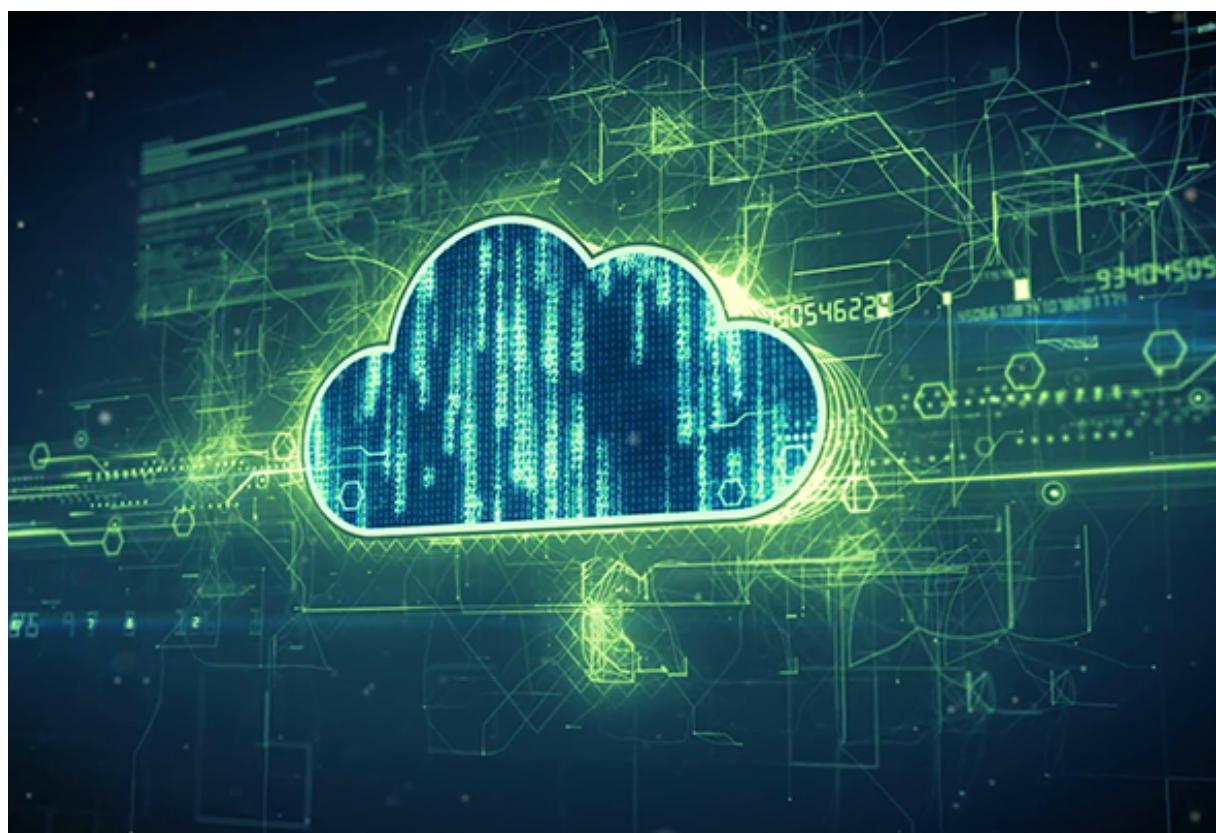


Guía Práctica para el uso profesional de la nube



Por Juan Carlos Pérez de la Torre

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>	 CERTIFIED IQNet <small>QUALITY SYSTEM</small>
Pág 2 de 106			2021/2022

Índice

1. Planificación del proyecto	3
2. Introducción	5
3. Datos generales del Proyecto	6
3.1. Título del proyecto	6
3.2. Descripción del proyecto	6
3.3. Necesidades a cubrir	6
3.4. Entorno Tecnológico del proyecto	6
3.5. Software	7
4. Descripción del proyecto	8
5. Definiciones Generales útiles	9
6. Desarrollo del Proyecto Integrado	16
6.1. Creación y configuración del sistema local base	16
6.2. Implementación cloud basada en la nube de AZURE	44
7. Pruebas	93
8. Conclusión final	95
9. Agradecimientos	97
10. Referencias web	98
10.1. Anexos previos	98
10.2. Anexos de la configuración base (6.1)	100
10.3. Anexos del Desarrollo enfocado a la nube (6.2)	104

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>	 CERTIFIED IQNet <small>QUALITY SYSTEM</small>
	Pág 3 de 106		2021/2022

1. Planificación del proyecto

Hito	Fecha de Entrega	Tareas incluidas en la entrega
0	30/03/2022	<i>Propuesta informal del proyecto</i>
1	8/04/2022 -	<i>Descripción detallada del proyecto con hitos</i>
		<i>Aprovisionamiento de fuentes y recursos</i>
2	25/04/2022	<i>Configuración de un sistema básico a imitación de un posible sistema empresarial profesional.</i>
3	16/05/2022	<i>Migración de los servicios a la nube</i>
4	6/06/2022	<i>Configuración y optimización de los servicios en la nube. Securización. Pruebas de fallos. Ataque y derribo para asegurar funcionamiento continuo. Prueba de tráfico.</i>
5	15/06/2022	<i>Entrega Final</i>

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 4 de 106		2021/2022

En este pequeño diagrama de Gantt se puede ver la planificación inicial del proyecto



 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 5 de 106		2021/2022

2. Introducción

Este proyecto nace del interés real y material de utilizar parte de las nuevas herramientas que los avances tecnológicos nos permiten para mejorar la situación de miles de empresas que dependen de terceros para gestionar sus datos. La idea primigenia era la creación de un entorno específico en la nube, exclusivo para el uso de una empresa con actividad real, es decir, adaptar para una empresa un entorno cloud para desarrollar su actividad, gestionada por ella misma, con un coste humano muy reducido y un coste de infraestructura igualmente bajo.

Esto que puede parecer muy práctico e incluso útil (esa es la idea), acaba siendo en realidad una tarea homérica, pues disponemos de una infinidad de herramientas para la solución de cualquier problema de cualquier empresa que podamos pensar. ¿Necesitamos IA? Todos los proveedores tienen una opción. ¿Necesitamos balanceo en nuestro sistema, creación de equipos para soportar más carga o integración continua? Todos los proveedores tienen una alternativa. ¿Necesita nuestra empresa servidores de datos seguros de uso continuo y rápido? ¿Por el contrario necesita quizás una base de datos de archivos “antiguos” y casi sin uso? La mayoría de proveedores ofrece alguna opción.

Esto y mucho más es posible. Como analogía para entenderlo, es como si partiesen de una caja de herramientas para arreglar un desperfecto hogareño y, al abrirla, tuviéramos desde los clavos más básicos, incluso herramientas que no esperamos/necesitamos, hasta encontrar los taladros más modernos, con funciones que ni siquiera pudiéramos soñar, todo solo al alargar el brazo.

Ante esta infinitud, y del intento de llevarlo al mundo práctico (y su imposibilidad), surge este proyecto final, una guía más general para el uso e implementación de servicios cloud.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 6 de 106			2021/2022

3. Datos generales del Proyecto

3.1. Título del proyecto

Guía práctica para uso profesional de la nube

3.2. Descripción del proyecto

Creación de un manual básico para la implementación de un servicio en la nube de manera práctica y económica, sirviendo de guía real para su uso profesional.

3.3. Necesidades a cubrir

Cada día la información, y sobre todo la gestión de ésta, es más importante. Empresas de todo el mundo se ven ante múltiples opciones muy costosas, tanto a nivel humano como a nivel de infraestructura. Ante este problema surge la nube pública como servicio, que gestiona los datos de manera más “user friendly” (no tan técnico) y también más barata en principio.

El problema es que no todas las empresas saben cómo utilizar los servicios o como replicar sus sistemas en la nube, a la misma vez que están faltos de conocimiento.

A este problema se plantea esta guía como solución.

3.4. Entorno Tecnológico del proyecto

Para este proyecto utilizamos fundamentalmente el entorno técnico cloud, la nube. Así como distintas aplicaciones para su uso más avanzado.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR IQNet CERTIFIED Quality System Empresa Registrada ER-0934 / 2008
Pág 7 de 106		2021/2022

3.5. Software

Azure

Docker

Opnsense/Pfsense/Snort

MariaDB, Apache

Versiones:

Pfsense CE- 2.6.0-Release

Snort 4.1.5_2 | Dependencia de Snort 2.9.19

Kali linux 2022.1

Ubuntu server 20.04.3

NMAP 7.92

Docker 20.10.14, build a224086

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 8 de 106		2021/2022

4. Descripción del proyecto

Para dotar de practicidad a este proyecto partiremos de un sistema ya creado. Este sistema que vamos a plantear se fundamenta en **una web** que llevará con un [gestor de contenidos \(Wordpress, Drupal, etc\)](#) que utilizaremos como tienda online, escaparate para nuestro comercio físico, blog, etc, según las necesidades de la empresa. En este caso, al ser el más utilizado^{4,5} utilizaremos **Wordpress**, por ser gratuito y [open-source](#), sin embargo existen alternativas open-source igual de válidas y competitivas como Drupal, que podemos instalar con la guia que aparece en su [página web](#)⁶. Además esta web necesita un lugar donde almacenar los datos que recojamos en nuestra página, para ello utilizaremos una **base de datos MariaDB**.

Así mismo, si pensamos almacenar datos sensibles, como pueden ser **datos bancarios** o localización, necesitamos otra [base de datos más segura](#). Para asegurar tanto nuestra web como esa base de datos más segura utilizaremos **un portero**, un software o hardware que actúe de firewall y de router, para que pueda controlar quién entra y bloquear el paso a quien sea sospechoso. Para esto existen muchas opciones, empresas como Cisco o Mikrotik producen equipos ya preparados para realizar esta función, pero son unos **equipos muy costosos**. Siguiendo la línea de la viabilidad económica y la practicidad, utilizaremos el software **Pfsense**, un software muy efectivo y eficiente, que puede ser instalado en equipos más humildes.

Una vez tenemos configurado de **manera funcional** nuestros servicios pasaremos a la configuración básica de la nube, de manera que una vez completada la mínima configuración podamos empezar con **la migración**. Esta migración pasará nuestros servicios de equipos físicos de nuestra empresa a la nube pública del proveedor que elijamos, ahorrando el coste humano y monetario de mantenimiento. La migración a una nube pública implica también **ciertos riesgos**, algunas empresas no se hacen cargo del resguardo de **datos sensibles** entre otros o lo aseguran a precios muy elevados, por ello mantendremos cierto equipamiento.

Nuestra prioridad en este paso es la capacidad de que **no se corte ningún servicio en ningún momento**, de modo que aunque las configuraciones nos llevasen tan solo cinco minutos o hasta diez horas, ningún cliente del mundo notase la diferencia.

Ya hemos configurado nuestro sistema, sentado las bases en la nube y migrado parte del servicio, así el punto final será optimizar y utilizar todos los servicios que nuestro proveedor cloud nos propone.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>
Pág 9 de 106		2021/2022

5. Definiciones Generales útiles

Cloud / Nube

La nube o cloud es un concepto que se refiere al uso de servidores remotos interconectados a través de internet. Estos servidores que parecen nubes para nosotros, son en realidad servidores físicos ubicados en centros de datos alrededor del mundo. Esto implica que para ejecutar algún programa o crear una web no es necesario comprar el equipamiento necesario para hacerlo, sino que se accede a la nube.

Sin embargo, existen muchos tipos de nubes lo que cambia el uso de la misma:

- **Nube privada:** Aquella que se dedica y mantiene exclusivamente una empresa u organización. Muchas empresas crean de manera interna una nube privada para gestionar datos, información y su flujo.
- **Nube pública:** Este tipo de nube es gestionada por un proveedor cloud externo, que gestiona muchas empresas y organizaciones. Estas empresas pueden compartir servidores en lo que se llaman “multitenancy” o “tenencia múltiple”. Este tipo de nube es el más conocido recientemente con propuestas como las de Microsoft Azure, Amazon Web Services o Google Cloud.
- **Nube híbrida:** Es aquella que combina los dos tipos anteriores de nube, incluyendo incluso servidores locales heredados. Las empresas de servicios suelen usar esta combinación de nubes para su actividad económica.

Aunque no es un tipo de nube otro concepto importante es el de **multinube**. Multinube o multicloud es un concepto que involucra más de un servicio de nube, por ejemplo el uso conjunto de la nube de Microsoft y la de Amazon, Azure y AWS. Elegir esta opción tiene diferentes razones, **flexibilidad, proximidad** a los usuarios, alta disponibilidad, **redundancia** que previene el fallo ante cortes de servicio, alta escalabilidad, etc.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 10 de 106			2021/2022

Cloud Provider/Proveedor de la nube

Los proveedores cloud son aquellas empresas que ofrecen ciertos servicios basados en la nube, ya sea infraestructura, almacenamiento, aplicativos, etc. Esta empresa mantiene el sistema, ahorrando dicho mantenimiento humano y físico al consumidor.



Además ofrecen ciertas características de cloud computing como son:

Infrastructure as a Service - IaaS

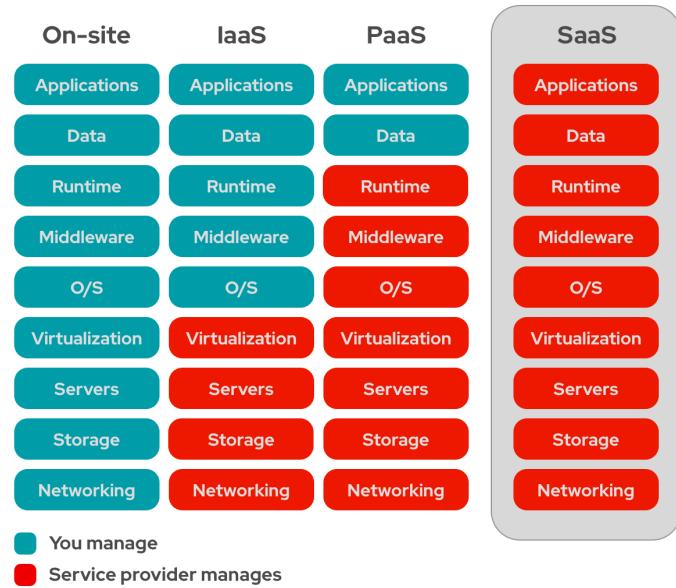
Con este servicio alquilas literalmente infraestructura tecnológica, es decir servidores, máquinas virtuales, redes, almacenamiento, etc fundamentándose en el “pay-as-you-go” o paga por consumo.

Platform as a Service - PaaS

Ideada para desarrolladores, este servicio asume la creación y mantenimiento de la infraestructura necesaria para el desarrollo de aplicaciones o webs sin preocupaciones sobre los servidores, redes, etc.

Software as a Service - SaaS

Con este servicio se contrata directamente una aplicación, sin administración ni de la infraestructura ni del software que mantiene el sistema, como mejoras y actualizaciones de seguridad, accediendo al mismo a través de internet.



Los proveedores mayoritarios además ofrecen servicios relacionados con Inteligencia Artificial y Machine Learning, actualizados a los últimos avances del mundo de la tecnología.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 11 de 106</i>			2021/2022

Gestor de contenidos o CMS

Un gestor de contenidos o Content Management System (CMS por sus siglas en inglés) es una herramienta que permite crear, modificar y administrar contenido en una página web personalizable sin necesidad de escribir código alguno.

Sin un CMS, a la hora de querer crear una página web deberíamos escribir el código HTML a mano, para terminar con una web estática.

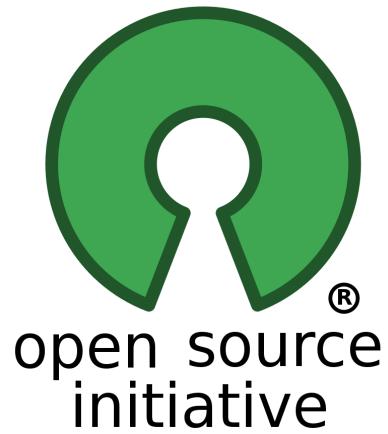
Algunos ejemplos de CMS muy populares se pueden ver en la imagen; Wordpress, Drupal, Joomla,etc



Open-source

Un software open-source o de código abierto es aquel en el que el código fuente que estructura el software y algunos derechos se hacen públicos bajo licencias de código abierto (de uso público).

A diferencia del software general (privativo) que conocemos, cualquiera puede copiar el código, aprender, alterarlo y compartirlo. Ejemplos de esto son el tipo de licencia GNU (usado por Linux) o programas cotidianos como LibreOffice.



 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 12 de 106</i>			<i>2021/2022</i>

Base de datos

Una base de datos es una herramienta que organiza datos estructurados que son administrados por un sistema gestor (de base de datos, DBMS por sus siglas en inglés). Estos datos se estructuran con el lenguaje estandarizado de base de datos SQL (Structured Query Language), y actualmente existen dos tipos de BBDD o DB (por si siglas en inglés DataBase), estos son:



- Relacionales (**SQL**)
- No-Relacionales (**No-SQL**)

Grandes empresas utilizan ambos tipos, siendo los NoSQL más conocidos: MongoDB, Redis o Cassandra . Sin embargo los más utilizados en general siguen siendo SQL, como por ejemplo MySQL, MariaDB o PostgreSQL, ampliamente utilizados hasta en las empresas que utilizan NoSQL para otros datos. En este proyecto nos centraremos en las DB SQL.

DNS

Un DNS o Domain Name Server (por sus siglas en inglés) es un sistema que traduce los nombres de los dominios a direcciones IP.



Cada dispositivo conectado a internet tiene una dirección numérica con la que se accede, y es accedido, a internet. El DNS se encarga de que no tengamos que recordar números para navegar, traduce nuestras letras a los números que manejan los sistemas para poder navegar.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 13 de 106</i>	<i>2021/2022</i>		

IDS/IPS

IDS (Sistema de Detección de Intrusión, o Intrusion Detection System por sus siglas en inglés) es ,por sus propias siglas, un sistema de detección ante intrusiones, usado para detectar accesos no reconocidos. Estos sistemas son solo de monitorización, al recibir un acceso no autorizado se emite una alerta para que el administrador actúe, es decir, no impide un posible ataque, solo avisa.

IPS (Sistema de Prevención de Intrusión, o Intrusion Prevention System por sus siglas en inglés) es un sistema de defensa ante ataques e intrusiones. Este sistema, al contrario que el IDS, toma un rol activo, controlando el acceso a red basándose en la monitorización. Este sistema no solo genera alertas sino que puede bloquear conexiones y paquetes a la red.

IDS vs IPS

Whats the Difference & Why You Need them!



PFSENSE

Pfsense es, según su propia web, un software que incluye características de las mejores y más caras soluciones de firewall.

Está basado en el sistema operativo FreeBSD y es una distribución de firewall de red, que incluye distintas funcionalidades de terceros.



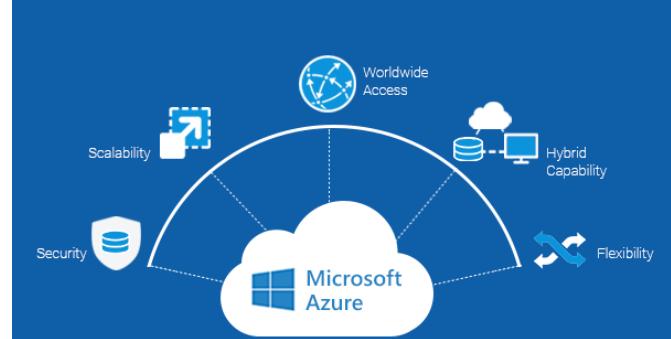
Su uso más común es usarlo como servidor DHCP y/o DNS, punto de acceso Wifi, servidor VPN, IDS/IPS y firewall. La instalación de paquetes de terceros, como Snort o Squid le dan a esta herramienta mucha más personalización y utilidad. Dado que es un software muy usado, su uso comercial/empresarial es cobrado y existe una migración a OpenSense que es similar.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 14 de 106			2021/2022

AZURE

Según su página Azure es “una plataforma en la nube con más de 200 productos y servicios en la nube diseñado para ayudarte a traer soluciones a la vida”.

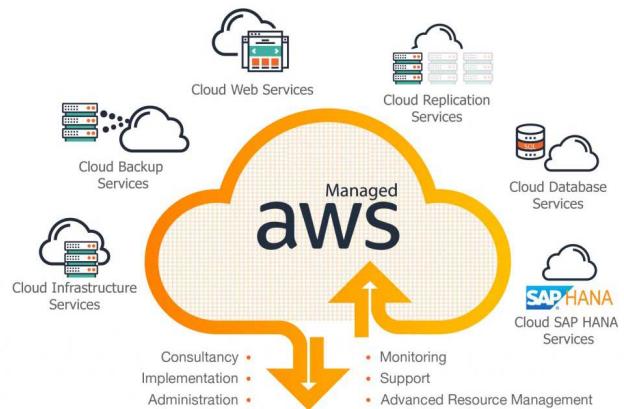
Microsoft Azure, conocido como Windows Azure o Azure, es la propuesta de Microsoft para la computación en la nube (cloud computing). Ofrece servicios IaaS, PaaS, SaaS, así como máquinas virtuales, almacenamiento, red y mucho más. Es conocido por sus avances en servicios de IA y IoT. Recientemente han desarrollado un servicio llamado **Azure Orbital** que plantea mover los innumerables datos recogidos por los satélites directamente a la nube, para procesarlos con mayor capacidad y velocidad. Esto ayuda al procesamiento y análisis de la información.



AWS

Según su página AWS es “la plataforma en la nube más adoptada y completa del mundo”. Quizás esta afirmación puede ser un poco exagerada, pero desde luego sí que es una plataforma en la nube muy usada y que ofrece una amplia gama de servicios.

Es un servicio de nube ofrecido por Amazon que ofrece desde IaaS, PaaS, SaaS combinado con distintas tecnologías nuevas, bases de datos y almacenamiento.



 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 15 de 106			2021/2022

Backup

Un respaldo o reserva (del inglés) es un guardado de datos con el objetivo de mantener dichos datos en caso de pérdida o destrucción de los datos originales.

El caso práctico más común sería el guardado de fotos en Google Drive, donde perdiéndose el dispositivo las fotos seguirán guardadas.



ISP

Un Proveedor de servicios de internet (Internet Service Provider) es una empresa que provee de internet a sus clientes. En el caso doméstico un ISP es aquella empresa que permite que tengas conexión a internet.

En España los más extendidos y populares son Telefónica, Vodafone y Orange



 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 16 de 106		2021/2022

6. Desarrollo del Proyecto Integrado

6.1. Creación y configuración del sistema local base

Para implementar nuestro sistema en la nube, y hacerlo de manera más realista y práctica, como ya hemos visto debemos diseñar primero nuestro sistema en sí.

Partimos de un sistema “simple” para que pueda ser aplicable, pero a la misma vez necesitamos un sistema potente que pueda aprovechar las herramientas de la nube y realizar multitud de tareas. De este ideal hemos creado el siguiente esquema:

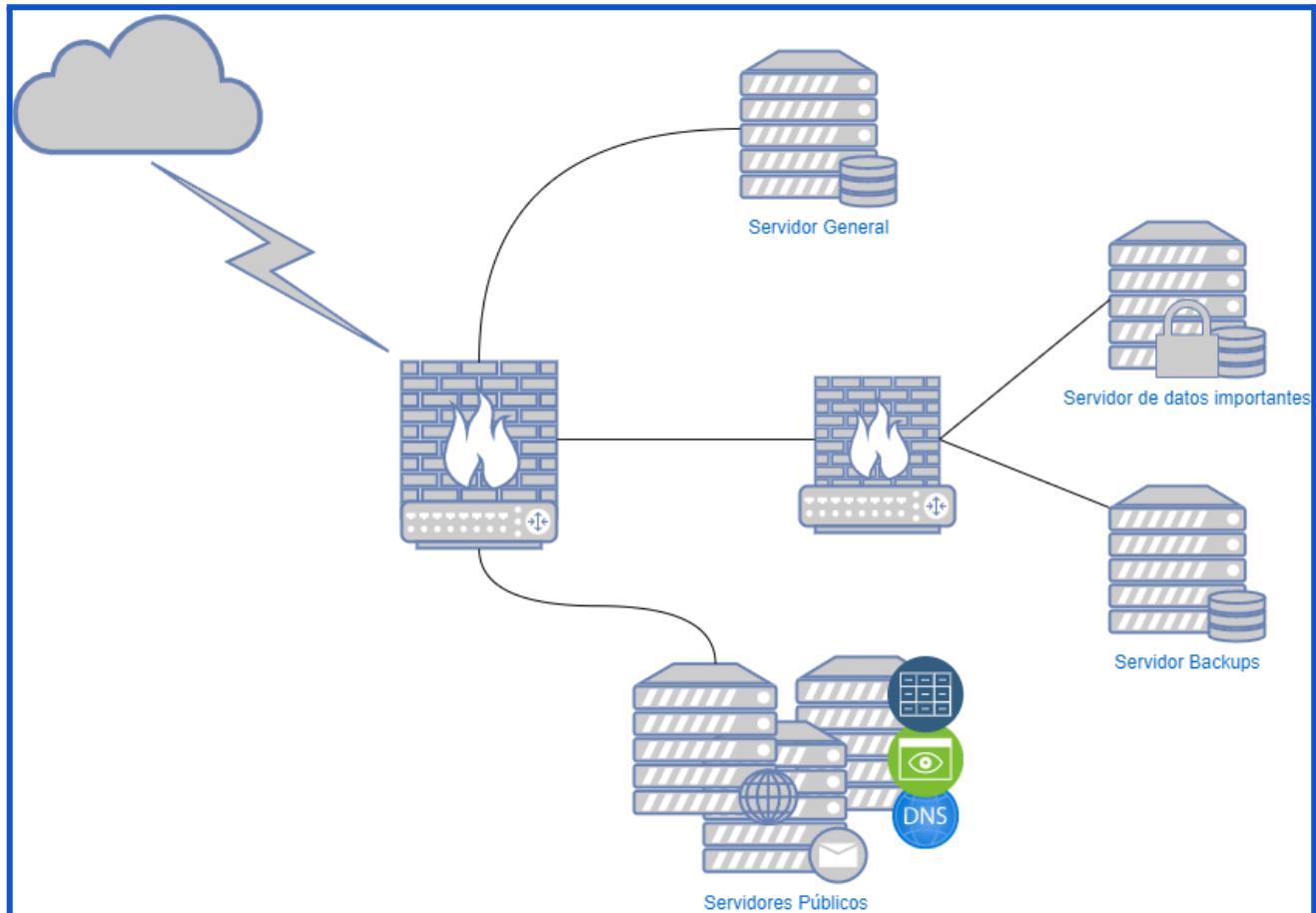


Figura 1. Esquema lógico.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 17 de 106		2021/2022

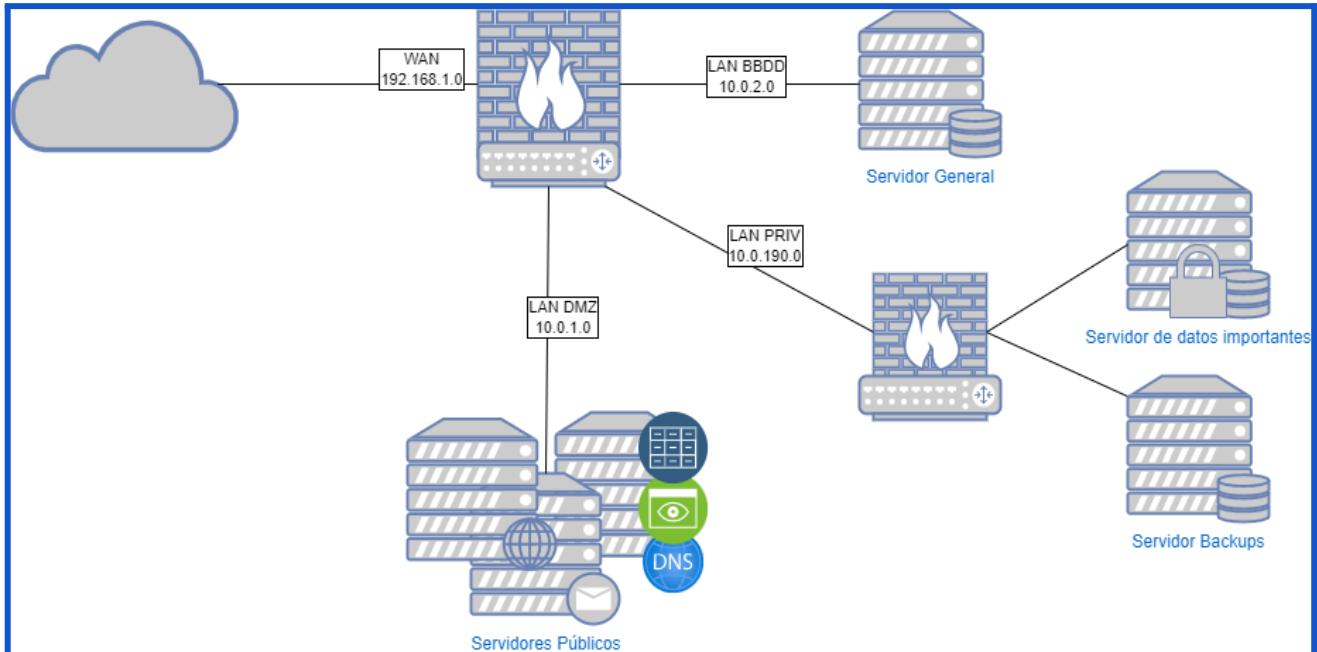


Figura 2, Esquema de red.

Tras tener el diseño base de nuestro servicio, toca ponerse manos a la obra y empezar la instalación y configuración del mismo.

A semejanza de nuestro esquema, empezaremos con la instalación de la primera puerta, lo que en nuestra red es “[Pfsense](#)”, que con la configuración correcta es uno de los mejores sistemas para proteger y asegurar nuestra red.

Una vez lo tenemos ya descargado e introducido en nuestra máquina podemos proceder con la instalación.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR CERTIFIED IQNet Quality System Empresa Registrada ER-0934 / 2008
Pág 18 de 106		2021/2022

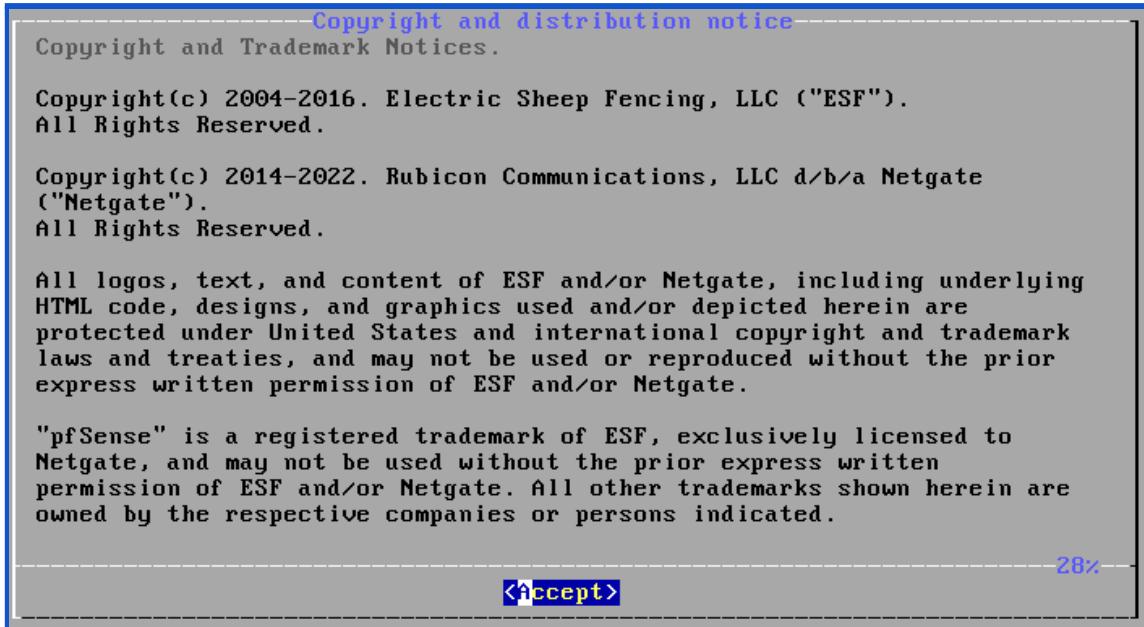


Figura 3. Pantalla instalación Pfsense.

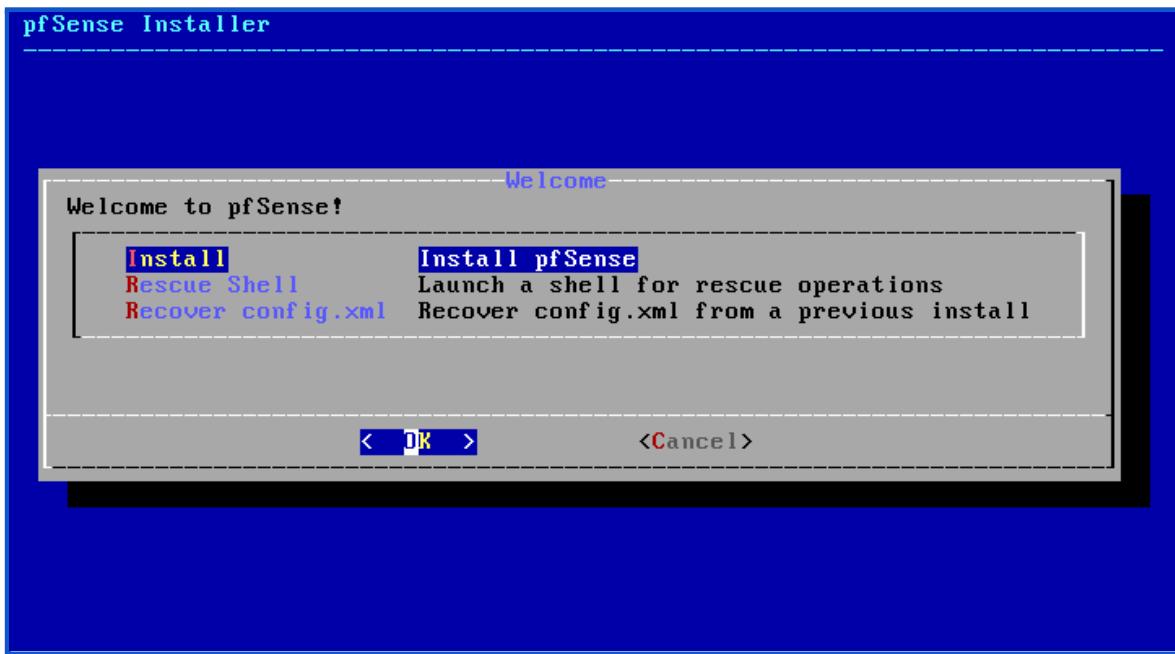


Figura 4. Pantalla instalación Pfsense.Opciones.

Una vez hemos aceptado podemos ver que se nos brinda tres opciones, dos de ellas a modo de recuperación (semejante al recovery mode de Windows). Como estamos instalando, continuamos.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 19 de 106		2021/2022

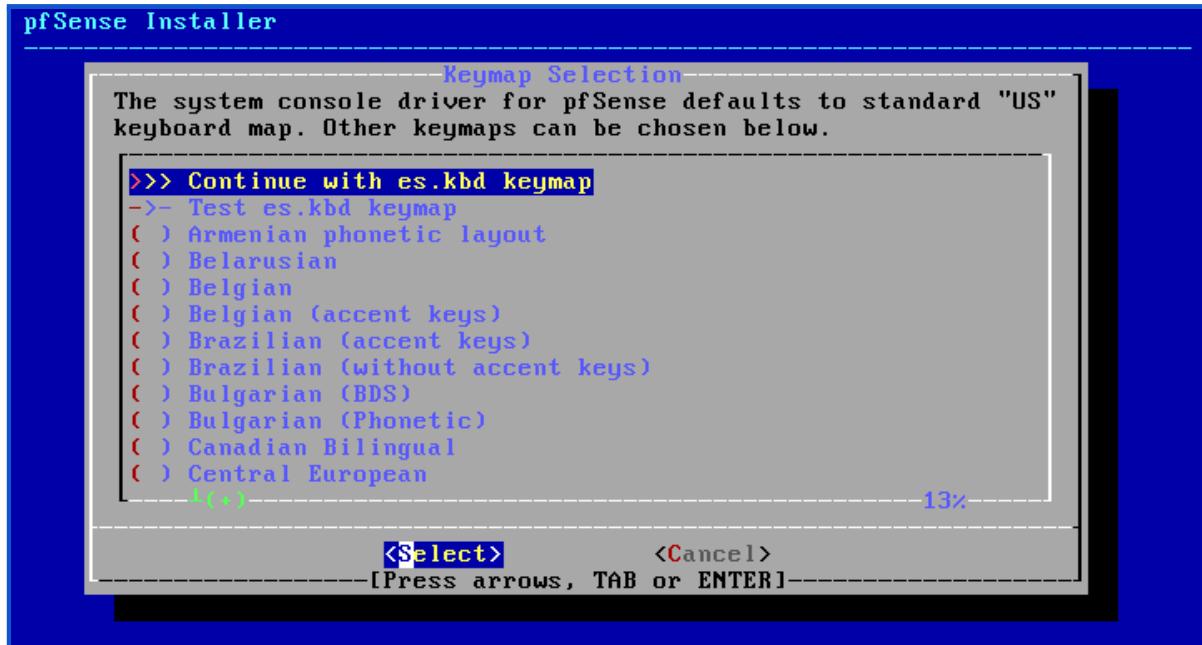


Figura 5. Pantalla instalación PfSense. Configuración del teclado.

Tras esto la consola de instalación nos requerirá el tipo de teclado que aceptará. Es importante ajustarlo ya que del teclado americano al español los símbolos especiales cambian su posición, lo que dificulta la navegación.

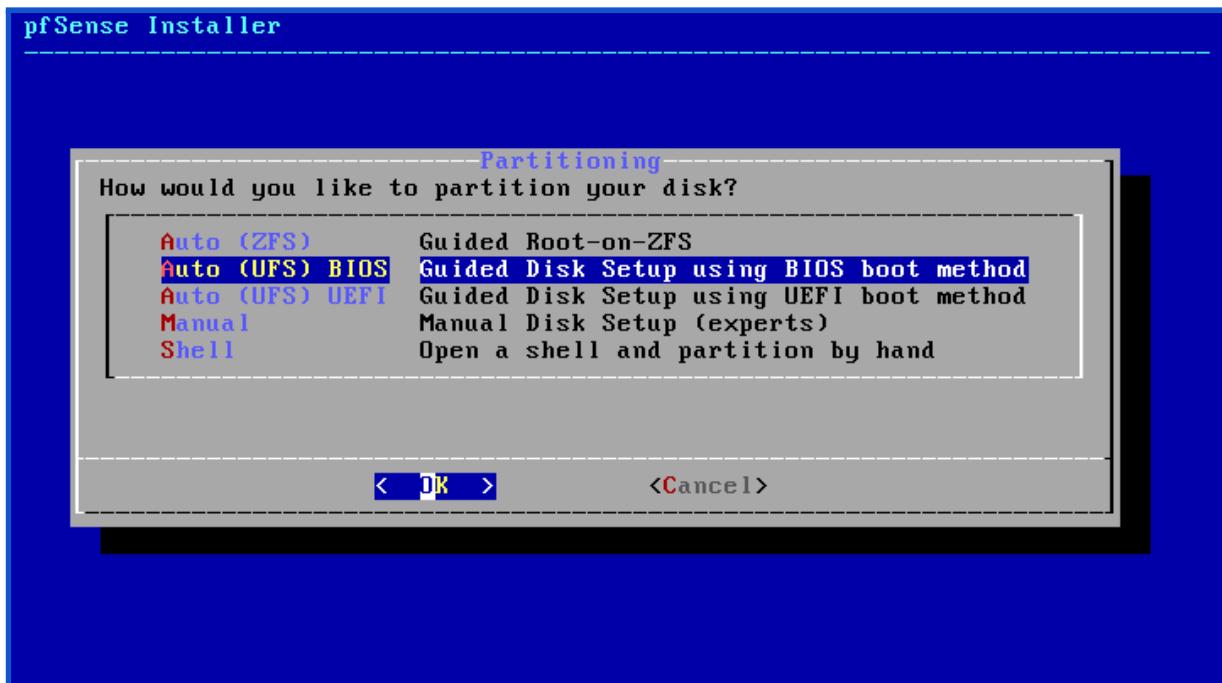


Figura 6. Pantalla instalación PfSense. Particiones del disco.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 20 de 106		2021/2022

Llegados a esta instalación se nos ofrecen distintos métodos de particiones.

“ZFS es más seguro y tiene más características que UFS, sin embargo ZFS puede ser ‘un comilón de memoria’... Pero si el uso de la RAM es crítico (...) UFS es una opción más conservadora” ([Anexo 8.2](#)).

Teniendo libre elección, y continuando en la idea de realizar un plan lo más económico (y por lo tanto real) posible, en este caso vamos a optar por **Auto (UFS) BIOS**.

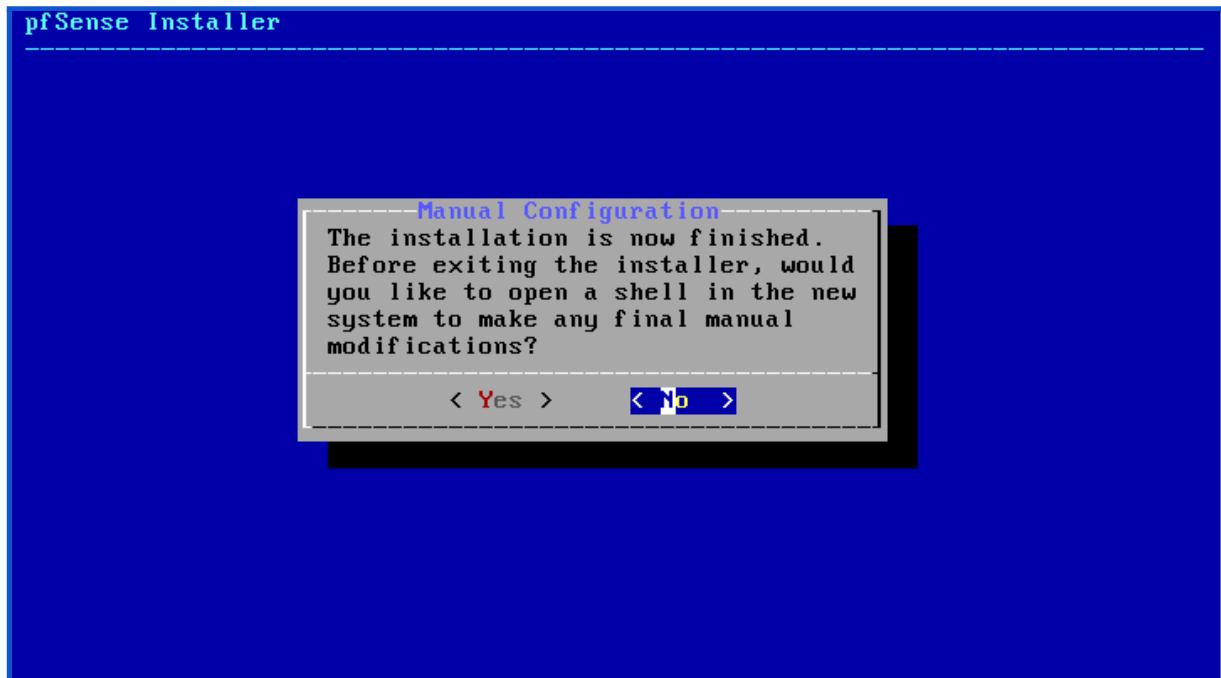


Figura 7. Pantalla instalación PfSense. Configuración adicional.

Tras completarlo todo nos dirá que la instalación ha terminado, y en caso de querer realizar alguna modificación más seleccionar “YES”. En nuestro caso, las configuraciones iniciales están terminadas y continuaremos.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>	 <small>CERTIFIED</small> IQNet <small>QUALITY SYSTEM</small>
Pág 21 de 106			2021/2022



Figura 8. Pantalla instalación PfSense. Reinicio.

Tras esto podemos reiniciar y comenzar a usar nuestro [Pfsense](#).

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: b78e8ee191e4d1c3bc84

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.16/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 

```

Figura 9. Inicio Pfsense.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet CERTIFIED Quality System ER-0934 / 2008
Pág 22 de 106		2021/2022

Como podemos comprobar en las redes asignadas, no tiene las IPs que nosotros hemos diseñado:

```

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.16/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
  
```

Figura 10. Redes PfSense.

Para ello, y siguiendo el menú elegiremos la opción 2:

```

8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
  
```

Figura 11. Configuración redes PfSense.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>
Pág 23 de 106		2021/2022

```

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.1.10
Enter the end address of the IPv4 client address range: 10.0.1.200
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 LAN address has been set to 10.0.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
  https://10.0.1.1/

Press <ENTER> to continue.■

```

Figura 12. IPV4 configurado en Pfsense.

Pfsense tiene una característica curiosa, protectora a la vez que molesta. Aunque tengamos la máquina dentro de nuestra red, accediendo a internet como nosotros, para que se pueda acceder desde internet a la interfaz gráfica debemos conectarnos a una red interna y entonces realizar las configuraciones necesarias para que esto sea así.

Es justo por esto en que la *Figura 12* hemos configurado el DHCP para el puerto interno desde .10 al .200, para que al conectar nuestra nueva máquina para configurar, sea capaz de reconocerlo de su red.

Para hacer esto, y dado que tras las configuraciones haremos las pruebas de seguridad pertinente, vamos a tomar una máquina con *Kali Linux*, aunque nos sirve cualquier máquina que podamos conectar a la red interna de nuestro Pfsense para habilitar la configuración externa (solo al principio y por facilidad).

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IoNet QUALITY SYSTEM
Pág 24 de 106			2021/2022

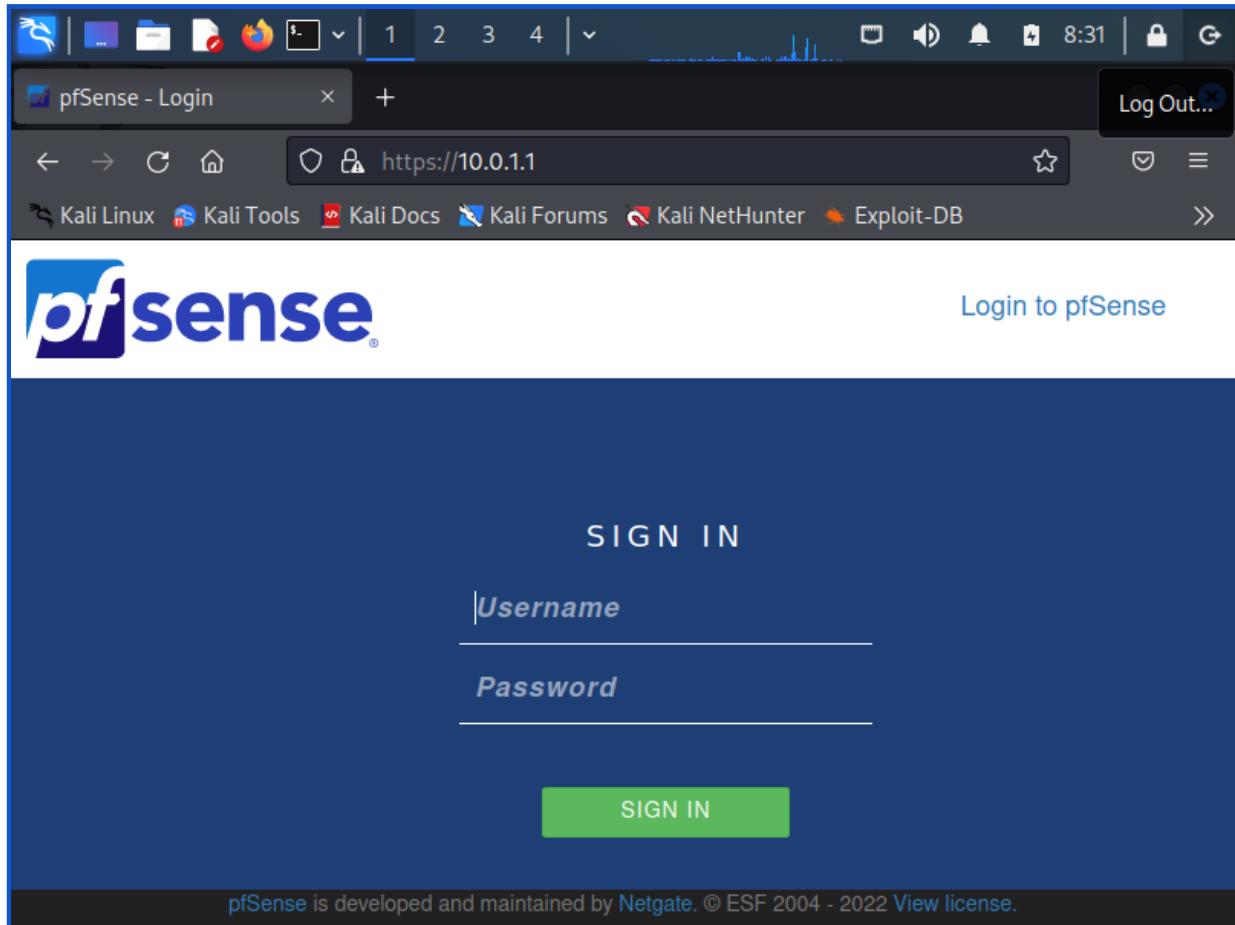


Figura 13. PfSense.

Como podemos comprobar ya tenemos acceso a la interfaz gráfica de configuración de nuestro [Pfsense](#). Aquí deberemos loguearnos por primera vez con las [credenciales predeterminadas](#).

Lo recomendable (y faro de esta guía) es cambiar las configuraciones básicas explotables. Por ejemplo el usuario y contraseña de admin, cosa que nada más entrar ya nos recomiendan:

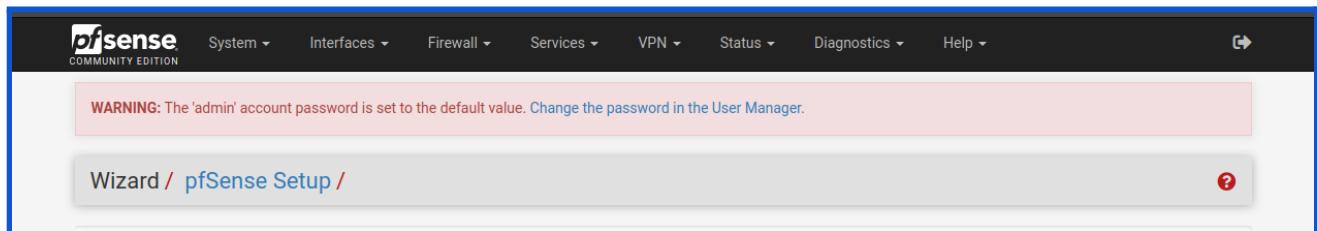


Figura 14. PfSense recomendación.

 I.E. Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 25 de 106		2021/2022

Para la autenticación y autorización existen muchas opciones dentro de la herramienta. Incluso para las contraseñas existen gestores muy conocidos a nivel empresarial como “LastPass”. En este caso, dado que es un campo de pruebas, no vamos a usar ninguno de esos sistemas y vamos a guardar las contraseñas a la vieja usanza, con frases nemotécnicas y papel.

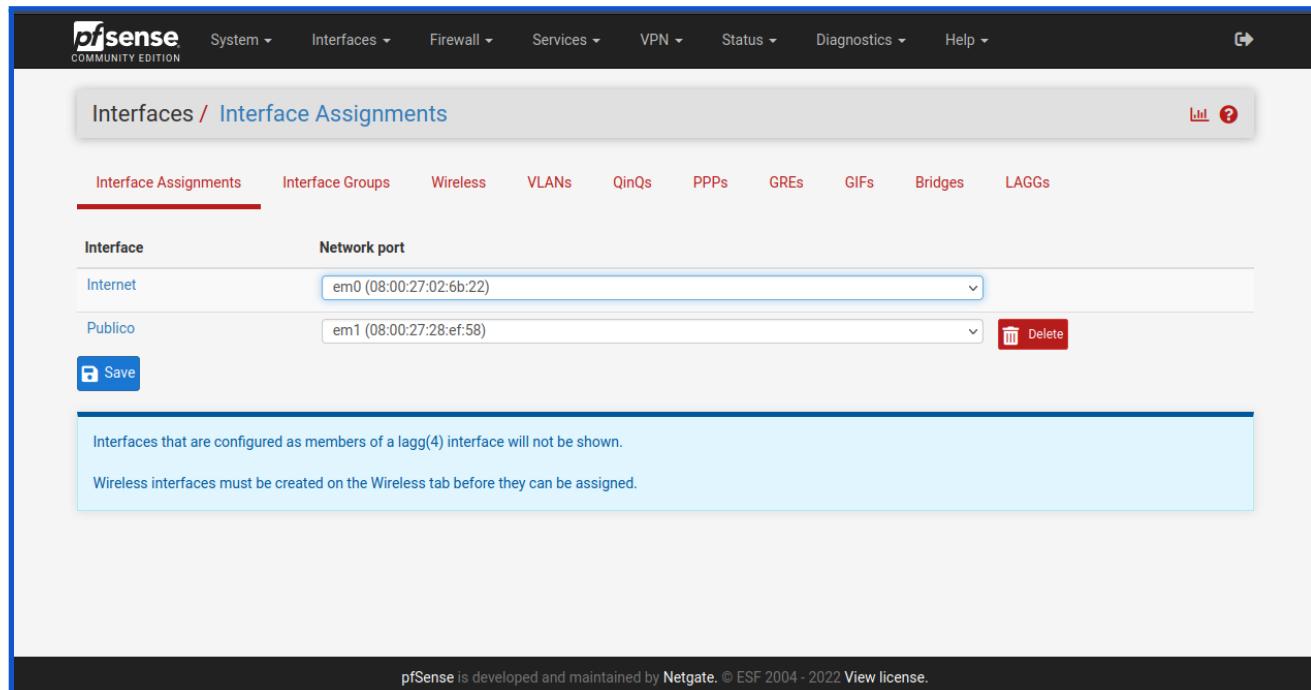


Figura 15. PfSense interfaces.

Ya dentro podemos ver las interfaces que hemos configurado por consola (WAN y LAN) y podemos modificarlas, renombrarlas y customizarlas todo lo que podamos pensar. Por facilidad llamamos a los puertos tal y como está puesto en el esquema de red ([Ver Figura 2](#)).

Antes de continuar con la configuración de los servidores públicos vamos a securizar nuestro PfSense con las herramientas que nos brinda. En la documentación oficial⁹ hay un apartado donde se comenta cuál es la mejor opción para restringir el tráfico, si bloquear(block) o rechazar(reject):

“...Aun así recomendamos usar “block” en las reglas para WAN. Hay cierto valor en no entregar activamente información a atacantes potenciales, y es una mala práctica responder automáticamente a todas las request externas (...) Para las reglas de interfaces internas si recomendamos usar “reject” en la mayoría de casos” ([Anexo 8.2](#))



The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0 /801 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0 /1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/> X 0 /0 B	IPv4+6	*	*	*	*	*	none		Bloquear todas las conexiones desconocidas	

Actions: Add Add Delete Save Separator

Figura 16. Reglas Firewall.

Así mismo las reglas siguen el patrón secuencial de Iptables, por ello en la Figura 16 hemos añadido a las 2 configuraciones básicas, una que deniegue TODO el tráfico que no tengamos previamente permitido. De manera que, al menos hasta la configuración total del sistema, no podamos tener fugas o problemas mientras habilitamos nuestros servidores.

Antes de poder configurar, bloquear o permitir más tráfico pasaremos a la configuración de nuestros servidores. Como vamos a empezar a bloquear todo el tráfico y a asegurar nuestro sistema, vamos a darle una ip estática a nuestro pc de administración que estamos usando para configurar todo el sistema:

DHCP Static Mappings for this Interface (total: 1)				
Static ARP	MAC address	IP address	Hostname	Description
	08:00:27:40:57:bd	10.0.1.5		pc admin

+ Add

Figura 17. DHCP estático para admin.

Una vez configurada nuestra IP fuera del rango de DHCP permitido, vamos a configurar nuestro servidor web, de correo, [DNS](#)...

¡Efectivamente vamos a usar Docker! Para aprovechar al máximo nuestros recursos vamos a instalar en un mismo servidor varios servicios, asumiendo que en nuestro caso la empresa local (todavía no exportada a la nube) no va a tener tanto tráfico. En caso de que así fuera,

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 27 de 106			2021/2022

recomendamos dedicar a cada servicio su propio servidor si así lo demanda su uso (en principio el DNS de la empresa no será tan usado como el servidor web).

Sobre un Ubuntu Server, instalaremos un servidor de SSH, para poder conectarnos a configurar nuestro servidor, y Docker, para poder desplegar todos los servicios que queramos instalar. ([Ambas guías en el Anexo 8.2](#)).

A modo de buenas prácticas cambiaremos el puerto por defecto se “ssh” y bloquearemos cualquier dirección externa que intente acceder al puerto 22(ssh) y al que hayamos cambiado, igualmente aplicaremos la siguiente configuración:

Port 55055

Con esta opción cambiamos el puerto por defecto para nuestro servicio. Los servicios de escaneo se realizan de manera secuencial hasta el 65536. De esta manera poniendo el servicio en un puerto alto dificultamos un poco a los posibles atacantes.

LogLevel VERBOSE

Con la opción VERBOSE incluimos muchas más información de las conexiones ssh que se hagan a nuestro servidor

LoginGraceTime 30

Esta opción reduce el tiempo permitido para introducir la contraseña. Los usuarios permitidos no necesitarán 2 horas.

PermitRootLogin no

Esta opción se explica sola, no queremos que nadie entre con permisos de root a nuestro servidor y acabemos sin servicios.

StrictModes yes

Esta opción protege a los archivos de ser modificados sin sus permisos correspondientes.

MaxAuthTries 3

MaxSessions 1

Con estas opciones restringimos primero el número de intentos antes de que el servidor te bloquee por intentarlo demasiado, y la cantidad de usuarios que pueden estar conectados a la misma vez al servidor. En este caso solo hay 1 admin/developer/cloud architect así que con una sesión es suficiente.

PermitEmptyPasswords no

Otro problema que encuentra ssh es la explotación de contraseñas vacías, así como una posible inundación del servidor, por eso es recomendable no permitirlo.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 28 de 106			2021/2022

AllowTcpForwarding no

X11Forwarding no

Para securizar más nuestro servicio bloquearemos el forwarding de los puertos, lo que puede bloquear otros servicios.

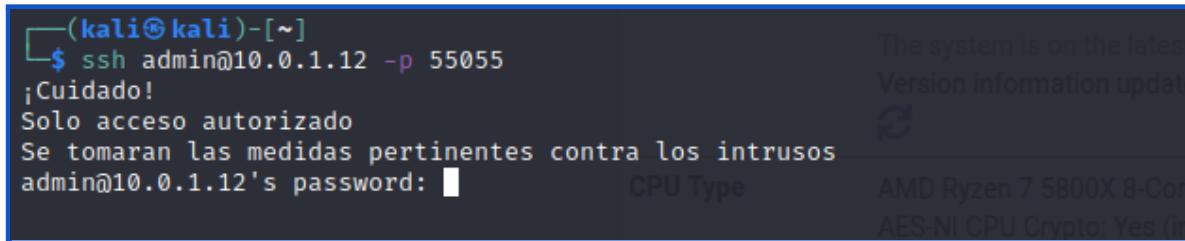
PrintLastLog no

PrintMotd yes

Banner /etc/motd.net

Con estas opciones primero NO mostramos información de la última conexión, reduciendo superficie explotable, a la misma vez que mostramos un mensaje de advertencia (guardado en la ruta) para ahuyentar posibles atacantes más precavidos.

Existen más maneras de securizar las conexiones, por ejemplo, podríamos hacer uso del doble factor de autenticación (**2FA**) de Google con el módulo libpam-google-authenticator, podríamos instalar el servicio fail2ban directamente en el servidor para banear aquellas IPs que, por ejemplo intenten un escaneo de nuestros puertos, otra, que sí usaremos en la nube, es el uso de claves criptográficas, que se realiza casi de manera obligatoria por su seguridad.

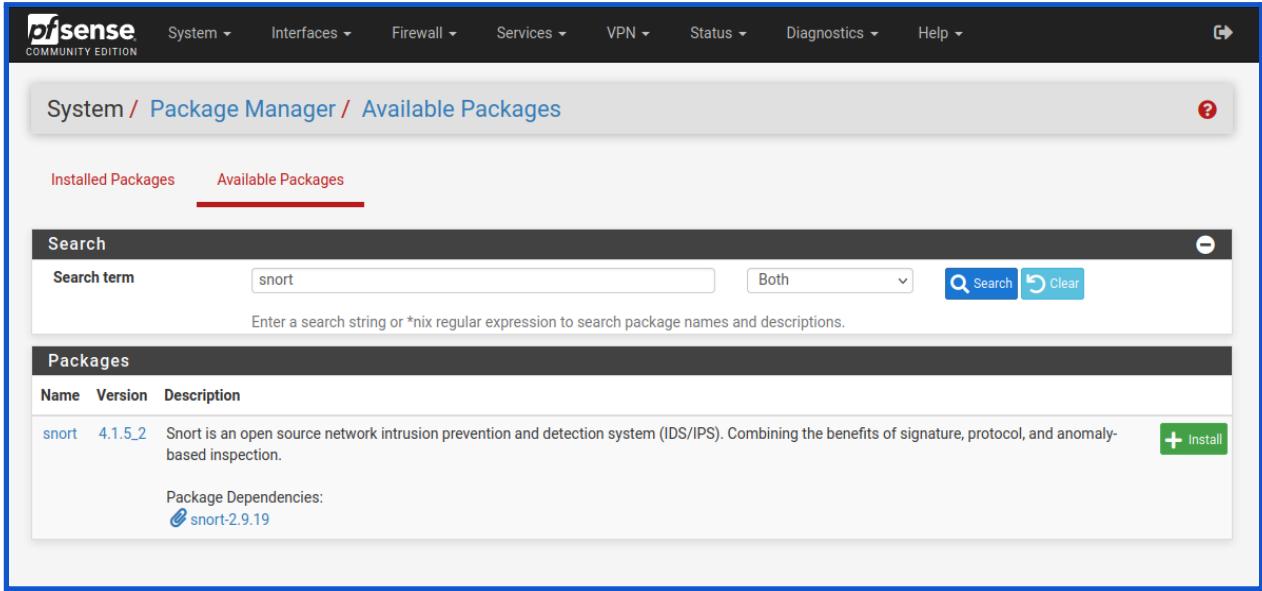


```
(kali㉿kali)-[~]
└─$ ssh admin@10.0.1.12 -p 55055
¡Cuidado!
Solo acceso autorizado
Se tomaran las medidas pertinentes contra los intrusos
admin@10.0.1.12's password: [REDACTED] CPU Type
The system is on the latest
Version information updat
AMD Ryzen 7 5800X 8-Core
AES-NI CPU Crypto Yes
```

Figura 18. SSH configurado.

Con esto tendríamos configurado completamente el acceso por ssh a nuestro servidor web, pero antes de continuar, y queriendo ser prevenido, vamos a instalar SNORT en nuestro pfSense.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IoNet QUALITY SYSTEM
Pág 29 de 106			2021/2022



The screenshot shows the pfSense Package Manager interface. At the top, there are tabs for 'Installed Packages' and 'Available Packages', with 'Available Packages' being the active tab. Below the tabs is a search bar with 'Search term' set to 'snort', a dropdown for 'Both', and buttons for 'Search' and 'Clear'. The main area is titled 'Packages' and lists the 'snort' package. The table includes columns for Name, Version, and Description. The 'snort' entry shows version 4.1.5_2 with the description: 'Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.' To the right of the description is a green '+ Install' button.

Figura 19. Snort en pfSense.

Como podemos ver solo debemos ir a la configuración del sistema, y en Package Manager buscamos el plugin que queramos instalar. Hay cientos compatibles, pero nosotros solo queremos un grado más de seguridad en la que va a ser nuestra puerta al exterior.

Una vez instalado nos da las pautas para configurarlo, en la página oficial (<https://www.snort.org/documents>). En este caso, como es un proyecto de estudio no vamos a aplicar una configuración muy complicada, habilitaremos el uso de Snort en la interfaz “Internet”, lo que sería nuestra WAN, de cierta manera es poner un vigilante en nuestra puerta para reducir la posibilidad de colarse. Así mismo vamos a habilitar el logeo de las actividades que pueda haber, para que desde los archivos podamos comprobar más datos en caso de intrusión. Aun así en los anexos dejaré más información para asegurar más y mejor la puerta de nuestro negocio.

Una vez tenemos el servicio SSH securizado y vigilada nuestra puerta pasaremos a la instalación de nuestros servicios en los containers de Docker. Para ello usaremos una adaptación de [Docker Compose](#)²³, quedaría tal que así:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 30 de 106		2021/2022

version: "3"

```

services:
  wordpress:
    image: wordpress:latest
    volumes:
      - wordpress_data:/var/www/html/wordpress
    ports:
      - "80:80"
    restart: always
    depends_on:
      - db
    environment:
      WORDPRESS_DB_HOST: db:3306
      WORDPRESS_DB_USER: admin
      WORDPRESS_DB_PASSWORD: admin
      WORDPRESS_DB_NAME: wordb
    container_name: wordpress
# →
  db:
    image: mariadb:latest
    volumes:
      - db_data:/var/lib/mysql
      # - /home/admin/mysql:/var/lib/mysqlsec
      #command: sh -cx
      "/var/lib/mysqlsec/mysql_secure.sh"
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: wordpressadmin
      MYSQL_DATABASE: wordb
      MYSQL_USER: admin
      MYSQL_PASSWORD: admin
    container_name: db_wordpress
  volumes:
    db_data:
    wordpress_data:

```

Con esta configuración básica estamos creando un contenedor que tenga wordpress y una [base de datos](#) para gestionarlo, con sus configuraciones correspondientes, y todo en un solo archivo. Con esto ejecutamos “docker compose up -d” ([previa instalación](#))²⁰ y levantara nuestro servicio “detached”, es decir, en segundo plano.

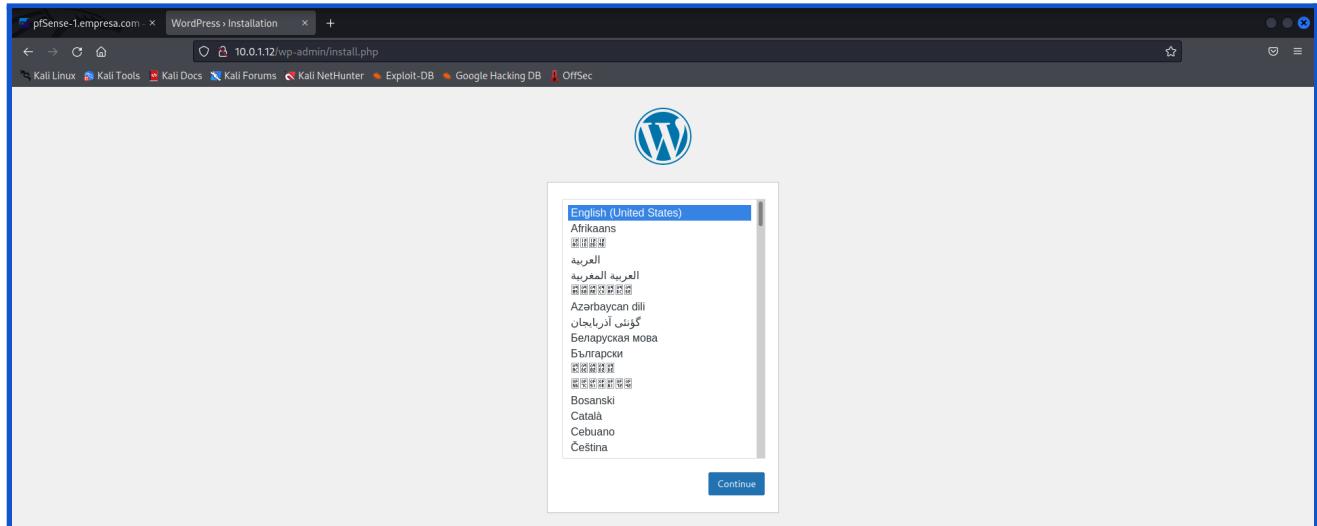


Figura 20. Wordpress tras docker compose.

Sin embargo esta configuración básica nos plantea un problema, la instalación base de mariadb/mysql trae consigo la creación de bases de datos y usuarios de prueba, que podrían

 I.E. Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 31 de 106</i>			<i>2021/2022</i>

plantear un riesgo de seguridad. Ante este problema surge la obligación, o al menos **recomendación**, de que se realice la instalación segura (`mysql_secure_installation`).

Para esto vamos a realizar una [adaptación⁷¹](#) de un [script⁷⁰](#) que correrá la instalación de `mysql_secure_installation` para reducir problemas, las modificaciones están diseñadas para nuestro entorno y para un funcionamiento correcto; siguiendo la estructura de la instalación, corrige lo siguiente:

```
# Set the root password
→Y (si), wordpressadmin
# Remove anonymous users
→ Y
# Disallow remote root login
→ Y
# Remove test database
→ Y
# Reload privilege tables
→ Y
```

Para la aplicación de este script tenemos dos opciones, o pegarlo entero en nuestro Docker-compose y relanzarlo con su nuevo añadido, o crear un Dockerfile, igual que nuestro Docker-compose, pero que llame al script y lo ejecute. La primera opción es realmente limpia y, aunque nos dejaría un compose algo más largo, quedaría acotado solo a un archivo. Por otra parte la realización con el Dockerfile, aunque muy práctica requiere que mantengamos un archivo del script para buscarlo y ejecutarlo (o integrarlo como en el compose, pero estaríamos iguales), el archivo de nuestro Dockerfile, y finalmente el Docker-compose que traiga a la vida (a nuestro navegador web en específico) todo nuestro servicio.

En este caso vamos a optar por la primera opción

Para securizar el servicio de [base de datos](#) (db) vamos a entrar en nuestro contenedor e instalar la securización de mysql:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 32 de 106		2021/2022

```

admin@server:~$ docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
44797e79e353        wordpress:latest   "docker-entrypoint.s..."   14 minutes ago    Up 14 minutes
c46cc2271eb7        mariadb:latest     "docker-entrypoint.s..."   14 minutes ago    Up 14 minutes
admin@server:~$ docker exec -it db_wordpress bash
root@c46cc2271eb7:/# mysql_secure_installation -u root --password=wordpress

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

Enable unix_socket authentication? [Y/n] n
... skipping.

Set root password? [Y/n] n
... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database ...
... Success!
- Removing privileges on test database ...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

```

Figura 21. Instalación segura de Mysql.

Tras esto continuamos con la vinculación de nuestra [base de datos](#) a local, es decir, que no se pueda acceder desde fuera de nuestro servidor. Para esto buscaremos en `/etc/` ya sea el archivo `my.cnf` directamente o la carpeta de nuestra base de datos donde se encuentre. Una vez aquí añadiremos a los parámetros de la db (mariadb/mysql) al final la línea “`bind-address = 127.0.0.1`”, que es la dirección de loopback.

Otro parámetro que debemos añadir es la línea “`local-infile = 0`”, que:

“Lee filas desde un archivo de texto a una tabla de una base de datos a una velocidad muy rápida.”³⁰ ([Anexo 8.2](#))
 Justo en el mismo enlace facilitado arriba, los propios desarrolladores de mariadb, recomiendan:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 33 de 106			2021/2022

Description

LOAD DATA INFILE is unsafe for statement-based replication.

Figura 22. Recomendación mariadb.

Otra recomendación de seguridad muy recomendable es cambiar el puerto de los servicios que ya son conocidos, igual que hemos hecho con el servicio SSH. En este caso para mantener de manera sencilla nuestro archivo de docker-compose no vamos a cambiarlo, pero desde luego mantenemos la recomendación. Al archivo de configuración de nuestra db, el archivo my.cnf, añadiremos “Port 32343”(Si queremos usar el puerto 32343).

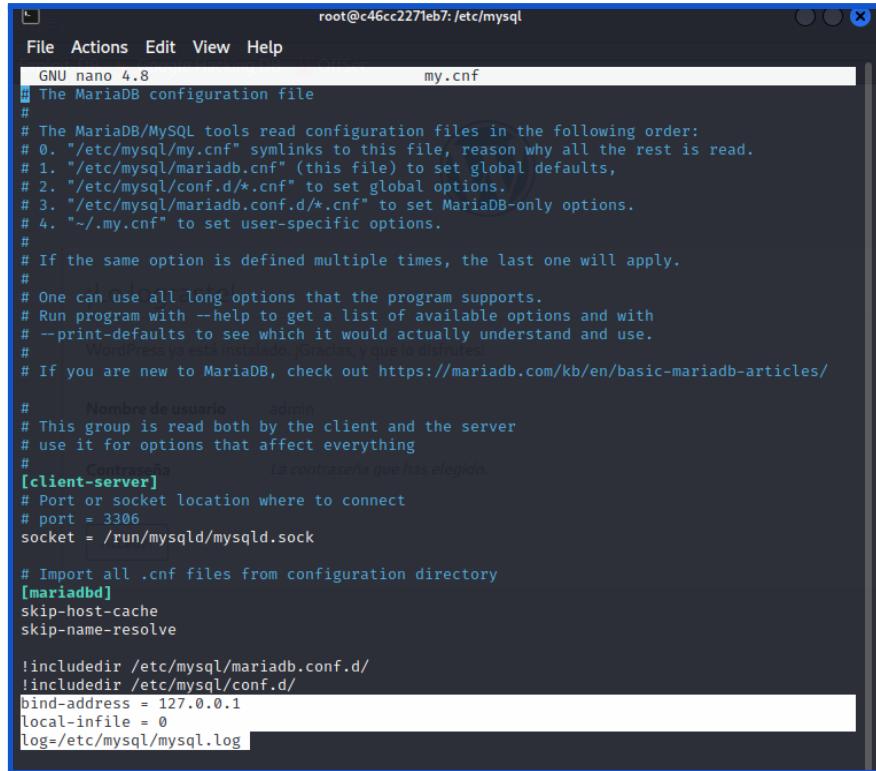
Ante un ataque o intrusión el saber es poder, para poder dotarnos de saber, vamos a habilitar el log de nuestro servicio en el mismo archivo, añadiendo “log=/var/log/mysql.log”. Sin embargo, incluir todos los logs en una carpeta llamada “logs” puede facilitar al atacante borrar sus rastros, por eso nosotros lo incluiremos en otra carpeta relacionada con nuestra db.

Tras esto cambiaremos los permisos del archivo *my.cnf* de manera que solo nosotros los administradores podamos cambiar el archivo. Esto lo realizaremos con el comando “chmod 644 /etc/mysql/my.cnf”. Por el código de permisos vamos a restringir a “solo lectura” a todos menos a nosotros.

Finalmente podemos instalar algún plugin o añadido más para mejorar la seguridad, pero nuevamente, como este proyecto debe cumplirse de manera real, con estas medidas será suficiente. Aun así, en los anexos se incluye información sobre lo mismo.

Hasta aquí nuestro archivo de configuración quedaría así:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008
	<i>Pág 34 de 106</i>	2021/2022



```

root@c46cc2271eb7:/etc/mysql
File Actions Edit View Help
GNU nano 4.8 my.cnf
# The MariaDB configuration file
#
# The MariaDB/MySQL tools read configuration files in the following order:
# 0. "/etc/mysql/my.cnf" symlinks to this file, reason why all the rest is read.
# 1. "/etc/mysql/mariadb.cnf" (this file) to set global defaults,
# 2. "/etc/mysql/conf.d/*.cnf" to set global options.
# 3. "/etc/mysql/mariadb.conf.d/*.cnf" to set MariaDB-only options.
# 4. "~/.my.cnf" to set user-specific options.
#
# If the same option is defined multiple times, the last one will apply.
#
# One can use all long options that the program supports.
# Run program with --help to get a list of available options and with
# --print-defaults to see which it would actually understand and use.
# WordPress ya está instalado. ¡Gracias, y que lo disfrutes!
# If you are new to MariaDB, check out https://mariadb.com/kb/en/basic-mariadb-articles/
#
#     Nombre de usuario      admin
# This group is read both by the client and the server
# use it for options that affect everything
# [client-server]           La contraseña que has elegido.
# Port or socket location where to connect
# port = 3306
socket = /run/mysqld/mysqld.sock

# Import all .cnf files from configuration directory
[mariadb]
skip-host-cache
skip-name-resolve

!includedir /etc/mysql/mariadb.conf.d/
!includedir /etc/mysql/conf.d/
bind-address = 127.0.0.1
local-infile = 0
log=/etc/mysql/mysql.log

```

Figura 23. Archivo configuración de db.

Con todo y un poquito de edición podemos tenemos una pagina tal que:



Figura 24. Estilo página web.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 35 de 106		2021/2022

Aunque este proyecto no se centra en la parte “front-end” de las webs, desde luego existen muchísimas herramientas para crear la página web de nuestros sueños, ya sea con Wordpress, Drupal, etc. Si bien en este ejemplo no lo hemos implementado existen plugins y complementos tanto de compra online, como de securización, monitorización, y muchísimo más.

Anotación

Aunque tenemos la página funcional de manera interna, al acceso interno Docker con la redirección de puertos produce un error que imposibilita el acceso a nuestra web, por ello vamos a cambiar en la base de datos unos parámetros, los que tenemos actualmente son:

```
MariaDB [wordb]> select * from wp_options where option_name = 'home' or option_name = 'siteurl' ;
+-----+-----+-----+-----+
| option_id | option_name | option_value | autoload |
+-----+-----+-----+-----+
| 2 | home | http://10.0.1.12 | yes |
| 1 | siteurl | http://10.0.1.12 | yes |
+-----+-----+-----+-----+
2 rows in set (0.000 sec)
```

Figura 25. Configuración en la BBDD funcional.

Para solucionar esto en el [anexo⁷³](#) dejare la serie de comandos para poder actualizar la base de datos. Una vez hemos solucionado el problema con Wordpress podemos buscar externamente y vemos:



Figura 26. Página funcional empresa.

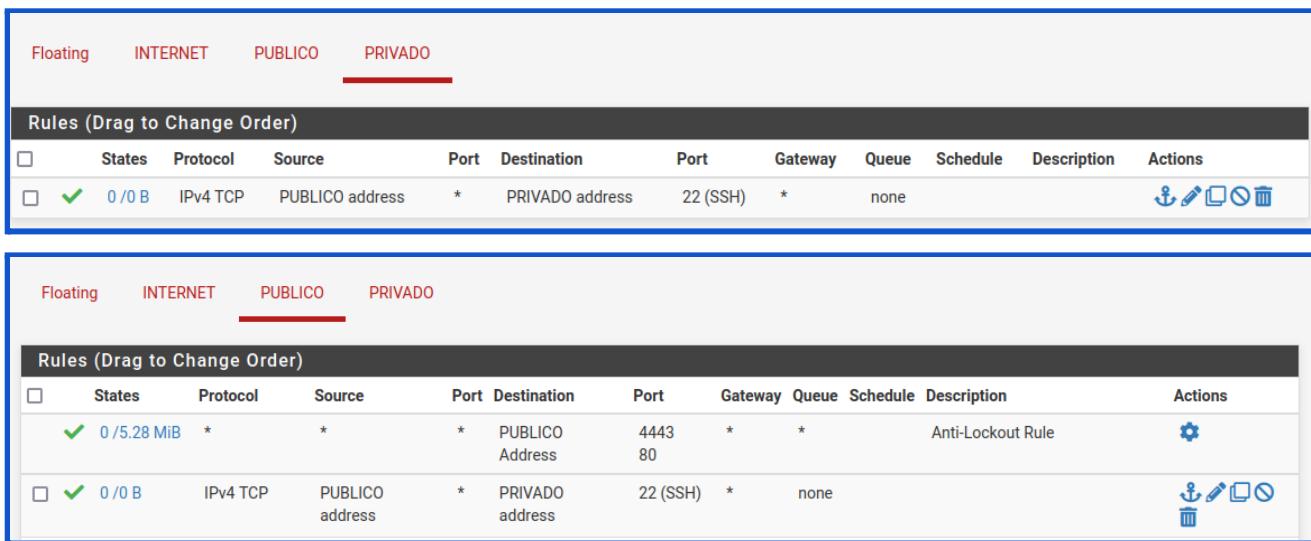
 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 36 de 106		2021/2022

Ya tenemos nuestros servicios funcionando, sin embargo, no hemos terminado. La información y los datos que guardamos son realmente importantes, por eso es imprescindible plantearnos un método de backup.

Existen distintas herramientas e imágenes de gestión de backups⁶²⁻⁶⁷, pensados mayoritariamente para unos volúmenes muy grandes de información. En este caso tan reducido, y pensado solo temporalmente hasta la migración a la nube, la herramienta lógica es un script para copiar los datos.

Usaremos un script que se ejecute diariamente utilizando la utilidad UNIX de “cron” y “anacron”, para la ejecución del script utilizaremos cifrado asimétrico entre los servidores a copiar, guardando las credenciales para facilitar el script. Así mismo utilizaremos SCP, utilidad de SSH para copiar los datos que nos importan de los servidores al servidor de backup.

Coparemos solo los registros de la base de datos y las configuraciones, y personalizaciones de la página web, para poder volver a producción en caso de fallo.



The screenshot displays two separate firewall rule configurations:

Top Rule Set:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	IPv4 TCP	PUBLICO address	*	PRIVADO address	22 (SSH)	*	none			
<input checked="" type="checkbox"/>	0 /0 B									

Bottom Rule Set:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	IPv4 TCP	PUBLICO address	*	PRIVADO address	22 (SSH)	*	none			
<input checked="" type="checkbox"/>	0 /5.28 MiB	*	*	*	PUBLICO Address	4443 80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>										

Figura 27. Reglas firewall para backup.

Para poder ejecutar nuestro script obviamente debemos permitir en las reglas del firewall un acceso cruzado entre cada red (bloqueando obviamente las que vengan de internet).

Comprobamos el acceso SSH, y tras confirmarlo ejecutaremos una configuración al servicio como hemos hecho anteriormente.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
	Pág 37 de 106	2021/2022

```
(kali㉿kali)-[~]
└─$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:F4rDaGlWGLt2suy7AB6ghi2jRukIWtA1kM08w11GNR4 kali㉿kali
The key's randomart image is:
+---[RSA 4096]---+
| .Bo. o+.E |
| ... B ... .o |
| o . .o= .o |
| o+. % = .. |
| *+= 0 * S . |
| 0= * . . . |
| +o. . . |
| . . . |
| .o. |
+---[SHA256]---+
          States   Protocol  Source
  ✓ 0/5.28 MiB  *          *
  ✓ 0/0 B       IPv4 TCP  PUBLICO
                                address
  ✓ 1/18.79    IPv4 *     *
```

Figura 28. Creación de llave criptográfica.

Para realizar un cifrado entre servidores y el guardado de la llave criptográfica primero deberemos generarla. Con este comando estamos generando una llave de 4096 bits para el algoritmo criptográfico RSA, un algoritmo matemático ya antiguo, de ahí que hayamos elegido un número tan alto de bits para generar la clave. Tras los avances hechos en ciberseguridad y criptografía, por muy larga llave que produzca RSA se está recomendando el uso de ECDSA a futuro, importante anotarlo.

```
(kali㉿kali)-[~]
└─$ ssh-copy-id -i ~/.ssh/id_rsa.pub admin@10.0.190.100
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/kali/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
admin@10.0.190.100's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'admin@10.0.190.100'"
and check to make sure that only the key(s) you wanted were added.
```

Figura 29. Copia de llave al servidor backups.

Una vez generada nuestra llave debemos copiarla al servidor que queramos, en este caso el de backup (todavía no securizado). Una vez tenga copiada las claves de los servidores, bloquearemos el acceso por contraseña y cambiaremos el puerto de acceso de SSH.

Tras la copia podemos comprobar que podemos acceder al servidor sin contraseña y de manera segura. Completada la copia de id en los servidores y el acceso correcto, securizaremos el servicio SSH como ya hemos visto y creamos el script de copia que ejecutaremos en este servidor:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 38 de 106			2021/2022

```
#Creamos una variable temporal para saber en que dia se creó el backup
dia="$(date +\%d\%m\%Y)"
```

```
#Creamos una carpeta donde se copie todo el contenido que necesitamos
sudo mkdir backup_wordpress_$dia
```

```
sudo docker container cp wordpress:/var/www/html ~/backup_wordpress_$dia
```

```
# Copiamos nuestro contenido al servidor de backups
# -i copiamos nuestra llave, unica vía de acceso.
#-C comprimimos los archivos.
#-q evitamos el diálogo de todos los archivos transfiriéndose.
# -r indicamos que se copien recursivamente los archivos, es decir que copie toda
la carpeta.
scp -i ~/.ssh/id_rsa -P 37037 -C -q -r ~/backup_wordpress_$dia
admin@10.0.190.100:~/wordpress
```

```
sudo mkdir backup_db_$dia
```

```
sudo docker container cp db_wordpress:/var/lib/mysql ~/backup_db_$dia
```

```
scp -i ~/.ssh/id_rsa -P 37037 -C -q -r ~/backup_db_$dia
admin@10.0.190.100:~/db_wordpress
#Tras copiar los archivos borramos por seguridad las copias en local
sudo rm -r backup_wordpress_$dia backup_db_$dia
```

```
admin@backupserver:~$ ls
db_wordpress  wordpress
admin@backupserver:~$ cd wordpress/
admin@backupserver:~/wordpress$ ls
backup_wordpress_15052022  backup_wordpress_16052022
admin@backupserver:~/wordpress$ cd .. /db_wordpress/
admin@backupserver:~/db_wordpress$ ls
backup_db_16052022
admin@backupserver:~/db_wordpress$ █
```

Figura 30. Comprobación de backups.

Con el script de backup funcionando debemos programar cuándo se ejecutarán dichos guardados masivos. Para ello Linux trae una herramienta fundamental, crontab. Con esta utilidad vamos a programar la ejecución de los guardados, asumiendo el funcionamiento continuo del servidor, en caso contrario, debido a mantenimientos, prueba o desarrollo, debemos usar conjuntamente la utilidad “anacron”.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 39 de 106</i>			<i>2021/2022</i>

Esta herramienta permite la ejecución de rutinas que no se hayan podido ejecutar a una hora por diversas razones (ej. apagado por mantenimiento).

Ejecutando el comando “crontab -e” podemos acceder a la listas de rutinas de nuestro servidor:

```
GNU nano 4.8                               /tmp/crontab.KVKzEi/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
```

Figura 31. Configuración de cron.

Está vacío pero vamos a rellenarlo para que se ejecute a una hora concreta, en el anexo^{76,77} hay un manual para entender correctamente la utilidad y una herramienta para crear sencillamente horarios:

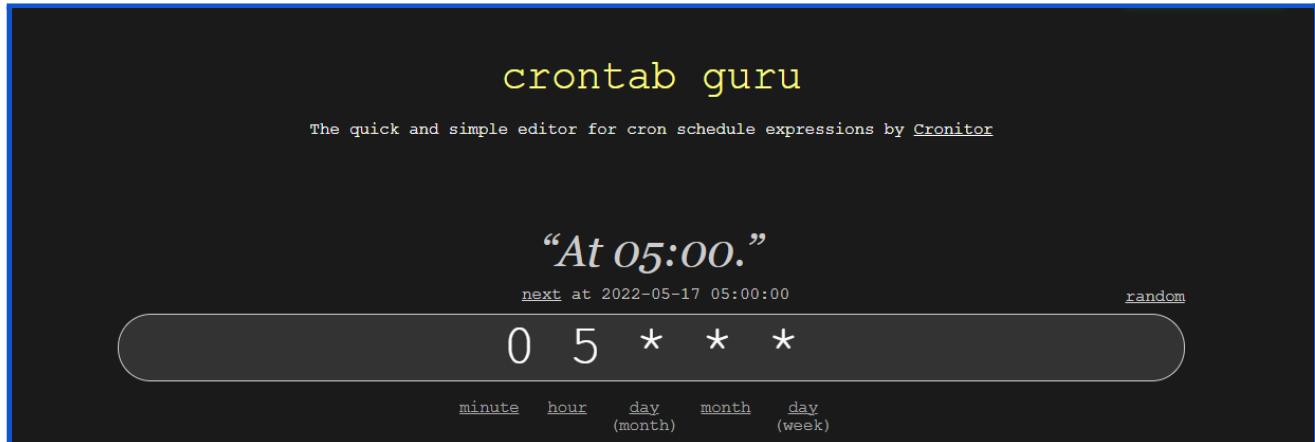


Figura 32. Herramienta cron.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 40 de 106			2021/2022

Con esta herramienta, y asumiendo que no se va a generar un contenido excesivo en la web, vamos a hacer una copia exacta de nuestro sistema cada día a las 5 AM, hora española en la que las web no tienen mucho tráfico todavía. Si hubiera mucha carga, recomiendo hacer los backups los fines de semana, con menos afluencia en la web y por tanto más resistente a sobrecargas.

```
# m h  dom mon dow   command
0 5 * * * ~/backups.sh
```

Figura 33. Configuración cron aplicada.

Aplicando nuestra configuración, debería de quedarnos algo así en el archivo de crontab.

Con el servicio en marcha solo queda un paso lógico antes de la entrada a producción, esto es, comprobar el sistema en sí. Todo esto puede ser maravilloso pero si nuestro firewall inteligente, ayudado con Snort, tiene un filtro tan fino que acaba bloqueando a potenciales compradores nuestro sistema no tendrá sentido. Al igual que no tendría sentido que toda la información y configuración pueda estar a la mano de cualquier atacante por inexperto que sea.

En ciberseguridad hay que tener en claro que no es un cómo o un por qué. es un cuando. Todos los sistemas informáticos son susceptibles de fallo y asalto, nuestra tarea es retrasarlo lo máximo posible y dificultar el acceso a los archivos que más nos importan. Alejado de eso, lo que queda es una prueba de pentesting. Nuestro firewall debe bloquear todo lo que no sea acceso web, pero incluso lo bloqueado puede presentar vulnerabilidades.

```
(kali㉿kali)-[~]
└─$ sudo nmap -T 1 -Pn -f -sV 172.16.0./*
[sudo] password for kali:
++Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 13:33 EDT

```

Figura 34. Escaneo de la red sigiloso.

Empezaremos, como haría un atacante externo, haciendo un escaneo de la red, en la Figura 34 podemos ver el grado de “agresividad” del ataque con **-T 1**, de 0 a 5 de agresividad, resultando este último en más velocidad del escaneo pero más trazas en caso de querer localizar al atacante. **-Pn** como opción realiza un escaneo SIN PING, lo que nos delata. **-f** es

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 41 de 106			2021/2022

una opción para fragmentar los paquetes enviados al objetivo, reduciendo la “visibilidad”. **-sV** es quizás el más importante porque nos muestra información sobre los servicios que corren en cada puerto y que versión, con esto podemos buscar y explotar vulnerabilidades que comprometan el servicio.

```
Stats: 0:10:22 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 15.88% done; ETC: 14:38 (0:55:00 remaining)
```

Figura 35. Coste temporal del escaneo sigiloso.

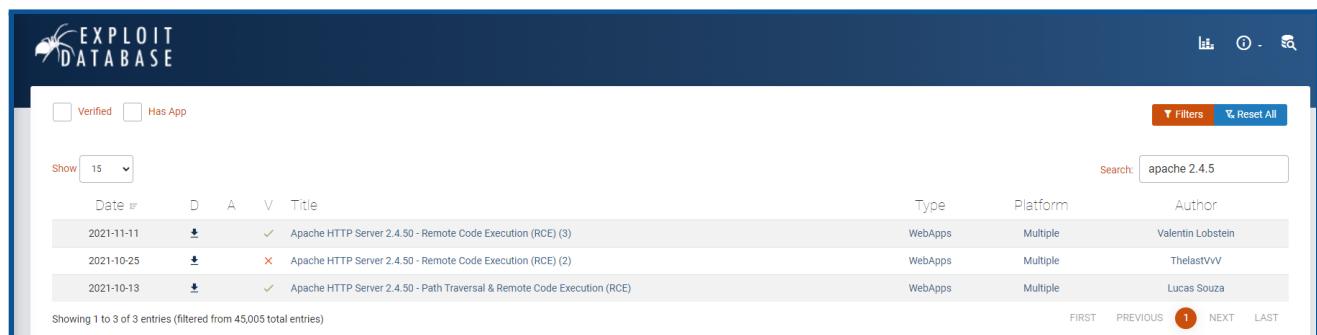
Podemos comprobar en la Figura 35 el escaneo tan preciso y sigiloso de TODA la red es algo que lleva mucho tiempo, haremos un pequeño “truco” en este caso y asumimos que ya sabemos la dirección del servidor a atacar.

```
Nmap scan report for 172.16.0.109
Host is up (0.00043s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.53 ((Debian))
MAC Address: 08:00:27:02:6B:22 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82620.35 seconds
```

Figura 36. Análisis del PfSense.

A destacar del análisis es el tiempo que ha tardado en realizarse, casi 22 horas (no consecutivas porque por suerte se puede guardar el estado de las máquinas). Lo segundo es que efectivamente solo encontramos el puerto 80 abierto, justo como nosotros queremos.



The screenshot shows the Exploit Database interface. At the top, there are filters for 'Verified' and 'Has App'. On the right, there's a search bar with 'apache 2.4.5' and buttons for 'Filters' and 'Reset All'. Below the search bar, there are buttons for 'Type', 'Platform', and 'Author'. The main table has columns for 'Date', 'Type', 'Platform', and 'Author'. There are three entries listed:

Date	Type	Platform	Author
2021-11-11	WebApps	Multiple	Valentin Lobstein
2021-10-25	WebApps	Multiple	Thelastvvv
2021-10-13	WebApps	Multiple	Lucas Souza

At the bottom, it says 'Showing 1 to 3 of 3 entries (filtered from 45,005 total entries)' and includes navigation buttons for 'FIRST', 'PREVIOUS', 'NEXT', and 'LAST'.

Figura 37. Exploit DB.

Podemos comprobar que no hay ningún CVE asociado a nuestro servicio en el puerto. Pero podemos ver más:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR CERTIFIED IQNet Empresa Registrada ER-0934 / 2008
Pág 42 de 106		2021/2022

```
(kali㉿kali)-[~]
$ nmap -v --script vuln 172.16.0.109
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-19 12:59 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:59
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 66.67% done; ETC: 12:59 (0:00:04 remaining) Platform
Completed NSE at 13:00, 34.45s elapsed
Initiating NSE at 13:00
Completed NSE at 13:00, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:                               WebApps      Multiple
|   Discovered hosts:
|     224.0.0.251                                     WebApps      Multiple
| After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).

Scanning 172.16.0.109 [1000 ports]
Discovered open port 80/tcp on 172.16.0.109
Completed Connect Scan at 13:00, 4.72s elapsed (1000 total ports)
NSE: Script scanning 172.16.0.109.
Initiating NSE at 13:00
NSE: [tls-ticketbleed] Not running due to lack of privileges.
NSE: [firewall-bypass] lacks privileges.
Completed NSE at 13:01, 69.49s elapsed
Initiating NSE at 13:01
Completed NSE at 13:01, 0.22s elapsed
Nmap scan report for 172.16.0.109
Host is up (0.00058s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE          Type      Platform
80/tcp    open  http           WebApps  Multiple
          |_ http-stored-xss: Couldn't find any stored XSS vulnerabilities. Multiple
          |_ http-dombased-xss: Couldn't find any DOM based XSS.
          |_ http-csrf: Couldn't find any CSRF vulnerabilities.
          |_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)  PREVIOUS
          |_ http-enum:
          |   /wp-login.php: Possible admin folder
          |   /wp-json: Possible admin folder
          |   /robots.txt: Robots file
          |   /readme.html: Wordpress version: 2
          |   /feed/: Wordpress version: 5.9.3
          |   /wp-includes/images/rss.png: Wordpress version 2.2 found.
          |   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
          |   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
          |   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
          |   /wp-login.php: Wordpress login page.  Professional Services
          |   /wp-admin/upgrade.php: Wordpress login page.  Penetration Testing
          |   /readme.html: Interesting, a readme.
          |_ /wp-content/themes/tema/0/: Potentially interesting folder  Advanced Attack Simulation
          |_ /wp-content/themes/tema/0/0/: Potentially interesting folder  Application Security Assessment
          |_ /wp-content/themes/tema/0/0/0/: Potentially interesting folder  All new for 2020

Search: apache
```

Figura 38. Análisis más agresivo del servicio.

Este análisis más agresivo nos muestra más datos, que en caso de proteger el servicio son importantes. En el escaneo de vulnerabilidades de NMAP se ejecutan distintos scripts de seguridad para comprobar el estado del host, en este caso, centrándonos únicamente en la última parte podemos ver como los scripts “http-X” han encontrado que no sufrimos vulnerabilidades, sin embargo, el último, “http-enum” ha accedido a carpetas de nuestro servicio que puede contener información importante a la hora de sufrir un ataque.

Este es el inicio para evitar que nos roben, aun así NMAP es una de las muchísimas herramientas que existen, pero debemos estar atentos para que no pase nada.

 <p>IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla</p>	<h2>Guía Práctica para el uso profesional de la nube</h2>	 <p>AENOR ER Empresa Registrada ER-0934 / 2008</p>  <p>CERTIFIED IQNet QUALITY SYSTEM</p>
	<p>Pág 43 de 106</p>	<p>2021/2022</p>

Siempre es aconsejable validar la seguridad de nuestra empresa cada cierto tiempo, así mismo para evitar estos ataques, creando filtros más finos en nuestro firewall y utilizando Snort de manera más ambiciosa podemos asegurarnos que estos intentos de análisis no sucedan y, nuevamente, retrasemos lo máximo posible a los malos.

Con esto podemos dar por “terminada” la configuración local. Trataré más profundamente en la conclusión, pero esta instalación y configuración únicamente nos deja acceso a nosotros, individualmente. Para que todo internet acceda a nuestra red deberemos, o contratar y contactar con nuestro [ISP](#) para poder darnos una IP fija, tras esto debemos contratar también un hosting para que nuestra empresa pueda ser buscada en internet con el nombre de nuestra empresa. Recomiendo también hacer el mismo análisis de red que hemos hecho pero de manera interna, es decir, si un atacante hubiera entrado, para seguir reduciendo riesgos y darnos más tiempo. Así mismo en caso de una empresa algo más mediana, el uso lógico de Active Directory también implica un riesgo en la seguridad que nos obliga a revisar políticas, acceso, históricos, etc.

Estas otras muchas configuraciones son necesarias para el seteo de un entorno digital en local correcto, puede parecer baladí, pero tener en un solo documento, con unos pasos y consejos, un walkthrough empresarial es fundamental en un mundo en el que cada empresa cobra a precio de oro esta información y su consiguiente aplicación. La mayoría de estos problemas desaparecerá en la nube.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER <small>Empresa Registrada</small> <small>ER-0934 / 2008</small>	 CERTIFIED IQNet <small>QUALITY SYSTEM</small>
<small>Pág 44 de 106</small>			2021/2022

6.2. Implementación cloud basada en la nube de AZURE

Ya tenemos un sistema funcional, una serie de servidores y ordenadores funcionando en nuestra oficina o local. Desde aquí ya podemos funcionar como empresa digital sin ningún problema, entonces **¿por qué avanzar a la nube?**.

Aunque parezca lógica, no es una respuesta elemental. Al construir nuestra empresa u organización en el entorno digital surgen mil y un problemas, por ejemplo, queremos poder gestionar nuestros datos parados en el semáforo, en algún rato libre en casa o quizás en otro país de viaje, queremos saber si todo va bien y poder trabajar. Esto puede hacerse con otros servicios y más servidores en nuestra oficina a mayor costo, pero la **nube soluciona este problema de un plumazo**, solo necesitamos conexión a internet et voilá!. Pero no lo único, en el crecimiento y mantenimiento de la empresa existe la posibilidad de mudanza, quizás una catástrofe como un incendio, algo normal como un corte de luz, etc. Todos estos problemas pueden solucionarse a un mayor coste, comprando más servidores, construyendo una zona separada, contratando distintos proveedores tanto de internet como de electricidad...

Sin embargo, con la nube todos estos problemas se solucionan, nuevamente de un toque. Al digitalizar hasta la infraestructura **se gana en espacio** en la oficina, **se ahorra** en planes y construcción y sobre todo, **se ahorra en preocupaciones**. Ante cualquier problema físico, tus datos y los de tus clientes quedan protegidos en la nube, listos para seguir trabajando en cualquier circunstancia.

 I.E. Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 45 de 106			2021/2022

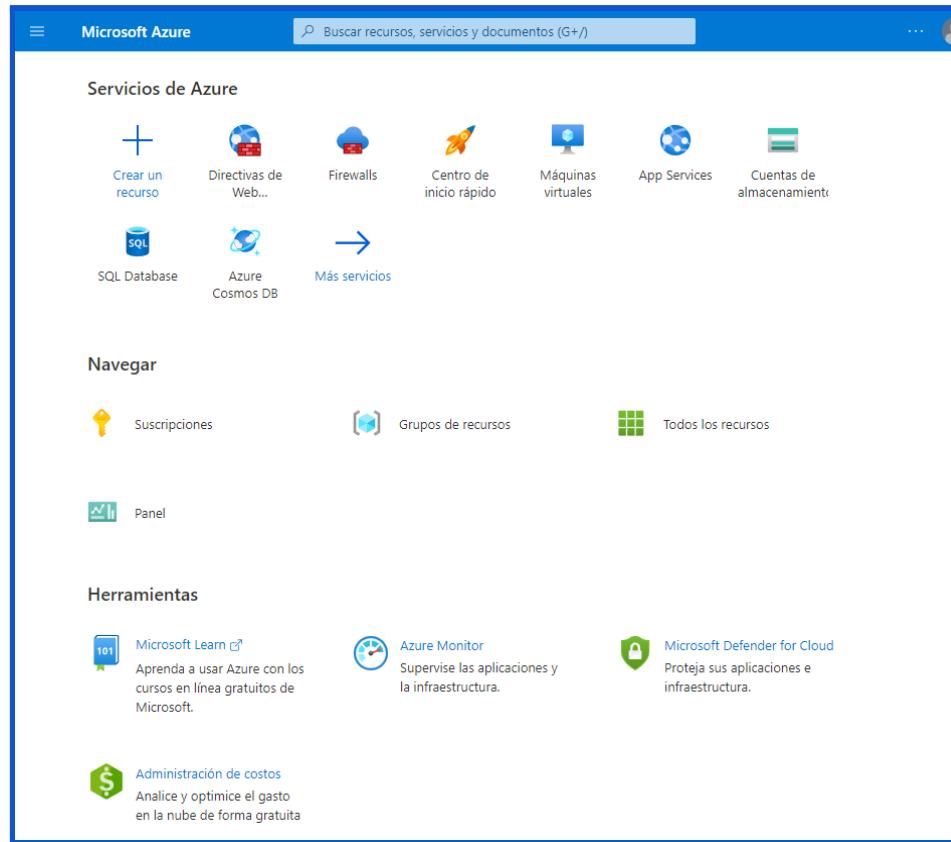


Figura 39. Inicio Azure.

Justo por eso acabamos en esta página, la página de inicio de Microsoft **Azure**. Actualmente **Azure** es el único proveedor de cloud que permite acceso a su nube de forma gratuita para estudiantes, lo que nos va a permitir en este caso (y seguro que en muchos otros, de ahí su crecimiento) crear nuestro primer entorno cloud de manera funcional y gratuita.

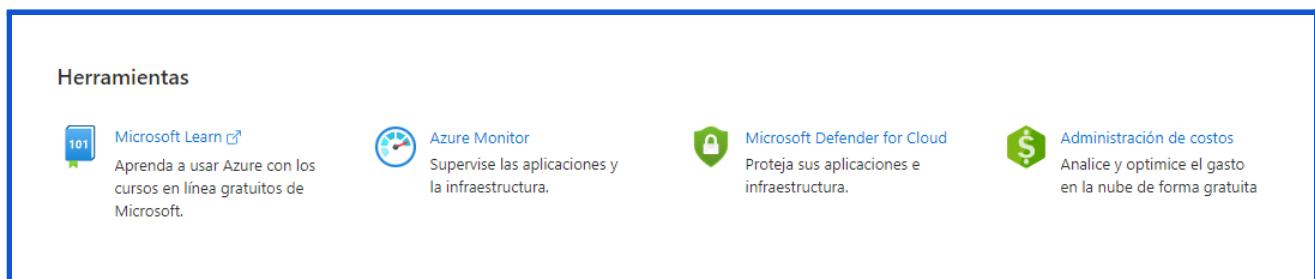


Figura 40. Herramientas de Azure.

No solo podemos acceder de manera gratuita, sino que Azure presta diferentes servicios gratuitos incluso a las suscripciones de pago. La imagen anterior ilustra muy bien las herramientas que ofrece, pero destaca la “Administración de costos”, un optimizador de gastos para que no malgastes recursos en la nube.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 46 de 106			2021/2022

Y sin entrar en la infinidad de recursos que nos ofrece Azure, vamos a empezar con nuestra migración a la nube.

En el proceso de la migración habrá distintos pasos que, aún tratandolos, los saltaremos de manera práctica porque son un coste añadido que una guía rápida de un estudiante no puede asumir. Así por ejemplo, el primer paso para la migración será un balanceador de carga.

Efectivamente, nuestra prioridad es mantener el servicio activo, para ello debemos ir creando un “duplicado”, que mientras no funcione te redirija a nuestro servidor local.

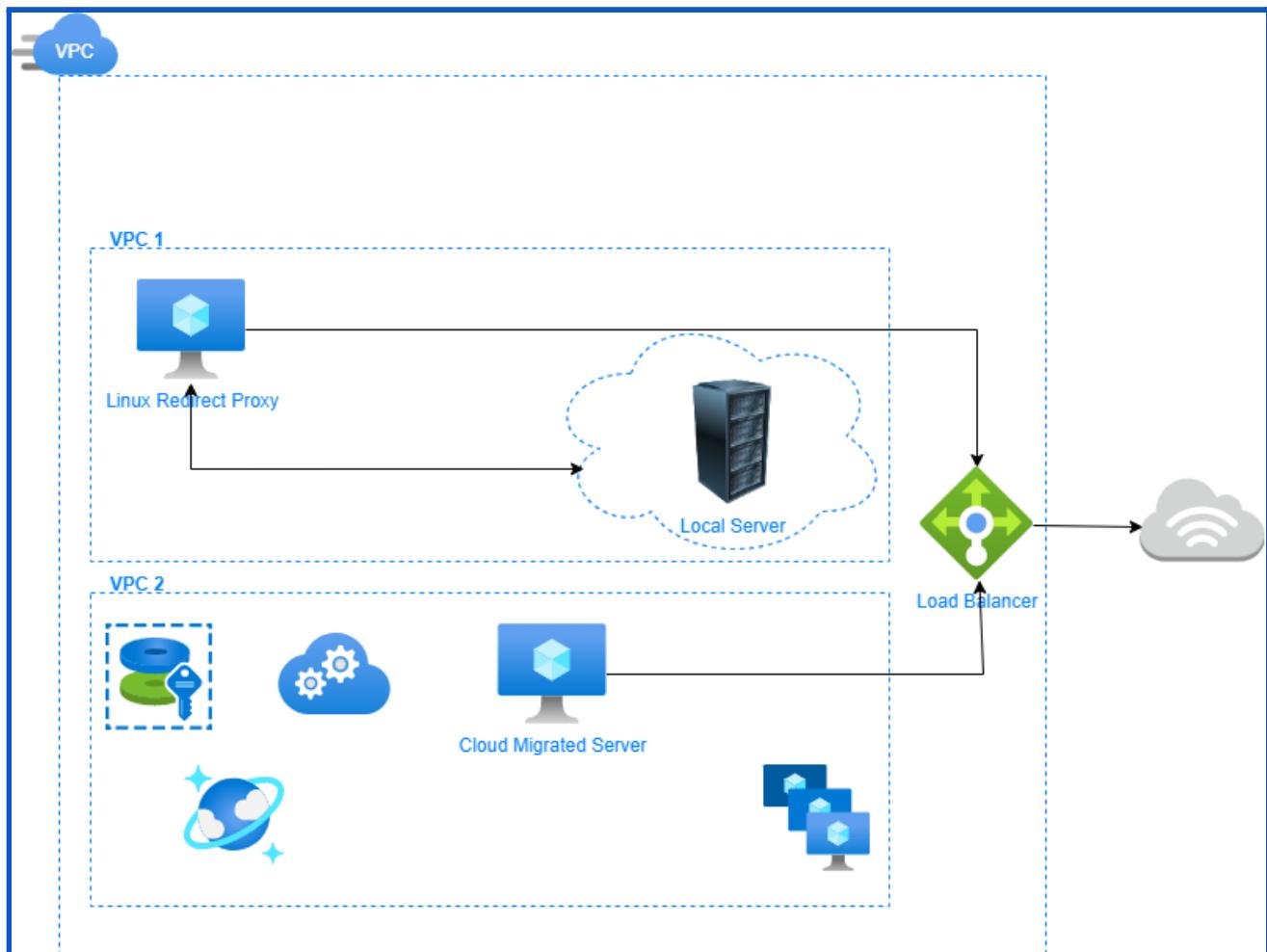


Figura 41. Esquema migración Azure.

Basándonos en este esquema vamos a migrar nuestros servicios a la nube.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 47 de 106</i>			<i>2021/2022</i>

Deberemos crear un balanceador de carga el tráfico entrante en nuestra red, de manera que al detectar que una, ahora mismo en cloud, no funciona nos redirija a nuestro servidor local, hasta que completamos la migración y podamos realizarlo al contrario.

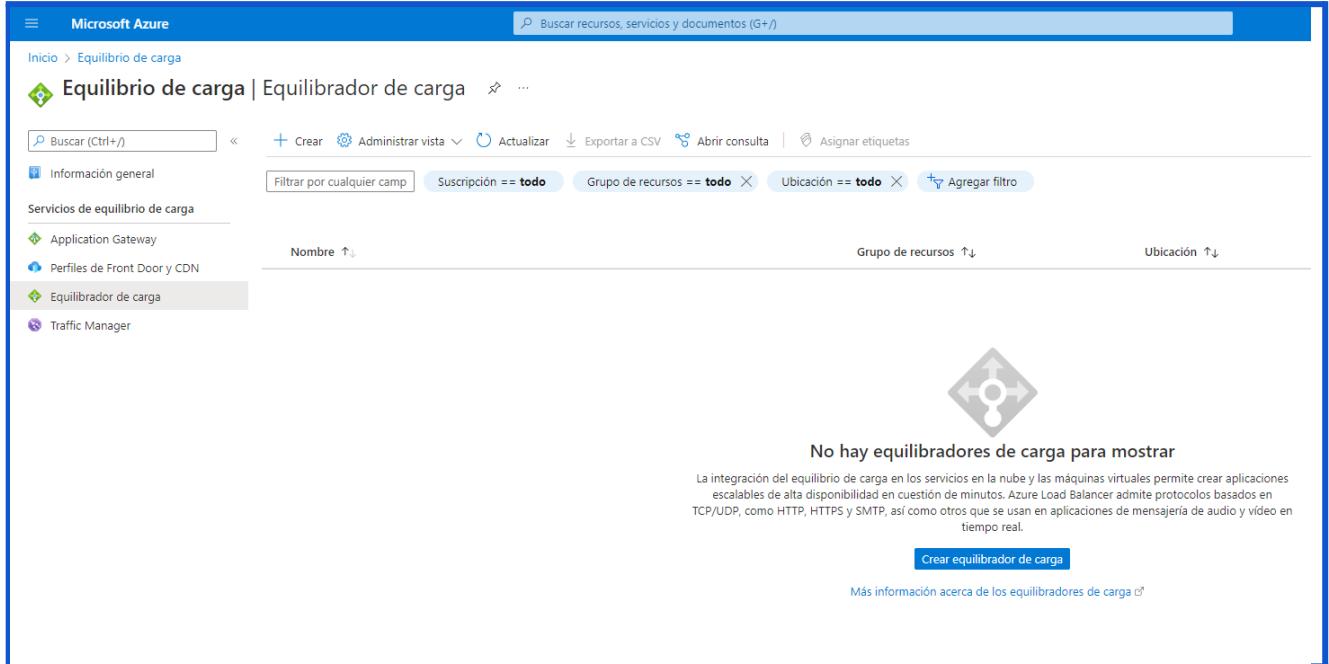


Figura 42- Azure Load Balancer.

La propia Microsoft tiene una [documentación](#) amplia y extensa sobre la creación de este recurso, y sobre ella nos vamos a basar.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresarial Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 48 de 106		2021/2022

Create load balancer

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *

Azure for Students

Resource group *

projeto

[Create new](#)

Instance details

Name *

balanceador_1

Region *

North Europe

SKU * ⓘ

- Standard
- Gateway
- Basic

 Microsoft recommends Standard SKU load balancer for production workloads.
[Learn more about pricing differences between Standard and Basic SKU](#) ⓘ

Type * ⓘ

- Public
- Internal

Tier *

- Regional
- Global

Figura 43-Azure Load Balancer.

Crear un balanceador en la nube de Azure como podemos ver más arriba es muy sencillo.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet Empresa Registrada ER-0934 / 2008
Pág 49 de 106		2021/2022

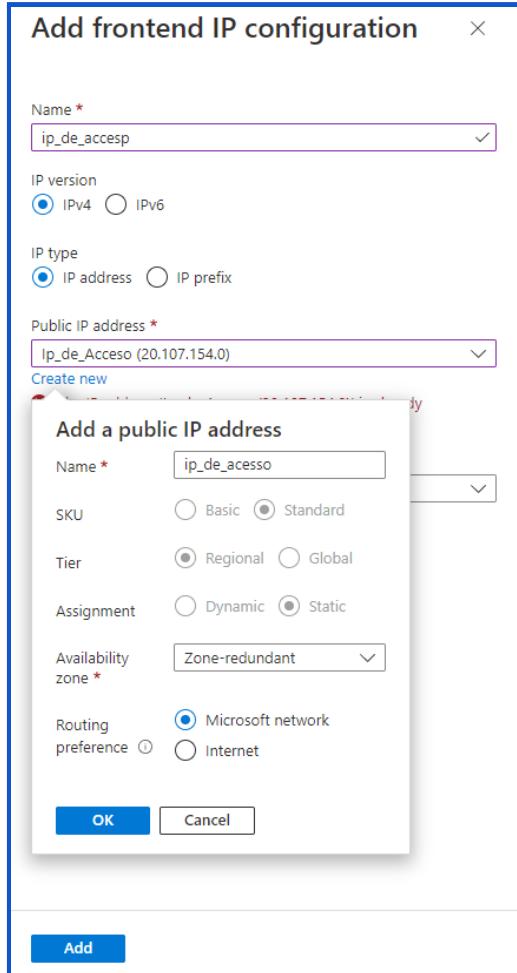


Figura 44- Azure Load Balancer.

Antes de terminar nuestro balanceador debemos darle una “cara”, la ip pública que administrará el balanceo de nuestro sistema.

Antes de adaptar el esquema debemos pensar que existen distintas maneras de migrar nuestros servicios a la nube. En este proyecto queremos cumplir el acceso total a nuestros servicios durante la migración y posterior, lo que es llamado “alta disponibilidad”, que no podemos cumplir de manera tan eficiente en local. Para cumplir esto utilizaremos la [idea⁸⁸](#) de crear una máquina en Azure y redirigirla a nuestra red local, mientras en otra red migramos el servicio.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 50 de 106			2021/2022

Esto puede realmente saltarse ya que Azure implanta un servicio automatizado de migración, Azure Migrate.

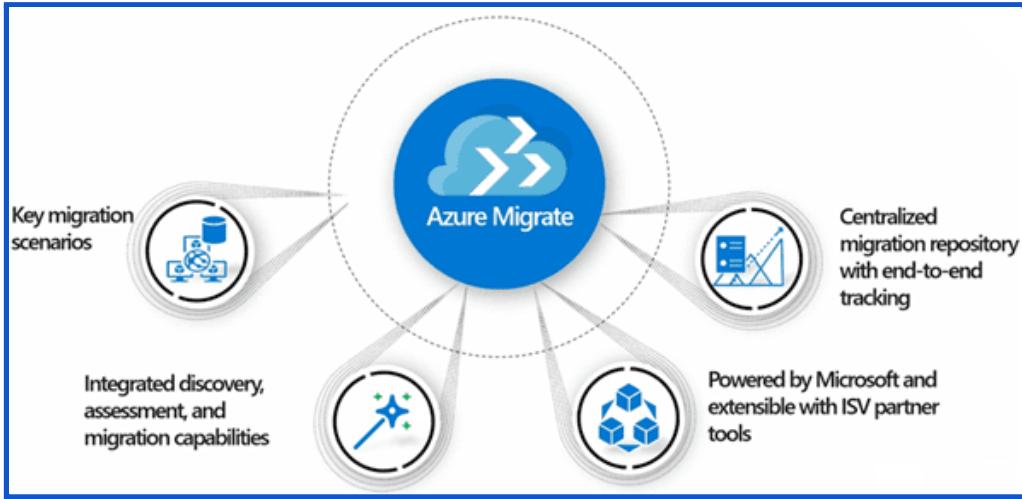


Figura 45. Azure Migrate.

Con Azure Migrate puedes migrar automáticamente distintos servicios a la nube, por ejemplo, si tuviéramos algún tipo de aplicación, máquina de Hyper-V, o VDI de Microsoft podríamos pasarlo rápidamente a la nube. Sin embargo nuestro entorno de pruebas ha sido creado con Virtualbox, que dificulta algo más esta migración con la herramienta.

Antes de encontrar una solución vamos a crear la máquina proxy que redirigirá el tráfico a nuestra red según el esquema de la *Figura 40*, saltándonos en este caso el problema del hosting de dominio que debería tener contratada la empresa. En este caso práctico ejecutaremos una configuración similar para completar los datos faltantes.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 51 de 106			2021/2022

Crear una máquina virtual ...

Datos básicos Discos Redes Administración Opciones avanzadas Etiquetas Revisar y crear

Cree una máquina virtual que ejecuta Linux o Windows. Seleccione una imagen de Azure Marketplace o use una imagen personalizada propia. Complete la pestaña Conceptos básicos y, después, use Revisar y crear para aprovisionar una máquina virtual con parámetros predeterminados o bien revise cada una de las pestañas para personalizar la configuración.

[Más información ↗](#)

Detalles del proyecto

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción * ⓘ

Azure for Students

Grupo de recursos * ⓘ

proyecto

[Crear nuevo](#)

Detalles de instancia

Nombre de máquina virtual * ⓘ

proxy-redireccion

Región * ⓘ

(Europe) North Europe

Opciones de disponibilidad ⓘ

No se requiere redundancia de la infraestructura

Tipo de seguridad ⓘ

Estándar

Imagen * ⓘ

Debian 11 "Bullseye" - Gen1

[Ver todas las imágenes](#) | [Configurar la generación de máquinas virtuales](#)

Instancia de Azure de acceso puntual ⓘ

Tamaño * ⓘ

Standard_D2as_v4 - 2 vcpu, 8 GiB de memoria (78,11 US\$/mes)

[Ver todos los tamaños](#)

Figura 46. Redirección Azure.

Para esta máquina intentaremos ser lo más escuetos posibles para no aumentar costes.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 52 de 106			2021/2022

Cuenta de administrador

Tipo de autenticación 

Clave pública SSH
 Contraseña

 Ahora, Azure genera automáticamente un par de claves SSH y le permite almacenarlo para usarlo en el futuro. Es una forma rápida, sencilla y segura de conectarse a la máquina virtual.

Nombre de usuario * 

redirectadmin 

Origen de clave pública SSH

Generar un par de claves nuevo 

Nombre de par de claves *

proxy-redireccion_key 

Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.

Puertos de entrada públicos * 

Ninguno
 Permitir los puertos seleccionados

Seleccionar puertos de entrada *

SSH (22) 

 **Este permitirá que todas las direcciones IP accedan a la máquina virtual.**
 Esto solo se recomienda para las pruebas. Use los controles avanzados de la pestaña Redes a fin de crear reglas para limitar el tráfico entrante a las direcciones IP conocidas.

Figura 47. Ssh en proxy.

Obviamente deberemos habilitar el servicio ssh para poder acceder a la máquina y configurar el servicio que utilizaremos.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR IQNet Empresa Registrada ER-0934 / 2008
<i>Pág 53 de 106</i>		<i>2021/2022</i>

Interfaz de red

Al crear una máquina virtual, se crea una interfaz de red automáticamente.

Red virtual *	<input type="text" value="(nuevo) proyecto-vnet"/> ▼ Crear nuevo
Subred *	<input type="text" value="(nuevo) default (10.0.0.0/24)"/> ▼
IP pública	<input type="text" value="(nuevo) proxy-redireccion-ip"/> ▼ Crear nuevo
Grupo de seguridad de red de NIC	<input type="radio"/> Ninguno <input checked="" type="radio"/> Básico <input type="radio"/> Opciones avanzadas

Equilibrio de carga

Puede colocar esta máquina virtual en el grupo de back-end de una solución de equilibrio de carga de Azure existente. [Más información ↗](#)

¿Quiere colocar esta máquina virtual como subyacente respecto a una solución de equilibrio de carga existente?

Configuración de equilibrio de carga

- **Application Gateway** es un equilibrador de carga para tráfico web HTTP/HTTPS con enrutamiento basado en direcciones URL, terminación SSL, persistencia de sesión y Web Application Firewall. [Más información sobre Application Gateway ↗](#)
- **Azure Load Balancer** admite todo el tráfico de red TCP/UDP, el enrutamiento de puerto y los flujos salientes. [Más información sobre Azure Load Balancer ↗](#)

Opciones de equilibrio de carga *	<input type="text" value="Azure Load Balancer"/> ▼
Seleccionar un equilibrador de carga *	<input type="text" value="balanceador_01"/> ▼
Seleccionar un grupo de back-end *	<input type="text" value="(nuevo) proyecto-back"/> ▼ Crear nuevo

Figura 48. Red del proxy.

Así mismo nos creará automáticamente las redes virtuales y la ip pública, permitiéndonos así mismo añadir nuestra máquina al balanceador que hemos creado previamente.

Esta configuración plantea un problema base que uno no se plantea en la creación. La utilización de claves públicas ssh necesita de una utilidad que windows no dispone, **chmod**. Necesitamos cambiar los permisos de la clave o nos bloqueara por siempre:

```
@@@@@@@@@@@@@@@@@@@  
@      WARNING: UNPROTECTED PRIVATE KEY FILE!      @  
@@@@@@@@@@@@@@@  
Permissions 0777 for 'privkey.pem' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
Load key "privkey.pem": bad permissions  
Permission denied (publickey).
```

Figura 49. Bloqueo de la clave privada.

Para solucionar esto podemos o acceder desde una máquina Linux, donde podemos hacer el cambio de permisos, o implementar [WSL⁹⁵](#) una utilidad de windows para utilizar el cli de linux. Aun así seguiríamos teniendo el problema aun ejecutando, por ejemplo, Powershell con permisos de administrador, pues el subsistema de Ubuntu no tiene los permisos para modificarlo. Como siempre la solución está investigada y añadida al [anexo⁹⁷](#). Con la solución implementada podemos conectarnos:

RDP **SSH** Bastion

Connect via SSH with client

1. Open the client of your choice, for example [WSL on Windows](#), [Terminal on Mac](#) or [Shell on Linux](#).
2. Ensure you have read-only access to the private key. Chmod is only supported on Linux subsystems (e.g. WSL on Windows or Terminal on Mac).

```
chmod 400 <keyname>.pem
```
3. Provide a path to your SSH private key file. [Replace/reset your SSH private key.](#) ⓘ
Private key path
4. Run the example command below to connect to your VM.

```
ssh -i <private key path> redirectadmin@20.107.204.214
```

Figura 50. Requisitos para la conexión.

```
jc@DESKTOP-KNSMPES:/mnt/c/Users/Jc/Downloads$ ls -la | grep proxy-redireccion_key.pem  
-rwxr--r-- 1 jc jc      2498 May 29 23:56 proxy-redireccion_key.pem  
jc@DESKTOP-KNSMPES:/mnt/c/Users/Jc/Downloads$ chmod 400 proxy-redireccion_key.pem  
jc@DESKTOP-KNSMPES:/mnt/c/Users/Jc/Downloads$ ls -la | grep proxy-redireccion_key.pem  
-r----- 1 jc jc      2498 May 29 23:56 proxy-redireccion_key.pem  
jc@DESKTOP-KNSMPES:/mnt/c/Users/Jc/Downloads$
```

Figura 51. Cambio correcto de permisos.

Como podemos comprobar en la *Figura 50* sin los permisos nos sería imposible, en la *Figura 51* nos aseguramos que los permisos son correctos para evitar el bloqueo y la dificultosa creación de nuevas llaves de acceso.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
	Pág 55 de 106	2021/2022

Si aun con esta solución nos es imposible acceder deberemos hacer lo siguiente:

```

jc@DESKTOP-KN5MPES:~/ssh $ ls
id_rsa id_rsa.pub known_hosts
jc@DESKTOP-KN5MPES:~/ssh $ ssh-keygen -m PEM -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/jc/.ssh/id_rsa): proxy-redirect
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in proxy-redirect
Your public key has been saved in proxy-redirect.pub
The key fingerprint is:
SHA256:OoB+J6CFjGNpJ+sdDN22+Vp/c5U+yX9AOkgXFtm1j+8 jc@DESKTOP-KN5MPES
The key's randomart image is:
+---[RSA 4096]----+
|          .+ .. |
|          + .. |
|          . .. |
| o.o...     . .o |
| +B+o.o S. o o. o |
| o=*. .o. . o + |
| ...oo+. .+o |
| . . .oo.. o . * |
| . . . . . o E |
+---[SHA256]----+
jc@DESKTOP-KN5MPES:~/ssh $ ls
id_rsa id_rsa.pub known_hosts proxy-redirect proxy-redirect.pub
jc@DESKTOP-KN5MPES:~/ssh $ cat proxy-redirect.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQADQzDz7E+P0Rp8h+htBt0gRHfjQtndZ9c0018R1FRgYHZ3A+XtPkt7vmaj1qXbx0K1zX2vEouyyLb6g8g33z
QnL538dYl+7V/w6XpoYc1XY1M0R4r/0mrHRzf4MYB5x6qo17cU6wp43Q01rUGS2g9EBXXGNeU0yGwEpsWzbhh87m+rwlub1vMJ/V5zIv4yiJ07bjCV
tphKpjRj9Q71fc5U3z1pNT3NjKsMr00uW9QsaNv37+m4Jgj7ZypS2JuTPHf+aJAQ0vB+S30Zk/BPkv514EcBMMdNGj2Fj775pGGXqT1wUr4hqGzshaZ8v
Ag7ZFjMF77ESGiHB-JWxHrmF7eDC1EfCZj26M9wg/SFQC+hF9hRMj1ke856equHc5N4909w4xLUL3d9cz3MwyPH094x9KNkY7oUQ2I966uhHG8qKUTyvm1Nh
GtBs9k0q3vVM50c8XT2jU2je1TWEKS5BUS1oCgaSgi5CU2Ktj9EuzN1Adsj/++y1DbeuxhjywTuRLQnx2N1I1eUDx2pJRgoJ9ApcOe6WApbNTLs4M8zgk+
M1QdG+pLVywBpTJ7n5FVJkcCcjd8HCqTDyBax5eB9HE2pNTCqe1puo8GuuJPBjvd4tYoJAIRD9VQ+66TS0gS7282fKZzcBDEPz9302OhimJvhe0ZHwbHEwa
cQ== jc@DESKTOP-KN5MPES
jc@DESKTOP-KN5MPES:~/ssh $

```

Figura 52. Creación de nueva pareja de claves.

En la imagen anterior lo que podemos ver es el proceso de creación de un par de claves (proxy-redirect y proxy-redirect.pub). Con este par de claves pasaremos al reseteo de nuestro acceso, donde copiaremos nuestra clave pública (.pub).

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet CERTIFIED QUALITY SYSTEM ER-0934 / 2008
Pág 56 de 106		2021/2022

Reset password or SSH key ...

proxy-redireccion

Updating...

 Update

This uses the VMAccessForLinux extension to reset the credentials of an existing user or create a new user with sudo privileges, and reset the SSH configuration. [Learn more](#)

Mode ⓘ

Reset password

Reset SSH public key

Reset configuration only

Username * ⓘ

redirectadmin

SSH public key * ⓘ

```
ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQACQD5dz7E+P0Rp8h+htBtOgRHfjQtnZD9c0O18R1FRgYHZ3A+XtPkt7vmaj1qXbx0K1zX2vEouyyLb6g8g33zQnL538dYW+7Y
IpNT3NjKsMr00uW9QsaNv37+m4Jgj7ZypS2JuTPHf+aJAQ0vB+S30Zk/BPkv5l4ECbMmMdNgj2Fj775pGGXqT1wUr4hqGzshaZ8vAg7ZFjMF77ESGiHB+jWxHrmF7e
```

Figura 53. Reset de clave ssh.

```
jc@DESKTOP-KNSMPES:~/ssh$ ls -la
total 28
drwx----- 2 jc jc 4096 May 30 00:04 .
drwxr-xr-x 4 jc jc 4096 May 29 22:40 ..
-rw----- 1 jc jc 2610 May 29 22:37 id_rsa
-rw-r--r-- 1 jc jc 572 May 29 22:37 id_rsa.pub
-rw-r--r-- 1 jc jc 666 May 30 00:00 known_hosts
-r----- 1 jc jc 3243 May 30 00:04 proxy-redirect
-rw-r--r-- 1 jc jc 744 May 30 00:04 proxy-redirect.pub
jc@DESKTOP-KNSMPES:~/ssh$ ssh -i proxy-redirect redirectadmin@20.107.204.214
Linux proxy-redireccion 5.10.0-14-cloud-amd64 #1 SMP Debian 5.10.113-1 (2022-04-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
redirectadmin@proxy-redireccion:~$ ls
redirectadmin@proxy-redireccion:~$
```

Figura 54. Acceso correcto.

Una vez implementado todo lo anterior podemos comprobar que accedemos a la máquina de manera correcta, asegurándonos que hemos cambiado los permisos de lectura correctamente (observar en la Figura 54).

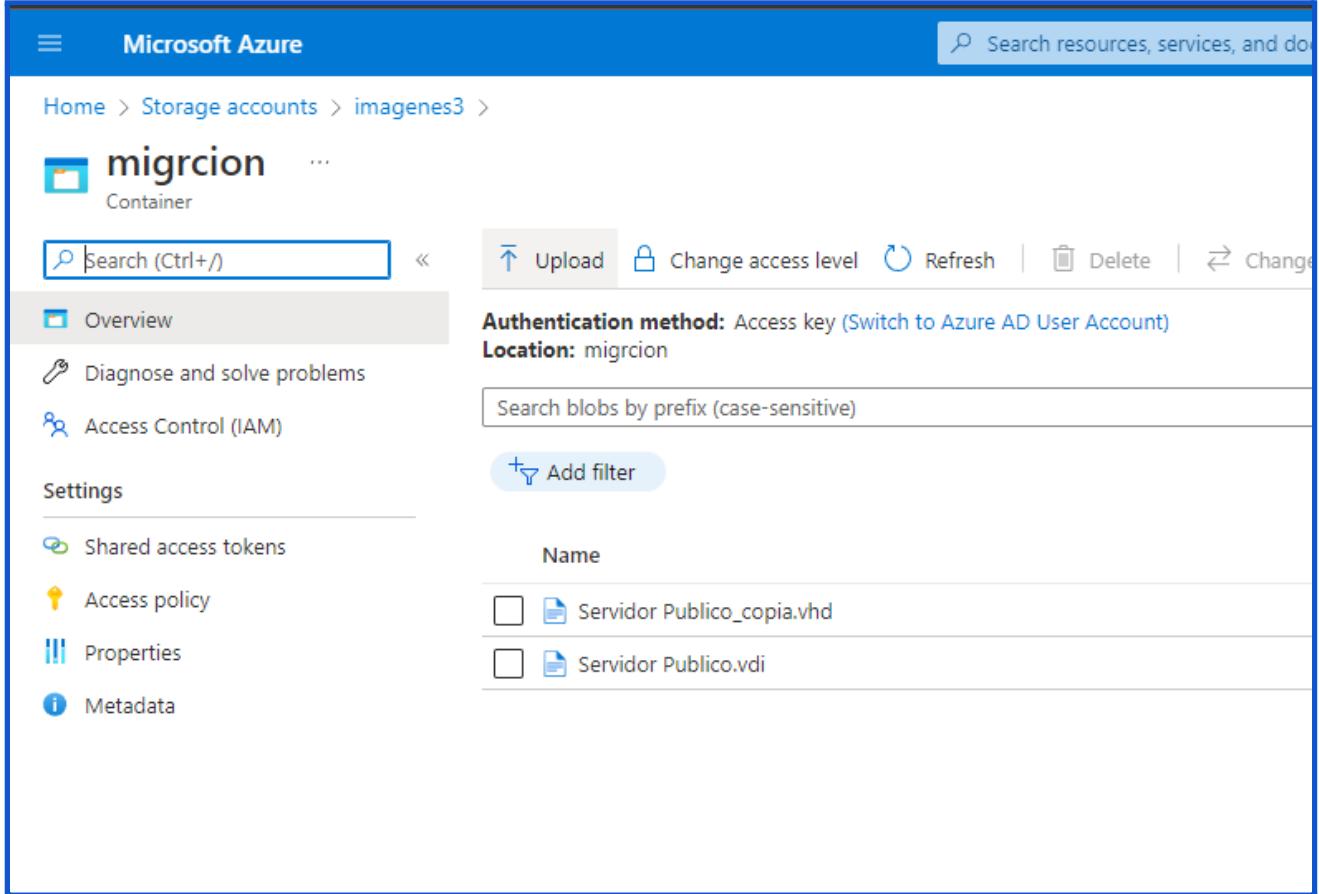
Pasamos así a la instalación del servicio según la guía facilitada en el anexo. Cabe remarcar que para la completación total de esta redirección necesitamos una IP fija para acceder a

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 57 de 106			2021/2022

nuestro servidor, tarea que requiere de una inversión monetaria fuera de Azure, por eso no mostraremos pruebas de este proceso en particular.

Una vez puesto en marcha nuestro balanceador y nuestro proxy de redirección, solo queda hacer realidad la migración. Existen muchas [técnicas¹](#) a la hora de llevar a cabo una migración, en este caso particular podríamos debatirnos entre un “rehost”, llevar los datos a servidores ya creados en la nube, o “rebuild”, con el que reconstruiremos los servicios en la nube. Azure provee con herramientas como para poder hacer cualquier tipo, sin embargo transportar los datos a servidores ya creado implica un trabajo doble de creación y transporte seguro (así como optimización a la nube).

Reconstruir el servicio es más sencillo para una guía de esta índole:



The screenshot shows the Microsoft Azure Storage Accounts interface. The main navigation bar at the top says "Microsoft Azure". Below it, the breadcrumb navigation shows "Home > Storage accounts > imagenes3 >". The main content area displays a storage container named "migracion". On the left, there's a sidebar with options like "Overview", "Diagnose and solve problems", "Access Control (IAM)", "Settings", "Shared access tokens", "Access policy", "Properties", and "Metadata". The "Overview" tab is selected. In the main pane, there's a search bar labeled "Search (Ctrl+/" followed by "Upload", "Change access level", "Refresh", "Delete", and "Change". Below that, it says "Authentication method: Access key (Switch to Azure AD User Account)" and "Location: migracion". There's also a "Search blobs by prefix (case-sensitive)" input field and a "Add filter" button. A table lists blobs with columns "Name" and "Type". The table contains two entries: "Servidor Publico_copia.vhd" and "Servidor Publico.vdi".

Figura 55. Cuenta de almacenamiento.

En el servicio blob tenemos varias imágenes, dado que Azure no permite la importación directa de imágenes, debemos convertir nuestros discos. Existen varios métodos, pasarlo a Hyper-V, con Powershell o con distintas herramientas. Aquí mostraremos 2 de ellas:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet CERTIFIED Quality System ER-0934 / 2008
Pág 58 de 106		2021/2022

Con una herramienta de pago que permite este uso como gratuito, llamada StarWind V2V:

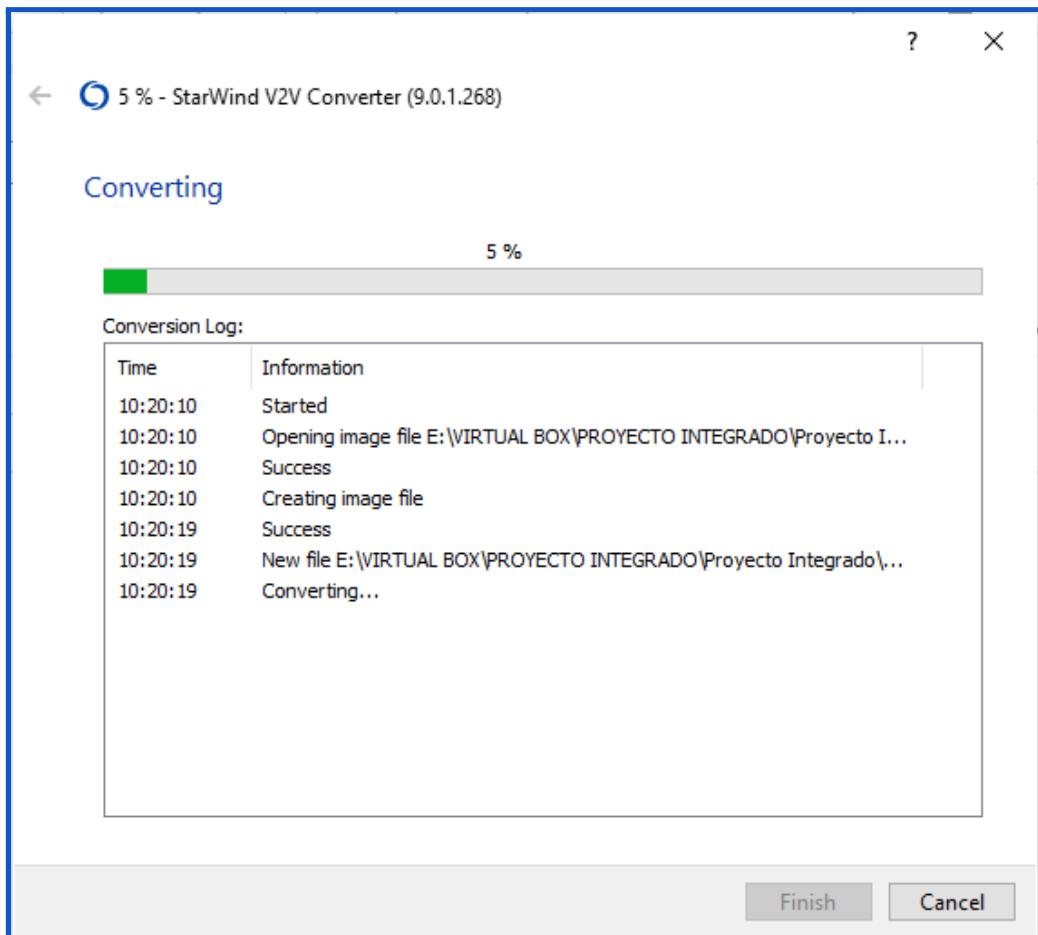


Figura 56. Conversión con StarWind.

Y con un clásico fiable, Powershell, quien inspira más confianza que una aplicación de terceros:

```
PS E:\VIRTUAL BOX\PROYECTO INTEGRADO\Proyecto Integrado\Servidor Publico> Convert-VHD -Path 'Servidor Publico_copia.vhd' -DestinationPath 'Servidor Publico_fixed.vhd' -VHDTtype Fixed
```

Figura 57. Conversión con Powershell.

Con Powershell existe, sin embargo, un problema añadido, y es que generalmente la utilidad de Powershell para “convertir discos” no está habilitada. Esta utilidad la provee Hyper-V de Windows, así que en caso de que Powershell desconozca esta comando tenemos varias vías para [habilitarlo](#)⁹⁹⁻¹⁰⁴. En este caso particular con las Características del Sistemas hemos podido usar el cliente de Hyper-V pero no hemos podido usar el comando de Convert-To-VHD, por ello al final hemos utilizado la herramienta DISM.exe que ha resultado

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 59 de 106			2021/2022

correcta. Con estas herramientas hemos conseguido dos archivos de disco que Azure si ha aceptado en convertir en imágenes:

Create an image ...

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Azure for Students

Resource group * ⓘ proyecto [Create new](#)

Instance details

Name * vhd_imag_ser_pub

Region * ⓘ (Europe) France Central

Zone resiliency

OS disk

OS type * ⓘ Windows Linux

VM generation * ⓘ Gen 1 Gen 2

Storage blob * ⓘ https://imagenes3.blob.core.windows.net/migracion/Servidor Publico_copia(1)... [Browse](#)

Account type * ⓘ Standard HDD

Host caching * ⓘ Read/write

Figura 58. Creación de imágenes Azure.

Para crear la imagen sin errores es importante que esta esté en misma localización que el servicio de blob, sino al intentar compilar la imagen nos dará un error que impide la creación. (Así mismo, aunque Azure lo implementa predeterminadamente, se recomienda crear como “Page Blob” aquellos archivos cuya finalidad sea crear imágenes y máquinas virtuales)

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet CERTIFIED Quality System ER-0934 / 2008
Pág 60 de 106		2021/2022

Create an image

Validation passed

Basics Tags Review + create

Basics

Subscription	Azure for Students
Resource group	proyecto
Region	France Central
Name	vhd_imag_ser_pub
Zone resiliency	false

OS disk

OS type	Linux
VM generation	V1
Storage blob	https://imagenes3.blob.core.windows.net/migracion/Servidor_Publico_copia(1).vhd
Account type	Standard HDD LRS
Host caching	Read/write
SSE encryption type	Platform-managed key

Tags

(none)

Figura 59. Resumen creación imagen.

Antes de crear la imagen nos dará una validación previa (de características). Aconsejamos que, en caso de no tener una región de datos disponible en su país, se acojan al más cercano por calidad del servicio.

✓ Your deployment is complete

 Deployment name: Microsoft.Image-20220602210843 Start time: 6/2/2022, 9:10:04 PM
 Subscription: Azure for Students Correlation ID: f34c8a40-b788-4db6-af9e-d9e235d0072a 
 Resource group: proyecto

Deployment details [\(Download\)](#)

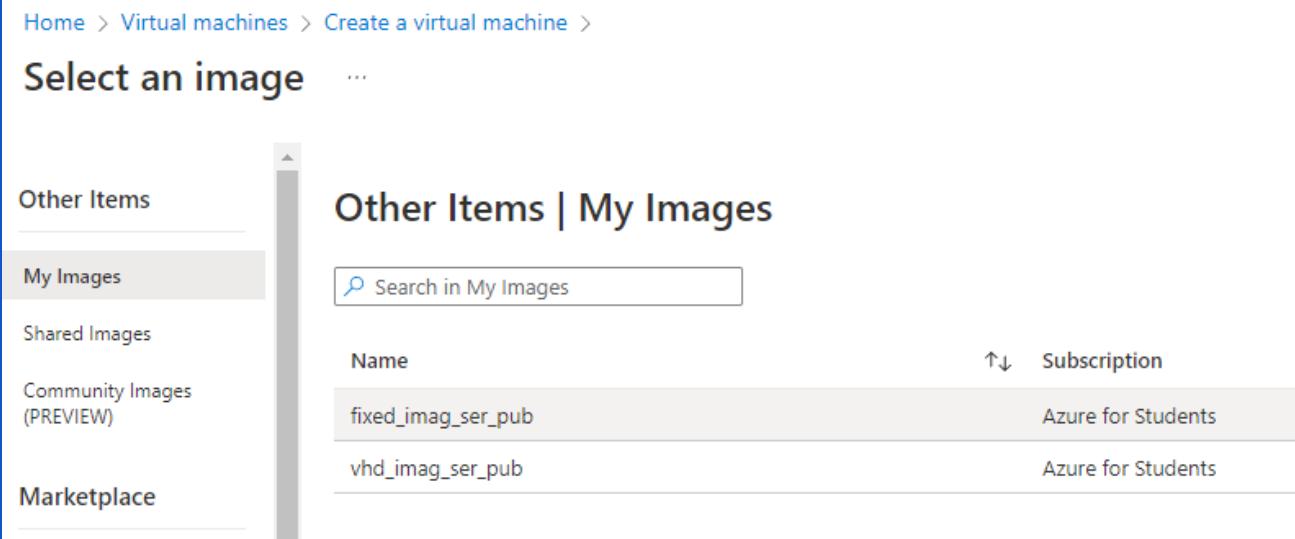
Next steps

[Go to resource](#)

Figura 60. Creación correcta de imagen en Azure.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 61 de 106			2021/2022

Cuando los archivos por fin son correctos, cuando las configuraciones y las medidas están en sintonía, podemos crear una imagen. En nuestro caso hemos creado 2 imágenes, una para cada método, para comprobar cual es falible y cual óptimo. Añadir que en el intento de subir el disco de Virtualbox sin tratar, incluso engañando a Azure, la creación de una Máquina Virtual se hace imposible, de ahí la comprobación por dos medios.



Name	Subscription
fixed_imag_ser_pub	Azure for Students
vhd_imag_ser_pub	Azure for Students

Figura 61. Selección de imágenes.

Para crear las máquinas virtuales haremos lo mismo que anteriormente, con la única diferencia que seleccionaremos una imagen creada por nosotros mismos, como en la Figura 61.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet Empresa Registrada ER-0934 / 2008
Pág 62 de 106		2021/2022

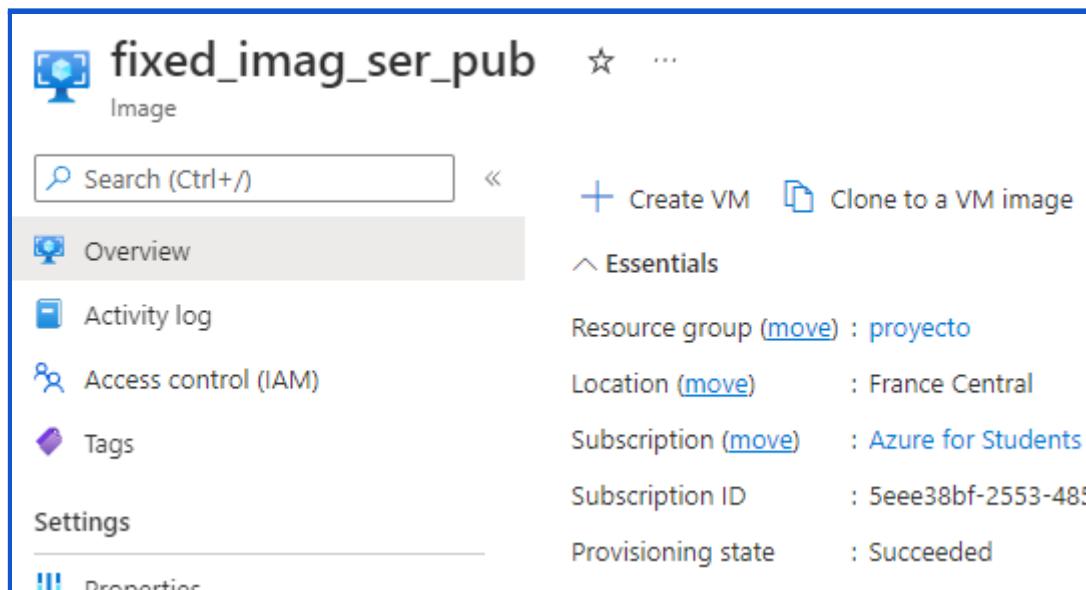
Instance details

Virtual machine name *	fixedservpubl
Region	(Europe) France Central
Availability options	No infrastructure redundancy required
Security type	Standard
Image *	fixed_imag_ser_pub - Gen1
See all images Configure VM generation	
Azure Spot instance	<input type="checkbox"/>
Size *	Standard_D2as_v4 - 2 vcpus, 8 GiB memory (81,76 US\$/month)
See all sizes ✖ This size is currently unavailable in franccentral for this subscription: NotAvailableForSubscription.	

Administrator account

Figura 62. Troubleshoot.

Como siempre hay que tener muy en cuenta que Azure no permite distintas situaciones y configuraciones, en este caso nos encontramos que nuestra imagen, asociada al CPD de Azure de Francia (el más cercano actualmente) no permite el acceso con nuestra suscripción.



fixed_imag_ser_pub

Image

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Create VM

Clone to a VM image

Resource group (move) : proyecto

Location (move) : France Central

Subscription (move) : Azure for Students

Subscription ID : 5eee38bf-2553-485

Provisioning state : Succeeded

Figura 63. Movimiento entre localizaciones Azure.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 63 de 106		2021/2022

Para solucionar este problema, en la imagen ya creada podemos ver cómo podemos mover la imagen entre regiones. En caso de no ser posible por suscripción, deberíamos mover el blob original y repetir los pasos anteriores en otra localización que sí permite creación.
(Este problema sólo surge por tener una suscripción genérica de estudiante)

Create a virtual machine

Validation passed

Basics Disks Networking Management Advanced Tags Review + create

⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

fixed_imag_serpub1	Standard D2as v4
Image	2 vcpus, 8 GiB memory
Basics	
Subscription	Azure for Students
Resource group	proyecto
Virtual machine name	servpublico1
Region	North Europe
Availability options	No infrastructure redundancy required
Security type	Standard
Image	fixed_imag_serpub1 - Gen1
Size	Standard D2as v4 (2 vcpus, 8 GiB memory)
Authentication type	SSH public key
Username	publicadmin
Key pair name	claveservidorpublico
Public inbound ports	SSH, HTTP
Azure Spot	No

Figura 64. Creación de MV en localización permitida .

Con la configuración de nuestra nueva máquina virtual, movida a una localización permitida debería solucionar nuestro problema.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 64 de 106			2021/2022

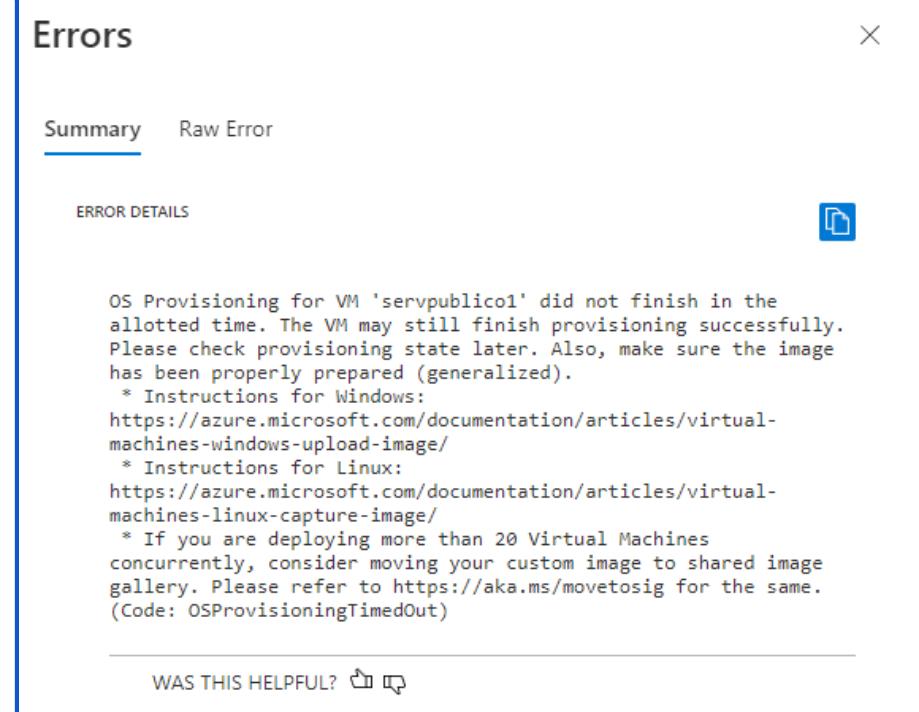


Figura 65. Error 1 en creación de MV.

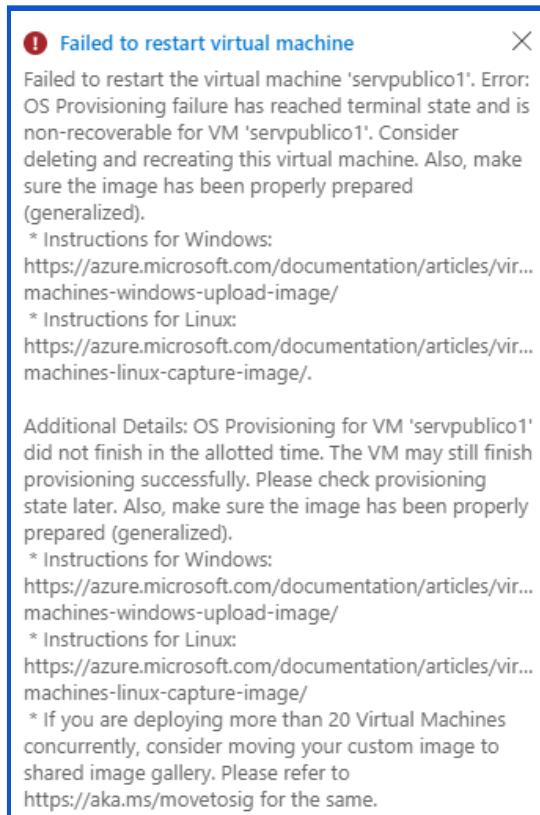


Figura 66. Error 2 en creación de MV.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 65 de 106			2021/2022

Como podemos comprobar sin embargo en las imágenes anteriores, la MV creada mediante el comando-utilidad de Hyper-V, ejecutado con Powershell no soluciona nuestro problema.

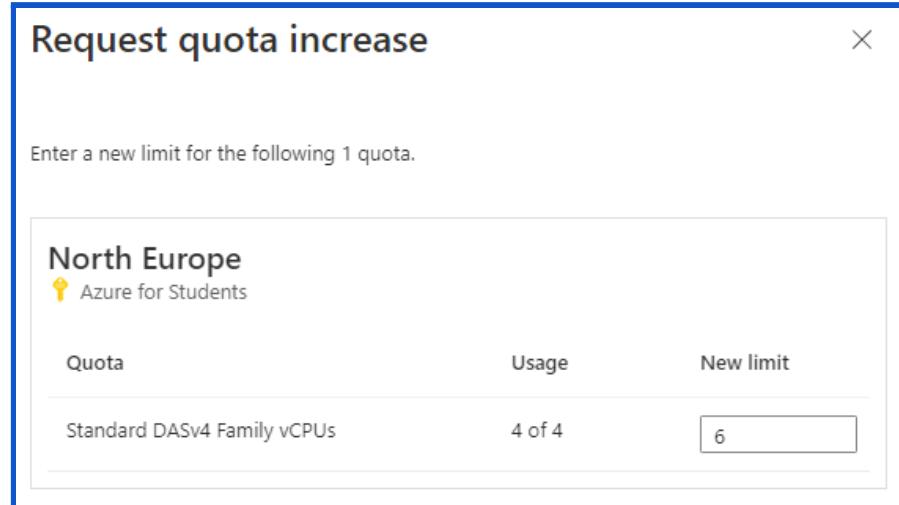


Figura 67. Cuota máxima permitida.

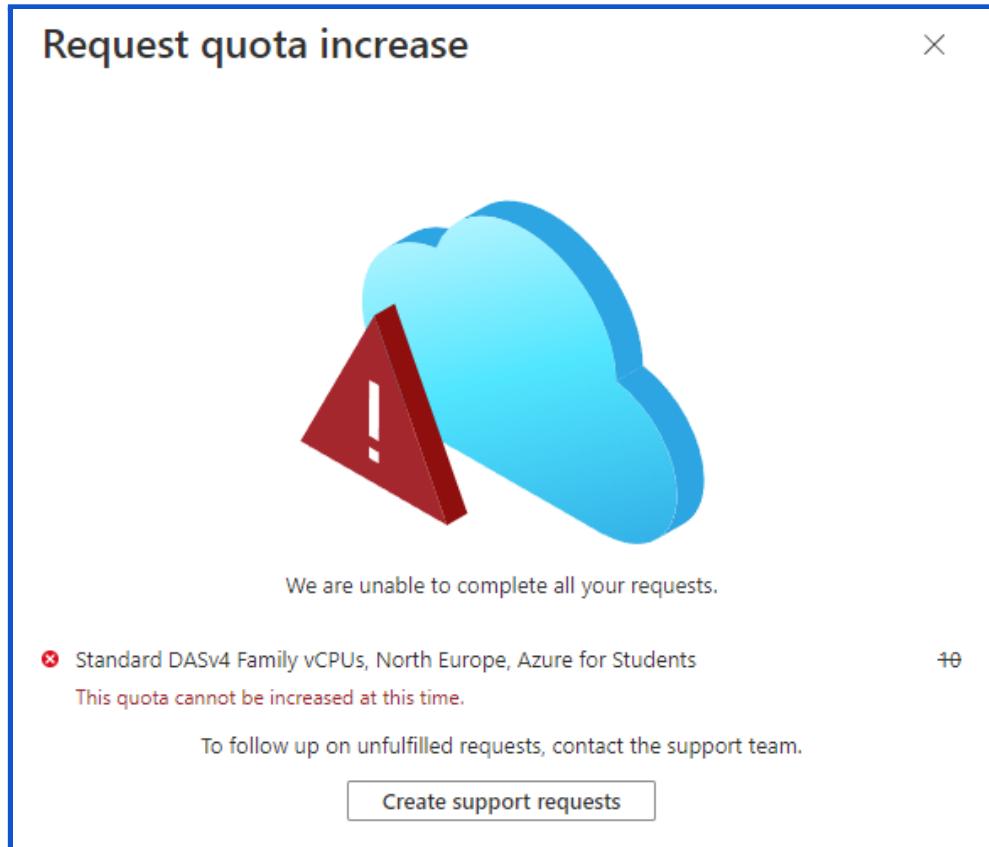


Figura 68. Deniegan ampliar la cuota de máquinas.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 66 de 106			2021/2022

Con este problema añadido nos enfrentamos, no podemos exportar nuestro sistema según las herramientas de Azure, y además no podemos tener más de dos máquinas corriendo en nuestro servicio. Sin embargo tenemos la redirección hecha, durante este proceso, aun con problemas, nuestro servicio ya está “en la nube”.

Ante esto se propone lo siguiente:

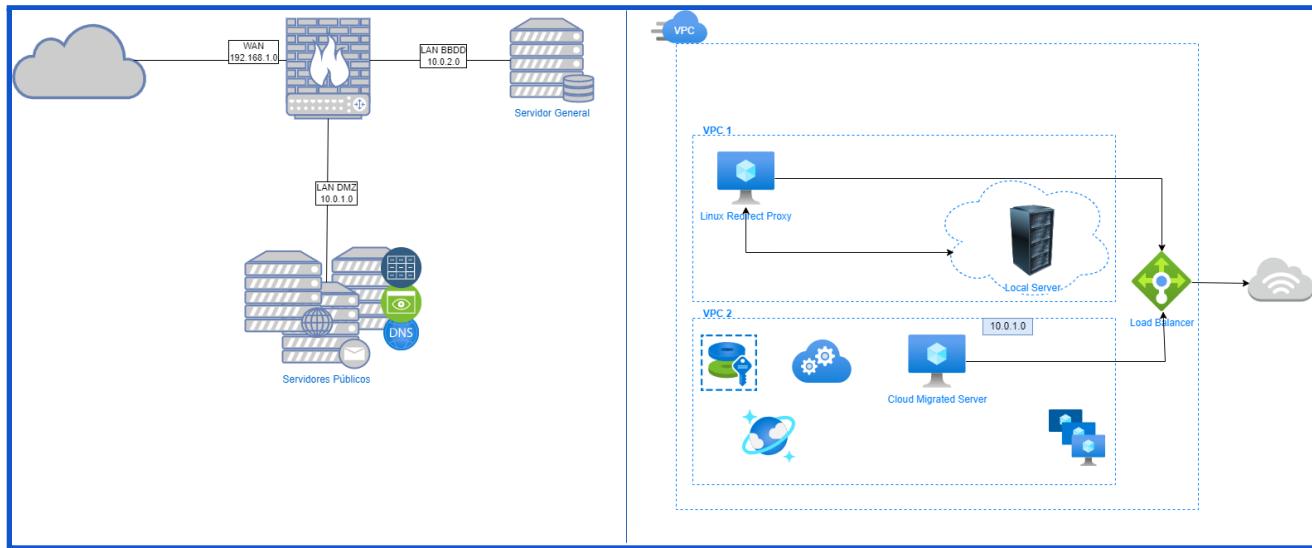


Figura 69. Esquema conjunto.

Proponemos un esquema superreducido (2 máquinas por la suscripción estudiante), lo que nos lleva a asumir ciertos servicios, que gracias a la nube podemos suplir.

El servidor de backups es lo más fácil, pues azure implementa un servicio, *Backup Center*:

Operation	Failed	In progress	Completed
Scheduled backup	0	0	0
On-demand backup	0	0	0
Restore	0	0	0

Figura 70. Backup Center.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 67 de 106			2021/2022

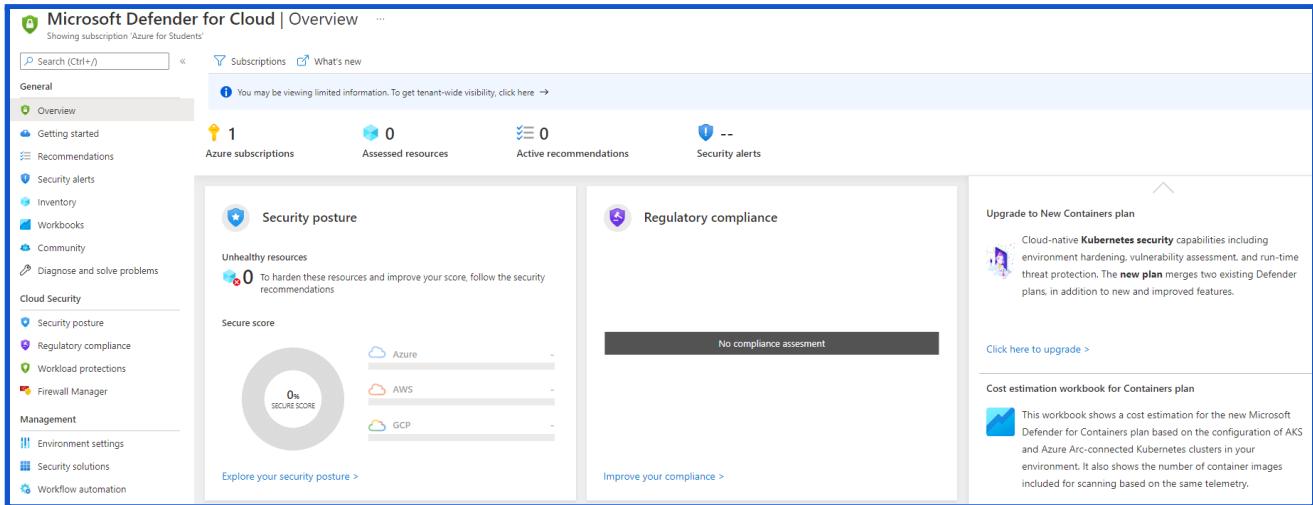
En este centro de Backups podemos crear políticas para nuestros guardados, programarlos, etc.

The screenshot shows the 'Create policy' dialog for an Azure Virtual Machine. The policy name is set to 'DailyPolicy-l41oyq2t'. The backup schedule is configured with a daily frequency at 4:00 AM UTC+01:00. The instant restore setting retains 5 days of instant recovery snapshots. Under the retention range, there are two main options: 'Retention of daily backup point' (checked, at 4:00 AM for 60 days) and 'Retention of monthly backup point' (checked, week-based, on the first Sunday at 4:00 AM for 10 months). There is also an unchecked option for 'Retention of yearly backup point'.

Figura 71. Backup Policies.

Habiendo solucionado el problema del backup, el siguiente problema sería nuestro IPS/IDS, que en la nube juegan un rol distinto. En la nube, las reglas de firewall clásicas se convierten en políticas asociadas a nuestro Defender:

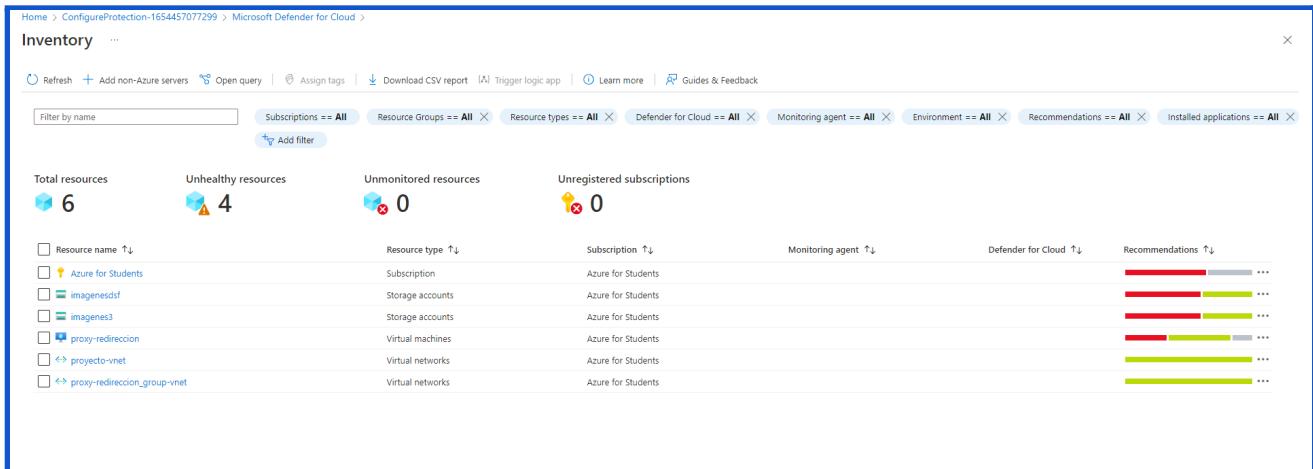
 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 ER Empresa Registrada ER-0934 / 2008
Pág 68 de 106		2021/2022



The screenshot shows the Microsoft Defender for Cloud Overview page. It features a navigation bar with 'General' (selected), 'Subscriptions', and 'What's new'. A message indicates limited information for the current tenant. Key metrics are displayed: 1 Azure subscription, 0 Assessed resources, 0 Active recommendations, and 0 Security alerts. The 'Security posture' section shows an unhealthy score of 0% and a call to action to harden resources. The 'Regulatory compliance' section shows 'No compliance assessment' with a link to 'Improve your compliance >'. On the right, there's a sidebar for 'Upgrade to New Containers plan' and a 'Cost estimation workbook for Containers plan' with a preview of its contents.

Figura 72. Microsoft Defender for cloud.

Este servicio que Azure presta incluso a otras nubes (ver Figura 72) rige las reglas de acceso externo a nuestros servicios. Aquí cumpliríamos la parte de IPS, la de IDS se cumple al crear alertas personalizadas para nuestros servicios.



The screenshot shows the Microsoft Defender Inventory page. It includes a top navigation bar with 'Home', 'ConfigureProtection-1654457077299', 'Microsoft Defender for Cloud', and a search bar. Below is a filter bar with various dropdowns and a 'Add filter' button. The main area displays four categories: 'Total resources' (6), 'Unhealthy resources' (4), 'Unmonitored resources' (0), and 'Unregistered subscriptions' (0). A detailed table follows, listing resources by type, subscription, monitoring agent, and Defender for Cloud status. The table includes columns for Resource name, Resource type, Subscription, Monitoring agent, Defender for Cloud, and Recommendations. Each row has a checkbox and a 'More details' link.

Figura 73. Recomendaciones Defender.

A la misma vez, migrar a la nube nos permite una consulta gratuita para la mejora de la seguridad de nuestra nube. El Defender hace inventario de nuestros servicios, los analiza y hace una recomendación para aumentar la seguridad en cada uno, ya sea una máquina virtual, una VPC, etc.

Con esto tendríamos simplificado y ajustado nuestro sistema a la nube, ahora solo falta nuestro servidor público ejecutado con Docker. Para la nube de Azure podríamos sustituir incluso esta máquina por un cluster de Kubernetes.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 69 de 106</i>			<i>2021/2022</i>

Create Kubernetes cluster ...

Basics Node pools Access Networking Integrations Advanced Tags Review + create

Azure Kubernetes Service (AKS) manages your hosted Kubernetes environment, making it quick and easy to deploy and manage containerized applications without container orchestration expertise. It also eliminates the burden of ongoing operations and maintenance by provisioning, upgrading, and scaling resources on demand, without taking your applications offline.

[Learn more about Azure Kubernetes Service](#)

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Azure for Students

Resource group * ⓘ

projeto

[Create new](#)

Cluster details

Cluster preset configuration

Cost-optimized (\$)

To quickly customize your Kubernetes cluster, choose one of the preset configurations above. You can modify these configurations at any time.

[Learn more and compare presets](#)

Kubernetes cluster name * ⓘ

serpublic

Region * ⓘ

(Europe) North Europe

Availability zones ⓘ

None

Kubernetes version * ⓘ

1.22.6 (default)

API server availability ⓘ

- 99.9%
Optimize for availability. 99.95% is available when at least one availability zone is selected.
 - 99.5%
Optimize for cost.
- 99.5% API server availability is recommended for cost optimized configuration.

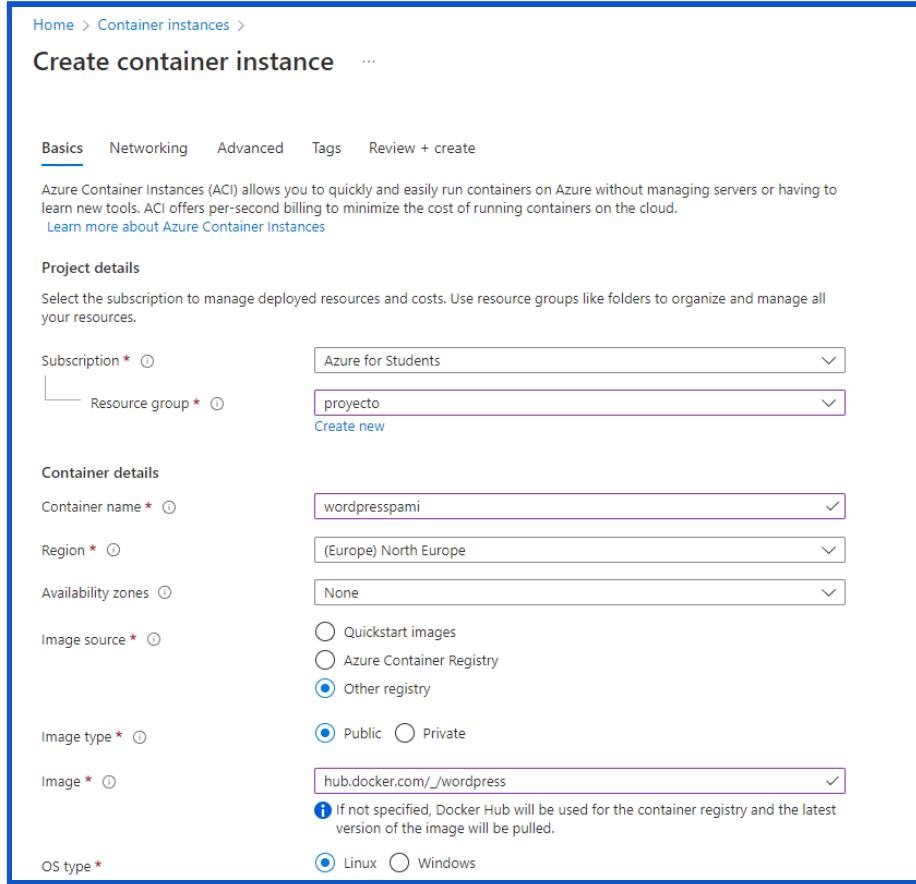
Figura 74. Creación cluster Kubernetes.

Azure nos ayuda (en todo momento) a hacer la creación del cluster lo más “cost-effective” (económico) posible si es nuestro deseo, o podemos hacerlo lo más eficiente sea cual sea el precio, Azure nos lo deja a libre elección.

Sin embargo, comprender, ejecutar y plantear un servicio en Azure es ya en sí una tarea titánica para un novato en el entorno cloud como es servidor, como para además profundizar en Kubernetes. Por eso, porque es interesante, de contar con más tiempo sería mi elección predilecta.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 70 de 106			2021/2022

Aun así no es nuestra última posibilidad. La limitada suscripción de estudiante no nos permite mucho margen, pero podemos exprimir al máximo la experiencia cloud qué es Azure para llevar nuestro servicio a la nube.



The screenshot shows the 'Create container instance' wizard in the Azure portal. The 'Basics' tab is selected. Key configuration details include:

- Subscription:** Azure for Students
- Resource group:** proyecto
- Container name:** wordpresspami
- Region:** (Europe) North Europe
- Availability zones:** None
- Image source:** Other registry (selected)
- Image type:** Public (selected)
- Image:** hub.docker.com/_/wordpress
- OS type:** Linux (selected)

Figura 75. Azure Container Instances.

Con los contenedores de Azure consumimos 1 vcpu por contenedor, disponiendo de 4 para nuestra suscripción, y consumiendo 2 por el proxy de redirección, ¡incluso nos sobra uno para crear otro servicio más!

 <p>IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla</p>	<h2>Guía Práctica para el uso profesional de la nube</h2>	 <p>AENOR ER Empresa Registrada ER-0934 / 2008</p>  <p>CERTIFIED IQNet QUALITY SYSTEM</p>
	Pág 71 de 106	2021/2022

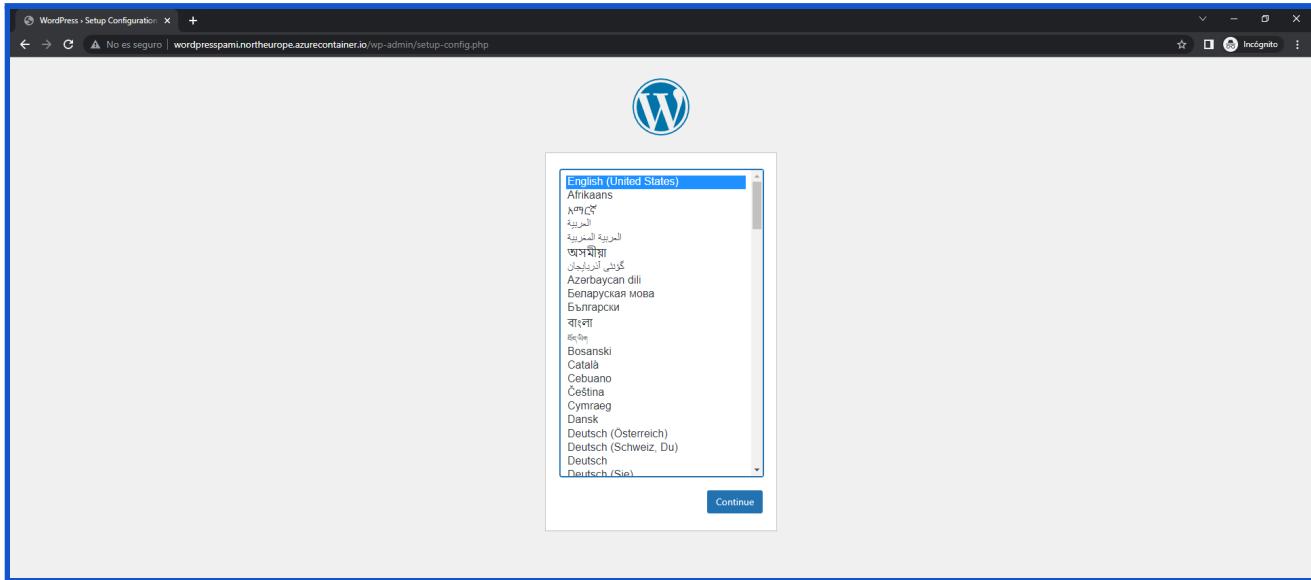


Figura 76. Contenedor de Azure con Wordpress.

Con esto completo ya tenemos nuestros servicios en la nube, solo deberemos de ir copiando los datos a la nube y podemos acceder a nuestros recursos, que hasta implantación, estarán en desarrollo o preproducción para implementarse al 100% en la nube.

Sin embargo, y por la practicidad de esta guía, existe otra manera. Azure tiene un potencial grandísimo, uno que solo usándolo puede ver. No es necesario conocer técnicamente las tecnologías para implementar los servicios.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	<i>Pág 72 de 106</i>		2021/2022

Home >

Create a resource

...

Get Started

Recently created

Categories

- AI + Machine Learning
- Analytics
- Blockchain
- Compute
- Containers
- Databases
- Developer Tools
- DevOps
- Identity
- Integration
- Internet of Things
- IT & Management Tools
- Media
- Migration
- Mixed Reality
- Monitoring & Diagnostics
- Networking
- Security
- Storage
- Web

Popular Azure services [See more in All services](#)

-  API Management [Create](#) | [Docs](#) | [MS Learn](#)
-  App Service Environment v3 [Create](#) | [Learn more](#)
-  Communication Services [Create](#) | [Learn more](#)
-  Media Services [Create](#) | [Docs](#)
-  Azure Cognitive Search [Create](#) | [Docs](#) | [MS Learn](#)
-  Static Web App [Create](#) | [Docs](#) | [MS Learn](#)
-  Web App [Create](#) | [Docs](#) | [MS Learn](#)

Getting Started? Try our Quickstart center

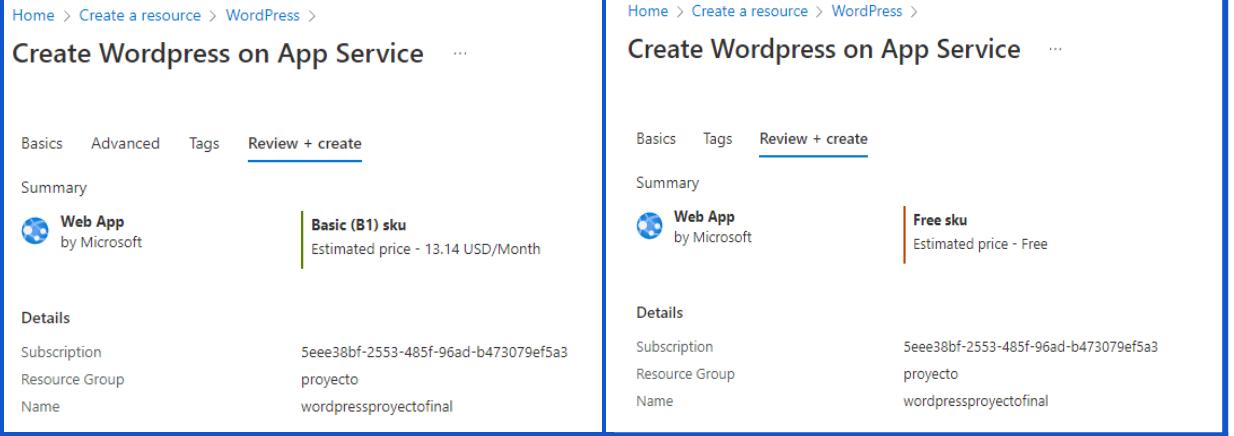
Popular Marketplace products [See more in Marketplace](#)

-  cPanel & WHM - Bring your own license [Create](#) | [Learn more](#)
-  Bitnami LMS powered by Moodle(TM) LMS [Create](#) | [Learn more](#)
-  WordPress packaged by Bitnami [Create](#) | [Learn more](#)
-  ProcessMaker Community packaged by Bitnami [Create](#) | [Learn more](#)
-  wordpress-5.7.1 [Create](#) | [Learn more](#)
-  Free [Set up + subscribe](#) | [Learn more](#)
-  WordPress Web Server on Ubuntu 18.04 + Apache SSL [Create](#) | [Learn more](#)
-  WordPress on Ubuntu 20.04 LTS + Apache Web Server [Create](#) | [Learn more](#)
-  OpenLiteSpeed WordPress [Create](#) | [Learn more](#)
-  Licensed cPanel Pro Edition [Create](#) | [Learn more](#)

Figura 77. Recursos instantáneos de Azure.

Al final, el objetivo de este proyecto es mostrar todo el potencial de la nube, pero también mostrar que ante cada problema encontrado en nuestro servicio local, la nube encuentra una manera rápida, eficaz, elegante (y barata) de solucionar nuestro problema sin mucha complicación. Por eso, en el inicio del Portal Azure, al crear un recurso nuevo, predeterminado, Azure ya cuenta con la mayoría de servicios más usados implementados, a un solo click de empezar.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 73 de 106			2021/2022



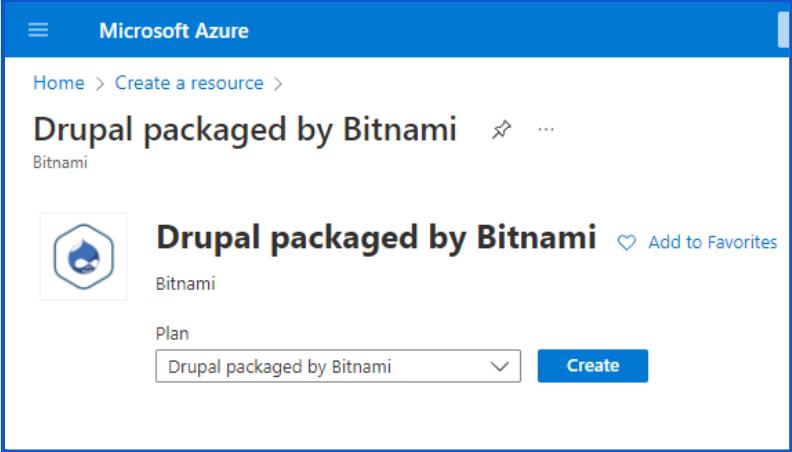
The screenshot shows the Microsoft Azure 'Create a resource' interface for 'WordPress'. It displays two options:

- Basic (B1) sku**: Estimated price - 13.14 USD/Month. This option is highlighted.
- Free sku**: Estimated price - Free.

Both options include details such as Subscription ID, Resource Group, and Name.

Figura 78. App Service Wordpress.

Por solo 13.14\$ (12,26€) al mes en Linux, y gratis en Windows, podemos tener nuestra propia página web de wordpress, sin conocer nada técnicamente, y además será muy seguro porque lo implementa Azure, y lo complementa Microsoft Defender con distintas recomendaciones de seguridad. Un plato caliente listo para ser comido.



The screenshot shows the Microsoft Azure 'Create a resource' interface for 'Drupal'. It displays the following information:

- Drupal packaged by Bitnami** (by Bitnami)
- Drupal packaged by Bitnami** icon
- Add to Favorites** button
- Plan** dropdown menu: 'Drupal packaged by Bitnami'
- Create** button

Figura 79. Drupal también en Azure.

Recordatorio de que Azure cumple en el caso de que queramos usar un CMS distinto, y muy usado, como es Drupal. Por consecuencia del proyecto continuaremos con Wordpress pero existen muchas alternativas a estudiar.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 74 de 106		2021/2022

Para migrar nuestros datos, en este método, deberemos copiar los archivos de un servidor a otro. Teniendo en cuenta que se encuentran en nuestro contenedor de Docker debemos sacarlos al servidor local y luego copiarlos. Para eso:

```
admin@server:~$ docker cp wordpress:/var/www/html ~/wordpress
admin@server:~$ ls
backup    backup.sh.save      check.txt  docker-compose.yml  mysql      wordpress
backup.sh  backup_wordpress_15052022  denied    Dockerfile        permission
admin@server:~$ cd wordpress/
admin@server:~/wordpress$ ls
index.php   wp-activate.php    wp-config-docker.php  wp-cron.php     wp-login.php    wp-trackback.php
license.txt  wp-admin          wp-config.php       wp-includes    wp-mail.php     xmlrpc.php
readme.html  wp-blog-header.php wp-config-sample.php wp-links-opml.php wp-settings.php
wordpress   wp-comments-post.php wp-content         wp-load.php     wp-signup.php
admin@server:~/wordpress$
```

Figura 80. Copia de wordpress en docker.

Con los archivos ya copiados en el servidor, hacemos un simple scp:

```
jc@DESKTOP-KN5MPES:/mnt/c/Users/Jc$ scp -r -P 55055 admin@172.16.0.58:/home/admin/wordpress ~/wordpress
!Cuidado!
Solo acceso autorizado
Se tomaran las medidas pertinentes contra los intrusos
admin@172.16.0.58's password:
wp-login.php                           100%   47KB  24.0MB/s  00:00
wp-settings.php                         100%   22KB  25.4MB/s  00:00
wp-config-docker.php                   100%  5480   12.5MB/s  00:00
generic.png                            100%    719   1.8MB/s  00:00
post-formats-vs.png                   100%  2450   5.2MB/s  00:00
no.png                                 100%    755   1.7MB/s  00:00
icons32-vs-2x.png                     100%   21KB  26.8MB/s  00:00
list-2x.png                            100%  1523   3.6MB/s  00:00
media-button-video.gif                100%   133  409.5KB/s  00:00
about-header-credits.svg              100%  5410   10.4MB/s  00:00
```

Figura 81. Copia de wordpress a intermedio.

Una vez tenemos los archivos copiados a nuestro cliente intermedio, que tiene la clave pública, lo copiaremos a nuestro servidor

```
jc@DESKTOP-KN5MPES:~/.ssh$ scp -i wordpress -r ~/wordpress/wp-content adminwordpres@wordpressproyectofinal.northeurope.cloudapp.azure.com:/home/adminwordpress
hello.php                           100%  2578   54.3KB/s  00:00
.htaccess                          100%   633   14.0KB/s  00:00
wrapper.php                         100%  6438  136.5KB/s  00:00
predefined.php                     100%   318   7.1KB/s  00:00
connect-jp.php                     100%  4985  102.7KB/s  00:00
activate.php                        100%   177   3.9KB/s  00:00
```

Figura 82. Copia de intermedio a la nube.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 75 de 106		2021/2022

Como en este caso estamos ejecutando una imagen de Bitnami, necesitamos las credenciales para entrar en nuestra web:

```
$ sudo cat /home/bitnami/bitnami_credentials
Welcome to the WordPress packaged by Bitnami

*****
The default username and password is 'user' and 'z7dmadv8ANdo'.
*****

You can also use this password to access the databases and any other component the stack includes.

Please refer to https://docs.bitnami.com/ for more details.
```

Figura 83. Credenciales bitnami.

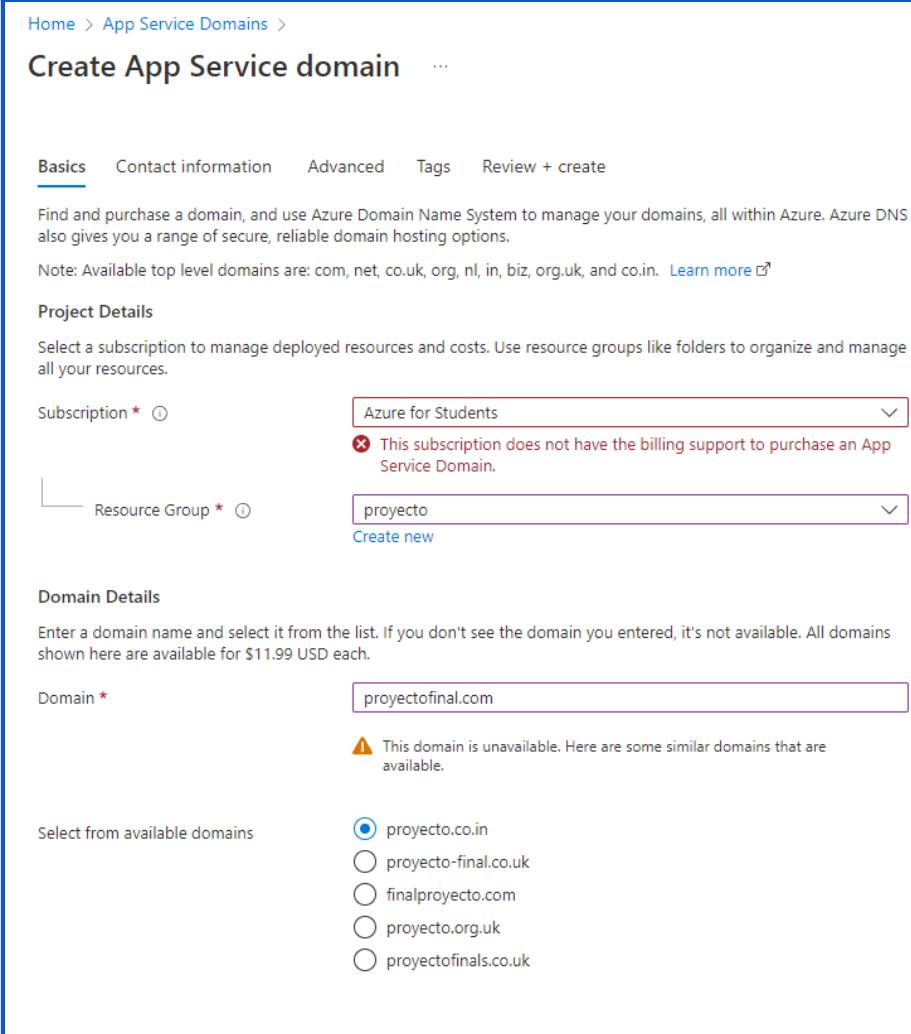
Y aun cuando todo parecía estar en contra:



Figura 84. Wordpress finalmente en la nube.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 76 de 106			2021/2022

Pero esto no termina aquí, porque una de las herramientas que nos provee Azure es el poder sustituir los hostings generales por el mismo Azure:



Home > App Service Domains >

Create App Service domain

Basics Contact information Advanced Tags Review + create

Find and purchase a domain, and use Azure Domain Name System to manage your domains, all within Azure. Azure DNS also gives you a range of secure, reliable domain hosting options.

Note: Available top level domains are: com, net, co.uk, org, nl, in, biz, org.uk, and co.in. [Learn more](#)

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ ⓘ This subscription does not have the billing support to purchase an App Service Domain.

Resource Group * ⓘ ⓘ Create new

Domain Details

Enter a domain name and select it from the list. If you don't see the domain you entered, it's not available. All domains shown here are available for \$11.99 USD each.

Domain *

⚠ This domain is unavailable. Here are some similar domains that are available.

Select from available domains

- projecto.co.in
- projecto-final.co.uk
- finalprojecto.com
- projecto.org.uk
- projectofinals.co.uk

Figura 85. Dominio personalizado.

Finalmente con las limitaciones de la suscripción no hemos podido explorar los dominios personalizados, pudiendo dejar de pagar a un proveedor externo y utilizar las herramientas que Azure nos brinda.

Con esto nos hemos quedado con nuestro servicio TOTALMENTE migrado a la nube en:

<http://wordpressproyectofinal.northeurope.cloudapp.azure.com/>

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 77 de 106		2021/2022

Sin embargo, con Azure, cada característica y perspectiva se puede llevar más allá.

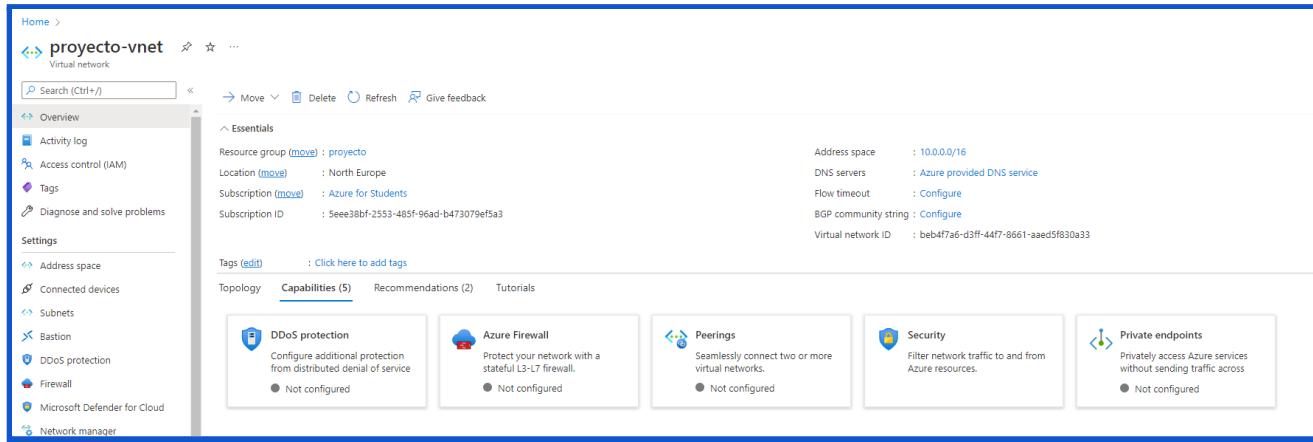


Figura 86. VPC principal.

Por ejemplo, una vez migrado el servicio, podemos darle redundancia a nuestro sistema, esto se puede conseguir tanto de manera “clásica” como de manera actual. Esto es, duplicar servicios manualmente y balancearlos para que funcionen como uno, uso que se hace con aquellos servicios que sufren distintas fases de desarrollo.

Si necesitamos un servicio (o web como nuestro caso) y queremos mejorarla, probar cosas nuevas, sin cerrar el acceso a nuestra web y fuente de ingresos, debemos pasar por un estado de “Desarrollo”, donde se planifica y crea una posible mejora para nuestro servicio, otro de “Preproducción”, donde se implanta la mejora o actualización en un entorno controlado para verificar si es lo suficientemente estable para el público general, y finalmente se integra totalmente en el estado de “Producción”, donde ya se disfruta para el público general de la mejora/actualización.

Justo por este método de mejora continua, de Desarrollo Continuo, un balanceo manual es una opción real muy válida. Para ello un buen inicio sería determinar un dominio:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 78 de 106			2021/2022

Home > App Service Domains >

Create App Service domain

Basics Contact information Advanced Tags Review + create

Find and purchase a domain, and use Azure Domain Name System to manage your domains, all within Azure. Azure DNS also gives you a range of secure, reliable domain hosting options.

Note: Available top level domains are: com, net, co.uk, org, nl, in, biz, org.uk, and co.in. [Learn more](#)

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * 

 This subscription does not have the billing support to purchase an App Service Domain.

Resource Group * 

[Create new](#)

Domain Details

Enter a domain name and select it from the list. If you don't see the domain you entered, it's not available. All domains shown here are available for \$11.99 USD each.

Domain *

 This domain is unavailable. Here are some similar domains that are available.

Select from available domains

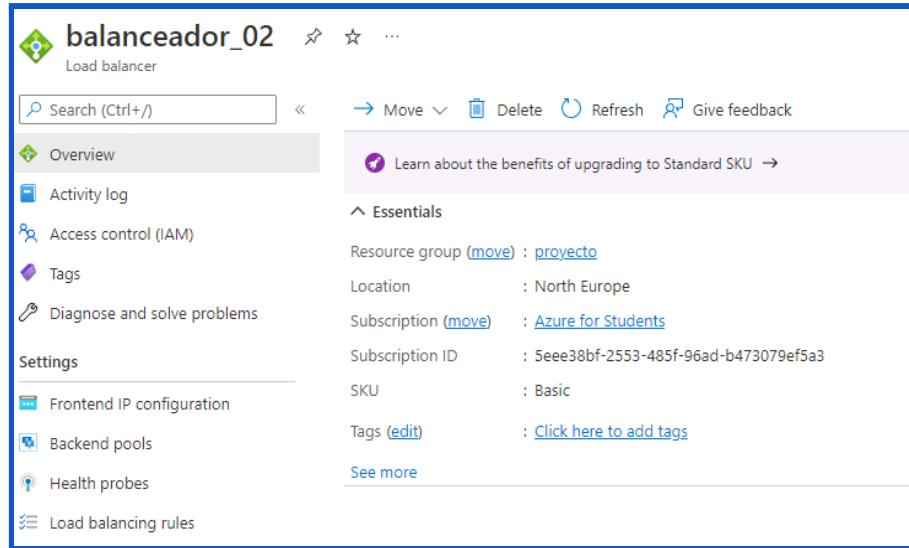
- finalwordpress.co.uk
- proyectofinal.net
- proyectowordpressfinal.com
- proyectowordpressfinal.co.uk
- proyectofinal.org

[Review + create](#) [< Previous](#) [Next : Contact information >](#)

Figura 87. Creación de dominio.

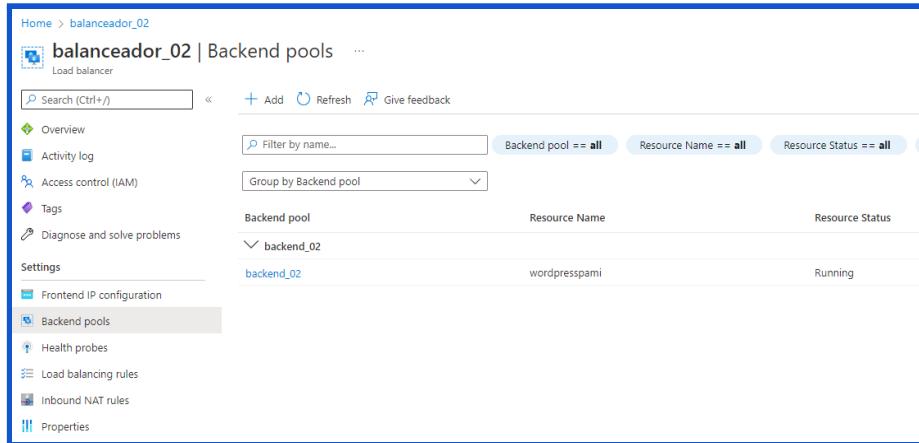
Aquí mostramos nuevamente una idea de creación de dominio (imposible para la suscripción de estudiante). Este dominio estaría conectado con nuestro balanceador de carga para redundancia de manera que podamos configurarlo todo sin obligar al usuario a buscar nuestra IP.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR IQNet Empresa Registrada ER-0934 / 2008
Pág 79 de 106		2021/2022



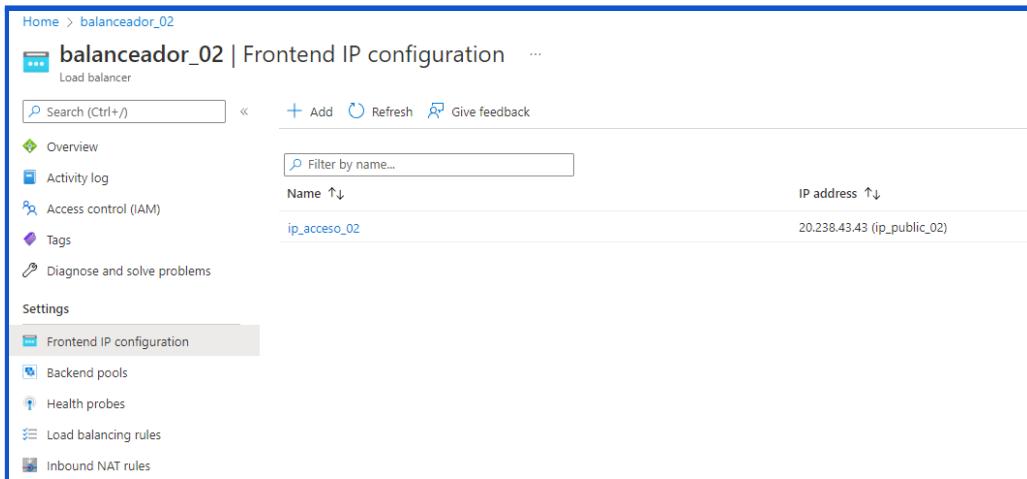
The screenshot shows the Azure portal interface for a 'balanceador_02' load balancer. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with sub-options: Frontend IP configuration, Backend pools, Health probes, Load balancing rules), and Inbound NAT rules. The main content area is titled 'balanceador_02' and 'Load balancer'. It includes a search bar, move, delete, refresh, and feedback buttons. A callout box points to the 'Learn about the benefits of upgrading to Standard SKU' link. The 'Essentials' section displays resource group (proyecto), location (North Europe), subscription (Azure for Students), subscription ID, SKU (Basic), and tags (Click here to add tags). There is also a 'See more' link.

Figura 88. Balanceador de redundancias.



The screenshot shows the 'Backend pools' section of the 'balanceador_02' load balancer. The left sidebar shows 'Backend pools' is selected. The main content area lists a single backend pool named 'backend_02' with a resource name 'wordpresspami' and status 'Running'. Filter and grouping options are available at the top of the table.

Figura 89. Backend pool.



The screenshot shows the 'Frontend IP configuration' section of the 'balanceador_02' load balancer. The left sidebar shows 'Frontend IP configuration' is selected. The main content area lists a single frontend IP configuration named 'ip_acceso_02' with an IP address '20.238.43.43 (ip_public_02)'. A filter bar is present at the top of the table.

Figura 90. Frontend IP.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 80 de 106</i>			<i>2021/2022</i>

En las Figuras anteriores hemos creado un balanceador de carga para nuestra sistema de redundancia manual (*Figura 88*), hemos creado un conjunto asociado al balanceador donde se encuentran nuestras maquinas (*Figura 89*) y le hemos asignado una IP de acceso a estos a través del balanceador (*Figura 90*).

Con esto nuestro servicio puede accederse ahora a través de la IP del balanceador o del dominio que hemos asociado si nuestra suscripción lo permite.



Figura 91. Prueba balanceador redundante.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 81 de 106		2021/2022

Sin embargo existe una manera más actualizada, esto es con el servicio de Auto scaling. Azure provee máquinas que se autorregulan en caso de necesitar más o menos capacidad, ahorrando costos y uso del servicio.

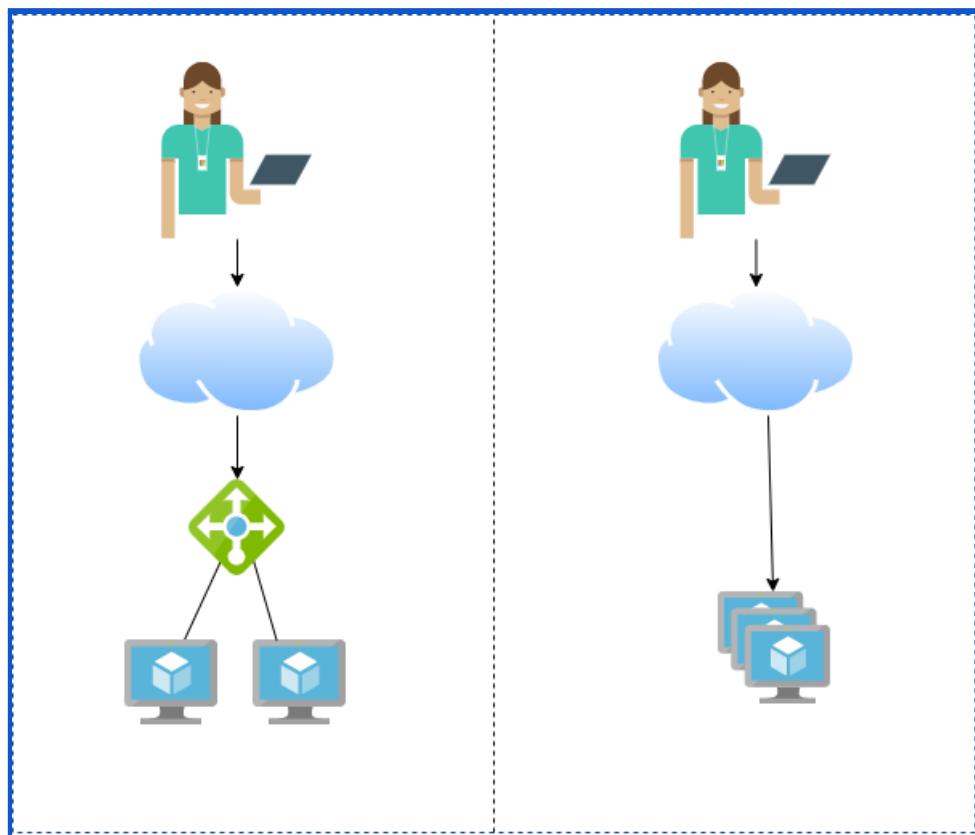
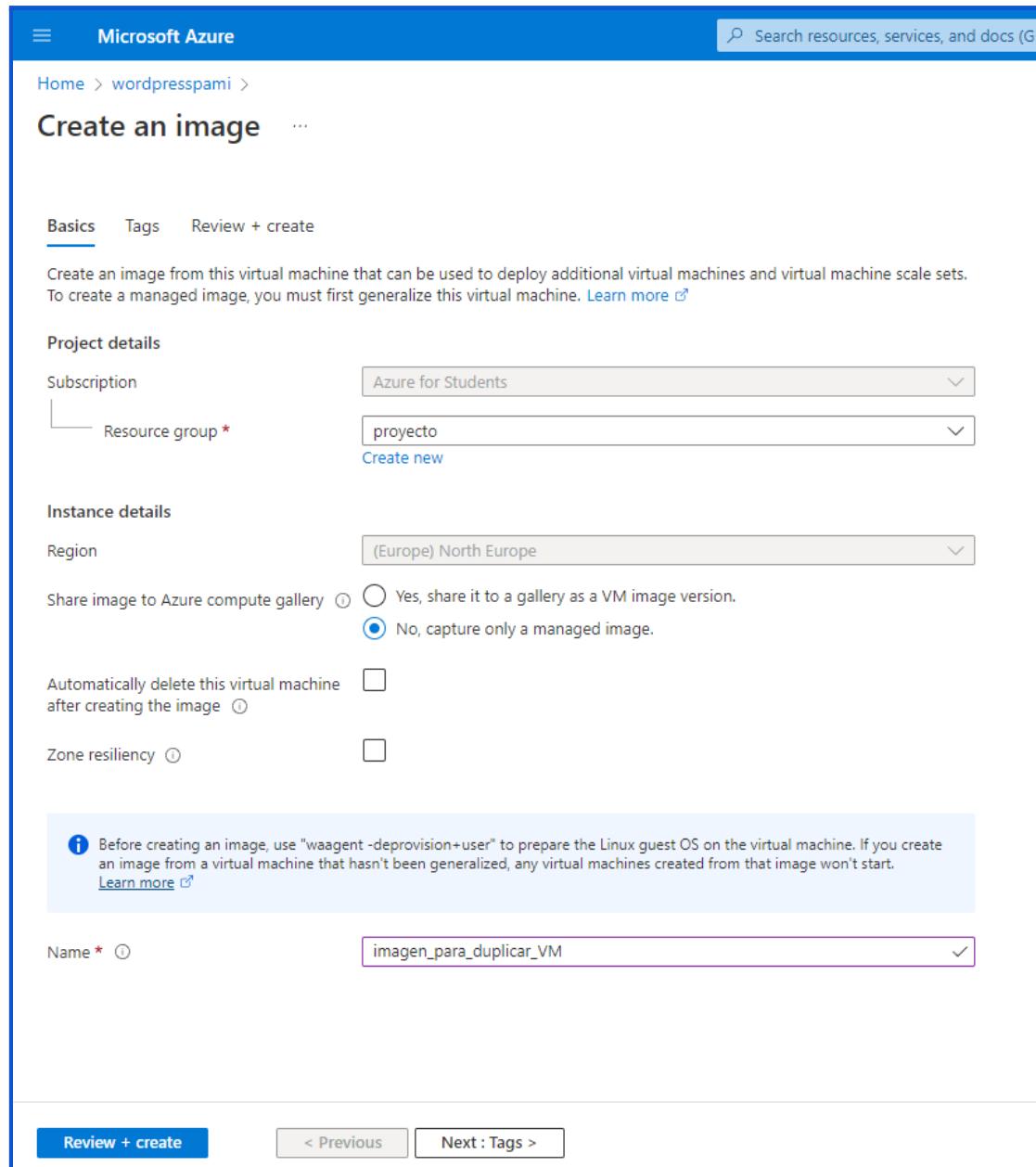


Figura 92. Esquema balanceo clásico-actual.

El primer esquema parte de la concepción local de la alta disponibilidad, mantener un recurso muy caro activo durante el tiempo necesario hasta que sea útil (si es que llega). Con Azure esos costos se reducen, es cierto, pero mantener activo un recurso que no usamos sigue siendo un gasto sin razón. Una solución práctica es el IaC, crear un código autoescalable que cree y configure máquinas, ejemplos como Terraform son el indicativo de que es una solución práctica muy aplicable. Sin embargo, obliga nuevamente a contratar y tratar con equipos técnicos que intermedien otro paso más en esta migración.

El servicio de los Scale Sets de Azure soluciona este problema, porque hace esta característica de manera más sencilla. La creación es casi igual que la de una MV normal, pero para explorar más allá la nube vamos a generar una imagen de nuestra MV que usamos:

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 82 de 106			2021/2022



Microsoft Azure

Home > wordpresspami >

Create an image

Basics Tags Review + create

Create an image from this virtual machine that can be used to deploy additional virtual machines and virtual machine scale sets. To create a managed image, you must first generalize this virtual machine. [Learn more](#)

Project details

Subscription: Azure for Students

Resource group: proyecto

Instance details

Region: (Europe) North Europe

Share image to Azure compute gallery:

- Yes, share it to a gallery as a VM image version.
- No, capture only a managed image.

Automatically delete this virtual machine after creating the image:

Zone resiliency:

Note: Before creating an image, use "waagent -deprovision+user" to prepare the Linux guest OS on the virtual machine. If you create an image from a virtual machine that hasn't been generalized, any virtual machines created from that image won't start. [Learn more](#)

Name:

Review + create < Previous Next : Tags >

Figura 93. Generando imagen de un MV.

El proceso es así de sencillo, solo debemos entrar en nuestra MV, “Capturar” dicha máquina, y entramos en este menú tan sencillo, en el que después de poner los datos que necesitemos, tendremos una imagen igual que la máquina que tuviéramos.

IMPORTANTE.

Este proceso utiliza la máquina virtual que teníamos previamente, quizás desde un acercamiento más conservador es una opción menos deseable que configurar todo el servicio nuevamente.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR IQNet Empresa Registrada ER-0934 / 2008
Pág 83 de 106		2021/2022

Home > Virtual machine scale sets >

Create a virtual machine scale set ...

Basics Disks Networking Scaling Management Health Advanced Tags Review + create

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Initial instance count * ⓘ 2

Scaling

Scaling policy ⓘ Manual Custom

Scale-In policy

Configure the order in which virtual machines are selected for deletion during a scale-in operation. [Learn more about scale-in policies](#)

Scale-in policy Default - Balance across availability zones and fault domains, then delete V...

Figura 94. Creando Scale set.

En la creación del grupo de escalado podemos comprobar, por ejemplo, si queremos que de base tengamos algunas instancias corriendo de base y manualmente levantarlas.

Scaling

Scaling policy ⓘ Manual Custom

Minimum number of instances * ⓘ 1

Maximum number of instances * ⓘ 10

Scale out

CPU threshold (%) * ⓘ 75

Duration in minutes * ⓘ 10

Number of instances to increase by * ⓘ 1 ✓

Scale in

CPU threshold (%) * ⓘ 25

Number of instances to decrease by * ⓘ 1 ✓

Diagnostic logs

Collect diagnostic logs from Autoscale ⓘ

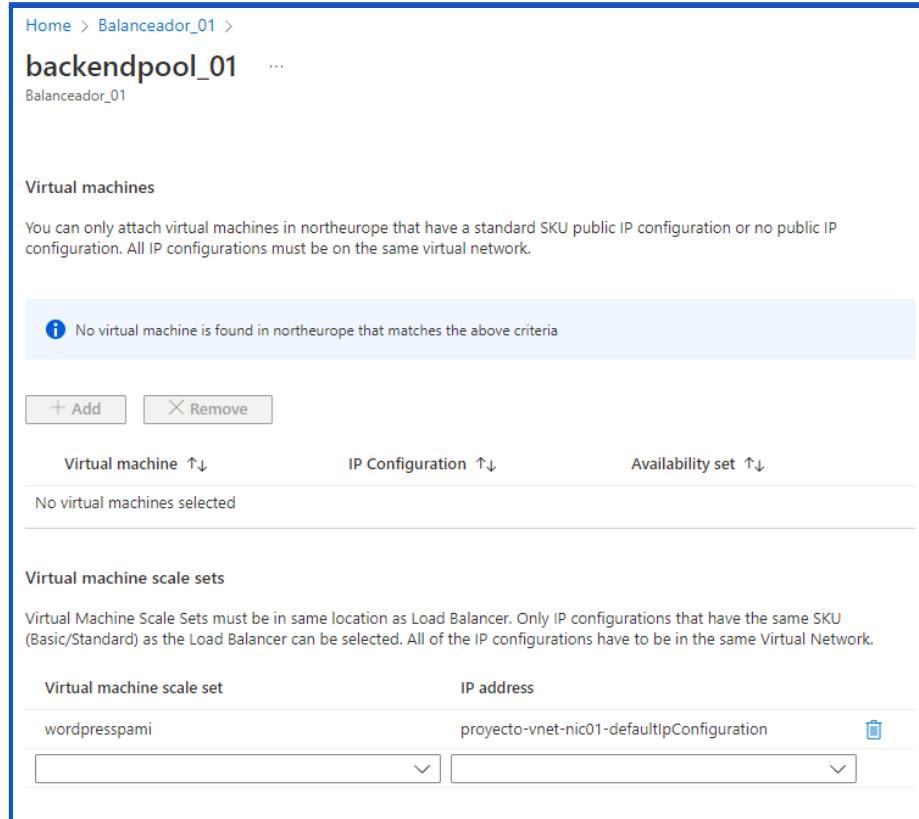
Diagnostic logs workspace * ⓘ No workspaces in current subscription.
Choose Workspace from different subscription

Figura 95. Creando Scale set 2.

Sin embargo también podemos aprovechar la nube al máximo y automatizar el despliegue en ciertas circunstancias, como un uso excesivo de CPU. Todo recogido y centralizado en logs que podemos guardar y revisar (por seguridad).

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 84 de 106			2021/2022

Este grupo es un recurso oculto, solo debemos añadirlo a nuestro balanceador de carga y ya estará 100% funcional.



The screenshot shows the Azure portal interface for managing a load balancer. The top navigation bar includes 'Home', 'Balanceador_01', and an ellipsis (...). The main content area is titled 'backendpool_01' with a subtitle 'Balanceador_01'. Below this, there's a section for 'Virtual machines' with a note: 'You can only attach virtual machines in northeurope that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.' A message box states: 'No virtual machine is found in northeurope that matches the above criteria'. There are '+ Add' and 'X Remove' buttons. Below this, there are three columns: 'Virtual machine ↑↓', 'IP Configuration ↑↓', and 'Availability set ↑↓'. A message 'No virtual machines selected' is displayed. The next section is 'Virtual machine scale sets', which contains a table with one row. The table has two columns: 'Virtual machine scale set' (containing 'wordpresspami') and 'IP address' (containing 'proyecto-vnet-nic01-defaultIpConfiguration'). There are dropdown menus below each column.

Figura 96. Scale set en el balanceador.

Y con esto nuevamente tendríamos nuestro servicio funcionando pero con escalabilidad en caso de flujo masivo.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2><i>Guía Práctica para el uso profesional de la nube</i></h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 85 de 106			2021/2022

Empresaficticia SL – Grupo Money

No es seguro | 20.223.236.224/sample-page/

Grup Money Una empresa de ensueños que no existen en la realidad Empresa Ficticia S.L. Search

Empresa Ficticia S.L.

Bienvenido al futuro, con nuestra empresa vas a ser rico. Tan solo debes seguir los 27 pasos que te proporcionamos adelante, ocultos un tercio en pdf de pago y el otro tercio en videos motivacionales a precio de oro.

¡No dudes en hacerte millonario!

Search SEARCH Archives

Recent Posts June 2022

Figura 96. Scale set desde balanceo.

Cómo coleta final a la configuración de la nube, nunca debemos olvidar la seguridad. Hemos configurado nuestro Defender Cloud, Microsoft ya trae reglas muy seguras de firewall, pero hemos incluso aumentado la seguridad... Pero no es del todo cierto, en la nube existen también muchos más vectores de ataque. Aquí las recomendaciones del Defender Cloud son muy buenas y un ejemplo a seguir, sin embargo, tenemos opciones “independientes” para auditar nuestro servicio. Este es el ejemplo de una de las herramientas (de tantas otras) para auditar la nube, CloudSploit.

CloudSploit es una herramienta de la empresa Aqua que tiene una versión de pago que corre desde servidores suyos, sin embargo, en el [anexo¹¹⁴](#) dejaré el acceso al software que ellos mismos han publicado en Github. Esta herramienta se vale de las APIs que cada proveedor cloud dispone, y con las credenciales válidas ejecuta distintas pruebas para hacer una auditoría.

25 lines (24 sloc) | 1.3 KB

<>

CloudSploit For Microsoft Azure

Cloud Provider Configuration

1. Log into your Azure Portal and navigate to the Azure Active Directory service.
2. Select App registrations and then click on New registration.
3. Enter "CloudSploit" and/or a descriptive name in the Name field, take note of it, it will be used again in step 3.
4. Leave the "Supported account types" default: "Accounts in this organizational directory only (YOURDIRECTORYNAME)".
5. Click on Register.
6. Copy the Application ID and Paste it below.
7. Copy the Directory ID and Paste it below.
8. Click on Certificates & secrets.
9. Under Client secrets, click on New client secret.
10. Enter a Description (i.e. Cloudsploit-2019) and select Expires "In 1 year".
11. Click on Add.
12. The Client secret value appears only once, make sure you store it safely.
13. Navigate to Subscriptions.
14. Click on the relevant Subscription ID, copy and paste the ID below.
15. Click on "Access Control (IAM)".
16. Go to the Role assignments tab.
17. Click on "Add", then "Add role assignment".
18. In the "Role" drop-down, select "Security Reader".
19. Leave the "Assign access to" default value.
20. In the "Select" drop-down, type the name of the app registration (e.g. "CloudSploit") you created and select it.
21. Click "Save".
22. Repeat the process for the role "Log Analytics Reader"

Figura 97. CloudSploit para Azure.

Siguiendo los pasos de la *Figura 97* podemos obtener todo lo necesario para ejecutar la herramienta.

```
GNU nano 4.8                                     config.js
// CloudSploit config file

module.exports = {
  credentials: {
    azure: {
      application_id: process.env.AZURE_APPLICATION_ID || '',
      key_value: process.env.AZURE_KEY_VALUE || '',
      directory_id: process.env.AZURE_DIRECTORY_ID || '',
      subscription_id: process.env.AZURE_SUBSCRIPTION_ID || ''
    }
  }
};
```

Figura 98. Configuración CloudSploit para Azure.

Figura 99. Ejecución CloudSploit 1.

Figura 100. Ejecución CloudSploit 2.

En la *Figura 99* y *Figura 100* podemos observar las posibilidades de la herramienta. Por predeterminado, la herramienta hace una análisis total, mostrando también aquellos aspectos que **si** están correctamente securizados, con el parámetro “ignore-ok” lo que estamos haciendo es que obvie en el análisis final aquellos puntos que ya estén seguros, para centrarnos en los no-securizados. En ambas imágenes se muestra también cómo exportar el análisis a CSV o JSON. Como una manera de recolectar la información y poder ir subsanando fallo a fallo.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR IQNet CERTIFIED QUALITY SYSTEM Empresa Registrada ER-0934 / 2008
	Pág 88 de 106	2021/2022

CloudSploit by Aqua Security, Ltd.
 Cloud security auditing for AWS, Azure, GCP, Oracle, and GitHub

```

INFO: Using CloudSploit config file: /home/jc/cloudsploit/config.js
INFO: Ignoring passing results
INFO: Skipping AWS pagination mode
INFO: Determining API calls to make...
INFO: Found 90 API calls to make for azure plugins
INFO: Collecting metadata. This may take several minutes...
INFO: Metadata collection complete. Analyzing...
INFO: Analysis complete. Scan report to follow...
Plugin Virtual Network Peering returned no results. There may be a problem with this plugin.
Plugin VM Desired SKU Size returned no results. There may be a problem with this plugin.
Plugin VM Approved Extensions returned no results. There may be a problem with this plugin.
Plugin Database Tier CMK In Use returned no results. There may be a problem with this plugin.
Plugin Allowed Certificates Key Types returned no results. There may be a problem with this plugin.
Plugin App Tier CMK In Use returned no results. There may be a problem with this plugin.
INFO: Collection file written to file.json
  
```

C a t e g o r y	Plugin	Description	Resource	R e s o u r c e	S t a t u s	Message
V i r t u a l N e t w o r k s	Multiple Subnets	Ensures that Virtual Networks have multiple networks to provide a layered architecture	/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/proyecto/providers/Microsoft.Network/virtualNetworks/proyecto-vnet	n o r t h e u r o p e	F A I L	Only one subnet in the Virtual Network is used
V i r t u a l N e t w o r k s	DDoS Standard Protection Enabled	Ensures that DDoS Standard Protection is enabled for Microsoft Azure Virtual Networks	/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/proyecto/providers/Microsoft.Network/virtualNetworks/proyecto-vnet	n o r t h e u r o p e	F A I L	DDoS Standard Protection is not enabled for Microsoft Azure Virtual Network

Figura 101. CloudSploit análisis.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
	Pág 89 de 106	2021/2022

Key Vault In Use	Ensures that Key Vaults are being used to store secrets.	N/A	c a n a d a c e n t r a l	F A I L	Key Vaults are not being used to store secrets
Key Vault In Use	Ensures that Key Vaults are being used to store secrets.	N/A	c a n a d a e a s t	F A I L	Key Vaults are not being used to store secrets
Active Advisor Recommendations	Ensure that all Microsoft Azure Advisor recommendations found are implemented to optimize your cloud deployments, increase security, and reduce costs.	N/A	g l o b a l	F A I L	Active Advisor Recommendations found
Enable Defender For Storage	Ensures that Microsoft Defender is enabled for Storage.	/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/providers/Microsoft.Security/pricings/StorageAccounts	g l o b a l	F A I L	Azure Defender is not enabled for Storage Accounts
Enable Defender For Containers	Ensures that Microsoft Defender is enabled for all containers.	/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/providers/Microsoft.Security/pricings/Containers	g l o b a l	F A I L	Azure Defender is not enabled for Containers
Enable Defender For SQL Servers	Ensures that Microsoft Defender is enabled for Azure SQL Server Databases.	/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/providers/Microsoft.Security/pricings/SqlServers	g l o b a l	F A I L	Azure Defender is not enabled for SQL Server Databases

INFO: Scan complete

Figura 102. CloudSploit análisis.

En la Figura 101 y Figura 102 podemos ver la salida en prompt de los fallos de seguridad, que por cantidad pueden bloquear la visión, de ahí la recomendación de exportarlo como documento íntegro. Entre ambas imágenes hay **muchas** tablas.

```
jc@jc:~/cloudsploit$ ls | grep .csv
file.csv
jc@jc:~/cloudsploit$ cat file.csv
category,title,description,resource,region,statusWord,message
Virtual Networks,Multiple Subnets,Ensures that Virtual Networks have multiple networks to provide a layered architecture.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/proyecto/providers/Microsoft.Network/virtualNetworks/proyecto-vnet,northeurope,FAIL,Only one subnet in the Virtual Network is used
Virtual Networks,DDoS Standard Protection Enabled,Ensures that DDoS Standard Protection is enabled for Microsoft Azure Virtual Network.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/proyecto/providers/Microsoft.Network/virtualNetworks/proyecto-vne,northeurope,FAIL,DDoS Standard Protection is not enabled for Microsoft Azure Virtual Network
Virtual Networks,Managed NAT Gateway In Use,Ensure Azure Virtual Network Managed NAT (Network Address Translation) Gateway service is enabled for Virtual Network.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/proyecto/providers/Microsoft.Network/virtualNetworks/proyecto-vnet,northeurope,FAIL,Azure Virtual Network Managed NAT (Network Address Translation) Gateway service is disabled for Virtual Network
Virtual Machines,VM Endpoint Protection,Ensures that VM Endpoint Protection is enabled for all virtual machines.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/PROYECTO/providers/Microsoft.Compute/virtualMachines/wordpresspami,northeurope,FAIL,Endpoint protection is not installed on the virtual machine
Virtual Machines,VM Availability Set Enabled,Ensures that Virtual Machines have Availability Set enabled.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/PROYECTO/providers/Microsoft.Compute/virtualMachines/wordpresspami,northeurope,FAIL,The Virtual Machine does not have Availability Set enabled
Virtual Machines,VM Daily Backup Retention Period,Ensures that VM daily backup retention policy is configured to retain backups for the desired number of days.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/PROYECTO/providers/Microsoft.Compute/virtualMachines/wordpresspami,northeurope,FAIL,No backup policies are configured for the virtual machine
Virtual Machines,VM Backups Enabled,Ensures that Azure virtual machine backups are enabled.,/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/PROYECTO/providers/Microsoft.Compute/virtualMachines/wordpresspami,northeurope,FAIL,Azure virtual machine does not have backups enabled
Virtual Machines,Accelerated Networking Enabled,Ensures that accelerated networking is enabled on Azure virtual machines(VM),/subscriptions/5eee38bf-2553-485f-96ad-b473079ef5a3/resourceGroups/PROYECTO/providers/Microsoft.Compute/virtualMachines/wordpresspami,northeurope,FAIL,Accelerated networking is not enabled on the Azure virtual machine
```

Figura 103. CloudSploit análisis observable.

Como punto final del análisis, desde un prompt de un server no se verá tan bonito como un desktop pero podemos comprobar como se ha generado y guardado la información correctamente para luego solventar cada uno de los problemas.

Seleccionar problema a problema de seguridad en la nube podría ser perfectamente el objetivo de otro proyecto igual o más completo que el que traemos aquí, sin embargo, por no duplicar ni hacer soporífera esta guía que pretende ser básica, dejaremos que el Microsoft Defender Cloud con sus consejos, aseguren originalmente nuestro sitio. Siempre es recomendable realizar auditorías periódicas para asegurar que no hay fugas en nuestro sistema, por eso recomiendo que se amplíe más en el ámbito técnico de seguridad si se quiere o se aspira a albergar un servicio muy usado y reconocido. Pues a mayor exposición tenga la web, mayor exposición tienen sus fallas y más probabilidad hay de que alguien con intenciones maliciosas aproveche las fallas.

 I.E. Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 91 de 106			2021/2022

Tal y como hemos montado el servicio, podemos replegar y abandonar los servidores locales y explorar, con una suscripción de pago mejor, todas las herramientas que Azure nos proporciona.

Como análisis final, antes de terminar el desarrollo, Azure nos brinda mucha información con respecto a los gastos y nos ayuda a optimizarlos:

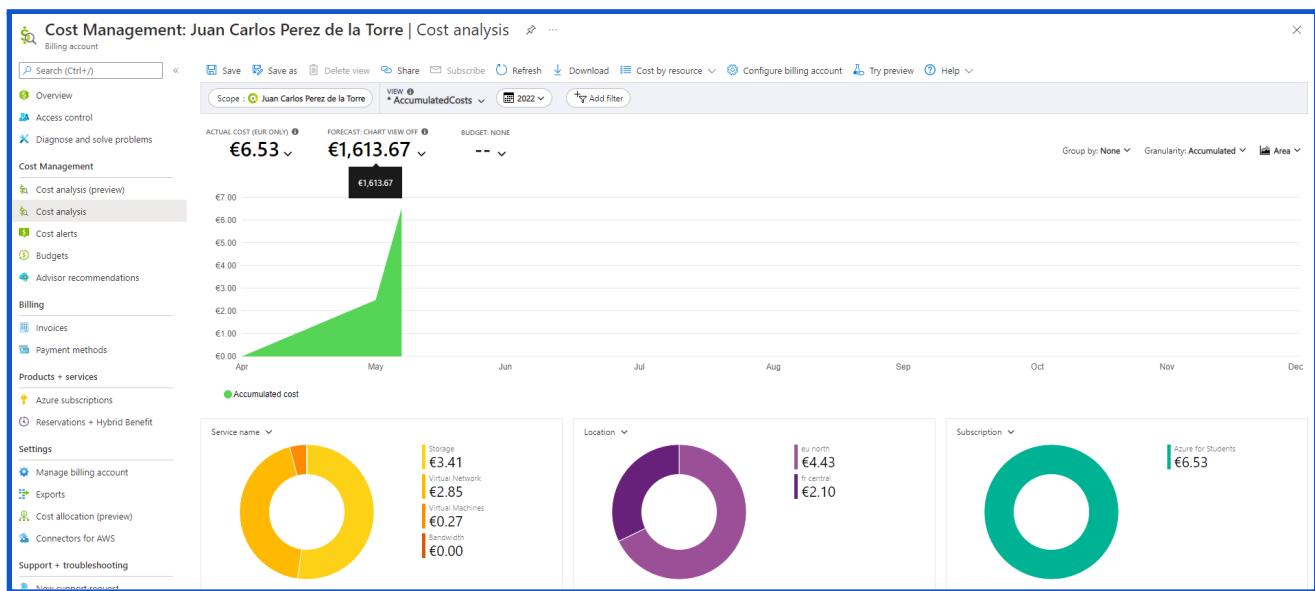


Figura 97. Gestor de Gastos de Azure.

Como podemos ver, hemos hecho un gasto aproximado de 6.53€. Dado el abrupto consumo del último mes (muchas pruebas y despliegues no salen en el proyecto final) hace una estimación anual aproximada. Desde luego, con más tiempo y con una empresa los análisis serán mucho más certeros y fiables

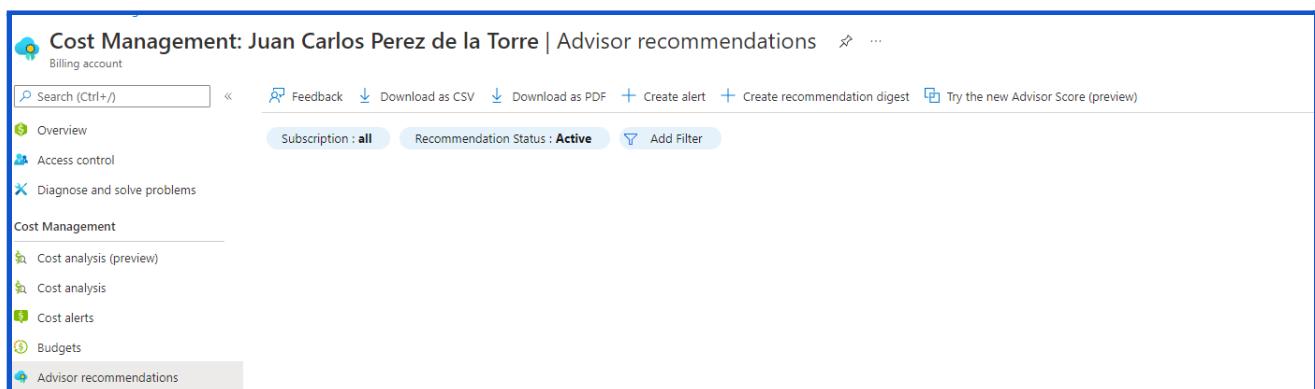
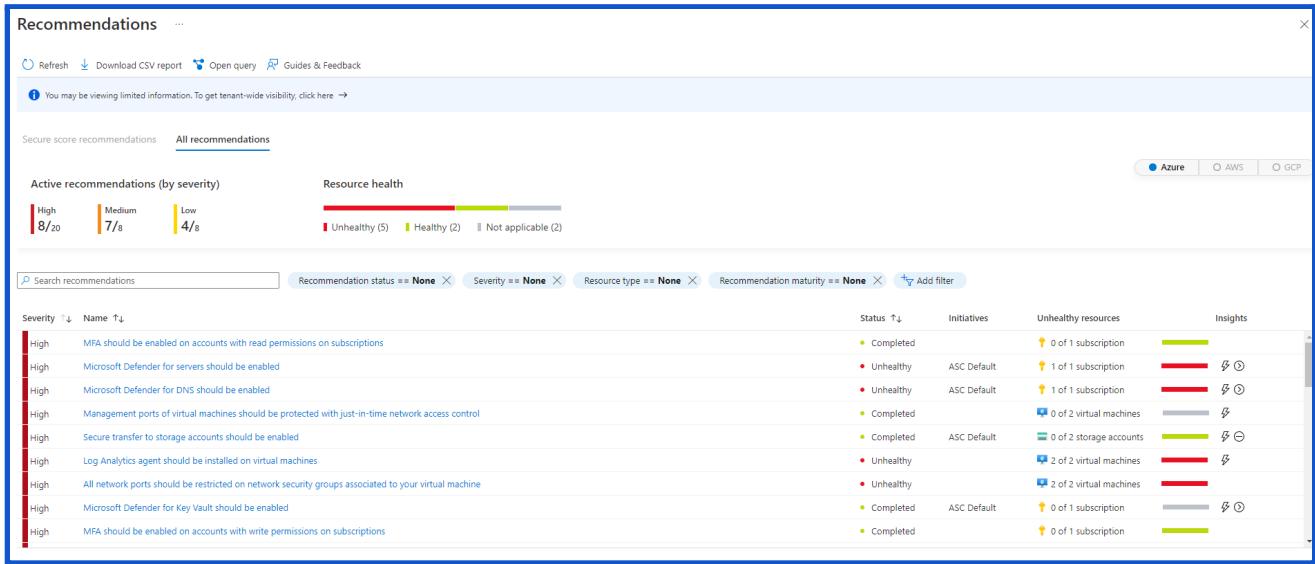


Figura 98. Consejos del Gestor de gastos.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2>Guía Práctica para el uso profesional de la nube</h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 92 de 106	2021/2022		

Dado que hemos montado muy pocos recursos y que el gasto por la suscripción es gratuito no nos puede recomendar nada mejor, pero el consejero de gastos de Azure es una bandera que Microsoft enarbola frente a la competencia (además de la seguridad y privacidad).

Terminando con la seguridad, el Defender de la nube continúa con las recomendaciones:



The screenshot shows the Microsoft Defender interface for Azure. At the top, there's a header with 'Recommendations' and various navigation links like 'Refresh', 'Download CSV report', 'Open query', 'Guides & Feedback', and a note about viewing limited information. Below the header, there are sections for 'Secure score recommendations' (with a 'High' score of 8/20), 'Active recommendations (by severity)' (High: 8/20, Medium: 7/8, Low: 4/8), and 'Resource health' (a bar chart showing 5 Unhealthy, 2 Healthy, and 2 Not applicable resources). A search bar and filter options are available. The main table lists 10 recommendations, each with a severity level (High) and a detailed description. To the right of the table, columns show 'Status' (Completed or Unhealthy), 'Initiatives' (ASC Default), 'Unhealthy resources' (e.g., 0 of 1 subscription, 1 of 1 subscription), and 'Insights' (represented by colored bars).

Severity	Name	Status	Initiatives	Unhealthy resources	Insights
High	MFA should be enabled on accounts with read permissions on subscriptions	Completed	ASC Default	0 of 1 subscription	█
High	Microsoft Defender for servers should be enabled	Unhealthy	ASC Default	1 of 1 subscription	█
High	Microsoft Defender for DNS should be enabled	Unhealthy	ASC Default	1 of 1 subscription	█
High	Management ports of virtual machines should be protected with just-in-time network access control	Completed	ASC Default	0 of 2 virtual machines	█
High	Secure transfer to storage accounts should be enabled	Completed	ASC Default	0 of 2 storage accounts	█
High	Log Analytics agent should be installed on virtual machines	Unhealthy		2 of 2 virtual machines	█
High	All network ports should be restricted on network security groups associated with your virtual machine	Unhealthy		2 of 2 virtual machines	█
High	Microsoft Defender for Key Vault should be enabled	Completed	ASC Default	0 of 1 subscription	█
High	MFA should be enabled on accounts with write permissions on subscriptions	Completed		0 of 1 subscription	█

Figura 99. Consejos de Microsoft Defender.

Todos puntos a tener en cuenta desde luego, como el multiple factor de autenticación, transferencias seguras, análisis de logs, restricciones de red, etc.

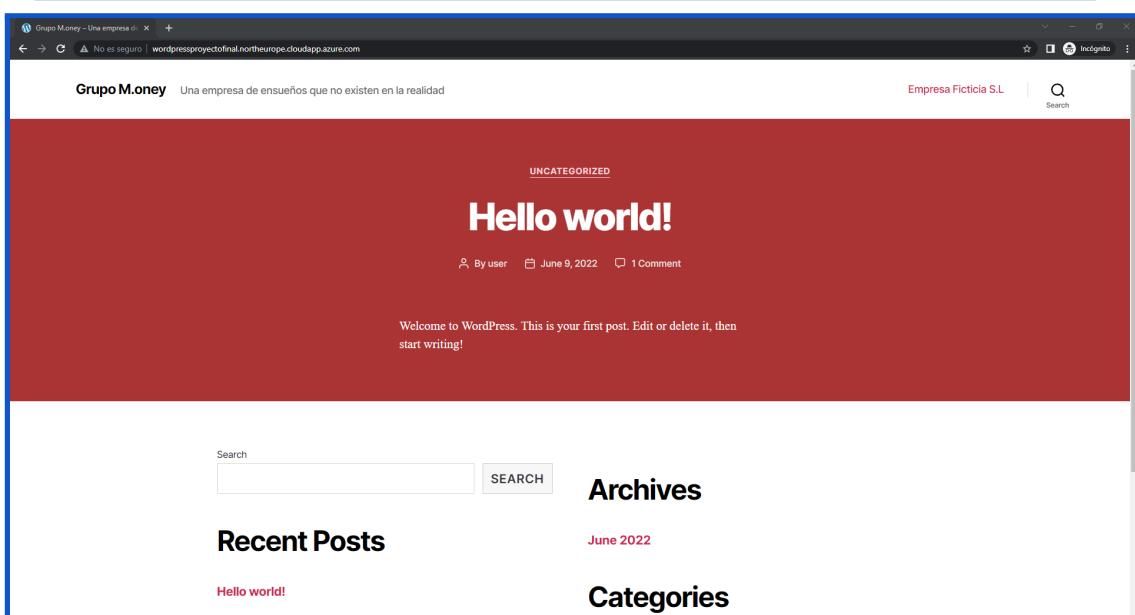
Las posibilidades son casi infinitas, el tiempo es muy limitado, por eso explorar la nube de Azure es una tarea que no quedará aquí.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<i>Guía Práctica para el uso profesional de la nube</i>	 AENOR ER Empresa Registrada ER-0934 / 2008
Pág 93 de 106		2021/2022

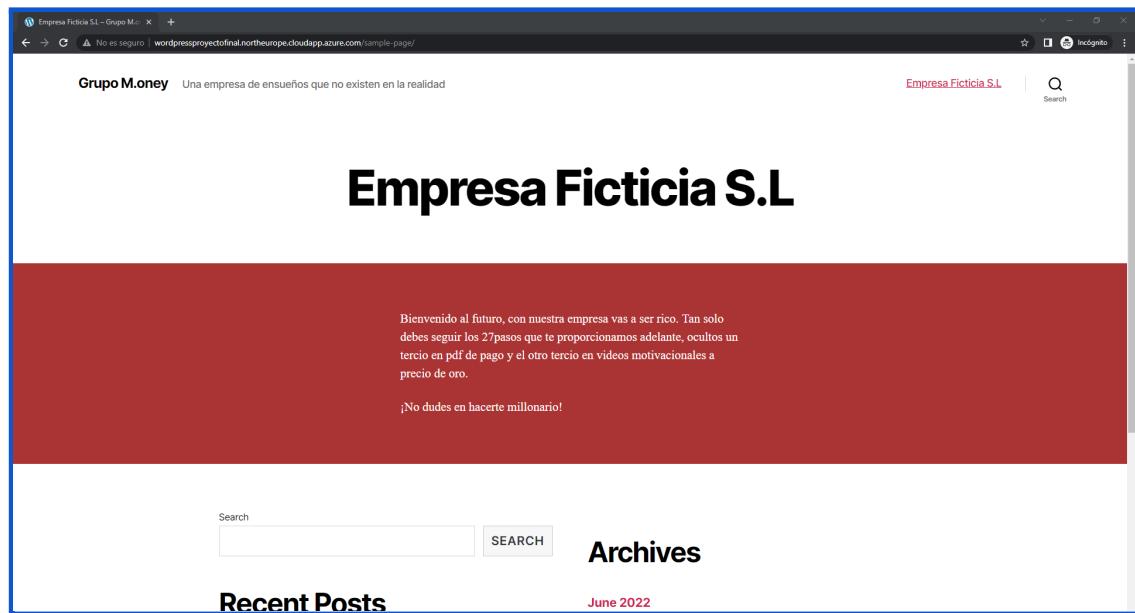
7. Pruebas

<http://wordpressproyectofinal.northeurope.cloudapp.azure.com/>

20.223.236.224



The screenshot shows a WordPress website with a red header and white content area. The header contains the text "Grupo M.oney Una empresa de ensueños que no existen en la realidad" and "Empresa Ficticia S.L.". The main content features a large heading "Hello world!" with a "UNCATEGORIZED" tag above it. Below the heading is a small note: "Welcome to WordPress. This is your first post. Edit or delete it, then start writing!". The footer includes a search bar, "Archives", "Recent Posts" (listing "Hello world!"), and "Categories".



The screenshot shows a sample page from the website. The main heading is "Empresa Ficticia S.L.". Below it is a red content area containing the text: "Bienvenido al futuro, con nuestra empresa vas a ser rico. Tan solo debes seguir los 27 pasos que te proporcionamos adelante, ocultos un tercio en pdf de pago y el otro tercio en videos motivacionales a precio de oro." and "¡No dudes en hacerte millonario!". The footer includes a search bar, "Archives", "Recent Posts" (listing "Hello world!"), and "Categories".

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	<h2><i>Guía Práctica para el uso profesional de la nube</i></h2>	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	<i>Pág 94 de 106</i>		2021/2022

Empresa Ficticia S.L – Grupo M.

No es seguro | 20.223.236.224 /sample-page/

Grupo M.oney Una empresa de ensueños que no existen en la realidad Empresa Ficticia S.L Search

Empresa Ficticia S.L

Bienvenido al futuro, con nuestra empresa vas a ser rico. Tan solo debes seguir los 27pasos que te proporcionamos adelante, ocultos un tercio en pdf de pago y el otro tercio en videos motivacionales a precio de oro.

¡No dudes en hacerte millonario!

Search SEARCH Archives

Recent Posts June 2022

Web tanto por enlace normal como por IP de balanceador

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 95 de 106		2021/2022

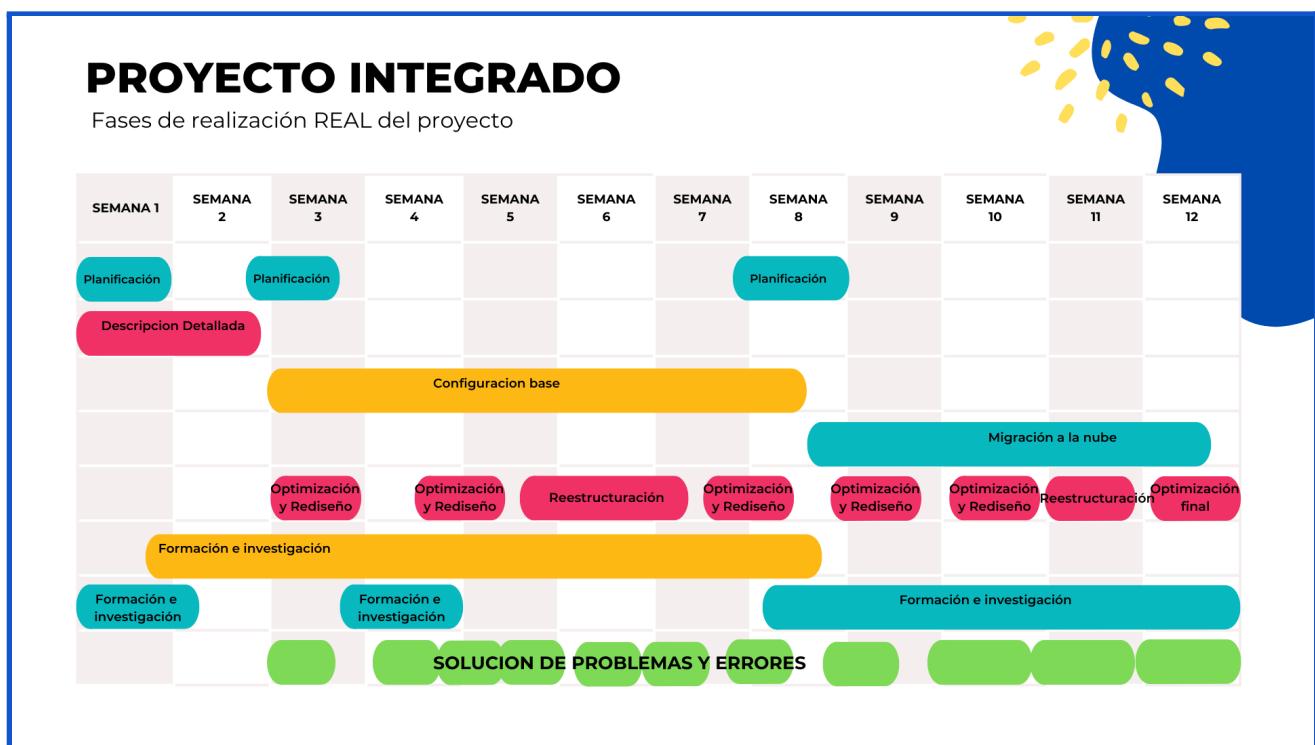
8. Conclusión final

Humildad, si algo me ha enseñado este proyecto es humildad. Las capacidades de la nube, de Azure, son tan grandes y tan poderosas que se convierten en embriagadoras. Este proyecto se ideó como una construcción megalítica, pensando que el arquitecto sabría manejar la máquina (Azure) y que la máquina podría hacerlo todo en dos simples clicks.

Sin duda es en el estudio y en la práctica de llevar la nube a la realidad cuando realmente se puede ver lo grande que son sus posibilidades y lo grande que es el estudio necesario para aprovechar todas esas posibilidades. Todo este proyecto ha sufrido algún grado de megalomanía y otro grado más grande aún de **inocencia e ignorancia**.

Equipos enteros alrededor del mundo se forman y trabajan para llevar empresas “analógicas” a la nube, o de optimizar en la nube empresas ya digitalizadas. Sería un pecado pensar que una persona en su casa, **sola**, con un **tiempo reducido** y unos **recursos incluso menores** podría crear algo mucho mejor, más potente y seguro que decenas de personas ya formadas.

Esa es la primera barrera que ha tenido que superar este proyecto, el de la ignorancia y el de la inocencia. En comparación con la planificación inicial, aquí muestro (en general) una planificación más realista de lo que ha sido llevar a la nube a una empresa.



 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 96 de 106			2021/2022

La planificación cuanto menos fue **optimista**, muestra el final de este proyecto. Se han podido cumplir los objetivos pero nos hemos encontrado muchas **más dificultades de las esperadas**. Se asumió de manera general $\frac{1}{4}$ de tiempo total del proyecto para cada tarea, siendo la optimización final la más larga pues asumió también algo de exploración con Azure.

La realidad es que el desarrollo del entorno local ha sido lo que **más problemas ha causado**, desde compatibilidades a bloqueos internos por seguridad, entre otros muchos, así como la construcción y configuración del sistema, ha sido lo más tedioso de manera práctica.

La resolución de fallos locales ha desarrollado una habilidad más en este joven arquitecto de ideas que necesitaba mas simplificación. Desde problemas en la web más básica hasta problemas de redes y seguridad con Pfsense.

La 2^a parte, el desarrollo de la nube también ha sido **más largo** de lo esperado, en este caso no por dificultad práctica sino **por dificultad teórica**. Comprender y analizar todos los recursos que Azure presta así como la mejor forma de disponerlos requiere de una formación y estudio que no se previó. Más **técnicamente** podemos decir a ciencia cierta que si el servidor central fuera Windows o la virtualización fuera de Hyper-V, **la migración sería mucho más sencilla**. Ahorrando no solo el tiempo de troubleshooting sino optimizando los recursos para la nube sin perder configuraciones. Quitando los primeros escollos, el resto ha sido, **sinceramente**, jugar en una cacharrería. Azure tiene una cantidad de herramientas y posibilidades (la mayoría no permitidas o muy restringidas para estudiantes) que pondría celoso a cualquier niño que pudiera verlo, o en este caso, a cualquiera que quiera acercarse a sus posibilidades.

Ha sido una experiencia increíble (a la vez que frustrante) que deja con la miel en la boca para explorar aún más todo el mundo de la nube.

Termina el proyecto con el consejo, o quizás las ganas, de experimentar más con la seguridad y la alta disponibilidad en local. Terraform es una herramienta muy útil, pero quería hacer ver durante todo el proyecto que la nube es un avance, una evolución lógica de las infraestructuras. Escalado automático, disponibilidad regional o global, seguridad incrementada, y un largo etc. Plantear alternativas sería **poner palos en las ruedas** de este proyecto.

Como guinda, sigo investigando en foros y documentación la implementación del script completo de docker que quería hacer funcionar, si al lector le interesa le actualizará (si es posible) de las novedades. Por ahora vamos 10-0 perdiendo yo por goleada, necesitaremos un Messi de la informática hable el idioma que hable.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 97 de 106</i>			2021/2022

9. Agradecimientos

Gracias a todos los profesores por esforzarse en enseñarnos y a los compañeros que tanto me han ayudado en el curso con mis circunstancias. Que me han explicado cuando no entendía o me echaban una cuerda cuando me perdía. Sin vosotros la cuesta seria montaña.

Este curso 21/22 lo he pasado trabajando a jornada completa y estudiando el resto. Si he podido ser tan diligente y correcto es gracias a la mujer que, embarazada me ha permitido estudiar y trabajar aguantandose los dolores hasta el parto, y que como madre ha permitido horas y horas de investigación y trabajo para hacer “un proyecto de informática muy importante”.

Sin esa mujer que calma los llantos de bebé a todas horas, que se esfuerza al 200% para que todo funcione, que hace feliz a padre y a hija, sin ella, este proyecto no sería posible. Me hubiera conformado y no hubiera explorado un mundo tecnológico tan rico e interesante. Me has motivado, ilusionado y animado en los peores momentos, cuando nada salía bien.

Por eso gracias Elisabeth, porque este año es tuyo y lo has trabajado tanto o más que yo para poder hacer lo que hago. **Este proyecto es para ti.**

Y gracias por el regalo que es nuestra niña, Alicia.

A ella, que es nuestro proyecto de vida, le dedicaré el siguiente proyecto.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
Pág 98 de 106			2021/2022

10. Referencias web

10.1. Anexos previos

**** Importante, estos anexos recogen sólo información básica, útil y necesaria para la realización del proyecto. En su creación ha hecho falta mucho más material e información para entenderlo y realizarlo, en su ejecución puede necesitar de más material y estudio que el presentado en estos anexos ****

1. Perry, Y. (2021). Cloud Migration Strategy with NetApp Cloud Volumes ONTAP. [online] Cloud.netapp.com.
Available at: <https://cloud.netapp.com/blog/cloud-migration-strategy-challenges-and-steps> [Accessed 2022].
2. Perry, Y. (2021). AWS Migration: Migrating to AWS in 5 Steps. [online] cloud.netapp.com.
Available at: <https://cloud.netapp.com/blog/aws-migration-5-key-challenges-and-solutions> [Accessed 2022].
3. Kovacs, G. (2019). Azure Migration: Successful Migration from AWS or On-Premise. [online] cloud.netapp.com.
Available at: <https://cloud.netapp.com/blog/enterprise-migration-to-azure-keys> [Accessed 2022].
4. Builtwith.com. (2022). CMS technologies Web Usage Distribution on the Entire Internet. [online]
Available at: <https://trends.builtwith.com/cms/traffic/Entire-Internet> [Accessed 2022].
5. W3techs.com. (2022). Usage Statistics and Market Share of Content Management Systems, April 2022. [online]
Available at: https://w3techs.com/technologies/overview/content_management [Accessed 2022].
6. Drupal.org. (2016). Installing Drupal. [online]
Available at: <https://www.drupal.org/docs/installing-drupal> [Accessed 2022].
7. Antoniy Yushkevych (2021). What is a CMS? [online] MonoVM.com.
Available at: <https://monovm.com/blog/what-is-a-cms/> [Accessed 2022].
8. Kinsta®. (2021). What Is a Content Management System (CMS)? [online]
Available at: <https://kinsta.com/knowledgebase/content-management-system/> [Accessed 2022].
9. Opensource.com. (2021). What is open source? [online]
Available at: <https://opensource.com/resources/what-open-source> [Accessed 2022].
10. Oracle.com. (2014). ¿Qué es una base de datos? [online]
Available at: <https://www.oracle.com/co/database/what-is-database/> [Accessed 2022].
11. Microsoft.com. (2021). Conceptos básicos sobre bases de datos. [online]
Available at:
<https://support.microsoft.com/es-es/office/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204> [Accessed 2022].
12. Marín, R. (2019). Los gestores de bases de datos (SGBD) más usados. [online] Canal Informática y TICS.
Available at:
<https://revistadigital.inesem.es/informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/> [Accessed 2022].
13. Cloudflare. (2022). ¿Qué es la nube? | Conceptos esenciales | Cloudflare. [online]
Available at: <https://www.cloudflare.com/es-es/learning/cloud/what-is-the-cloud/> [Accessed 2022].
14. Redhat.com. (2022). What is multicloud? [online]
Available at: <https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud> [Accessed 2022].
15. Redhat.com. (2022). What are cloud service providers? [online] Available at:
<https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-providers> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
<i>Pág 99 de 106</i>			<i>2021/2022</i>

16. Microsoft.com. (2022). What Is Cloud Computing? A Beginner's Guide | Microsoft Azure. [online] Available at: <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#cloud-deployment-types> [Accessed 2022].
17. Cloudflare. (2022). ¿Qué es DNS? | Nociones básicas | Cloudflare. [online] Available at: <https://www.cloudflare.com/es-es/learning/dns/what-is-dns/> [Accessed 2022].
18. INCIBE. (2020). ¿Qué son y para qué sirven los SIEM, IDS e IPS? [online] Available at: <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips> [Accessed 2022].
19. Teklager.se. (2022). what is pfSense - introduction to open source router/firewall operating system. [online] Available at: <https://teklager.se/en/pfsense-introduction-open-source-router-firewall/> [Accessed 2022].
20. Amazon Web Services, Inc. (2014). ¿Qué es AWS? [online] Available at: <https://aws.amazon.com/es/what-is-aws/> [Accessed 2022].
21. Microsoft.com. (2022). What is Azure—Microsoft Cloud Services | Microsoft Azure. [online] Available at: <https://azure.microsoft.com/en-us/overview/what-is-azure/> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	<i>Pág 100 de 106</i>		<i>2021/2022</i>

10.2. Anexos de la configuración base (6.1)

22. VanMSFT, olprod, OpenLocalizationService and Saisang (2021). Proteger SQL Server - SQL Server. [online] [docs.microsoft.com](https://docs.microsoft.com/es-es/sql/relational-databases/security/securing-sql-server?view=sql-server-ver15). [Accessed 2022]. Available at: <https://docs.microsoft.com/es-es/sql/relational-databases/security/securing-sql-server?view=sql-server-ver15> [Accessed 2022].
23. programmerclick.com. (n.d.). 12 mejores prácticas de seguridad de MySQL / MariaDB para Linux - programador clic. [online] Available at: <https://programmerclick.com/article/46611504989/> [Accessed 2022].
24. Golubchik, S. (2020). MariaDB Security Process - Sergei Golubchik - MariaDB Server MiniFest 2020. [online] [www.youtube.com](https://www.youtube.com/watch?v=otVUoJW5PUQ). Available at: <https://www.youtube.com/watch?v=otVUoJW5PUQ> [Accessed 2022].
25. Kaeo, M. (2003). Designing and Implementing a Designing and Implementing a Secure Network Infrastructure Secure Network Infrastructure. [online] Available at: <https://archive.nanog.org/meetings/nanog29/presentations/kaeo.pdf> [Accessed 2022].
26. P, D. (n.d.). Security Architecture, Secure Network Design | IINS 210-260. [online] www.learniscisco.net. Available at: <https://www.learniscisco.net/courses/iins/common-security-threats/security-architecture-design-guidelines.html> [Accessed 2022].
27. docs.netgate.com. (2022). Installing and Upgrading – Perform the Installation – Installation Walkthrough | pfSense Documentation. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/install/install-walkthrough.html> [Accessed 2022].
28. gambit (2019). Installation | Kali Linux Documentation. [online] Kali Linux. Available at: <https://www.kali.org/docs/installation/> [Accessed 2022].
29. docs.netgate.com. (2020). User Management and Authentication – Default Username and Password | pfSense Documentation. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/usermanager/defaults.html#:~:text=The%20default%20credentials%20for%20a> [Accessed 2022].
30. docs.netgate.com. (n.d.). Firewall – Firewalling Fundamentals | pfSense Documentation. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html> [Accessed 2022].
31. Blumira. (2021). Best Practices For Configuring Firewall Rules. [online] Available at: <https://www.blumira.com/firewall-best-practices/> [Accessed 2022].
32. Check Point Software. (2021). What is a DMZ Network? [online] Available at: <https://www.checkpoint.com/cyber-hub/network-security/what-is-a-dmz-network/> [Accessed 2022].
33. Ubach Manau, J. (n.d.). Iniciar Sesión | OpenWebinars. [online] OpenWebinars.net. Available at: <https://openwebinars.net/academia/aprende/firewall-pfense/> [Accessed 2022].
34. Gite, V. (2018). Ubuntu Linux install OpenSSH server. [online] nixCraft. Available at: <https://www.cyberciti.biz/faq/ubuntu-linux-install-openssh-server/> [Accessed 2022].
35. Docker Documentation. (2020). Install Docker Engine on Ubuntu. [online] Available at: <https://docs.docker.com/engine/install/ubuntu/> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 101 de 106		2021/2022

36. Digital Avenue (2019). How To Setup DHCP with DNS Server on pfSense - Complete Guide. YouTube. Available at: <https://www.youtube.com/watch?v=J50FFKkzpD0> [Accessed 2022].
37. <https://www.redhat.com/sysadmin/users/dgarn> and Garn, D. (2020). Eight ways to protect SSH access on your system. [online] Enable Sysadmin. Available at: <https://www.redhat.com/sysadmin/eight-ways-secure-ssh> [Accessed 2022].
38. derechodelared (2022). SSH Commands Cheat Sheet | Derecho de la Red. [online] Derecho de la Red. Available at: <https://derechodelared.com/ssh-commands-cheat-sheet/> [Accessed 2022].
39. Alvaro De León (2012). Securizando el servicio SSH - Hosting Diario. [online] Hosting Diario. Available at: <https://hostingdiario.com/securizando-el-servicio-ssh/> [Accessed 2022].
40. Docker.com. (2022). Docker Hub. [online] Available at: https://hub.docker.com/_/wordpress [Accessed 2022].
41. Docker Documentation. (2022). Install Docker Compose. [online] Available at: <https://docs.docker.com/compose/install/> [Accessed 2022].
42. VirtualCoin CISSP, PMP, CCNP, MCSE, LPIC2 (2020). Tutorial - Snort Installation on PfSense [Step by Step]. [online] TechExpert. Available at: <https://techexpert.tips/pfsense/snort-installation-pfsense/#:~:text=Access%20the%20PfSense%20System%20menu,and%20install%20the%20Snort%20package>. [Accessed 2022].
43. Netgate.com. (2022). Packages – IDS / IPS – Configuring the Snort Package | pfSense Documentation. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html> [Accessed 2022].
44. Docker Documentation. (2022). Quickstart: Compose and WordPress. [online] Available at: <https://docs.docker.com/samples/wordpress/> [Accessed 2022].
45. Mins (2022). Automating mysql_secure_installation. [online] Gist. Available at: https://gist.github.com/Mins/4602864#file-mysql_secure-sh [Accessed 2022].
46. Docker Documentation. (2022). Use multi-stage builds. [online] Available at: <https://docs.docker.com/develop/develop-images/multistage-build/> [Accessed 2022].
47. hannesHier (2020). Wordpress Docker 'Error establishing a database connection'. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/60366969/wordpress-docker-error-establishing-a-database-connection> [Accessed 2022].
48. TJ L (2010). Have bash script answer interactive prompts. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/3804577/have-bash-script-answer-interactive-prompts> [Accessed 2022].
49. Mysql.com. (2019). MySQL :: MySQL 8.0 Reference Manual :: 4.2.2.1 Using Options on the Command Line. [online] Available at: <https://dev.mysql.com/doc/refman/8.0/en/command-line-options.html> [Accessed 2022].
50. Netgate.com. (2022). Firewall | pfSense Documentation. [online] Available at: <https://docs.netgate.com/pfsense/en/latest/firewall/index.html> [Accessed 2022].
51. MariaDB KnowledgeBase. (2022). LOAD DATA INFILE. [online] Available at: <https://mariadb.com/kb/en/load-data-infile/> [Accessed 2022].
52. Mysql.com. (2022). MySQL :: MySQL 5.7 Reference Manual :: 6.4 Security Plugins. [online] Available at: <https://dev.mysql.com/doc/refman/5.7/en/security-plugins.html> [Accessed 2022].
53. César Marín (2021). Segundo factor de autenticación (2FA) en SSH. [online] Derecho de la Red. Available at: <https://derechodelared.com/segundo-factor-de-autenticacion-ssh/> [Accessed 2022].
54. twitter-forks (2012). mysql/mysql_secure_installation.sh at master · twitter-forks/mysql. [online] GitHub.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 102 de 106		2021/2022

Available at:

https://github.com/twitter-forks/mysql/blob/master/scripts/mysql_secure_installation.sh [Accessed 2022].

55. juancarlospd (2022). `projectointegrado/mysqlsecure.sh` at `main` · `juancarlospd/projectointegrado`. [online] GitHub.
 Available at: <https://github.com/juancarlospd/projectointegrado/blob/main/mysqlsecure.sh> [Accessed 2022].
56. Kear, S. (2011). Port Forwarding in pfSense: How to Configure NAT. [online] TurboFuture.
 Available at:
<https://turbofuture.com/computers/Port-Forwarding-in-pfSense-How-to-Configure-NAT#:~:text=To%20set%20up%20port%20forwarding%2C%20click%20on%20NAT%20from%20the,rule%20you%20want%20to%20change>. [Accessed 2022].
57. Netgate.com. (2016). Network Address Translation – Port Forwards | pfSense Documentation. [online]
 Available at: <https://docs.netgate.com/pfsense/en/latest/nat/port-forwards.html> [Accessed 2022].
58. Netgate.com. (2022). Network Address Translation – 1:1 NAT | pfSense Documentation. [online]
 Available at: <https://docs.netgate.com/pfsense/en/latest/nat/1-1.html> [Accessed 2022].
59. Netgate.com. (2022). pfSense® software Configuration Recipes – Accessing Port Forwards from Local Networks | pfSense Documentation. [online]
 Available at:
<https://docs.netgate.com/pfsense/en/latest/recipes/port-forwards-from-local-networks.html> [Accessed 2022].
60. Netgate.com. (2022). pfSense® software Configuration Recipes – Accessing Port Forwards from Local Networks | pfSense Documentation. [online]
 Available at:
<https://docs.netgate.com/pfsense/en/latest/recipes/port-forwards-from-local-networks.html> [Accessed 2022].
61. AssinetInformatica (2012). Tutorial pfSense Firewall NAT 1:1. YouTube.
 Available at: <https://www.youtube.com/watch?v=5lMRA1ntgz8> [Accessed 2022].
62. SZZ HowConfigure (2017). pfsense: Nat 1:1 (dmz,outside). YouTube.
 Available at: <https://www.youtube.com/watch?v=gBjKBoyByDQ> [Accessed 2022].
63. Netgate.com. (2022). pfSense® software Configuration Recipes – Routing Public IP Addresses | pfSense Documentation. [online]
 Available at: <https://docs.netgate.com/pfsense/en/latest/recipes/route-public-ip-addresses.html> [Accessed 2022].
64. Netgate.com. (2022). Services – NTPD – NTP Server Configuration | pfSense Documentation. [online]
 Available at: <https://docs.netgate.com/pfsense/en/latest/services/ntp/server.html> [Accessed 2022].
65. Areca-backup.org. (2022). Areca Backup - Official Website. [online]
 Available at: <http://www.areca-backup.org/> [Accessed 2022].
66. Bacula. (2015). The best free enterprise open source backup software for Linux. [online]
 Available at: <https://www.bacula.org/> [Accessed 2022].
67. Amanda.org. (2017). Amanda Network Backup: Open Source Backup for Linux, Windows, UNIX and OS X. [online]
 Available at: <http://www.amanda.org/> [Accessed 2022].
68. Latina (2019). 9.4 Community Bacula Installation. YouTube.
 Available at: <https://www.youtube.com/watch?v=oNamNX9Y6-I> [Accessed 2022].
69. Bacula. (2018). Deb and rpm Packages | Bacula. [online]
 Available at: <https://www.bacula.org/bacula-binary-package-download/> [Accessed 2022].
70. ITarian (2021). Steps to Bacula Setup and Installation. [online] ITarian.
 Available at: <https://www.itarian.com/msp-tools/bacula-setup.php> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	<i>Pág 103 de 106</i>		<i>2021/2022</i>

71. Bacula.org. (2017). Baculum Web GUI Tool. [online]
 Available at: https://www.bacula.org/7.4.x-manuals/en/console/Baculum_Web_GUI_Tool.html [Accessed 2022].
72. How (2021). How To Install amanda-server on Ubuntu 20.04. [online] Installati.one.
 Available at: <https://installati.one/ubuntu/20.04/amanda-server/> [Accessed 2022].
73. Bisson, M. (2020). Introducing Amanda Backup Tool For Linux. [online] ElderNode Blog.
 Available at: <https://blog.eldernode.com/amanda-backup-tool-for-linux/> [Accessed 2022].
74. Autoize. (2017). Multiple WordPress Sites on Docker - Autoize. [online]
 Available at: <https://autoize.com/multiple-wordpress-sites-docker/> [Accessed 2022].
75. Frimley Computing (2020). pfSense DNS Resolver Setup. YouTube.
 Available at: https://www.youtube.com/watch?v=1fhS_gGHMck [Accessed 2022].
76. WP Beaches (2018). Change WordPress URLs in MySQL Database when site is moved to new host. [online] WP Beaches.
 Available at:
<https://wpbeaches.com/updating-wordpress-mysql-database-after-moving-to-a-new-url/> [Accessed 2022].
77. CodePen. (2022). Wordpress SQL Wizard. [online]
 Available at: <https://codepen.io/EightArmsHQ/full/kaZyJd> [Accessed 2022].
78. Docker Documentation. (2022). docker container cp. [online]
 Available at: https://docs.docker.com/engine/reference/commandline/container_cp/ [Accessed 2022].
79. Crontab.guru. (2022). Crontab.guru - The cron schedule expression editor. [online]
 Available at: <https://crontab.guru/> [Accessed 2022].
80. sk (2019). A Beginners Guide To Cron Jobs. [online] OSTechNix.
 Available at: <https://ostechnix.com/a-beginners-guide-to-cron-jobs/> [Accessed 2022].
81. Esteban, S. (2015). ¿Cómo realizar un Pentesting sigiloso con Nmap? [online] Backtrack Academy.
 Available at:
<https://backtrackacademy.com/articulo/como-realizar-un-pentesting-sigiloso-con-nmap> [Accessed 2022].
82. NetworkChuck (2021). your home router SUCKS!! (use pfSense instead). YouTube.
 Available at: <https://www.youtube.com/watch?v=lUzSsX4T4WQ> [Accessed 2022].
83. Network \u00026 Software Solutions (2022). 27 - Qué es NAT 1:1 - Curso PfSense. YouTube.
 Available at: <https://www.youtube.com/watch?v=rwP3VXv0-8E> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 41013. Sevilla	Guía Práctica para el uso profesional de la nube	 AENOR ER Empresa Registrada ER-0934 / 2008
	Pág 104 de 106	2021/2022

10.3. Anexos del Desarrollo enfocado a la nube (6.2)

84. Gafnit Amiga (2021). AWS RDS Vulnerability Leads to AWS Internal Service Credentials. [online] Lightspin.io. Available at: <https://blog.lightspin.io/aws-rds-critical-security-vulnerability> [Accessed 2022].
85. asudbring (2022). What is Azure Load Balancer? - Azure Load Balancer. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview> [Accessed 2022].
86. asudbring (2021). Manage a public IP address with a load balancer - Azure Virtual Network. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/configure-public-ip-load-balancer> [Accessed 2022].
87. asudbring (2022). Quickstart: Create a public load balancer - Azure portal - Azure Load Balancer. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal> [Accessed 2022].
88. redirection.io (2021). Setting up a redirection server on Azure Cloud - Knowledge base | redirection.io. [online] redirection.io. Available at: <https://redirection.io/documentation/knowledge-base/setting-up-a-redirection-server-on-azure-cloud> [Accessed 2022].
89. Ibm.com. (2021). IBM Docs. [online] Available at: <https://www.ibm.com/docs/en/sva/9.0.7?topic=mas-uploading-azure-compliant-vhd-azure-creating-azure-image> [Accessed 2022].
90. Plain Concepts. (2021). Introduction to Azure Migrate. [online] Available at: <https://www.plainconcepts.com/azure-migrate-introduction/> [Accessed 2022].
91. Robinson, D. (2017). Migrating VirtualBox VDI Virtual Machines to Azure. [online] Kloud.com.au. Available at: <https://blog.kloud.com.au/2017/04/05/migrating-virtualbox-vdi-virtual-machines-to-azure/> [Accessed 2022].
92. Warner, T. (2020). Upload a Local VM Image to Microsoft Azure. YouTube. Available at: https://www.youtube.com/watch?v=iM1t_in-OuQ [Accessed 2022].
93. cynthn (2022). Creación y uso de un par de claves SSH para máquinas virtuales Linux en Azure - Azure Virtual Machines. [online] Microsoft.com. Available at: <https://docs.microsoft.com/es-es/azure/virtual-machines/linux/mac-create-ssh-keys> [Accessed 2022].
94. craigloewen-msft (2022). Install WSL. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/windows/wsl/install> [Accessed 2022].
95. craigloewen-msft (2021). What is Windows Subsystem for Linux. [online] Microsoft.com. Available at: <https://docs.microsoft.com/en-us/windows/wsl/about> [Accessed 2022].
96. How (2020). How to change file permissions on Windows via powershell / cmd? [online] Super User. Available at: <https://superuser.com/questions/1539172/how-to-change-file-permissions-on-windows-via-powershell-cmd> [Accessed 2022].
97. to, U. (2018). Unable to change file permissions on Ubuntu Bash for Windows 10. [online] Super User.

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube			 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 105 de 106				2021/2022

Available at:

<https://superuser.com/questions/1323645/unable-to-change-file-permissions-on-ubuntu-bash-for-windows-10> [Accessed 2022].

98. cynthn (2022). Use SSH keys to connect to Linux VMs - Azure Virtual Machines. [online] Microsoft.com.

Available at:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows#provide-an-ssh-public-key-when-deploying-a-vm> [Accessed 2022].

99. Chen, K. (2015). How To Enable, Configure and Use Hyper-V on Windows 10 - NEXTOFWINDOWS.COM. [online] Next of Windows.

Available at:

<https://www.nextofwindows.com/how-to-enable-configure-and-use-hyper-v-on-windows-10> [Accessed 2022].

100. bsiva (2021). Migrate Hyper-V VMs to Azure with Azure Migrate Server Migration - Azure Migrate. [online] Microsoft.com.

Available at: <https://docs.microsoft.com/en-us/azure/migrate/tutorial-migrate-hyper-v?tabs=UI> [Accessed 2022].

101. Andre Da Costa (2016). How to Migrate VirtualBox VMs to Windows 10 Hyper-V. [online] groovyPost.

Available at: <https://www.groovypost.com/howto/migrate-virtual-box-vms-windows-10-hyper-v/> [Accessed 2022].

102. IT Blog. (2019). Zeljko Medic. [online]

Available at:

<https://www.informaticarnet.net/convert-vhd-hyper-v-encountered-an-error-trying-to-access-an-object-on-computer-yourcomputername-because-the-object-was-not-found/> [Accessed 2022].

103. Microsoft.com. (2016). PowerShell Convert-VHD. [online]

Available at:

<https://social.technet.microsoft.com/Forums/en-US/92cbba79-27e9-4a8b-8309-d4a06b7f34cb/powershell-convertvhd?forum=winserverhyperv> [Accessed 2022].

104. scooley (2022). Enable Hyper-V on Windows 10. [online] Microsoft.com.

Available at:

<https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v> [Accessed 2022].

105. cynthn (2022). Captura de una imagen administrada de una máquina virtual Linux con la CLI de Azure - Azure Virtual Machines. [online] Microsoft.com.

Available at:

<https://docs.microsoft.com/es-es/azure/virtual-machines/linux/capture-image?toc=%2Fazure%2Fvirtual-machines%2Flinux%2Ftoc.json> [Accessed 2022].

106. cynthn (2022). Creación de una máquina virtual a partir de un disco duro virtual de Windows generalizado cargado - Azure Virtual Machines. [online] Microsoft.com.

Available at:

<https://docs.microsoft.com/es-es/azure/virtual-machines/windows/upload-generalized-managed?toc=%2Fazure%2Fvirtual-machines%2Fwindows%2Ftoc.json> [Accessed 2022].

107. Docker Documentation. (2022). docker cp. [online]

Available at: <https://docs.docker.com/engine/reference/commandline/cp/> [Accessed 2022].

108. rohinkoul (2021). Quickstart: Create a DNS zone and record - Azure portal - Azure DNS. [online] Microsoft.com.

Available at: <https://docs.microsoft.com/en-us/azure/dns/dns-getstarted-portal> [Accessed 2022].

109. Zion3R (2022). Cloudsploit - Cloud Security Posture Management (CSPM). [online] KitPloit - PenTest & Hacking Tools.

Available at: <https://www.kitploit.com/2022/02/cloudsploit-cloud-security-posture.html> [Accessed 2022].

 IES Polígono Sur c/ Esclava del Señor, 2 41013. Sevilla	Guía Práctica para el uso profesional de la nube			 AENOR ER Empresa Registrada ER-0934 / 2008	 CERTIFIED IQNet QUALITY SYSTEM
	Pág 106 de 106				2021/2022

110. greg-lindsay (2022). Quickstart: Create a public load balancer - Azure portal - Azure Load Balancer. [online] Microsoft.com.
 Available at:
<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-create-load-balancer-standard> [Accessed 2022].
111. cynthn (2022). Create a managed image in Azure - Azure Virtual Machines. [online] Microsoft.com.
 Available at:
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource> [Accessed 2022].
112. cynthn (2022). Create VM from a managed image in Azure - Azure Virtual Machines. [online] Microsoft.com.
 Available at:
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/create-vm-generalized-managed> [Accessed 2022].
113. Zion3R (2022). Cloudsploit - Cloud Security Posture Management (CSPM). [online] KitPloit - PenTest & Hacking Tools. Available at:
<https://www.kitploit.com/2022/02/cloudsploit-cloud-security-posture.html> [Accessed 2022].
114. aquasecurity (2020). cloudsploit/azure.md at master · aquasecurity/cloudsploit. [online] GitHub.
 Available at:
<https://github.com/aquasecurity/cloudsploit/blob/master/docs/azure.md#cloud-provider-configuration> [Accessed 2022].
115. aquasecurity (2021). Error loading config file · Issue #498 · aquasecurity/cloudsploit. [online] GitHub. Available at: <https://github.com/aquasecurity/cloudsploit/issues/498> [Accessed 2022].
- 116.
- 117.
- 118.
- 119.
- 120.
- 121.
- 122.
- 123.
- 124.
- 125.
- 126.

Ideas olvidadas

127. Ver (2022). DevSecOps y detección de vulnerabilidades con Trivy. [online] Seguridad en Sistemas y Técnicas de Hacking. TheHackerWay (THW).
 Available at: <https://thehackerway.com/2022/05/05/devsecops-y-deteccion-de-vulnerabilidades-con-trivy/> [Accessed 2022].
128. albesplab (2022). Vulnerabilidad Azure expone bases de datos PostgreSQL. [online] Una al Día. Available at: <https://unaaldia.hispasec.com/2022/05/vulnerabilidad-azure-expone-bases-de-datos-postgresql.html> [Accessed 2022].
129. Herrero, H. (2022). Auditoría de acceso a ficheros con Elasticsearch y Grafana. [online] Blog Bujarra.com | Blog IT de Héctor Herrero.
 Available at: <https://www.bujarra.com/auditoria-de-acceso-a-ficheros-con-elasticsearch-y-grafana/> [Accessed 2022].
130. Zion3R (2022). Cloudsploit - Cloud Security Posture Management (CSPM). [online] KitPloit - PenTest & Hacking Tools.
 Available at: <https://www.kitploit.com/2022/02/cloudsploit-cloud-security-posture.html> [Accessed 2022]