

Guía de instalación de tpot

Se usará AWS Academy, en el que se debe crear una instancia EC2 de Ubuntu 24.04.

aws [Alt+S]

EC2 > Instancias > Launch an instance

Nombre y etiquetas Información

Nombre

tpot [Agregar etiquetas adicionales](#)

▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon) Información

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

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

Recientes 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)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Apto para la capa gratuita

ami-036841078a4b68e14 (64 bits (x86)) y ami-036841078a4b68e14 (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

La instancia debe ser del tipo t2.large

EC2 > Instancias > Launch an instance

Canonical, Ubuntu, 24.04, amd64 noble image

Arquitectura **ID de AMI** **Nombre de usuario** ⓘ

64 bits (x86) ami-036841078a4b68e14 ubuntu Proveedor verificado

▼ Tipo de instancia Información | Obtener asesoramiento

Tipo de instancia

t2.large

Familia: t2 2 vCPU 8 GiB Memoria Generación actual: true
Bajo demanda Linux base precios: 0.0928 USD por hora
Bajo demanda Ubuntu Pro base precios: 0.0963 USD por hora
Bajo demanda Windows base precios: 0.1208 USD por hora
Bajo demanda SUSE base precios: 0.1928 USD por hora
Bajo demanda RHEL base precios: 0.1216 USD por hora

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


Se aplican costos adicionales a las AMI con software preinstalado

Se crea un par de claves

▼ **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

 [Crear un nuevo par de claves](#)

Crear par de claves

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

El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.

Tipo de par de claves

☒ **RSA**
Par de claves pública y privada cifradas mediante RSA

☐ **ED25519**
Par de claves privadas y públicas cifradas ED25519

Formato de archivo de clave privada

☒ **.pem**
Para usar con OpenSSH

☐ **.ppk**
Para usar con PuTTY

⚠ Cuando 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](#)

Crear par de claves

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

El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.

Tipo de par de claves

☒ **RSA**
Par de claves pública y privada cifradas mediante RSA

☐ **ED25519**
Par de claves privadas y públicas cifradas ED25519

Formato de archivo de clave privada

☐ **.pem**
Para usar con OpenSSH

☒ **.ppk**
Para usar con PuTTY

⚠ Cuando 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](#)

Después podemos modificar el grupo de seguridad, para permitir el tráfico desde cualquier dirección.

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito

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

Crearemos un nuevo grupo de seguridad denominado **"launch-wizard-8"** con las siguientes reglas:

☒ **Permitir el tráfico de SSH desde**
Ayuda a establecer conexión con la instancia

☒ **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

0.0.0.0/0

⚠ Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

En almacenamiento dejamos unos 100 GB

▼ Configurar almacenamiento Información

Avanzado

1x 100 GB gp3 Volumen raíz (Sin cifrar)

Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS

Agregar un nuevo volumen

La AMI seleccionada contiene más volúmenes de almacén de instancias de los que permite la instancia. Solo se podrá obtener acceso desde la instancia a los primeros 0 volúmenes de almacén de instancias de la AMI

Haga clic en actualizar para ver la información de la copia de seguridad

Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia.

0 x sistemas de archivos

Editar

Imagen de software (AMI)

Canonical, Ubuntu, 24.04, amd64...más información

ami-036841078a4b68e14

Tipo de servidor virtual (tipo de instancia)

t2.large

Firewall (grupo de seguridad)

Nuevo grupo de seguridad

Almacenamiento (volúmenes)

Volúmenes: 1 (100 GiB)

Nivel gratuito: El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 750 horas de uso de direcciones IPv4 públicas al mes, 30 millones de EBS, 3 millones de EFS, 1 GB

Cancelar

Lanzar instancia

Modificar el grupo de seguridad, para permitir todo el tráfico, desde cualquier origen.

Instancias (1/8) Información

Última actualización Hace 20 minutos

Conectar

Estado de la instancia ▼

Ac

Buscar instancia por atributo o etiqueta (case-sensitive)

Todos los ... ▼

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al	Zona de dispon.
honeypot	i-037f211381a9b6e26	En ejecución	t2.xlarge	2/2 comprobaci...	Ver alarmas +	us-east-2a

i-037f211381a9b6e26 (honeypot)

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

▼ Detalles de seguridad

Rol de IAM

ID del propietario

Hora de lanzamiento

Grupos de seguridad

sg-0672c47bd923fb9d5 (launch-wizard-7)

975050253516

Sun Dec 29 2024 19:28:15

Detalles

Nombre del grupo de seguridad

ID del grupo de seguridad

Descripción

ID de la VPC

Propietario

Número de reglas de entrada

Número de reglas de salida

Reglas de entrada

Reglas de salida

Compartiendo : *novedad*

Asociaciones de VPC : *novedad*

Etiquetas

Reglas de entrada (6)

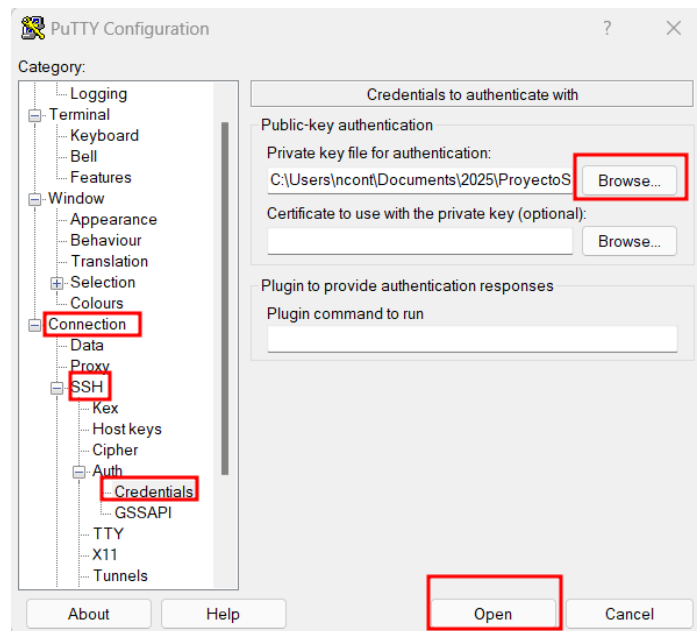
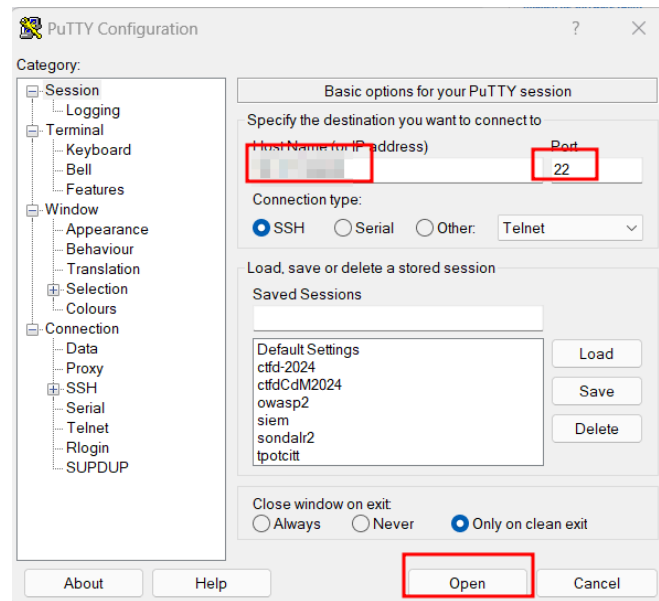
Administrar etiquetas

Editar reglas de entrada

Buscar

< 1 >

Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos
-	sgr-05e6a0323bc73639f	IPv4	SSH	TCP	22
-	sgr-09f070a9646f1ad88	IPv4	HTTPS	TCP	443



Instalar tptot en la instancia

Todo lo que viene, se debe hacer con el usuario Ubuntu, nunca con root

clonar el repositorio de tptot desde GitHub

git clone <https://github.com/telekom-security/tptotce>

```
ubuntu@ip-172-31-15-54:~$ git clone https://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 17180, done.
remote: Counting objects: 100% (170/170), done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 17180 (delta 89), reused 80 (delta 80), pack-reused 17010 (from 3)
Receiving objects: 100% (17180/17180), 323.47 MiB | 34.07 MiB/s, done.
Resolving deltas: 100% (9536/9536), done.
```

```
ubuntu@ip-172-31-4-173:~$ cd tpotce/
ubuntu@ip-172-31-4-173:~/tpotce$ ls
CHANGELOG.md  LICENSE  SECURITY.md  deploy.sh  docker  dps.ps1  genuser.sh  install.sh  uninstall.sh  version
CITATION.cff  README.md  compose     doc        docker-compose.yml  env.example  genuserwin.ps1  installer  update.sh
ubuntu@ip-172-31-4-173:~/tpotce$ ./install.sh

  T-Pot Installer

### This script will now install T-Pot and all of its dependencies.
### Install? (y/n) y
```

La instalación debe ser Hive, que incluye todo

```
### Playbook was successful.

### Choose your T-Pot type:
### (H)ive - T-Pot Standard / HIVE installation.
###         Includes also everything you need for a distributed setup with sensors.
### (S)ensor - T-Pot Sensor installation.
###           Optimized for a distributed installation, without WebUI, Elasticsearch and Kibana.
### (L)LM - T-Pot LLM installation.
###         Uses LLM based honeypots Beelzebub & Galah.
###         Requires Ollama (recommended) or ChatGPT subscription.
### M(i)ni - T-Pot Mini installation.
###         Run 30+ honeypots with just a couple of honeypot daemons.
### (M)obile - T-Pot Mobile installation.
###           Includes everything to run T-Pot Mobile (available separately).
### (T)arpit - T-Pot Tarpit installation.
###           Feed data endlessly to attackers, bots and scanners.
###           Also runs a Denial of Service Honeypot (ddospot).
### Install Type? (h/s/l/i/m/t) ### Install Type? (h/s/l/i/m/t) ### Install Type? (h/s/l/i/m/t) h
```

Indicamos usuario y contraseña de acceso WEB. No olvidar las credenciales.

```

### Install Type? (h/s/l/i/m/t) ### Install Type? (h/s/l/i/m/t) ### Install Type? (h/s/l/i/m/t) h

### Installing T-Pot Standard / HIVE.

### T-Pot User Configuration ...

### Enter your web user name: tpot
### Your username is: tpot
### Is this correct? (y/n) y

### Enter password for your web user:
### Repeat password you your web user:
### Creating base64 encoded htpasswd username and password for T-Pot config file: /home/ubuntu/tpotce/.env

### Now pulling images ...
[+] Pulling 98/39
[+] Pulling 113/39kipped - Image is already being pulled by conpot_kamstrup_382
[+] Pulling 116/39kipped - Image is already being pulled by conpot_kamstrup_382
[+] Pulling 116/39kipped - Image is already being pulled by conpot_kamstrup_382
  ✓ conpot_IEC104 Skipped - Image is already being pulled by conpot_kamstrup_382
  ✓ conpot_ipmi Skipped - Image is already being pulled by conpot_kamstrup_382
  ✓ conpot_guardian_ast Skipped - Image is already being pulled by conpot_kamstrup_382
  ✓ map_data Skipped - Image is already being pulled by map_web

```

Al finalizar solicita reiniciar y usar puertos distintos al por defecto.

Para SSH se debe usar el 64295

y para WEB https y el puerto 64297

```

### Please review for possible honeypot port conflicts.
### While SSH is taken care of, other services such as
### SMTP, HTTP, etc. might prevent T-Pot from starting.

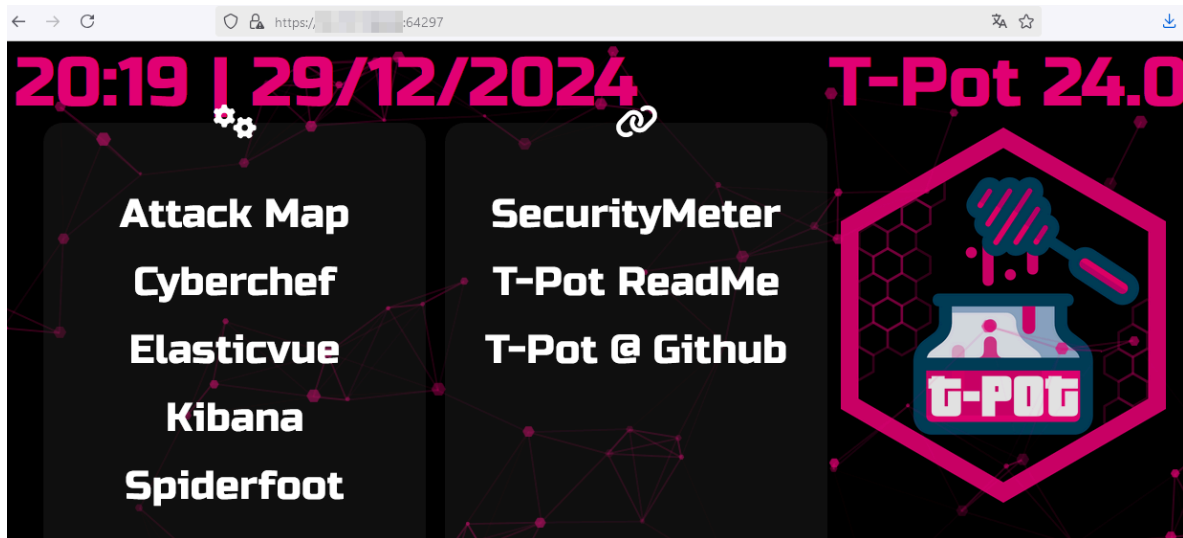
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User        Inode         PID/Program name
tcp        0      0 0.0.0.0:64295           0.0.0.0:*               LISTEN      0           52266          18079/sshd: /usr/sb
tcp6       0      0 :::64295                :::*                     LISTEN      0           52268          18079/sshd: /usr/sb
tcp6       0      0 :::22                   :::*                     LISTEN      0           5908           12365/sshd: /usr/sb
udp        0      0 172.31.4.173:68         0.0.0.0:*               0.0.0.0:*   998         23306          12393/systemd-netwo
udp        0      0 127.0.0.1:323           0.0.0.0:*               0.0.0.0:*   0           14956          3693/chronyd
udp6       0      0 :::1:323                :::*                     0           14957          3693/chronyd

### Done. Please reboot and re-connect via SSH on tcp/64295.

ubuntu@ip-172-31-4-173:~/tpotce$ sudo su
root@ip-172-31-4-173:/home/ubuntu/tpotce# reboot

```

Acceder a la plataforma, usando la IP pública y el puerto 64297



Accedemos a los dashboard a través de Kibana

