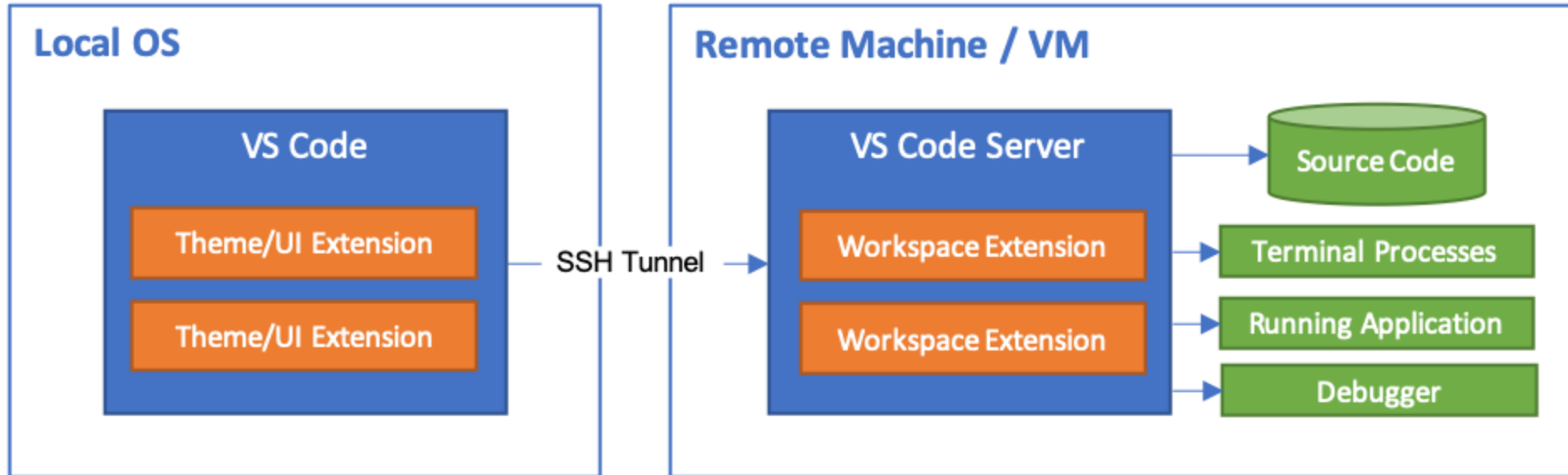


Desarrollo en remoto con vscode y SSH

- Como habéis visto desarrollar desde la terminal puede ser tedioso.
- vscode tiene una extensión llamada Remote - SSH que nos permite trabajar con nuestro vscode dentro de la máquina EC2.



- <https://code.visualstudio.com/docs/remote/ssh>

Los pasos para conectar nuestro Code a la máquina EC2 son los siguientes:

- Creamos una nueva instancia de EC2.

Instances (1/2) Info				Connect	Instance state ▼	Actions ▼	Launch Instances	▼
<input type="text" value="Filter instances"/>								< 1 >
	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼	
<input type="checkbox"/>	linux-machine	i-0b13d1204abb3a7ab	Running	t2.micro	2/2 checks passed	No alarms +	eu-west-3c	
<input checked="" type="checkbox"/>	-	i-035ea7861c8c38e6d	Running	t2.micro	2/2 checks passed	No alarms +	eu-west-3b	

Instance: i-035ea7861c8c38e6d

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
▼ Instance summary Info						
Instance ID i-035ea7861c8c38e6d		Public IPv4 address 15.188.185.255 open address		Private IPv4 addresses 172.31.16.151		
IPv6 address -		Instance state Running		Public IPv4 DNS ec2-15-188-185-255.eu-west-3.compute.amazonaws.com open address		
Private IPv4 DNS ip-172-31-16-151.eu-west-3.compute.internal		Instance type t2.micro		Elastic IP addresses -		
VPC ID vpc-7e15c216		AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more		IAM Role -		

- Es importante que tengamos habilitado el puerto 22 (SSH) desde nuestra ip.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

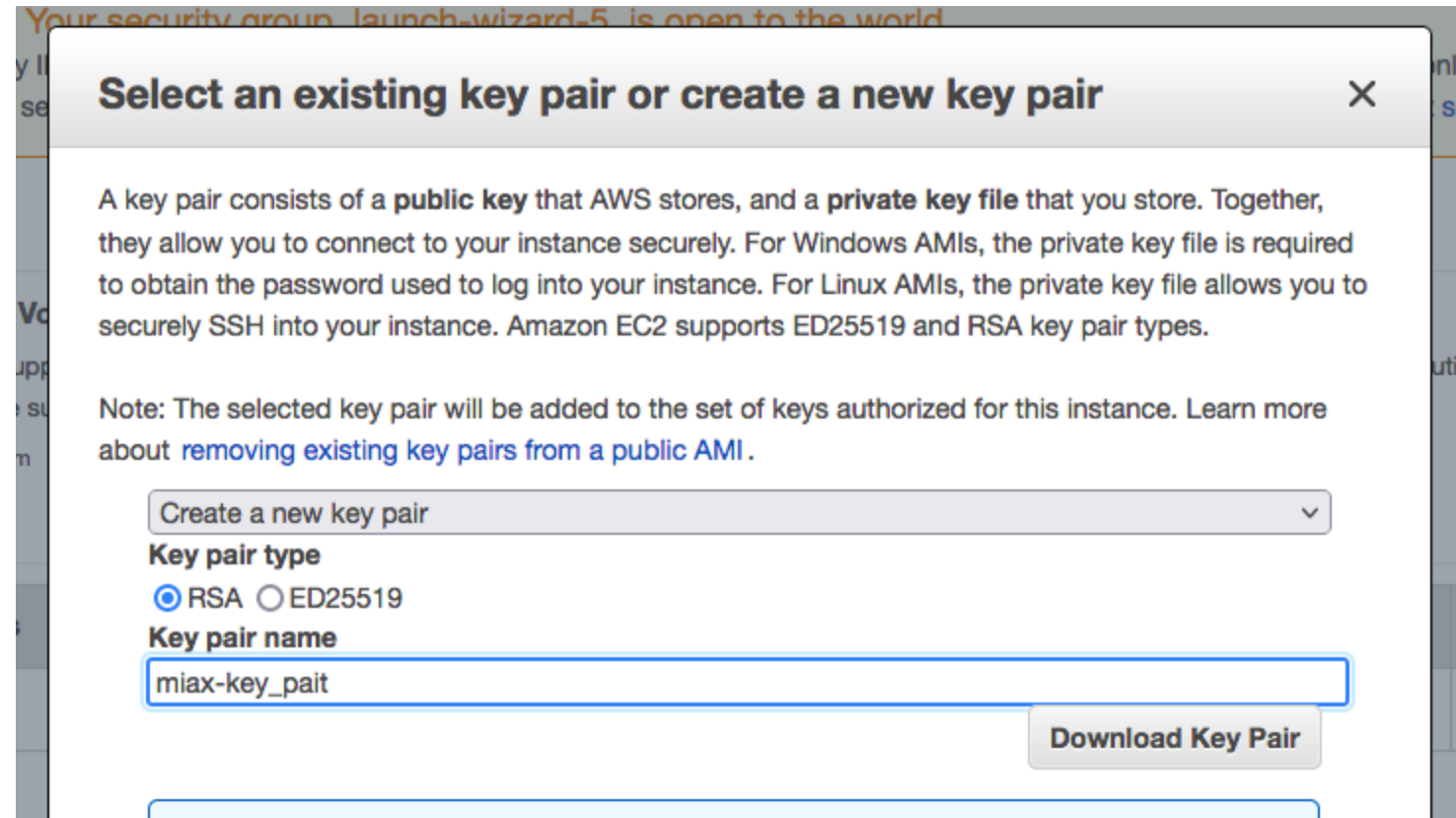
Security group name:

Description:

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>	
SSH <small>v</small>	TCP	22	Custom <small>v</small> 0.0.0.0/0	e.g. SSH for Admin Desktop	<small>×</small>

Add Rule

- En el último paso de la creación es necesario guardar el fichero con la clave privada.



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Create a new key pair ▾

Key pair type

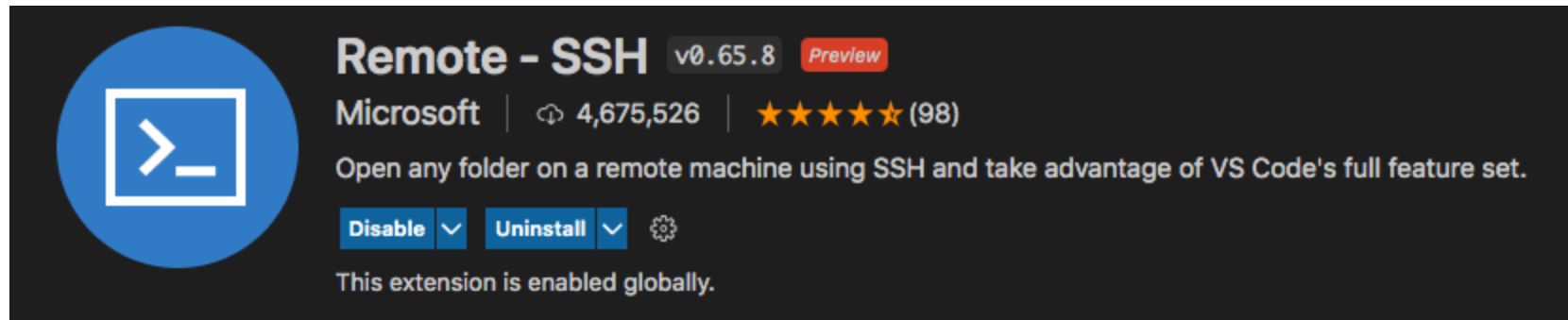
☒ RSA ☐ ED25519

Key pair name

miax-key_pait

Download Key Pair

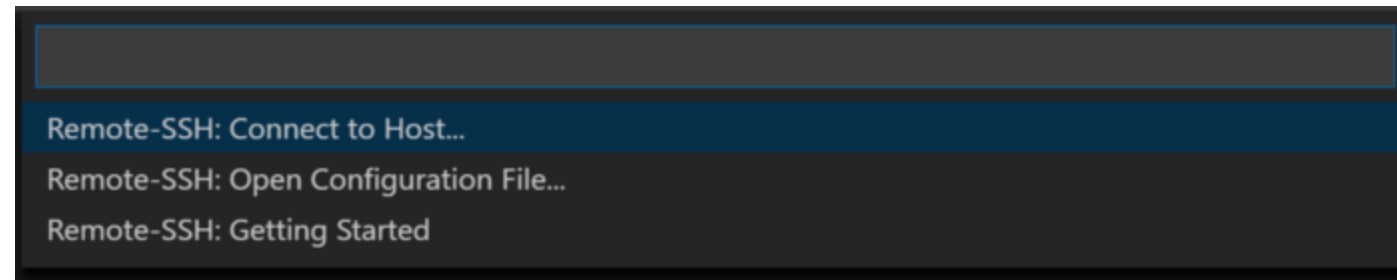
- Descargamos la extensión Remote - SSH.



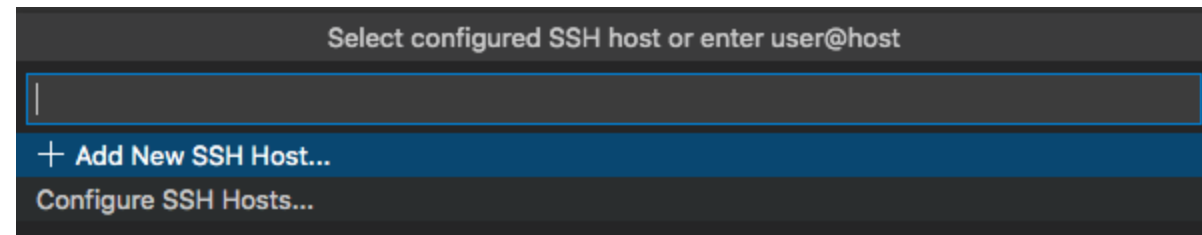
- Pulsamos el botón verde de la esquina inferior izquierda.



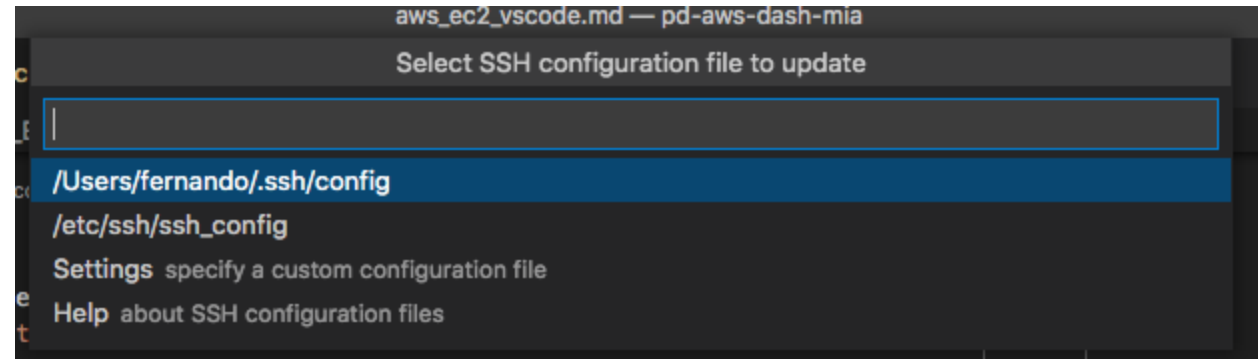
- Pulsamos: Remote - SSH: Connect to Host



- Pulsamos Configure SSH



- Pulsa el primero de los ficheros perteneciente a tu usuario.



- Se abrirá un fichero

Introduce lo siguiente:

```
Host aws-ec2
  HostName ec2-15-188-185-255.eu-west-3.compute.amazonaws.com
  User ec2-user
  IdentityFile /Users/fernando/git/pd-aws-dash-mia/auth/miax-key_pait.pem
```

Donde:

- Host (aws-ec2) es el nombre que queremos darle a la máquina, puede ser cualquiera.
- HostName es el host o IP del servidor.
- User es el nombre de usuario de la máquina EC2.
- IdentityFile es el path a la clave privada.

- Para obtener el HostName y User de tu instancia, entrar en la consola de EC2, seleccionar la instancia y pulsar conectar.

- Verás un diálogo como:

Connect to instance [Info](#)

Connect to your instance i-035ea7861c8c38e6d using any of these options


EC2 Instance Connect



Session Manager

SSH client


EC2 Serial Console


Instance ID

 [i-035ea7861c8c38e6d](#)

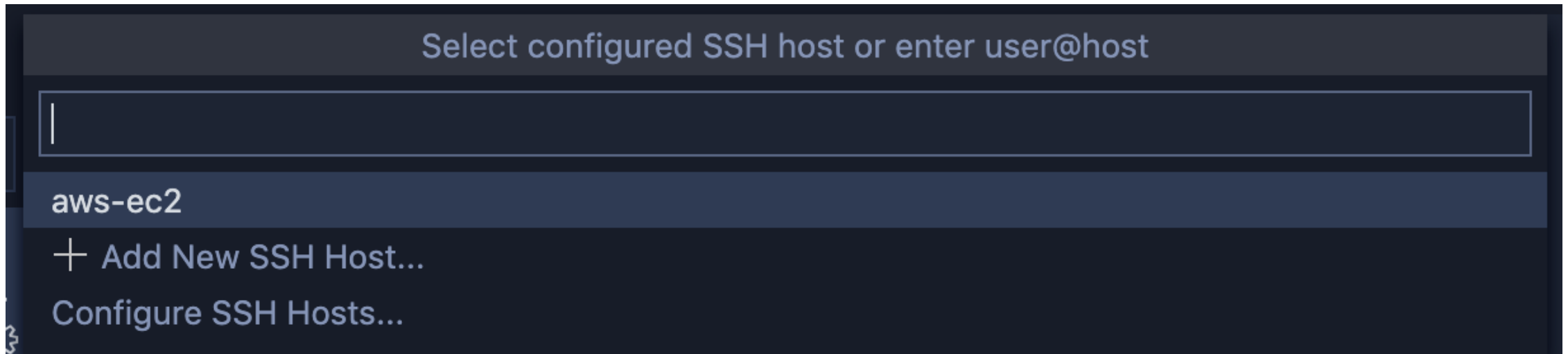
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is miax-key_pait.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 miax-key_pait.pem`
4. Connect to your instance using its Public DNS:
 `ec2-15-188-185-255.eu-west-3.compute.amazonaws.com`

Example:

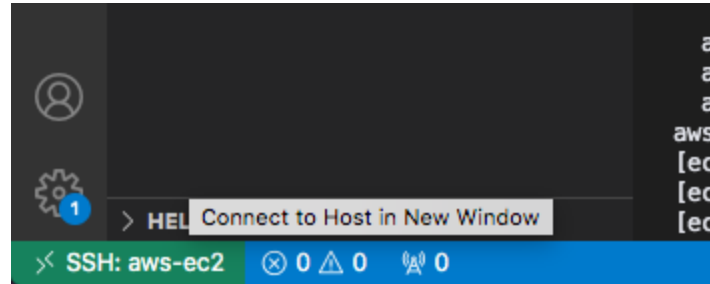
 `ssh -i "miax-key_pait.pem" ec2-user@ec2-15-188-185-255.eu-west-3.compute.amazonaws.com`

 **Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

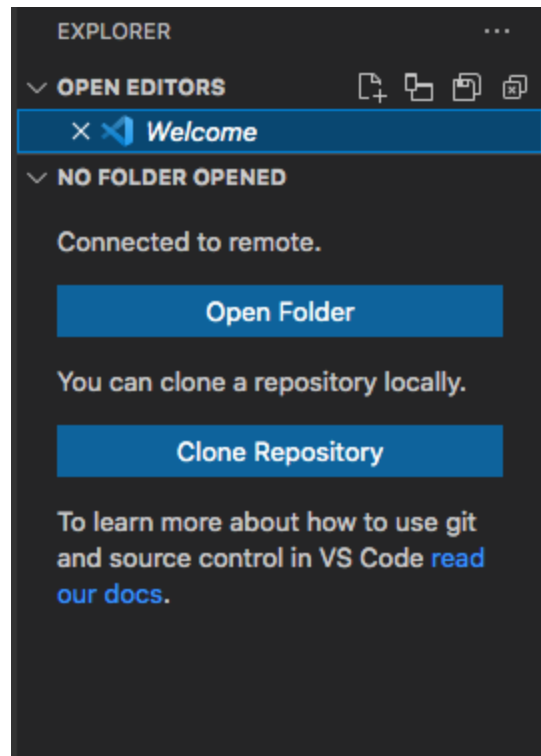
Una vez configurado, puedes pulsar otra vez el boton verde, elegir Connect to host, y tenderá que aparecer la instancia EC2.



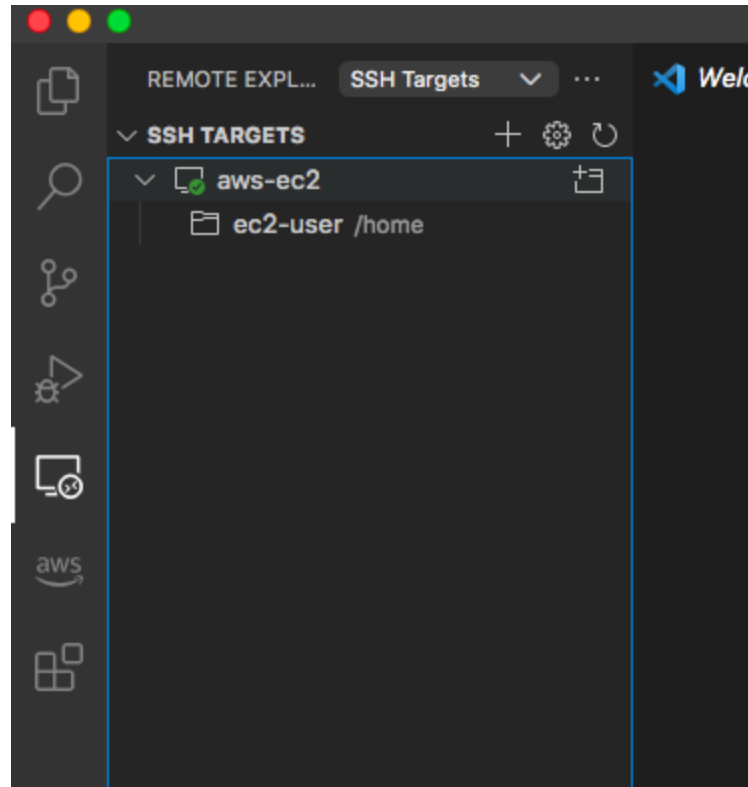
Se abrirá una nueva ventana, donde estarás conectado en tu máquina EC2:



Una vez conectado puedes abrir una carpeta en concreto de la máquina EC2:



Puedes ver todas tus máquinas en el menú de Remote Explorer:



- Si va a usar un cliente SSH en un equipo macOS o Linux para conectarse a su instancia de Linux, utilice el comando que se indica a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 my-key-pair.pem
```

Más info en:

<https://stackabuse.com/how-to-fix-warning-unprotected-private-key-file-on-mac-and-linux/>