

## Práctica 4.2. Administración de DNS con AWS Route 53

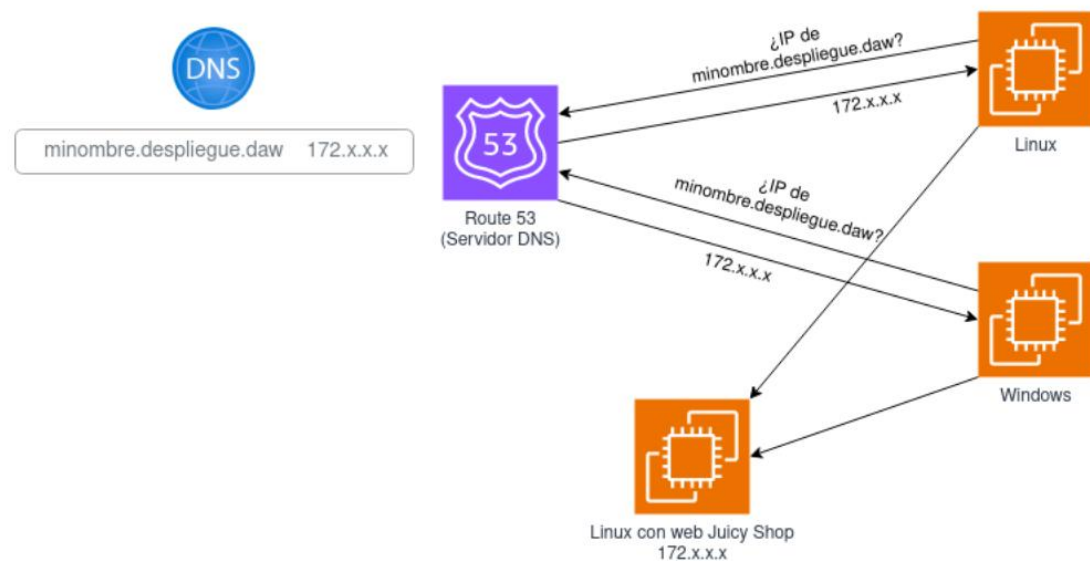
### 1. Introducción

En este caso vamos a realizar una práctica similar a la anterior, pero configurando el servidor DNS en un entorno de AWS.

Amazon **Route 53** es el **servicio de DNS escalable y administrado por AWS**. Además de las funciones típicas DNS también incluye:

1. **Registro de dominios.** Puedes comprar y gestionar dominios directamente desde AWS.
2. **DNS hosting.** Maneja las zonas DNS de tus dominios con alta disponibilidad y baja latencia. Soporta registros A, AAAA, CNAME, MX, TXT, SRV, etc.
3. **Routing (enrutamiento avanzado)**
  - a. **Simple:** Respuesta única (ej: una IP fija).
  - b. **Weighted:** Divide el tráfico por porcentajes entre múltiples recursos.
  - c. **Latency-based:** Envía al servidor más rápido según ubicación del usuario.
  - d. **Failover:** Redirige a recursos de respaldo si el principal falla.
  - e. **Geolocation / Geoproximity:** Según país o región del usuario.
4. **Health checks.** Supervisa la salud de endpoints (ej: un servidor web); y puede quitar automáticamente de la rotación a los que fallen.
5. **Integración con AWS** de forma nativa con otros servicios.

Esta será la estructura que hagamos:



## 2. Creación de Instancias EC2

Vamos a crear 3 instancias EC2 con **claves**:

- Servidor web → Linux con Docker corriendo la aplicación web Juicy Shop
- Cliente-Linux1 → Linux que actuará como cliente para realizar consultas DNS
- Cliente-Windows2 → Windows que actuará como cliente para realizar consultas DNS

Es importante tener en cuenta que por defecto, todas las instancias EC2 que creemos a parte de su IP pública, todas pertenecen a una Nube Privada Virtual (VPC).

### 2.1 Proceso en imágenes

#### 1. CREACIÓN SERVIDOR WEB

**Nombre y etiquetas**
[Información](#)

Nombre

Linux-Servidor

Agregar etiquetas adicionales


**Application and OS Images (Amazon Machine Image)**
[Información](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below


Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

**Inicio rápido**


Amazon Linux




macOS




Ubuntu




Windows




Red Hat



SUSE Linux




**Buscar más AMI**

Inclusión de AMI de AWS, Marketplace y la comunidad

**Imágenes de máquina de Amazon (AMI)**

**AMI de Amazon Linux 2023**

Apto para la capa gratuita

ami-0a3c3a20c09d6f377 (64 bits (x86), uefi-preferred) / ami-0bb6cbb99aec63c04 (64 bits (Arm), uefi)

Virtualización: hvm    ENA enabled: true    Tipo de dispositivo raíz: ebs

**Descripción**

▼ Tipo de instancia
 Información | Get advice

Tipo de instancia

t2.micro

Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true  
 Bajo demanda Windows base precios: 0.0162 USD por hora  
 Bajo demanda SUSE base precios: 0.0116 USD por hora  
 Bajo demanda RHEL base precios: 0.0716 USD por hora  
 Bajo demanda Linux base precios: 0.0116 USD por hora

☐ Todas las generaciones  
  
[Comparar tipos de instancias](#)

Se aplican costos adicionales a las AMI con software preinstalado

▼ Par de claves (inicio de sesión)
 Información

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio
 

Seleccionar

▲

Continuar sin un par de claves (no recomendado)
 Valor predeterminado

vockey

Tipo: rsa

3

**⚠ Para las solicitudes V2, debe incluir un token de sesión en todas las solicitudes de metadatos de la instancia. Las aplicaciones o agentes que utilizan V1 para el acceso a los metadatos de la instancia se interrumpirán.**

Límite de saltos de respuesta de metadatos [Información](#)


2

Permitir etiquetas en metadatos [Información](#)

Seleccionar ▼

Datos de usuario - *optional* [Información](#)

Cargue un archivo con los datos de usuario o escríbalo en el campo.

 **Choose file**

```
#!/bin/bash
yum update -y
yum install -y docker
service docker start
systemctl enable docker.service
docker pull bkimminich/juice-shop
docker run -d -p 80:3000 bkimminich/juice-shop
```

☐ Los datos de usuario ya han sido codificados en base64

El siguiente código despliega una aplicación web en el puerto 80 (no hace falta que lo entendamos), puede tardar en desplegar.:

```
#!/bin/bash
yum update -y
yum install -y docker
service docker start
systemctl enable docker.service
docker pull bkimminich/juice-shop
docker run -d --restart always -p 80:3000 bkimminich/juice-shop
```

## 2. CREACIÓN CLIENTE LINUX

[EC2](#) > [Instancias](#) > [Lanzar una instancia](#)

### Lanzar una instancia Información

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

#### Nombre y etiquetas Información

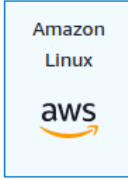
Nombre

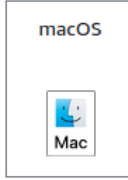
[Agregar etiquetas adicionales](#)


#### ▼ Application and OS Images (Amazon Machine Image) Información

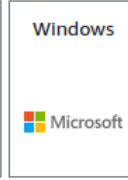
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below


#### Inicio rápido

















[Buscar más AMI](#)

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

5

### 3. CREACIÓN CLIENTE WINDOWS

Servicios

[Alt+S]

Nombre

Windows-Cliente2

Agregar etiquetas adicionales

▼ Application and OS Images (Amazon Machine Image) [Información](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Inicio rápido

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu®

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUS

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Microsoft Windows Server 2022 Base

Apto para la capa gratuita ▼

ami-00d990e7e5ece7974 (64 bits (x86))

Virtualización: hvm ENA enabled: true Tipo de dispositivo raíz: ebs

Descripción

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Arquitectura

ID de AMI

ami-00d990e7e5ece7974

Descargar imagen

6

## Crear par de claves



### Nombre del par de claves

Con los pares de claves es posible conectarse a la instancia de forma segura.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

### Tipo de par de claves

☒ **RSA**

Par de claves pública y privada cifradas mediante RSA

☐ **ED25519**

Par de claves pública y privada cifradas con ED25519 (no es compatible con instancias Windows)

### Formato de archivo de clave privada

☒ **.pem**

Para usar con OpenSSH

☐ **.ppk**

Para usar con PuTTY



Quando se le solicite, almacene la clave privada en un lugar seguro y accesible del equipo. **Lo necesitará más adelante para conectarse a la instancia.** [Más información](#)

Cancelar

Crear par de claves

## ▼ Configuraciones de red [Información](#)

Editar

Red [Información](#)

vpc-0143c27d846a5588f

Subred [Información](#)

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública [Información](#)

Habilitar

Firewall (grupos de seguridad) [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ **Crear grupo de seguridad**
☐ Seleccionar un grupo de seguridad existente

We'll create a new security group called 'launch-wizard-7' with the following rules:

☒ **Allow RDP traffic from**

Helps you connect to your instance

Cualquier lugar  
0.0.0.0/0

☐ **Permitir el tráfico de HTTPS desde Internet**

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

☐ **Permitir el tráfico de HTTP desde Internet**

Para configurar un punto de enlace, por ejemplo, al crear un servidor web



Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.



## 2.2 Configuración del grupo de seguridad

Debemos ir al panel de control de EC2 y ver las IP privadas de nuestros Cliente-Linux y Cliente-Windows:

<input type="checkbox"/>	Linux-Servidor	i-092543a1089cffe9e	En ejecución	t3.small	3/3 comprobaci	Ver alarmas +	us-east-1c
<input checked="" type="checkbox"/>	Cliente-Linux1	i-033356dc809364613	En ejecución	t3.micro	3/3 comprobaci	Ver alarmas +	us-east-1c
<input type="checkbox"/>	Cliente-Windows2	i-08c0578f0eb28431b	En ejecución	t3.micro	Inicializando	Ver alarmas +	us-east-1c

i-033356dc809364613 (Cliente-Linux1)

Detalles	Estado y alarmas	Monitoreo	Seguridad	Redes	Almacenamiento	Etiquetas
<b>Resumen de instancia</b> Información						
<b>ID de la instancia</b> i-033356dc809364613		<b>Dirección IPv4 pública</b> 18.212.219.206   dirección abierta		<b>Direcciones IPv4 privadas</b> 172.31.22.242		
<b>Dirección IPv6</b> -		<b>Estado de la instancia</b> En ejecución		<b>DNS público</b> ec2-18-212-219-206.compute-1.amazonaws.com   dire abierta		

Luego vamos a crearnos un grupo de seguridad para la práctica con el nombre: **apellidoNombre-practica-route53**:

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamientos dedicados

Reservas de capacidad

Novedad

Imágenes

AMI

Catálogo de AMI

Elastic Block Store

Volúmenes

Instantáneas

Administrador del ciclo de vida

Red y seguridad

Security Groups

Direcciones IP elásticas

Grupos de ubicación

Pares de claves

Interfaces de red

Grupos de seguridad (8) Información

Find resources by attribute or tag

Crear grupo de seguridad

	Name	Security group ID	Nombre del grupo de seguridad	ID de la VPC	Descripción	Propietario
<input type="checkbox"/>	-	sg-036b18ff7c1b3fcd2	launch-wizard-3	vpc-0143c27d846a5588f	launch-wizard-3 created 2024-01-22T...	944873386727
<input type="checkbox"/>	-	sg-040544d8568361921	launch-wizard-7	vpc-0143c27d846a5588f	launch-wizard-7 created 2024-01-23T...	944873386727
<input type="checkbox"/>	-	sg-038a6a0b96d3a9437	launch-wizard-2	vpc-0143c27d846a5588f	launch-wizard-2 created 2024-01-22T...	944873386727
<input type="checkbox"/>	-	sg-0d90e02769fad6ad8	launch-wizard-5	vpc-0143c27d846a5588f	launch-wizard-5 created 2024-01-23T...	944873386727
<input type="checkbox"/>	-	sg-0e60a2f0c3462b413	launch-wizard-6	vpc-0143c27d846a5588f	launch-wizard-6 created 2024-01-23T...	944873386727
<input type="checkbox"/>	-	sg-0856b54b0232a1a8f	default	vpc-0143c27d846a5588f	default VPC security group	944873386727
<input type="checkbox"/>	-	sg-05e99c6453728cb16	launch-wizard-1	vpc-0143c27d846a5588f	launch-wizard-1 created 2024-01-18T...	944873386727

8



## Crear grupo de seguridad [Información](#)

Un grupo de seguridad actúa como un firewall virtual para que la instancia controle el tráfico de entrada y salida.

### Detalles básicos

#### Nombre del grupo de seguridad [Información](#)

El nombre no se puede editar después de su creación.

#### Descripción [Información](#)

#### VPC [Información](#)



vpc-09686eaeff02483a0  
172.31.0.0/16

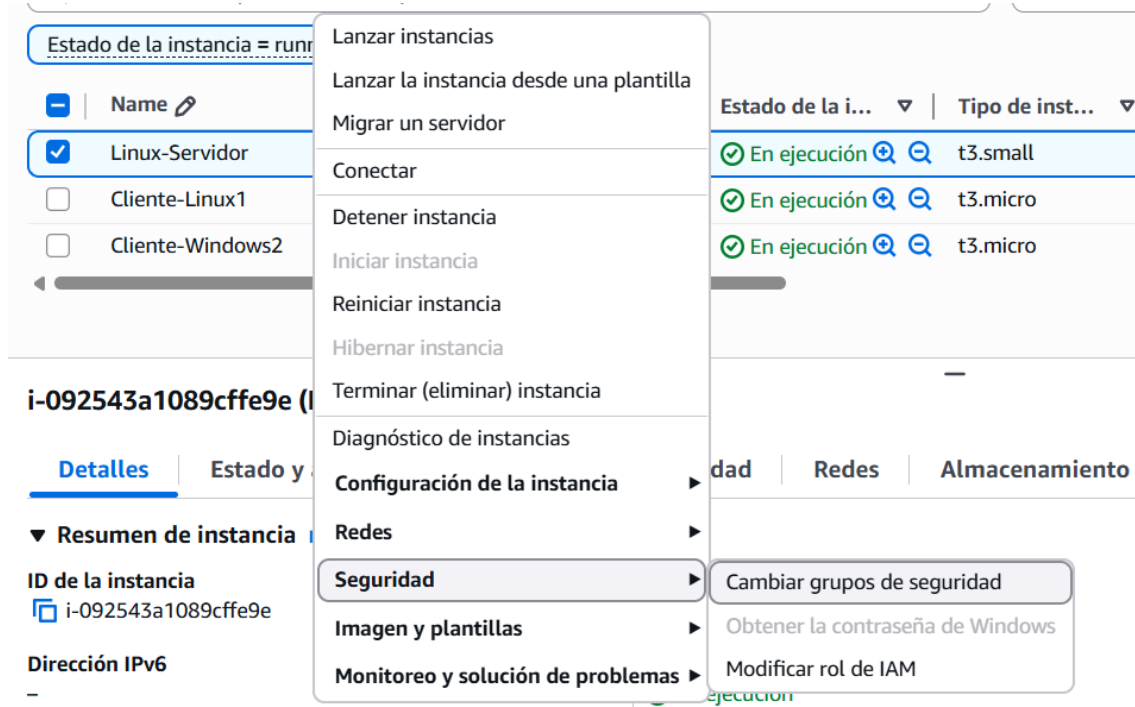
(predeterminada) ✓

En este grupo de seguridad permitiremos solicitudes HTTP por parte de nuestros clientes mediante las Reglas de Entrada:

### Reglas de entrada [Información](#)

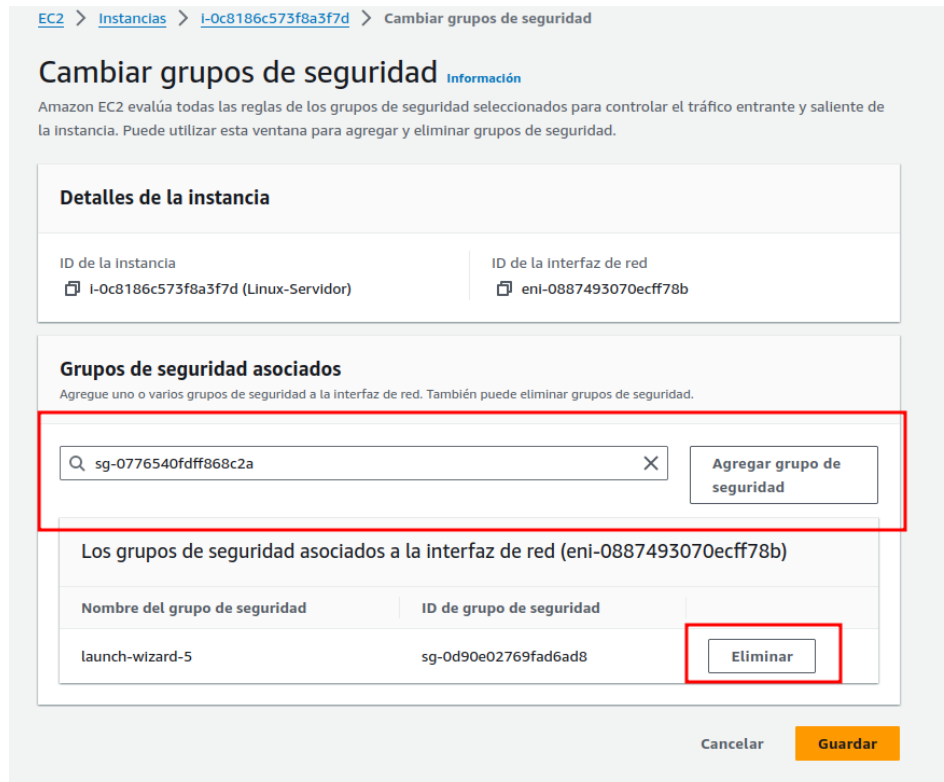
Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>	Descripción: opcional <a href="#">Información</a>	
HTTP	TCP	80	Person...	Q 172.31.22.242/32	Eliminar
HTTP	TCP	80	Person...	Q 172.31.24.238/32	Eliminar
Agregar regla					

Una vez creado el grupo de seguridad tenemos que asignárselo a nuestro Linux-Servidor:



The screenshot shows the AWS Management Console interface. On the left, a list of instances is visible, with 'Linux-Servidor' selected. A context menu is open, showing various actions for the instance. The 'Seguridad' (Security) option is highlighted, and a sub-menu is displayed with the following options: 'Cambiar grupos de seguridad' (Change security groups), 'Obtener la contraseña de Windows' (Get Windows password), and 'Modificar rol de IAM' (Modify IAM role). The 'Cambiar grupos de seguridad' option is the one we need to click to assign a security group to the instance.

Primero eliminamos el grupo de seguridad que se crea cuando se creamos el EC2 y luego añadimos nuestro grupo de seguridad:



The screenshot shows the 'Cambiar grupos de seguridad' (Change security groups) page in the AWS Management Console. The page displays the details of the instance and the associated security groups. The 'Detalles de la instancia' section shows the instance ID 'i-0c8186c573f8a3f7d (Linux-Servidor)' and the network interface ID 'eni-0887493070ecff78b'. The 'Grupos de seguridad asociados' section shows the current security group 'launch-wizard-5' with ID 'sg-0d90e02769fad6ad8'. A red box highlights the 'Eliminar' (Delete) button next to this group. Another red box highlights the search bar and the 'Agregar grupo de seguridad' (Add security group) button, indicating where to add a new security group.

### Grupos de seguridad asociados

Agregue uno o varios grupos de seguridad a la interfaz de red. También puede eliminar grupos de seguridad.

Q sg-027f8c087dbabaa37



Agregar grupo de seguridad

#### Los grupos de seguridad asociados a la interfaz de red (eni-0db362c924cfc2a11)

ID de grupo de seguridad	Nombre del grupo de seguridad	Descripción	ID del propietario
sg-027f8c087dbabaa37	arjonaSergio-practica-route53	Permite el acceso HTTP al servidor web por parte de los clientes	533267374462

## 2.2.1 Comprobación con Linux Cliente

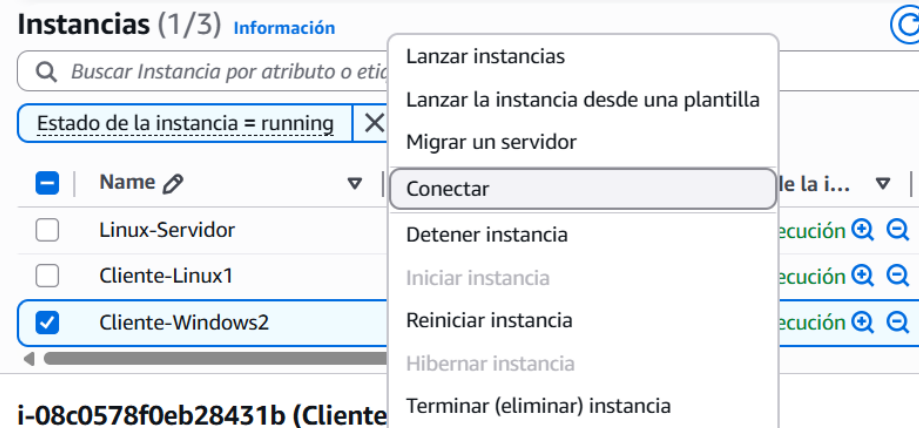
Para saber si se ha configurado bien debemos acceder por SSH a nuestro LinuxCliente1 (con el usuario ec2-user) y hacer un *curl* al servidor web:

```
[ec2-user@ip-172-31-22-242 ~]$ curl 172.31.25.253
<!--
~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors
.
~ SPDX-License-Identifier: MIT
-->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticated i
nsecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_
js.ico">
  <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/
cookieconsent2/3.1.0/cookieconsent.min.css">
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconse
nt.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></sc
ript>
```

## 2.2.2 Comprobación con Windows Cliente

Para comprobarlo con nuestro cliente Windows debemos hacerlo a través del protocolo RDP (Remote Desktop Protocol):



**Instancias (1/3)** Información

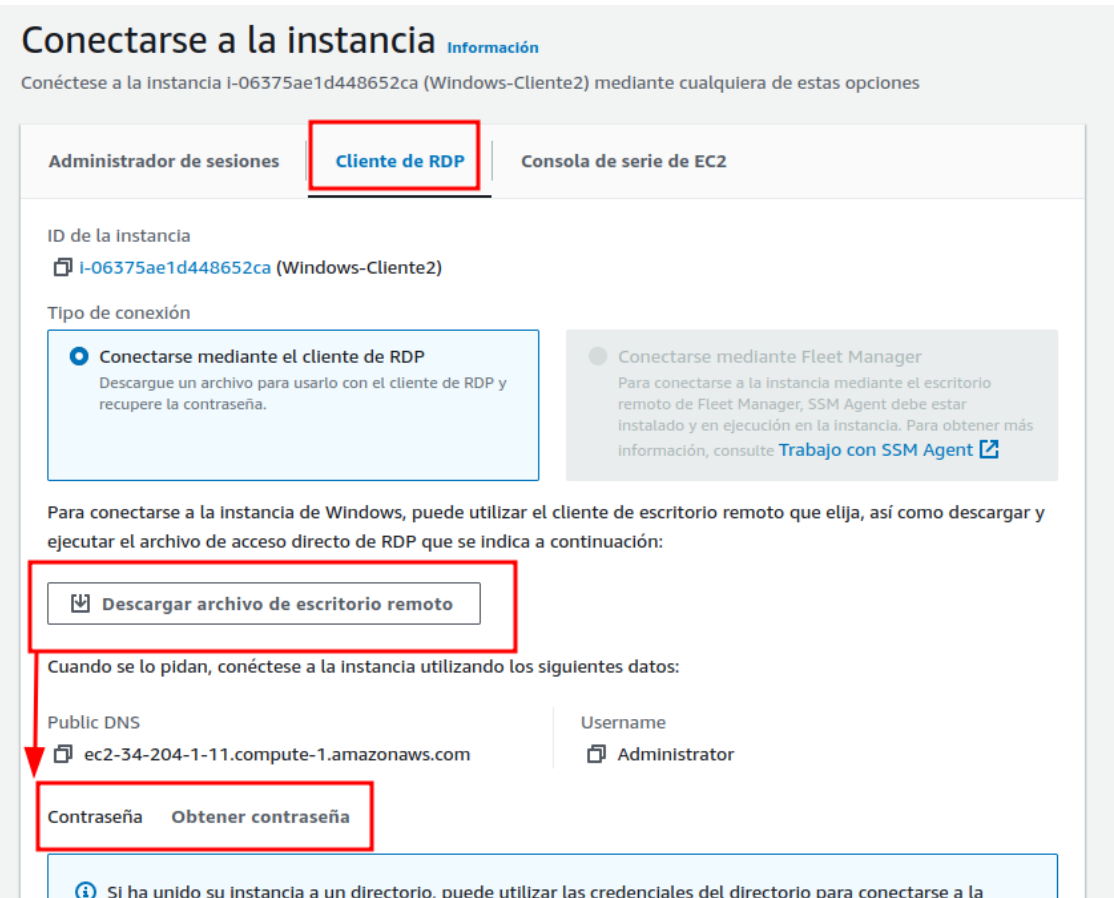
Buscar Instancia por atributo o etiqueta

Estado de la instancia = running

	Name
<input type="checkbox"/>	Linux-Servidor
<input type="checkbox"/>	Cliente-Linux1
<input checked="" type="checkbox"/>	Cliente-Windows2

**i-08c0578f0eb28431b (Cliente-Windows2)**

- Lanzar instancias
- Lanzar la instancia desde una plantilla
- Migrar un servidor
- Conectar**
- Detener instancia
- Iniciar instancia
- Reiniciar instancia
- Hibernar instancia
- Terminar (eliminar) instancia



### Conectarse a la instancia

Conéctese a la Instancia i-06375ae1d448652ca (Windows-Cliente2) mediante cualquiera de estas opciones

Administrador de sesiones | **Cliente de RDP** | Consola de serie de EC2

ID de la instancia  
i-06375ae1d448652ca (Windows-Cliente2)

Tipo de conexión

- Conectarse mediante el cliente de RDP**  
Descargue un archivo para usarlo con el cliente de RDP y recupere la contraseña.
- Conectarse mediante Fleet Manager  
Para conectarse a la instancia mediante el escritorio remoto de Fleet Manager, SSM Agent debe estar instalado y en ejecución en la instancia. Para obtener más información, consulte [Trabajo con SSM Agent](#)

Para conectarse a la instancia de Windows, puede utilizar el cliente de escritorio remoto que elija, así como descargar y ejecutar el archivo de acceso directo de RDP que se indica a continuación:

**Descargar archivo de escritorio remoto**

Cuando se lo pidan, conéctese a la instancia utilizando los siguientes datos:

Public DNS  
ec2-34-204-1-11.compute-1.amazonaws.com

Username  
Administrator

Contraseña **Obtener contraseña**

Si ha unido su instancia a un directorio, puede utilizar las credenciales del directorio para conectarse a la instancia.

EC2 > Instancias > i-06375ae1d448652ca > Obtener la contraseña de Windows

## Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia  
 i-06375ae1d448652ca (Windows-Cliente2)

Par de claves asociado a esta instancia  
 claves-Windows


Clave privada  
 Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.


✓ claves\_cliente2.windows.pem  
 1.674KB

Contenido de la clave privada: *opcional*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAY58dU4hZsglS4LITFotEI93d6bXA82Gr/Ns2dwOvmzgRcWC5
D65qAlida1zyxY/Jb0QAdEirSFHFJ8o/gCCKuGB2RQ8Ubp+rsBH450ir3mKkoQmcW
8yw5FmLuhdZB6xk+7+PxxgY4WV97AP9O4ZnuF5MJQXGJToh00xj9mPaLYL8RRQp
yk3dNesUJ2P63U7ztOOVLJNsJmsaCdhkqFnJYPTXCX6R8P2XM/47PGELCKImCOX2
hXbHEgVoRtVDPaDtM+orSzD/TfZJCkeEe1Jc+toNgPJfaS557H7kMVG9RwLUP5MA
4px7fRstYIIB4GkX4JanyTRE01UJWc5PvVgv+wIDAQABAolBADLr4vWvS56qOcz
FG3uiCDziEMAEqgpXqTK5jt8/QfXMglOJyTat9loPOZ9vlicLxSs3tuMyjva9hm
-----
```

Ahora para poder conectarnos de forma remota utilizaremos la aplicación Escritorio Remoto de Windows y abriremos el .rdp que hemos descargado antes e, introduciremos la contraseña que hemos obtenido previamente:


**Conexión a Escritorio remoto**  
 Aplicación


**Escritorio remoto**  
**Conexión**

General | Pantalla | Recursos locales | Rendimiento | Opciones avanzadas

**Configuración del inicio de sesión**

Escriba el nombre del equipo remoto.

Equipo: 2-54-158-22-207.compute-1.amazonaws.com

Usuario: Administrator

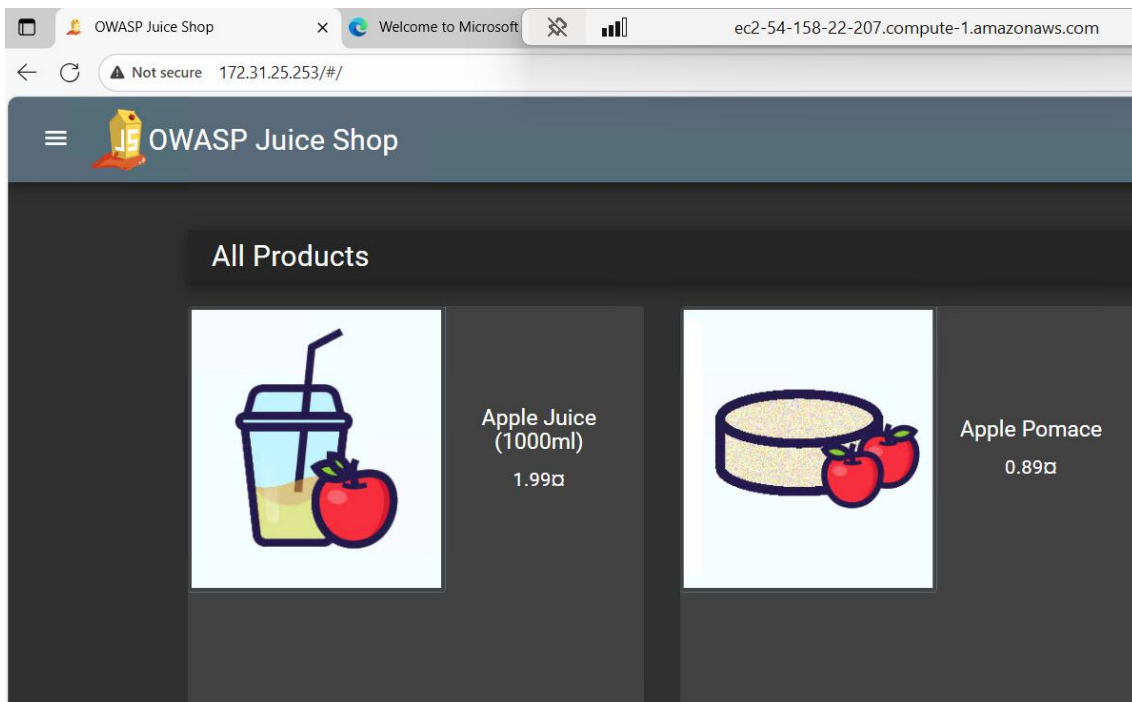
Se solicitarán credenciales al conectarse.

☐ Permitirme guardar las credenciales

**Configuración de la conexión**

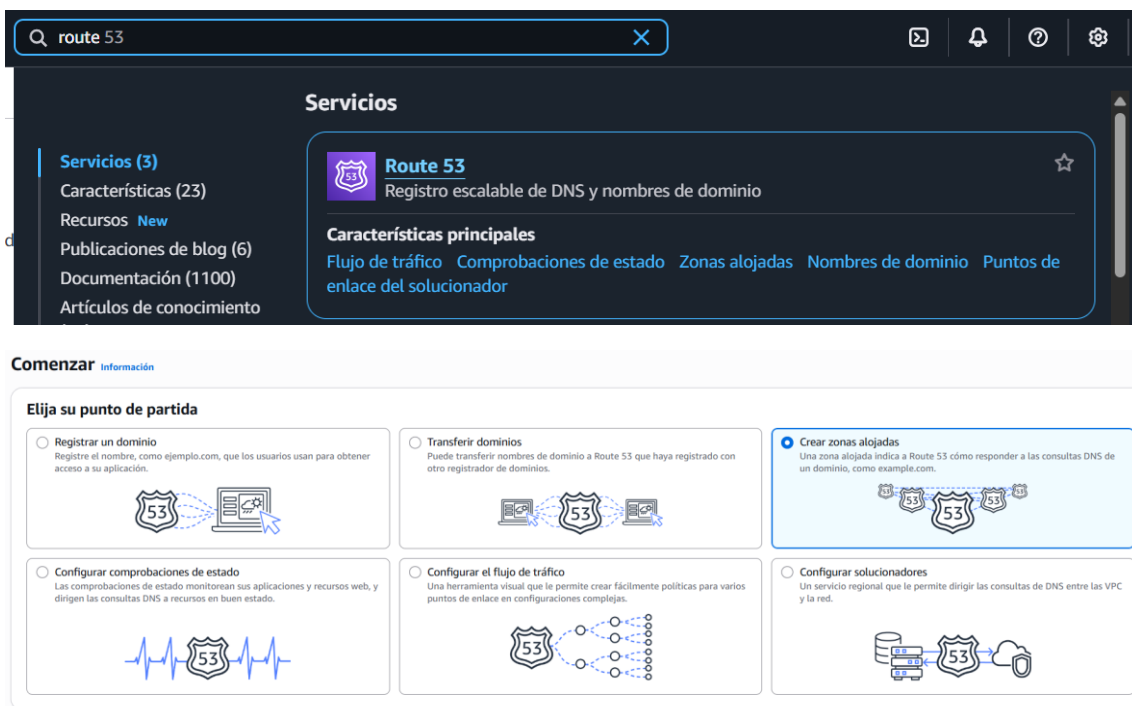
Guarde la configuración de conexión actual en un archivo RDP o abra una conexión guardada.

Y por último, comprobamos que podemos acceder a la web del servidor web:



### 3. Configuración Route 53

Ahora vamos a crear la zona privada despliegue.daw con Route 53





## Configuración de zona alojada

Una zona alojada es un contenedor que incluye información sobre cómo usted desea dirigir el tráfico de un dominio (como example.com) y sus subdominios.

### Nombre de dominio [Información](#)

Este es el nombre del dominio al que desea dirigir el tráfico.

despliegue.daw

Caracteres válidos: a-z, 0-9, ! " # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

### Descripción - *opcional* [Información](#)

Este valor le permite distinguir las zonas alojadas que tienen el mismo nombre.

La zona alojada se utiliza para...

La descripción puede tener un máximo de 256 caracteres. 0/256

### Tipo [Información](#)

El tipo indica si desea dirigir el tráfico en Internet o en una VPC de Amazon.



#### Zona alojada pública

Una zona alojada pública determina cómo se dirige el tráfico en Internet.



#### Zona alojada privada

Una zona alojada privada determina cómo se direcciona el tráfico dentro de una VPC de Amazon.

## VPC para asociar con la zona alojada [Información](#)

Para utilizar esta zona alojada a fin de resolver las consultas de DNS para una o varias VPC, elija las VPC. Para asociar una VPC creada con una cuenta de AWS diferente a una zona alojada, debe utilizar un método programático, como la CLI de AWS.



Para cada VPC que asocia a una zona alojada privada, debe establecer la configuración de Amazon VPC [enableDnsHostnames](#) y [enableDnsSupport](#) en verdadero.

### Región [Información](#)

EE.UU. Este (Norte de Virginia)

Agregar VPC

### ID de VPC [Información](#)

Elegir la VPC

vpc-0143c27d846a5588f

Eliminar VPC

Añadimos el registro A para nuestro servidor web, siendo nombre-apellido.despliegue.daw

Route 53 > Zonas hospedadas > despliegue.daw

Privada despliegue.daw Información Eliminar zona Probar el registro Configurar el registro de consultas

► Detalles de la zona alojada Editar zona alojada

Registros (2) Etiquetas de zona hospedada (0)

**Registros (2)** Información Eliminar registro Importar archivo de zona Crear registro

El modo Automatic es el comportamiento actual de búsqueda que se ha optimizado para obtener los mejores resultados del filtrado. [Para cambiar los modos, vaya a la configuración.](#)

Tipo ▼ Política de ... ▼ Alias ▼ < 1 > ⚙

<input type="checkbox"/>	Nombre del registro	Tipo	Política...	Difer...	Alias	Valor/Dirigir el tráfico a	TTL (s)
<input type="checkbox"/>	despliegue.daw	NS	Simple	-	No	ns-1536.awsdns-00.co.uk, ns-0.awsdns-00.com, ns-1024.awsdns-00.org, ns-512.awsdns-00.net.	17280
<input type="checkbox"/>	despliegue.daw	SOA	Simple	-	No	ns-1536.awsdns-00.co.uk. a...	900

## Registro de creación rápida

[Cambiar al asistente](#)

### ▼ Registro 1

Eliminar

**Nombre del registro** Información

sergio-arjona .despliegue.daw

Mantenga el espacio en blanco para crear un registro para el dominio raíz.

☒ Alias

**Valor** Información

172.31.16.76 IP DEL SERVIDOR WEB

Introduzca varios valores en líneas separadas.

**Tipo de registro** Información

A: dirige el tráfico a una dirección IPv4 y a algunos recursos de AWS



## 3.1 Comprobaciones

Desde nuestro cliente Linux:

```
[ec2-user@ip-172-31-29-225 ~]$ curl sergio-arjona.despliegue.daw
<!--
 ~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors
 ~
 ~ SPDX-License-Identifier: MIT
-->

<!doctype html>
<html lang="en" data-beasties-container>
<head>
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most modern and sophisticated i
nsecure web application">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon" href="assets/public/favicon_
js.ico">
  <link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/
cookieconsent2/3.1.0/cookieconsent.min.css">
  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconse
nt.min.js"></script>
  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></sc
ript>
  <script>
    window.addEventListener("load", function(){
      window.cookieconsent.initialise({
        "palette": {
          "popup": { "background": "var(--theme-primary)", "text": "var(--theme-
text)" },
          "button": { "background": "var(--theme-accent)", "text": "var(--theme-
text)" }
        }
      });
    });
  </script>
```

Desde nuestro cliente Windows:

