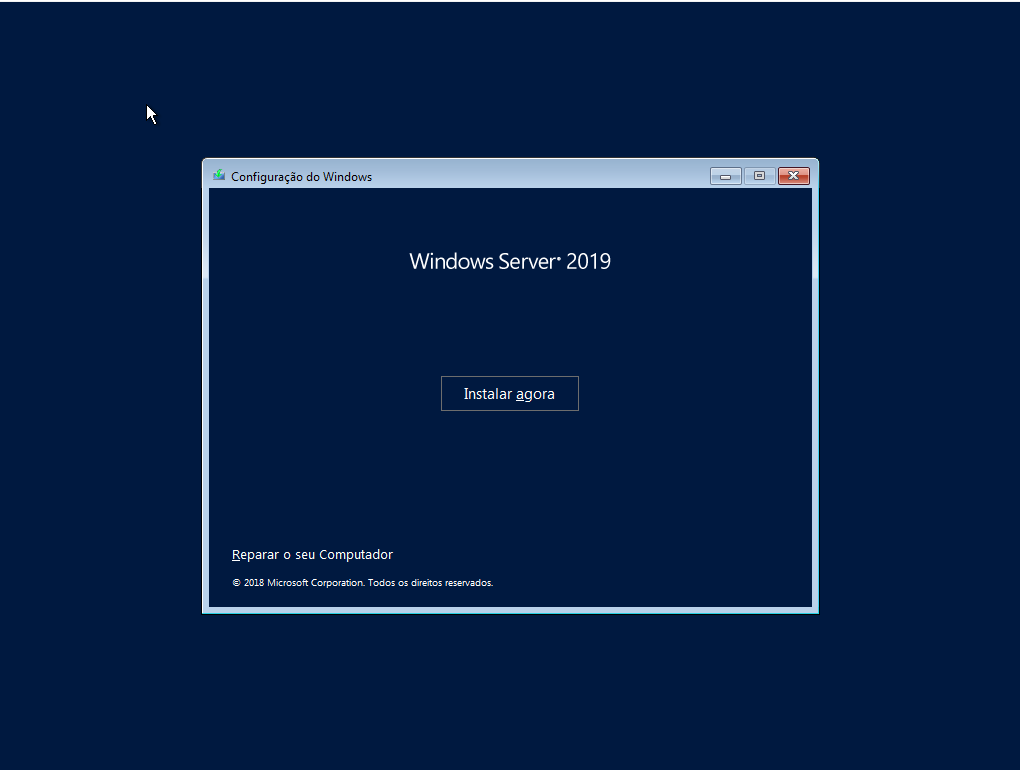
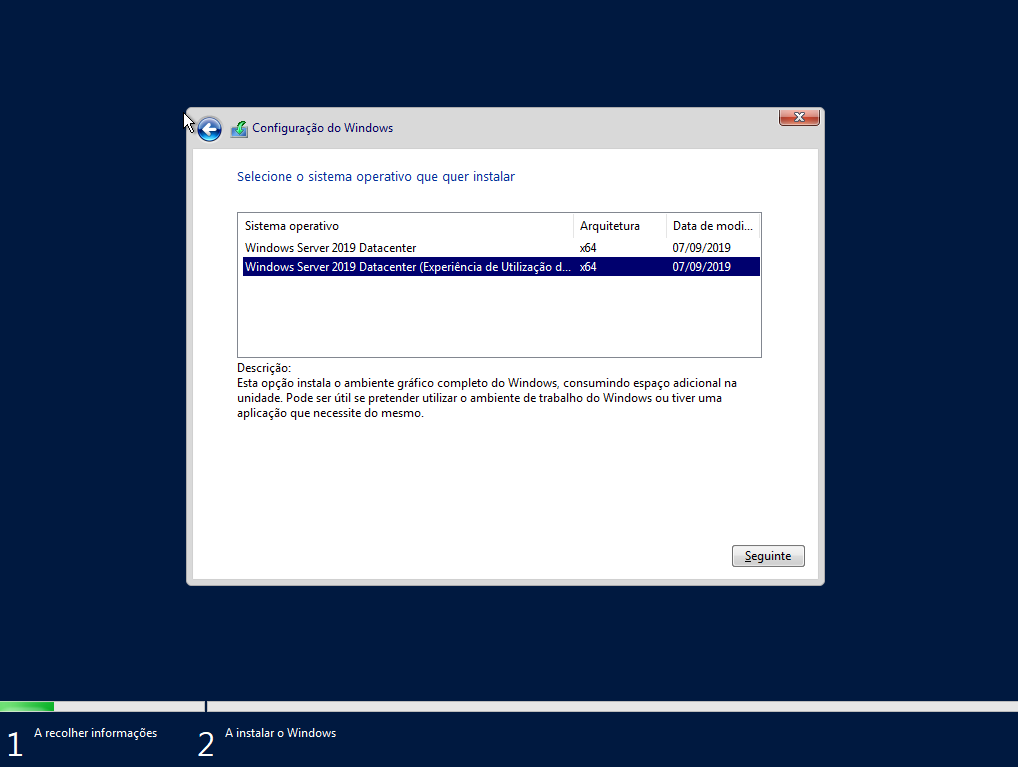
1. No menu inicial do VirtualBox, selecionamos o botão azul “New”. Esta ação resulta na abertura do assistente de criação de máquinas virtuais do software.
2. Escolhemos um nome para a nossa máquina virtual, que deverá ser autoexplicativo.
3. No menu de Memória RAM, é aconselhado utilizar o tamanho recomendado pelo software, no entanto, no caso de utilização de outro tamanho, será de evitar sair da seção verde da barra ajustável.

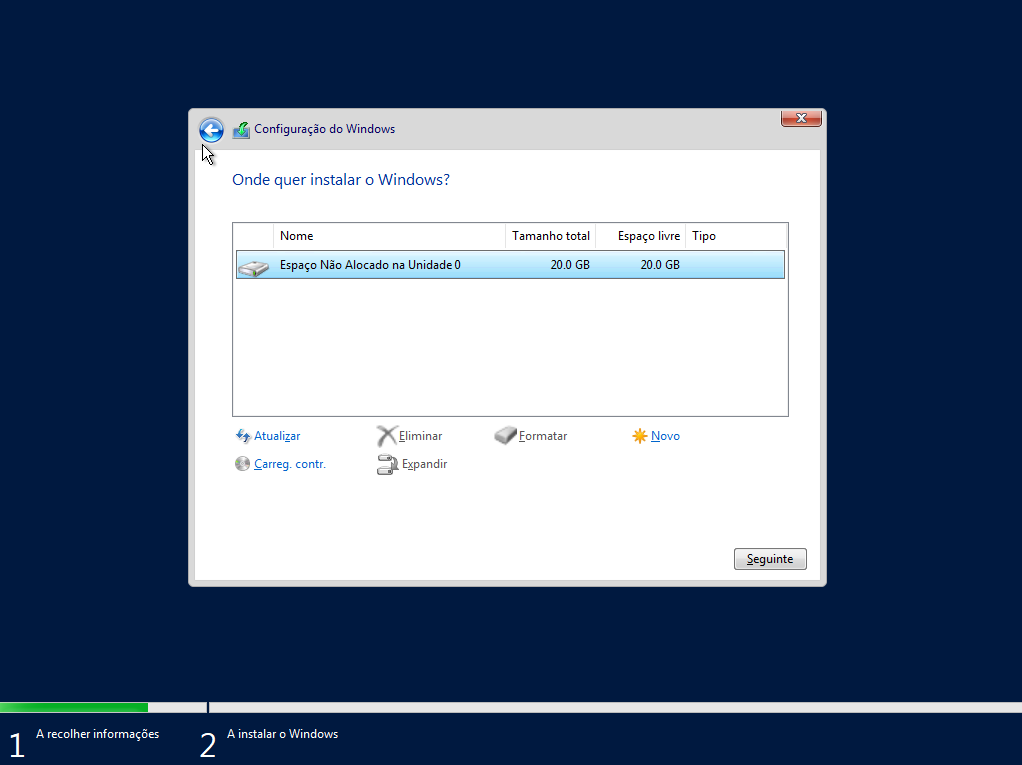


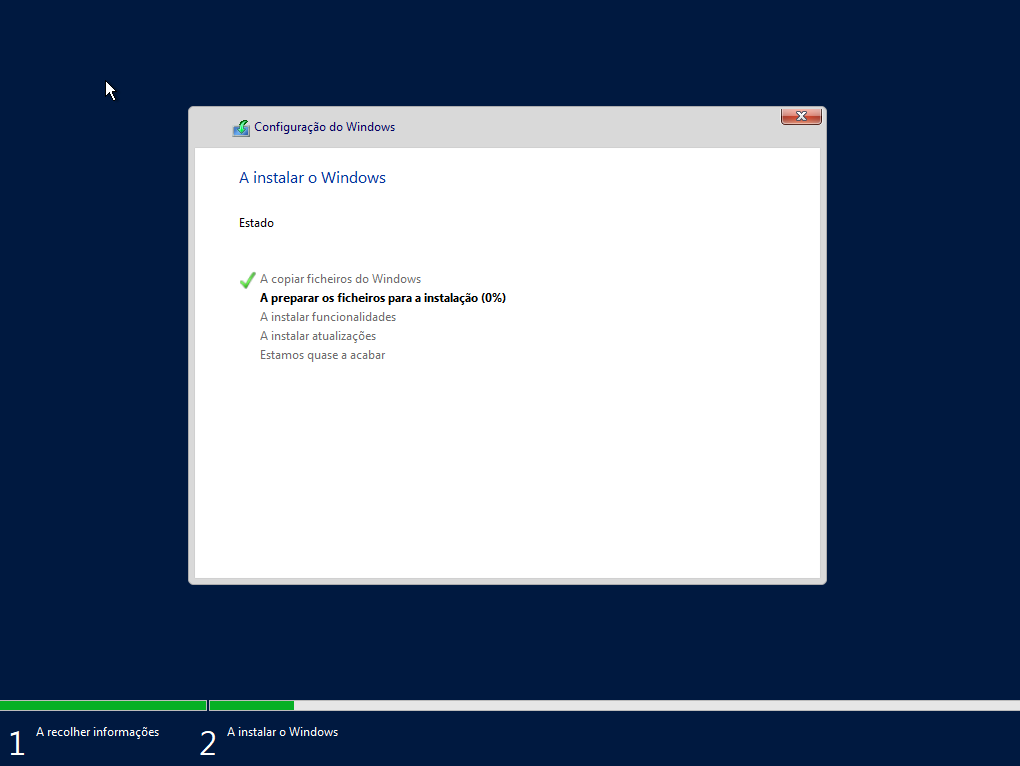
1. De seguida, criamos o disco rígido para a máquina virtual, que será utilizado para armazenar ficheiros e programas da mesma.
2. De seguida, alocamos um espaço alocado dinamicamente para este disco, o que faz com que a nossa máquina virtual apenas utilize o espaço necessário para o seu funcionamento.
3. Escolhemos o tamanho máximo que a nossa máquina poderá utilizar.
4. Finalmente, escolhemos o ficheiro ISO que será utilizado para a instalação do sistema operativo que será posteriormente utilizado na máquina virtual.

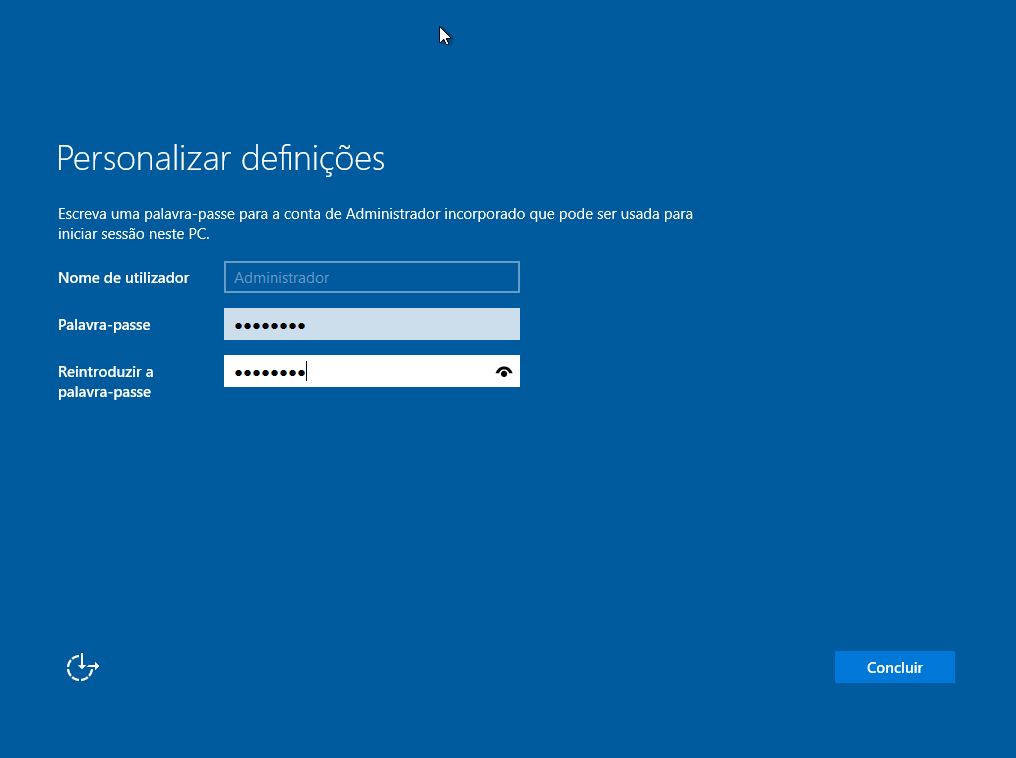


## Instalação Windows Server

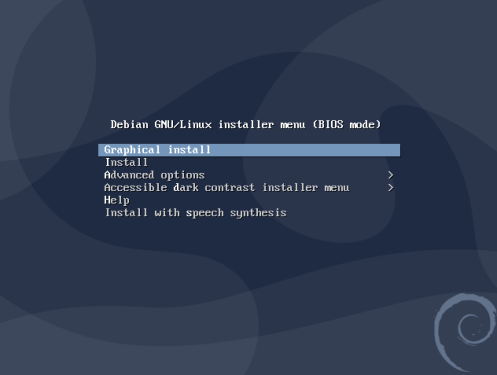
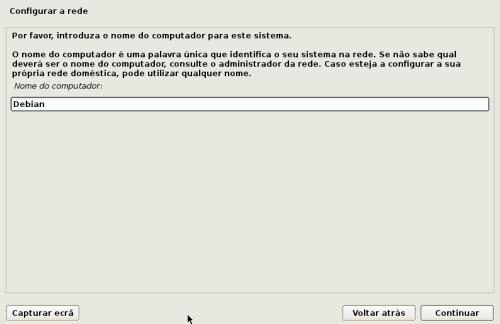
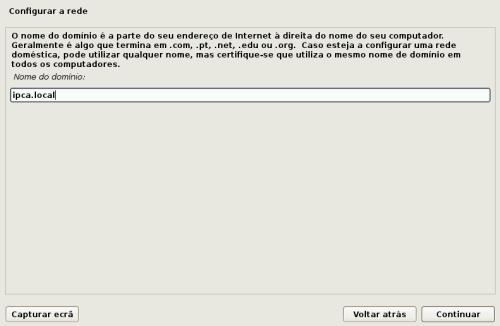
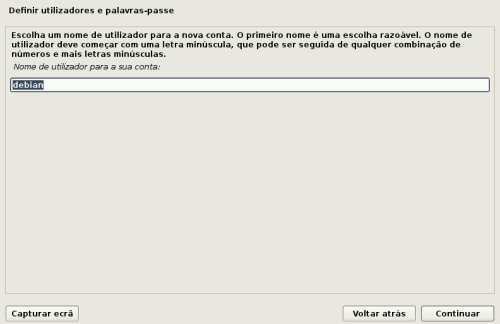
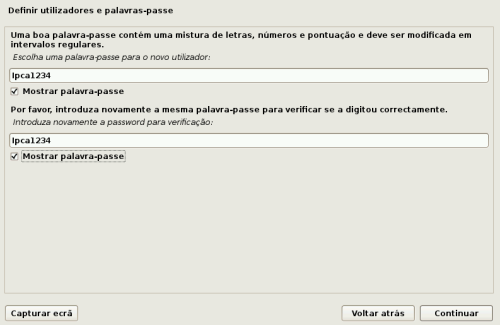
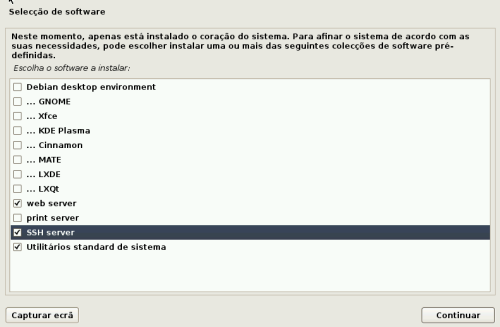
1. Selecionamos a linguagem desejada e clicamos em “Next”. De seguida, clicamos em “Install Now”
2. Escolhemos a opção “Windows Server 2019 Datacenter” e clicamos em “Next”.
3. Escolhemos o disco criado na criação da máquina virtual e clicamos em “Next”.

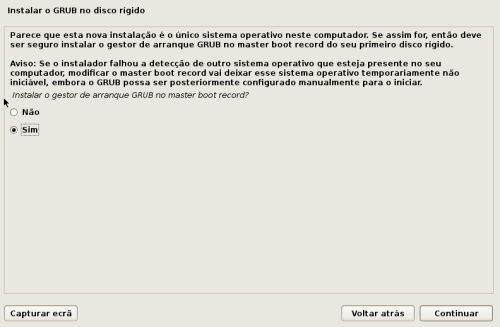


1. Aguardamos a conclusão da instalação do Windows Server na nossa máquina virtual.
2. Escolhemos uma password para o administrador do Servidor.



## Instalação Debian

1. No menu inicial da instalação do Debian, selecionamos a opção de “Graphical Install”, uma vez que, caso contrário, iriamos ter de proceder à instalação do Debian através da CLI, o que seria muito mais complicado.
2. Atribuímos um nome para o nosso superutilizador.
3. Introduzimos o nome do nosso domínio.
4. Selecionamos uma password para o nosso superutilizador.
5. Criamos um novo utilizador para o nosso OS.
6. Selecionamos uma password para o nosso novo utilizador.
7. Configuramos o Package Manager para utilizar o *mirror* “deb.debian.org”.
8. Selecionamos o software que queremos que seja instalado no nosso OS. Neste caso, utilizamos o “Utilitários standard de sistema”, o “SSH Server” e o “Web Server”. De notar que é de extrema importância desselecionar o “Debian desktop environment”, caso contrário será instalado o Debian com interface gráfica.
9. Por fim, instalamos o GRUB no nosso disco. O GRUB é um “Boot Loader” que é, resumidamente, o primeiro programa que é inicializado quando ligamos o computador. É responsável por carregar e transferir o controlo para o Kernel do OS. Este Kernel, depois, inicializa o resto do OS.



# Windows Server

O Windows Server é uma linha de sistemas operativos da Microsoft, criado especificamente para utilização em servidores. É quase exclusivamente utilizado em ambiente empresarial.

## Configuração do Windows Server

Inicialmente, tivemos de escolher entre os 3 tipos de placas de rede para utilizar no nosso sistema.

Esses tipos são os seguintes:

1. NAT

Permite que a máquina virtual tenha acesso à Internet, mas não dá acesso à rede Interna.

1. Bridged

Quando selecionada, o VirtualBox utiliza os drivers de rede do Host e fazem um ‘net filter’, intercetando e injetando dados na rede local.

Uma VM que possui este modo selecionado, aparece para o Host como se fosse uma máquina física conectada na rede.

1. Internal

As VM’s conseguem comunicar entre si, no entanto não são visíveis para o Host.

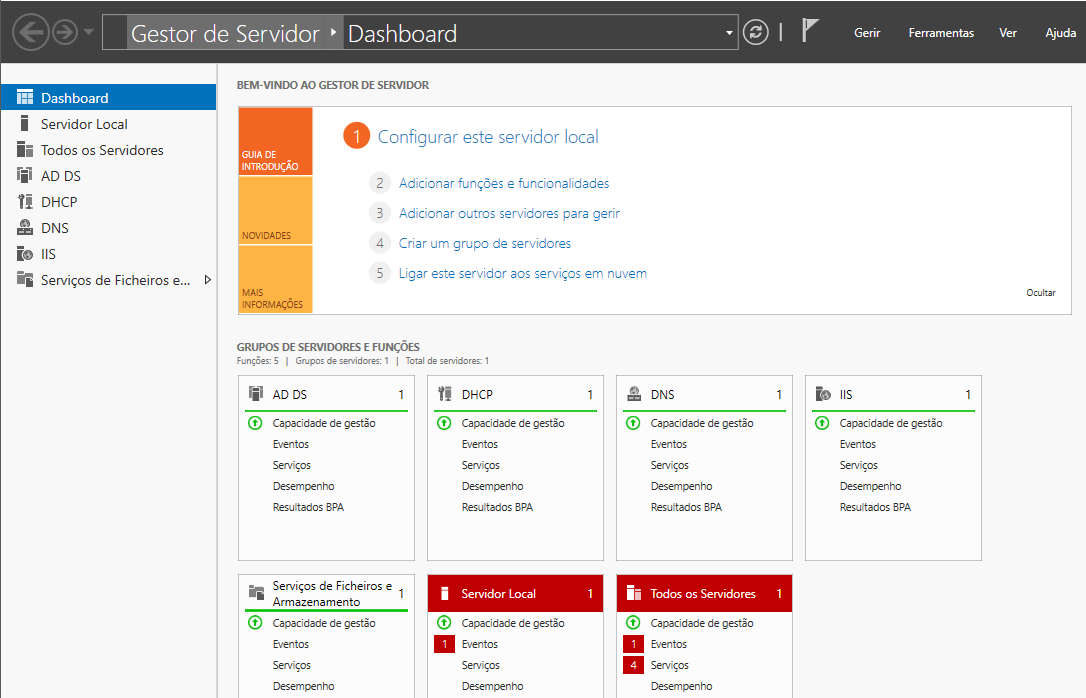
Ao contrário do Bridged, todos os pacotes ficam isolados na rede interna criada pelo VirtualBox.

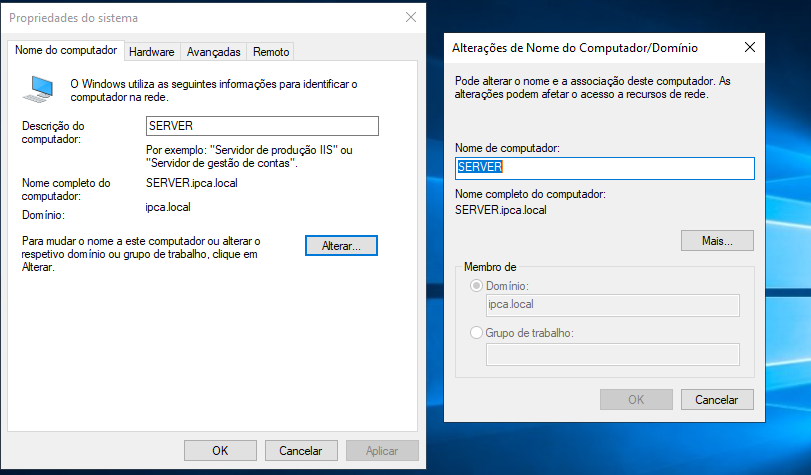
Assim, torna-se mais seguro, pois os “package Sniffers” não são capazes de capturar tráfego entre as VM’s.

A nossa opção recaiu para a placa de rede Internal.

Uma vez que se trata de um ambiente escolar, em que temos várias máquinas numa sala, se a rede estivesse em modo Bridged, e todos os alunos configurassem as suas máquinas de igual forma, iria haver conflito, uma vez que iriamos ter várias máquinas com o mesmo endereço IP.

Ao entrar na nossa máquina Windows Server, é-nos apresentado o Server Manager. Através deste menu podemos criar e gerir Funções e Recursos para o nosso servidor.

Posteriormente neste relatório, iremos abordar este recurso em maior pormenor.

Para nos ser mais fácil identificar o nosso servidor na Rede, iremos alterar o nome do nosso Windows Server para “SERVER”.

Agora que a configuração inicial do Windows Server foi realizada, iremos entrar no Active Directory.

# Active Directory

## O que é?

O Active Directory é um serviço de diretório utilizado no Windows Server.

A sua principal função é fornecer aos administradores funções para controlar permissões e acesso a recursos de rede.

No AD, os dados são guardados como objetos, incluindo utilizadores, grupos, aplicações e dispositivos, que serão categorizados de acordo com o nome e atributos.

O AD possui um componente chamado Domain Services que fornece um mecanismo para a autenticação de utilizadores e determinar os recursos de rede aos quais estes têm acesso.

Para além disto, fornece também direitos de acesso, certificados de Segurança, entre outros.

## DNS

O DNS, ou Domain Name System, é um diretório que traduz endereços IP em Nomes de Domínio.

Podemos comparar o DNS a uma lista telefónica. Tal como na lista, atribuímos nomes a números telefónicos, o DNS atribui nomes aos endereços IP.

Imaginemos que, para aceder a um Website, precisávamos decorar o endereço IP de cada Website. Ainda para mais, se o IP fosse alterado por algum motivo, o que pode acontecer, seria impossível aceder ao website em questão.

De tal forma, o DNS tornou-se rapidamente um dos aspetos mais importantes da Internet.

## DHCP

O DHCP, ou Dynamic Host Configuration Protocol é um protocolo de gestão de rede utilizado para automatizar o processo de configuração de dispositivos na rede, permitindo que estes usem alguns serviços como o DNS.

Um servidor DHCP, atribui dinamicamente um endereço IP a um dispositivo, permitindo que este comunique na rede com outros dispositivos.

O principal uso do DHCP é o de simplificar a gestão de endereços IP numa rede. Através deste, dois hosts não podem ter o mesmo IP, e a configuração manual dos mesmos, em casos de redes muito extensas, torna-se praticamente impossível.

## IP

Um endereço IP é um identificador único de cada dispositivo numa rede. IP significa Internet Protocol que é o conjunto de regras que administra os dados enviados numa rede.

O endereço IP permite que diferentes dispositivos comuniquem dentro de uma rede.

Temos 2 versões de IP: o IPV4 e o IPV6.

A versão mais utilizada atualmente é o IPV4, no entanto, uma vez que as reservas de endereços IPV4 se encontram neste momento a acabar, futuramente o IPV6 será a versão standard.

Isto deve-se ao tamanho do endereço de cada versão.

O IPV4 usa um endereço de 32 bits, o que significa que permite 2^32 endereços IP no total, o que se traduz em sensivelmente 4.29 biliões de endereços.

Já o IPV6 usa um endereço de 128 bits, suportando 2^128 endereços IP no total, o que se traduz em 340 undeciliões de endereços.

Em resumo, o IPV6 suporta 1028 vezes mais endereços que o IPV4.

## Configuração do AD DS

O Active Directory possui um conjunto de funções nucleares denominado de Active Directory Domain Services.

O AD DS permite que os administradores de sistema organizem os dados do servidor numa hierarquia lógica.

Assim sendo, será o primeiro passo a configurar no nosso Windows Server.

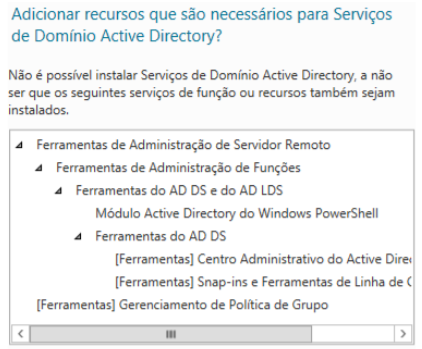
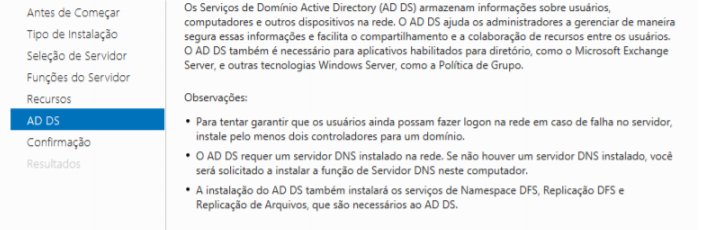
Para isso, na janela do Server Manager, clicamos em “Add Roles and Features”.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

 De seguida, selecionamos o nosso servidor.

No menu de funções a instalar, selecionamos o Active Directory Domain Services e finalizamos a instalação.



## Domínio vs. Grupo de Trabalho

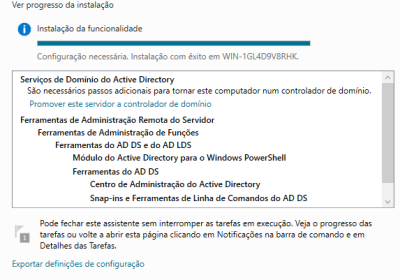
Um Grupo de Trabalho é uma rede “peer-to-peer” sem autenticação central. Cada computador presente num Grupo de Trabalho funciona tanto como um cliente como um servidor. Quando um utilizador num Grupo de Trabalho precisa de aceder ao computador de outro utilizador ou até um ficheiro partilhado, precisa de criar um utilizador nesse mesmo computador. Os Grupos de Trabalho são mais utilizados em ambientes empresariais mais pequenos.

Um domínio, por sua vez, oferece maior segurança, visto que podemos atribuir diferentes permissões para diferentes utilizadores e/ou grupos. Para além disso, podemos implementar políticas empresariais para administração. Se um utilizador precisar de aceder a um outro computador no domínio, não necessitam de criar outra conta.

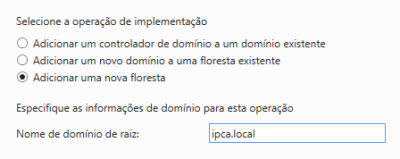
Todos os logins e pedidos de acesso dos utilizadores são geridos por um Domain Controller.

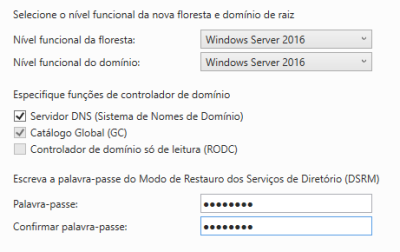
Um DC é um servidor centralizado que responde aos diversos pedidos, e atua como um “porteiro” para a rede. Tanto a autenticação como a autorização são feitas pelo DC.

No nosso sistema, iremos utilizar o nosso Servidor Windows Server como um DC, que irá controlar o nosso Domínio.

 Para tal, no final da instalação do AD DS iremos promover o nosso servidor a Domain Controller.

De seguida, adicionamos uma nova floresta e atribuímos um nome ao domínio, neste caso, “ipca.local”.



Atribuímos uma senha para restauro dos serviços.

De seguida atribuímos o nome NetBIOS. Este nome é uma maneira mais fácil de identificar o computador na rede e são utilizados por serviços e aplicações.

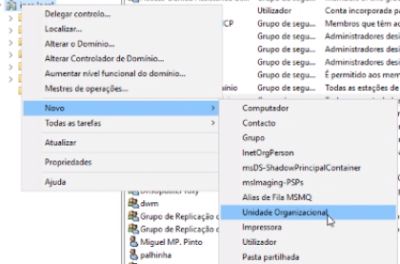
Finalmente, especificamos o local da base de dados do AD DS e finalizamos a configuração.

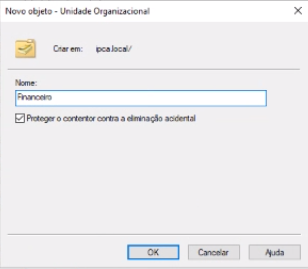
## Unidades Organizacionais e Utilizadores

Uma Unidade Organizacional é um tipo de objeto contido no domínio para o qual podem ser atribuídas Políticas de Grupos.

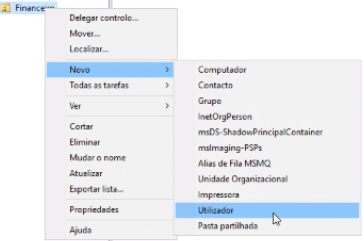
Este recurso facilita o trabalho do Administrador da Rede, uma vez que, como ocorre nos grupos, uma OU pode conter duas ou mais OU’s, formando uma hierarquia, ajudando a reduzir o número de domínios necessários para uma rede.

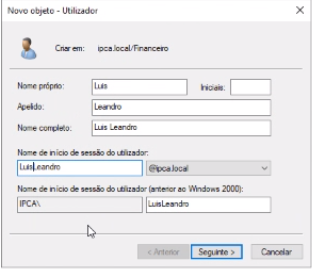
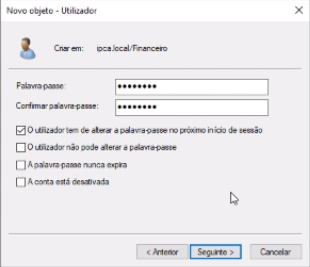
Estas OU’s são utilizadas principalmente para a aplicação de Políticas de Grupo e atribuição de permissões de gestão de objetos, que são herdadas para os utilizadores e OU’s que se encontrem dentro da mesma.

 Para criar uma Unidade Organizacional, no menu “Utilizadores e Computadores do Active Directory” selecionamos o nosso domínio e criamos uma nova Unidade Organizacional.

 De seguida, escolhemos um nome para a nossa OU, neste caso, “Financeiro”.

Agora, podemos adicionar um utilizador já existente à nossa OU, ou podemos também criar um novo Utilizador.

 Para isto, selecionamos a opção “Novo Utilizador”, na OU “Financeiro”.

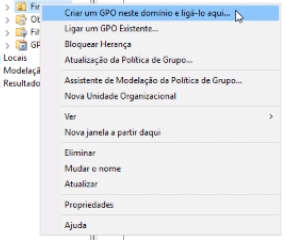
 De seguida, preenchemos as informações do nosso novo Utilizador.

## Políticas de Grupo (GPO)

Uma política de grupo é uma funcionalidade do Active Directory. É um conjunto de regras que podem ser aplicadas aos utilizadores e computadores da rede e fornece a gestão e configuração centralizada de sistemas operativos, aplicações e configurações dos utilizadores.

No fundo, uma GPO controla o que os utilizadores podem ou não fazer dentro da rede.

São geralmente utilizadas para restringir determinadas ações que podem representar potenciais riscos de segurança, como por exemplo: bloquear o acesso ao gestor de tarefas, restringir o acesso a determinadas pastas, desativar o download de arquivos executáveis, entre outras.

 Na nossa OU, podemos aplicar uma GPO já existente ou criar uma nova GPO.

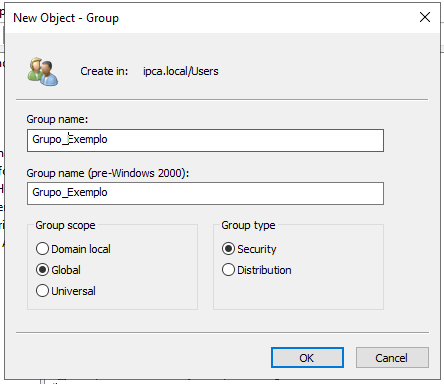
Como podemos presumir, será mais fácil e rápido criar OU’s para os diversos departamentos de uma empresa e aplicar políticas de grupo a cada OU do que aplicar individualmente a cada utilizador uma política de grupo.

De notar que, embora se chame Política de Grupo, as GPO’s não podem ser aplicadas diretamente a Grupos de Utilizadores. Daí a importância da criação de OU’s.

## Criação de Grupos de Utilizadores

Uma imagem com texto

Descrição gerada automaticamente No menu “Active Directory Users and Computers”, acedemos à pasta “Users” onde se encontram listados todos os utilizadores e grupos. De seguida, criamos um novo Grupo.

 Seguidamente, atribuímos o nome desejado ao nosso Grupo.

## Quotas de Armazenamento

No AD, possuímos a possibilidade de configurar quotas de armazenamento nos sistemas de ficheiros para limitar a quantidade de armazenamento de dados que os utilizadores podem consumir.

Após a definição dessas mesmas quotas, o Administrador de Rede pode monitorizar o estado da quota.

Ao aplicar as quotas, um utilizador que exceda a sua quota recebe uma mensagem de erro de “espaço insuficiente no disco”.

Podemos também aplicar Avisos que serão mostrados quando um utilizador se aproxime do limite da quota aplicada.

Existem dois tipos de quotas que podem ser definidos: a quota em Disco e a quota em Pasta.

### Quotas em Disco

Com este tipo de quotas, podemos definir qual o espaço em disco disponível para cada utilizador.

Uma imagem com texto

Descrição gerada automaticamente Para definir uma quota em disco, acedemos às propriedades do disco local, abrimos o separador “Quota” onde iremos ativar a gestão da quota e selecionamos a opção “Do not limit disk usage”, ou seja, negamos o espaço em disco para limites de quota excedidas.

De seguida, acedemos a “Quota Entries”.

Uma imagem com texto

Descrição gerada automaticamente

Neste separador, selecionamos o utilizador ao qual queremos atribuir a quota, neste caso o utilizador Pedro que se encontra no nosso domínio.

Uma imagem com texto

Descrição gerada automaticamenteDepois deste processo, o seguinte permite-nos limitar o espaço em disco para o utilizador anteriormente escolhido em 50MB e uma notificação ao atingir os 30MB.

Quando este utilizador se autenticar, ficará com um limite se quota de 50MB.

Assim, a pasta partilhada na rede para os utilizadores do domínio onde aplicamos, anteriormente, um limite de pasta de 100MB para todos os utilizadores, atribuirá este limite a todas os utilizadores, exceto ao Pedro que ficará com uma quota em disco de 50MB.

### Quotas em Pasta

As quotas em Pasta aumentam significativamente as possibilidades do Administrador de Rede de controlar de forma eficiente o uso excessivo do espaço em disco num servidor.

Uma imagem com texto

Descrição gerada automaticamente O recurso do Windows responsável por esta gestão é o “File Server Resource Manager (FSRM)”.

Uma imagem com texto, captura de ecrã, interior

Descrição gerada automaticamente Possibilita o controlo de quotas por volumes e pastas.

Uma imagem com texto

Descrição gerada automaticamenteÉ ainda possível gerar notificações quando os limites das quotas estiverem próximos ou forem excedidos.

Uma imagem com texto

Descrição gerada automaticamenteTambém permite gerar quotas de aplicação automática que se apliquem a todas as subpastas existentes num volume ou pasta e a todas as subpastas criadas no futuro.

Uma imagem com texto

Descrição gerada automaticamenteTambém permite criar *templates* de modelos de quotas para serem aplicados a pastas existentes ou novas pastas.

Uma imagem com texto

Descrição gerada automaticamenteAtribuição de um modelo de quota a uma pasta partilhada.

Uma imagem com texto

Descrição gerada automaticamente Podemos também gerar um relatório de quota, notificação quando a utilização chega a x%, mensagem de email, entre outros.

## Backup e Restauro Windows Server

Backup é uma cópia de segurança que é feita para garantir o acesso aos dados originais em casos de perda ou corrupção de dados por qualquer motivo.

Existem 3 tipos diferentes de Backup:

* Backup Completo – Cria uma cópia completa de todos os dados – alterados ou não;
* Backup Incremental – É uma cópia apenas dos dados que foram alterados desde que foi feito o último backup;
* Backup Diferencial – É uma cópia de todos os dados alterados desde que foi feito o último backup completo.

Estes tipos de Backup podem ser manuais, onde o utilizador faz o Backup manualmente, ou agendado, onde o utilizador configura a execução do Backup para uma determinada hora de um determinado dia.

De seguida, iremos demonstrar como realizar um Backup Agendado.

### Backup Agendado

Criamos uma pasta (“PRIVADA”) numa máquina dentro da mesma rede do nosso servidor, e partilhamos a mesma.

Uma imagem com captura de ecrã

Descrição gerada automaticamente No Windows Server, instalamos o recurso de Backup.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Acedemos a “Ferramentas e Backup Windows Server”.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Selecionamos os itens que queremos fazer Backup.

Especificamos a hora em que o Backup irá ser realizado.

Uma imagem com captura de ecrã

Descrição gerada automaticamente

Uma imagem com captura de ecrã

Descrição gerada automaticamenteEspecificamos o tipo de Backup a ser realizado.

Uma imagem com captura de ecrã

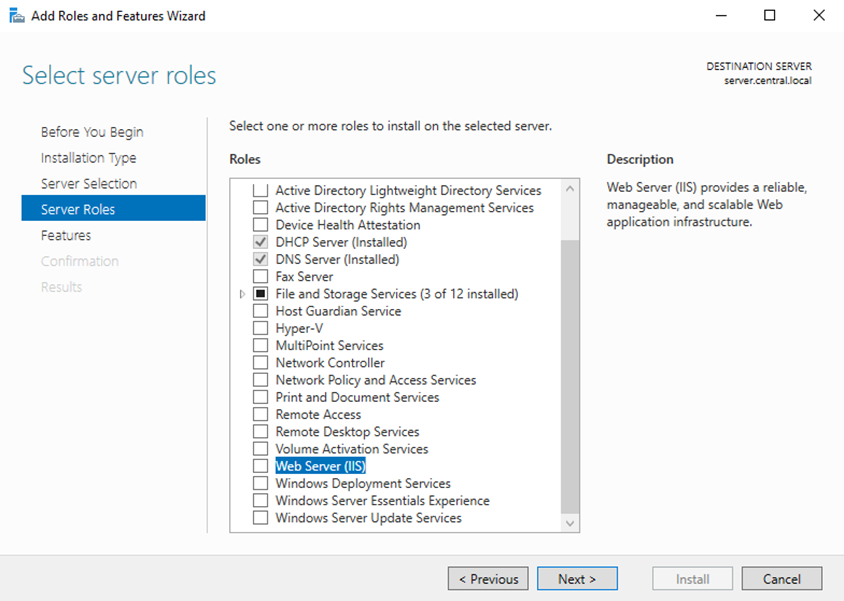
Descrição gerada automaticamenteEspecificamos a pasta partilhada remotamente.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Finalmente, verificamos se a cópia de segurança foi realizada com sucesso.

## IIS (Internet Information Services)

O IIS, é um Web Server que fornece uma plataforma segura, fácil de gerir, modular e escalonável para hospedar websites, serviços e aplicações.

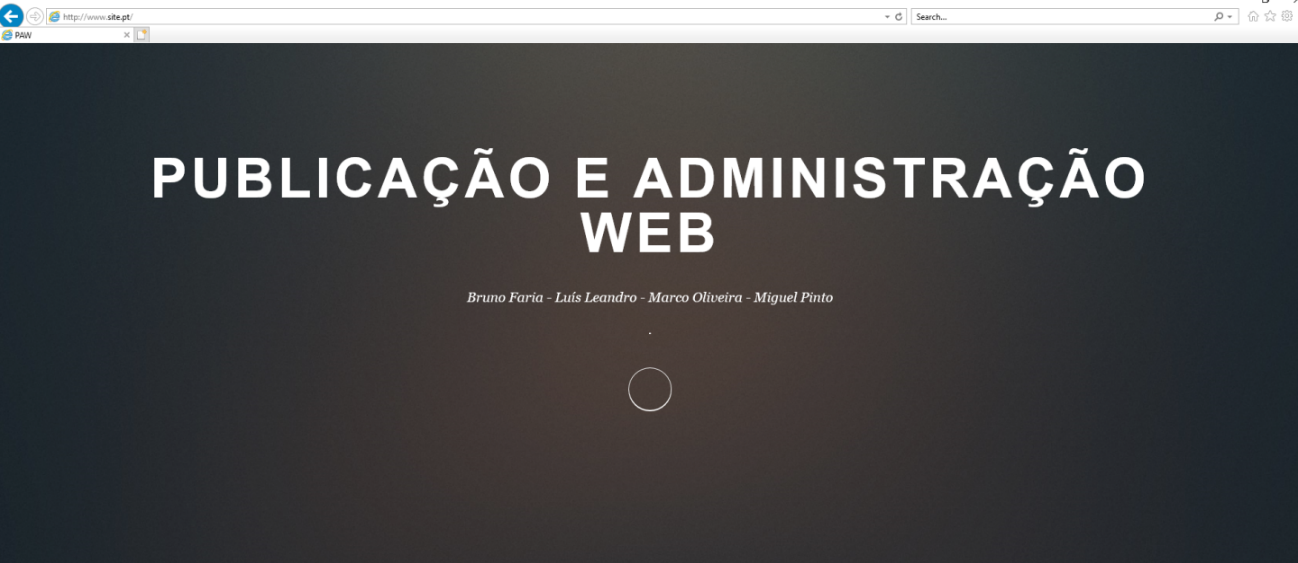
 Para ativarmos essa plataforma no Windows Server, no menu “Add Features and Roles”, selecionamos o Web Server (IIS).

Uma imagem com texto

Descrição gerada automaticamente No separador “Role Services”, selecionamos o “FTP Server” e finalizamos.

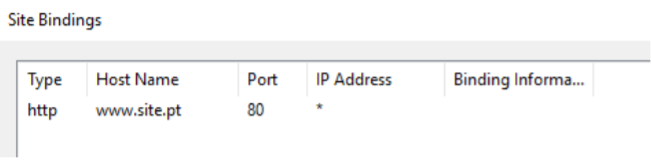
No processo de instalação foi criada a diretoria “C:\inetpub\”. O conteúdo do servidor a hospedar deverá ser colocado na subdiretoria “wwwroot”.

Para testar o Web Server (IIS), inicialmente, por defeito, é criado um site de testes, para verificar o funcionamento do Servidor Web IIS, a partir do browser no servidor. Para testar o acesso, acedemos a <http://127.0.0.1/>.



Uma imagem com texto

Descrição gerada automaticamente Para adicionar o nosso site, aceder a “Internet Information Services”.

 Atribuição do host que neste caso será [www.site.pt](http://www.site.pt) que servirá para acedermos no browser.

Uma imagem com texto

Descrição gerada automaticamente Criação de uma nova zona.

Se agora, acedermos ao website através do URL [www.site.pt](http://www.site.pt), iremos conseguir o mesmo resultado que anteriormente.

## DHCP

O servidor de DHCP permite a configuração automática da informação de rede dos dispositivos que o utilizem.

Dessa forma o utilizador não necessita de configurar manualmente o seu dispositivo com dados como: endereço IP, máscara de rede, gateway, servidores de DNS, etc.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém a gestão centralizada dos endereços IP usados na rede. No serviço é definido todo o endereçamento a atribuir dinamicamente.

Atribuição automática dos seguintes parâmetros da configuração de rede:

* Endereço IP;
* Máscara de rede;
* Gateway;
* Servidor de DNS.

### Configuração do Servidor DHCP

Uma imagem com texto

Descrição gerada automaticamente No menu “Add Roles and Features” selecionamos “DHCP Server”.

Uma imagem com captura de ecrã

Descrição gerada automaticamenteDe seguida, completamos a configuração do DHCP.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Posteriormente à sua instalação, informamos as credenciais para autorização do DHCP e clicamos em “Commit”.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Seguidamente, abrimos a consola do DHCP e Administrative Tools.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Clicamos com o botão direito do rato em IPV4 e vamos a New Scope.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Neste menu, introduzimos um nome para o novo escopo e clicamos em Next.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Introduzimos o range de IP para atribuição pelo DHCP.

Uma imagem com captura de ecrã

Descrição gerada automaticamente No menu seguinte podemos introduzir algum endereço IP que queiramos excluir do DHCP. Neste caso, clicamos em Next.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Definimos o período de renovação dos IP.

Uma imagem com captura de ecrã

Descrição gerada automaticamente De seguida, introduzimos o IP do nosso router e clicamos em “Add”.

Uma imagem com captura de ecrã

Descrição gerada automaticamente Informamos o IP do servidor DNS que é o próprio IP do Windows Server e finalizamos a configuração.

## Políticas de Auditoria

A auditoria é uma tarefa onde se realizam testes para verificar se tudo está a ser executado de forma correta. Esta tarefa poder ser realizada internamente.

Graphical user interface, application

Description automatically generated Primeiramente, procedemos à criação de uma pasta, na máquina servidor, e à configuração da sua partilha.

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application

Description automatically generated Seguidamente, procedemos à introdução de uma política de auditoria.

Graphical user interface, text, application

Description automatically generated Seguidamente, selecionamos todos os utilizadores.

Graphical user interface, text, application, email

Description automatically generatedFinalmente, selecionamos todos os parâmetros que pretendemos auditar.

Fazemos depois o login na máquina cliente, com as credenciais do utilizador.

Graphical user interface, text

Description automatically generated with medium confidencePara finalizar, procedemos ao mapeamento, na máquina cliente, da pasta partilhada com a política atribuída.

Graphical user interface, text, application, email

Description automatically generatedVisto o utilizador não possuir permissões para apagar o documento .txt que está dentro da pasta, ele irá receber um aviso:

Graphical user interface, application

Description automatically generatedE será também gerado um log, na máquina servidor, com um “event” desta tentativa:

## Permissões

Todos os objetos na rede possuem um conjunto de informações sobre o controlo de acesso anexado ao mesmo.

Este conjunto de informações são denominados de permissões e controlam o tipo de acesso permitido a utilizadores e grupos. Estas permissões são atribuídas a utilizadores e grupos específicos. Por exemplo, para o arquivo “OLA.txt”, ao grupo interno Administradores podem ser atribuídas as permissões Read, Write e Delete, enquanto ao grupo Financeiro podem ser atribuídas apenas as permissões Read e Write.

Cada atribuição de permissões a um utilizador ou grupo é representada no sistema como uma entrada de controlo de acesso.

O conjunto de entradas de permissão num descritor de segurança é conhecido como uma Lista de Controlo de Acesso.

Portanto, para o arquivo “OLA.txt”, a Lista de Controlo de Acesso inclui duas entradas de permissão, uma para o grupo interno Administradores e outra para o grupo Financeiro.

### Permissões Explicitas e Herdadas

Existem dois tipos de permissão: as explicitas e as herdadas.

As permissões explicitas são aquelas que são definidas por padrão em objetos que não são filho quando o objeto é criado, ou por ação do utilizador em objetos pai, filho ou não-filho.

Já as permissões herdadas são as que são propagadas até um objeto a partir de um objeto pai. Estas permissões facilitam a tarefa de gerir permissões e garantir a consistência das permissões em todos os objetos de um determinado recipiente.

Por padrão, os objetos de um recipiente herdam as permissões desse recipiente ao serem criados.

Por exemplo, quando criamos uma pasta denominada “Teste”, todas as subpastas e todos os arquivos criados dentro da mesma, herdam automaticamente as suas permissões. Desta forma, a pasta “Teste” possui permissões explicitas e as subpastas e os arquivos terão permissões herdadas.

# Linux

O Linux é um sistema operativo Open Source. Isto significa que, ao contrário dos seus concorrentes mais famosos, o Linux não foi desenvolvido para fins comerciais e qualquer pessoa pode criar e distribuir aplicações para o mesmo.

É baseado em UNIX e foi criado para o uso em desktops, mas é também muito utilizado em servidores, smartphones, tablets e outros tipos de dispositivos, incluindo Caixas ATM.

A parte básica do Linux é composta de um Kernel, software criado para fazer a comunicação com os programas e traduzi-los em comandos para a unidade de processamento e outros componentes eletrónicos.

A parte necessária e obrigatório do Linux é pequena, mas insuficiente para garantir uma experiência completa. A ideia é que cada utilizador personalize o uso com os seus programas favoritos, mas, na prática, isso é difícil e demorado.

Para simplificar este processo existem várias versões do sistema operativo disponíveis para o utilizador, chamadas distribuições (ou distros), com interfaces próprias.

Uma distro é composta por vários softwares, como interfaces gráficas, editores de texto e browsers já instalados, além de um gestor de pacotes – um sistema usado para instalar, desinstalar e atualizar programas.

A grande variedade de distros faz com que seja natural a existência de variantes especificas para determinados “niches”. O Ubuntu, por exemplo, é virado para utilizadores iniciantes, automatizando diversos processos que, em outras versões, seriam mais complicados. O ArchLinux, por sua vez é mais virado para programadores e entusiastas de Linux, enquanto o RedHat é mais virado para ambientes empresariais.

No nosso caso, iremos utilizar o Debian.

## Debian

O Debian é um dos sistemas operativos baseados no Kernel Linux mais antigos que existe.

É considerado a distro mais flexível em termos de desenvolvimento, para além de possuir garantias de estabilidade. Isto faz com que o Debian seja uma boa opção para implementações críticas e uma das distros mais utilizadas.

## SSH

SSH, também conhecido como Secure Shell, é um protocolo de comunicação de rede que permite que dois computadores comuniquem e partilhem dados. Uma das características inerentes dessa comunicação é o fato desta ser encriptada, o que significa que pode ser utilizado em redes sem segurança.

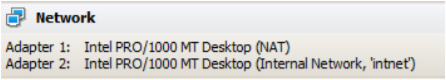
O SSH é frequentemente utilizado para realizar operações remotas noutros computadores, mas pode ser também utilizada para a transferência de dados.

Para utilizarmos o SSH, é necessário um programa (SSH client) para se conectar ao nosso servidor e transferir os dados de ou para o nosso armazenamento utilizando uma GUI (Graphical User Interface) ou a CLI.

No nosso caso, iremos utilizar o SSH através do programa “Putty” na nossa máquina Windows cliente.

Para tal, precisamos de alterar algumas configurações no nosso servidor Linux.

### Configuração SSH

 No nosso caso, temos primeiro que ativar 2 adaptadores de rede no nosso servidor Linux. O 1º adaptador colocamos em modo NAT para termos acesso à internet, enquanto o 2º adaptador colocamos em rede interna, a mesma rede da nossa máquina cliente, de forma que eles possam comunicar.

De seguida, para conseguirmos aceder ao nosso servidor através da nossa máquina cliente, necessitamos de atribuir um IP estático ao 2º adaptador, e para isso precisamos de aceder ao ficheiro de configuração das interfaces de rede, usando a CLI, visto que não instalamos ambiente gráfico.

 Assim sendo, na nossa CLI introduzimos o seguinte comando:

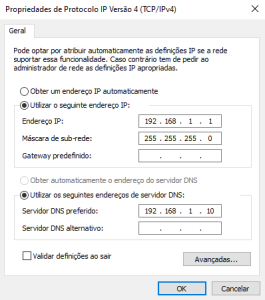
 De notar que, no Debian, o editor de texto VIM não vem instalado por defeito, podendo ser instalado através do comando:

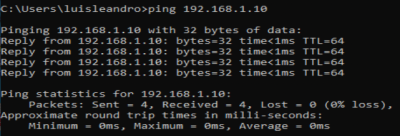
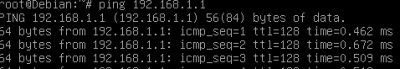
Caso não quisermos instalar o VIM no nosso servidor, podemos utilizar outro programa como o VI ou o Nano.

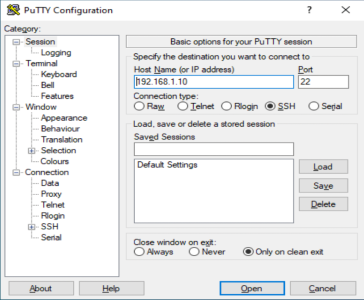
Uma imagem com texto

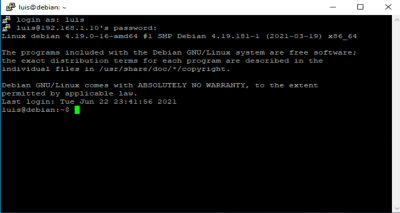
Descrição gerada automaticamente De seguida, necessitamos de assegurar que o 1º adaptador de rede cuja interface é a enp0s3 esteja em DHCP e atribuímos um endereço IP estático à segunda placa de rede. Neste caso, 192.168.1.10.

Para validar que as configurações das placas de rede do nosso servidor foram bem-sucedidas, podemos fazer um ping test entre o Servidor Linux e a nossa máquina cliente.

 Para tal, precisamos de saber o IP da máquina cliente, que, neste caso, é o 192.168.1.1.



 Uma vez que, à partida, está tudo bem configurado, é altura de testar o nosso cliente SSH. Na máquina cliente, abrimos o software Putty. Inserimos o IP do servidor, porta 22 e o tipo de ligação (SSH).

 Depois de confirmada a ligação, introduzimos as credenciais do utilizador do servidor. Podemos aceder ao servidor através deste terminal.

## Servidor Wordpress

O Wordpress é um sistema Open Source de gestão de conteúdo gratuito.

Um sistema de gestão de conteúdo é uma ferramenta que torna fácil a gestão de aspetos importantes de um website, como conteúdo, sem a necessidade de um background em programação.

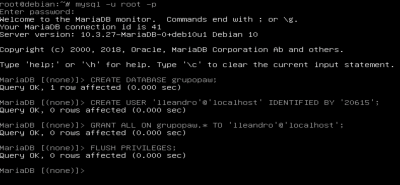
O Wordpress faz com que construir um website seja acessível para qualquer pessoa.

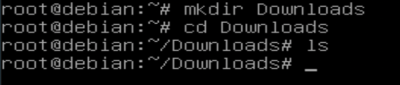
### Configuração de Servidor Wordpress

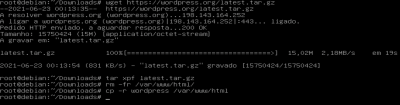
 Primeiramente, iremos proceder à instalação do servidor apache através do seguinte comando:

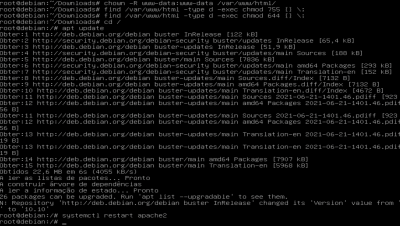
 De seguida, instalamos o sistema de gestão de base de dados MariaDB:

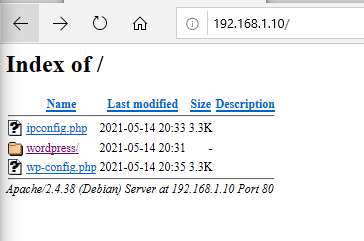
 Por fim, instalamos o PHP:

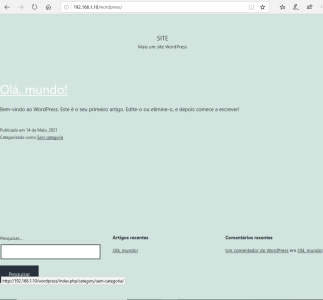
 Após termos instalado todas as ferramentas necessárias, iremos proceder à criação da base de dados e respetivo utilizador. Atribuímos todos os privilégios ao utilizador que criamos.

 De seguida, iremos criar a pasta Downloads.

 De seguida, vamos fazer o download do Wordpress, assim como a sua descompactação, eliminação do conteúdo da pasta html e cópia do Wordpress para a mesma. A opção “-f” após o “rm” (remove) força a remoção do conteúdo da pasta, no caso de possuir proteção. A opção “-r” efetua uma “tree-walk” e apaga todos os ficheiros e subdiretorias da pasta pai, recursivamente. No caso do copy (“cp”), a opção “-r” efetua a mesma “tree-walk”, mas copia os ficheiros e subdiretorias recursivamente, em vez de os eliminar.

 Após isto, iremos atribuir o dono, assim como as permissões para a pasta e ficheiros.

 Agora, na máquina cliente, acedemos ao IP do servidor.



## Servidor Email

Um servidor de email é uma máquina ou aplicação responsável para gerir emails. Por outras palavras, a função de um servidor de Email é receber e enviar emails.

Quando um email é enviado, a mensagem geralmente percorre uma série de servidores de email até chegar ao destinatário.

Este processo é tão rápido e eficiente que parece simples, no entanto, é bastante complexo.

Para evitar confusão, é importante ressalvar que o termo “servidor de email” pode ter diversos significados mediante o contexto. Por vezes significa um computador ou máquina que possui um sistema completo que inclui diferentes serviços ou aplicações. Outras vezes, o termo “servidor de email” pode ser usado como um sinonimo para alguns destes mesmos serviços ou aplicações.

### Configuração do Servidor Email

Uma imagem com texto

Descrição gerada automaticamente Primeiramente, iremos transferir o iRedMail para o nosso servidor Linux.

Uma imagem com texto

Descrição gerada automaticamenteDe seguida, descompactamos a pasta transferida e entramos na mesma.

Uma imagem com texto

Descrição gerada automaticamente

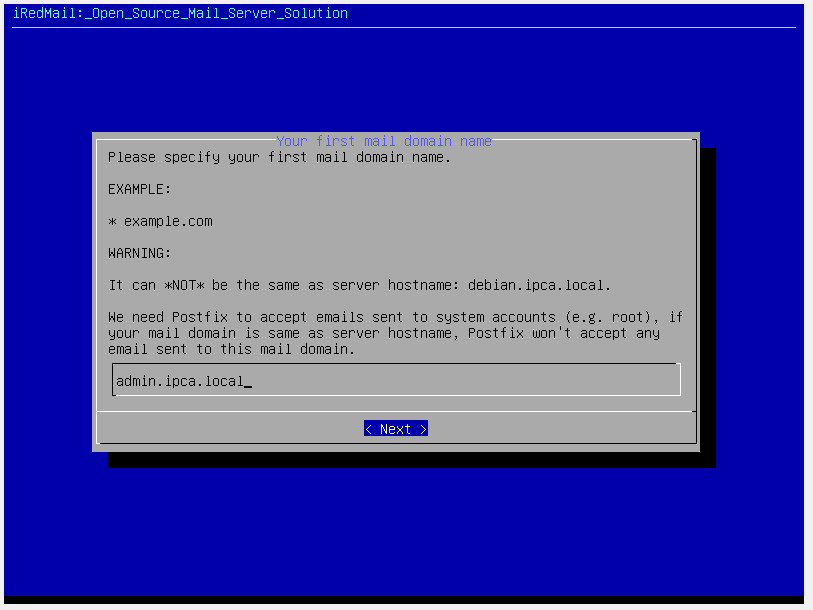
 De seguida, temos de executar o ficheiro de instalação, através do comando.

Uma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto

Descrição gerada automaticamente Selecionamos o sistema de gestão de base de dados MariaDB.

 Introduzimos o mail domain name pretendido, neste caso “ipca.local”.

Uma imagem com texto

Descrição gerada automaticamente Confirmamos as configurações e recebemos a confirmação da configuração ter sido bem-sucedida.

Agora, no browser da máquina cliente, podemos aceder a dois endereços:

192.168.1.10/iredadmin – Que é o endereço para criação de utilizadores;

192.168.1.10/mail – Que é o endereço onde os utilizadores poderão seguir para se autenticarem e utilizarem o servidor de email.

Podemos criar utilizadores para o servidor de email.

Uma imagem com texto

Descrição gerada automaticamenteUma imagem com texto, captura de ecrã, monitor

Descrição gerada automaticamente

Para testar a configuração do servidor de email, iremos enviar um email desde o utilizador [marco@ipca.local](mailto:marco@ipca.local) para o utilizador [jose@ipca.local](mailto:jose@ipca.local) .

Uma imagem com texto

Descrição gerada automaticamente Envio de email:

Uma imagem com texto

Descrição gerada automaticamente Receção de email:

## Firewall

Uma Firewall é um dispositivo de segurança de rede que monitoriza e filtra tráfego de rede. É essencialmente uma barreira entre a Internet e a rede interna privada.

O principal objetivo de uma Firewall é permitir que tráfego “limpo” possa passar para a rede interna, enquanto tráfego que seja perigoso (vírus, malwares, etc.) não passem para a rede interna.

Existem vários tipos de Firewall. No nosso caso iremos utilizar a UFW (Uncomplicated Firewall).

Esta firewall permite definir políticas de segurança de rede criando limitações ou permissões para o acesso a diversos serviços ou aplicações.

### Instalação da UFW

Uma imagem com texto

Descrição gerada automaticamente Através do gestor de pacotes do nosso servidor Linux, podemos executar o comando “apt install ufw” para instalar a firewall.

 Começamos por garantir o acesso remoto ao servidor via SSH e ativar o registo de eventos.

 Finalmente, ativamos a firewall.

Uma imagem com texto

Descrição gerada automaticamente Se, por algum motivo, for necessário verificar o estado atual da firewall, podemos correr o seguinte comando:

# Conclusão

Ao longo deste semestre, obtivemos o conhecimento necessário para a instalação e configuração de um Servidor, quer no Windows, como no Debian.

Ficamos também a conhecer melhor como funciona o trabalho de um administrador de rede, assim como as técnicas de segurança que podem ser implementadas numa rede empresarial.

Assim, sentimo-nos preparados para qualquer tipo de situação que possa surgir no futuro que requeira conhecimentos na Administração de Redes.

# Bibliografia

**Não existem fontes no documento atual.**