

Instalación del Takserver oficial

Nueva instalación: un servidor

1.- Comience con una instalación nueva de un sistema operativo Ubuntu 22.04 (LTS) x64

2.- Actualizamos todo

sudo apt update && apt full-upgrade -y

3.- Aumente el límite del sistema para el número de conexiones TCP simultáneas (hágalo una vez):

**echo -e "* soft nfile 32768\n* hard nfile 32768" | sudo tee - append
/etc/security/limits.conf > /dev/null**

4.- Instale el repositorio de postgres (requerido para instalar Postgresql y PostGIS actualizados) paquetes:

sudo mkdir -p /etc/apt/keyrings

**sudo curl https://www.postgresql.org/media/keys/ACCC4CF8.asc --output
/etc/apt/keyrings/postgresql.asc**

**sudo sh -c 'echo "deb [signed-by=/etc/apt/keyrings/postgresql.asc]
http://apt.postgresql.org/pub/repos/apt/ \$(lsb_release -cs)-pgdg main" >
/etc/apt/sources.list.d/postgresql.list'**

sudo apt update && apt full-upgrade -y

PASO EXTRA Descarga y actualiza java

Si al introducir el comando: **java -version** nos devuelve un mensaje de error procedemos de la siguiente manera:

apt install -y openjdk-17-jdk

add-apt-repository ppa:openjdk-r/ppa

[Intro]

sudo apt update && apt full-upgrade -y

update-alternatives --config java

Existe 1 opción para la alternativa java (que provee /usr/bin/java)

Selección	Ruta	Prioridad	Estado
* 0	/usr/lib/jvm/java-17-openjdk-amd64/bin/java	1711	modo automático
1	/usr/lib/jvm/java-17-openjdk-amd64/bin/java	1711	modo manual

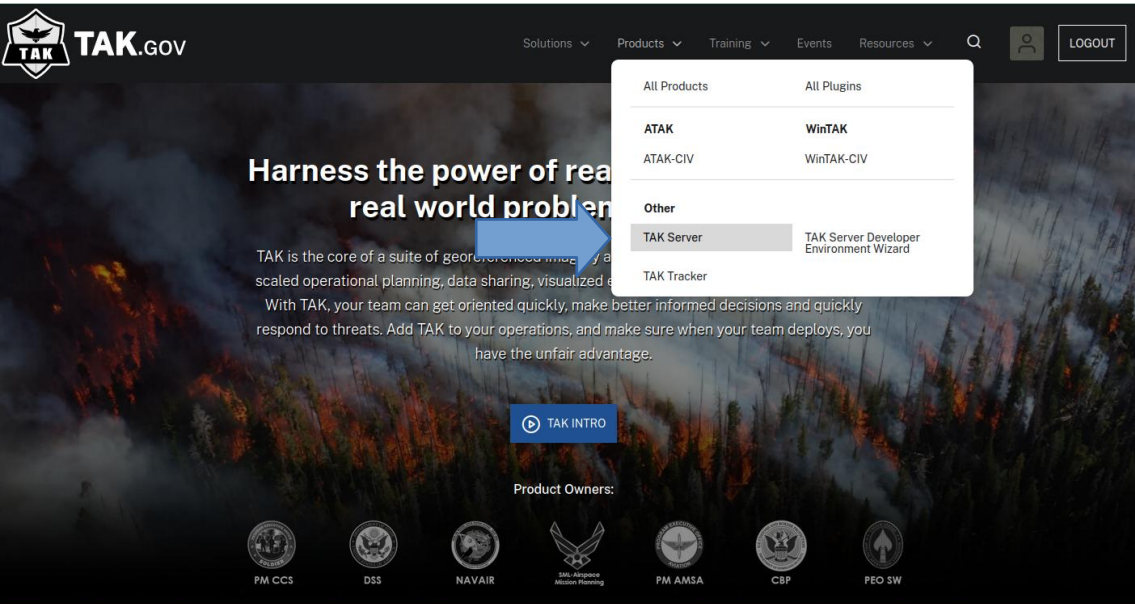
[Intro]

apt install -y maven gradle

sudo apt update && apt full-upgrade -y

5.- Descargar el instalable

El documento (takserver_5.2-RELEASE16_all.deb) ha de ser descargado de la página tak.gov y guardarlo en el Escritorio de la Máquina Virtual.



VULNERABILITY WARNING

TAK Server versions 5.0 or earlier are vulnerable to the novel CVE-2023-44487 Rapid-Reset HTTP/2 Denial of Service. This is due to TAK Server's use of Apache Tomcat version 10.1.11. This vulnerability was patched in Apache Tomcat v10.1.14 and TAK Server v5.1 is now running Apache Tomcat v10.1.16.



TAK Server Admins are advised to upgrade to TAK Server 5.1 to ensure their versions of Apache Tomcat are no longer vulnerable to this DoS attack.

For more information, please see:

<https://nvd.nist.gov/vuln/detail/CVE-2023-44487>

[Home](#) > [Products](#) > Product Detail

WATCH



TAK Server

TAK Server is a tactical information management platform that provides data access and encryption across disparate networks. TAK Server secures, brokers, and stores data in standalone and federated configurations. It is required whenever TAK clients are not operating in a peer-to-peer network or there is an operational need to encrypt and store mission data. Client plugins, such as DataSync and Execution Checklist, also require TAK Server.

VERSION

TAK Server 5.2.0

TAK Server
TAK Server 5.2.0

[Downloads](#)
[Description](#)

FEDERATION HUB
TAKSERVER-FED-HUB-5.2-RELEASE16.NOARCH.RPM [522 MB]
MD5: 71f52534a678a981babb4b74bac338d4

FEDERATION HUB
TAKSERVER-FEDHUB-DOCKER-5.2-RELEASE16.ZIP [522 MB]
MD5: 33215a8308937c6e2a37042091761d9c

FEDERATION HUB
TAKSERVER-FED-HUB_5.2-RELEASE16_ALL.DEB [522 MB]
MD5: ee0ed5a70c03f873b48c3247ae2159e0

UBUNTU AND RASPBERRY PI
TAKSERVER-DATABASE_5.2-RELEASE16_ALL.DEB [53.7 MB]
MD5: 19b3f6bf99b1c6040d1713de9da565f

UBUNTU AND RASPBERRY PI
TAKSERVER-CORE_5.2-RELEASE16_ALL.DEB [469 MB]
MD5: c0defe84924b73cd0086dd1f854eccf49

UBUNTU AND RASPBERRY PI
TAKSERVER-5.2-RELEASE16_ALL.DEB [74602 MB]
MD5: e159396b8dbbb8e4b467bea32b17e66

UBUNTU AND RASPBERRY PI
DEB_POLICY.POL [473 BYTES]
MD5: e159396b8dbbb8e4b467bea32b17e66

New in 5.2.0

7.- Crear el directorio para guardar el instalable

sudo mkdir -p /root/takserver

8.- Copiar el instalable y guardarlo en el directorio creado

cp takserver_5.2-RELEASE16_all.deb /root/takserver/

9.- Instalar TAKSERVER

9.1.- Acceder al directorio

cd /root/takserver

ls (para comprobar que el documento que queremos se ha copiado bien)

chmod 777 *

9.2.- Ejecutar la instalación

sudo apt install ./takserver_5.3-RELEASE4_all.deb -y

Ahora esperamos un poco hasta que se efectúe toda la instalación, es breve, no mas de 2-3 min

10.- Configurar la instalación del servidor TAKSERVER

10.1.- Recarga todos los servicios de nuevo

sudo systemctl daemon-reload

10.2.- Iniciar/detener todo el servicio del TAKSERVER

sudo systemctl start takserver

10.3.- Comprueba el servicio

sudo systemctl status takserver

10.4.- Configura el servidor TAKSERVER para que se inicie en el arranque ejecutando

sudo systemctl enable takserver

Generación de certificados

TAK Server incluye scripts para generar un enclave de seguridad privada, que creará un Certificado Autoridad (CA), así como certificados de servidor y cliente.

11.- Edite el archivo de configuración de generación de certificados, en esta ubicación:

sudo nano /opt/tak/certs/cert-metadata.sh

11.1.- Lo que aparece en el archivo de configuración sin editar

COUNTRY=US

STATE=\${STATE}

CITY=\${CITY}

ORGANIZATION=\${ORGANIZATION:-TAK}

ORGANIZATIONAL_UNIT=\${ORGANIZATIONAL_UNIT}

11.2.- Cómo debe de quedar el archivo de configuración una vez editado (según los parámetros que cada uno quiera)

COUNTRY=US

STATE=ESPANYA

CITY=**MELILLA**

ORGANIZATION=**BCG-COMGEMEL**

ORGANIZATIONAL_UNIT=**CIATRANS18**

CAPASS=\${CAPASS:-atakatak}

PASS=\${PASS:-\$CAPASS}

11.3.- Pasos para el guardado y salir del editor

Ctrl + O > Guardar

Enter > Confirmar

Ctrl + X > Salir del editor de texto

12.- Cambio de directorio:

cd /opt/tak/certs

chmod 777 *

13.- Cree un certificado de autoridad (CA):

./makeRootCa.sh

13.1.- Mensaje de nombre

Tras la ejecución del comando `./makeRootCa.sh` aparecerá este mensaje:
"Please give a name for your CA (no spaces). It should be unique. If you don't enter anything, or try something under 5 characters, I will make one for you" a lo que hay que contestar con el nombre que queramos ponerle al certificado.

Dale un nombre para el certificado o dale a enter para continuar

14.- Cree un certificado de servidor:

./makeCert.sh server SERVIDOR

Este comando dará como resultado un certificado de servidor llamado `/opt/tak/certs/files/takserver.jks`

A continuación cree uno o más certificados de cliente. Debe usar un certificado de cliente diferente para cada dispositivo ATAK en tu red. Este nombre de usuario será aprovisionado en el certificado como el CN (Nombre común). Cuando uses certificados en dispositivos que están conectados a una entrada que está configurada para el filtrado de grupos sin mensajes de autenticación, este nombre de usuario será utilizado por TAK Server para buscar miembros del grupo información en un repositorio de autenticación, como Active Directory (AD).

15.- Este comando creará un certificado para el usuario de nombre de usuario:

./makeCert.sh client USUARIO-PRUEBA

16.- Genere otro certificado, llamado admin para acceder a la interfaz de usuario de administración:

./makeCert.sh client WEBADMIN

Los almacenes de confianza y los certificados de CA generados se ubicarán aquí:

/opt/tak/certs/files

17.- Reinicia el servicio de TAKSERVER:

sudo systemctl restart takserver

18.- Autorice el certificado de administrador para realizar funciones administrativas mediante la interfaz de usuario:

**sudo java -jar /opt/tak/Utils/UserManager.jar certmod -A
/opt/tak/certs/files/WEBADMIN.pem**

18.1.- Confirmación

A continuación deberá de mostrarse el siguiente mensaje:

New User Added:

Username: 'WEBADMIN'

Role: ROLE_ADMIN

Fingerprint:

*40:1C:95:B5:12:AE:50:F3:F9:18:C3:7D:47:CE:8B:C2:D3:45:63:EF:F3:56:FE:B9:D6:5F:80:20:3E:BA
:B7:07*

Groups (read and write permission):

__ANON__

Este mensaje indica que exitosamente se han otorgado permisos de administración web al usuario que emplee el certificado WEBADMIN.

19.- Reinicia el servicio de TAKSERVER:

sudo systemctl restart takserver

Configuración firewall

Todos los puertos que se habiliten en el servidor tendrán que ser habilitados también en el router de internet del cual reciba la señal el servidor, para un correcto forwarding de paquetes.

20.- Instalación del Paquete del Firewall

sudo apt-get install ufw

21.- Habilitación del Firewall

sudo ufw enable

22.- Configuración de los puertos del Firewall

22.1.- Para TAKSERVER

sudo ufw allow 8089/tcp

22.2.- Para Administración por la web

sudo ufw allow 8443/tcp

23.- Comprobar estado del Firewall

sudo ufw status verbose

Tras este comando deberíamos de tener el siguiente mensaje:

Status: active

Logging: on (low)

Default: deny (incoming), allow (outgoing), deny (routed)

New profiles: skip

To	Action	From
--	-----	----
8089/tcp	ALLOW	Anywhere
8443/tcp	ALLOW	Anywhere
8089/tcp (v6)	ALLOW	Anywhere (v6)
8443/tcp (v6)	ALLOW	Anywhere (v6)

Corroborando que los puertos (8089 y 8443 para tcp están habilitados y funcionando)

24.- Reiniciamos el Firewall para que se asuman los cambios hechos

sudo ufw reload

Instalación de los certificados para la Administración por Web

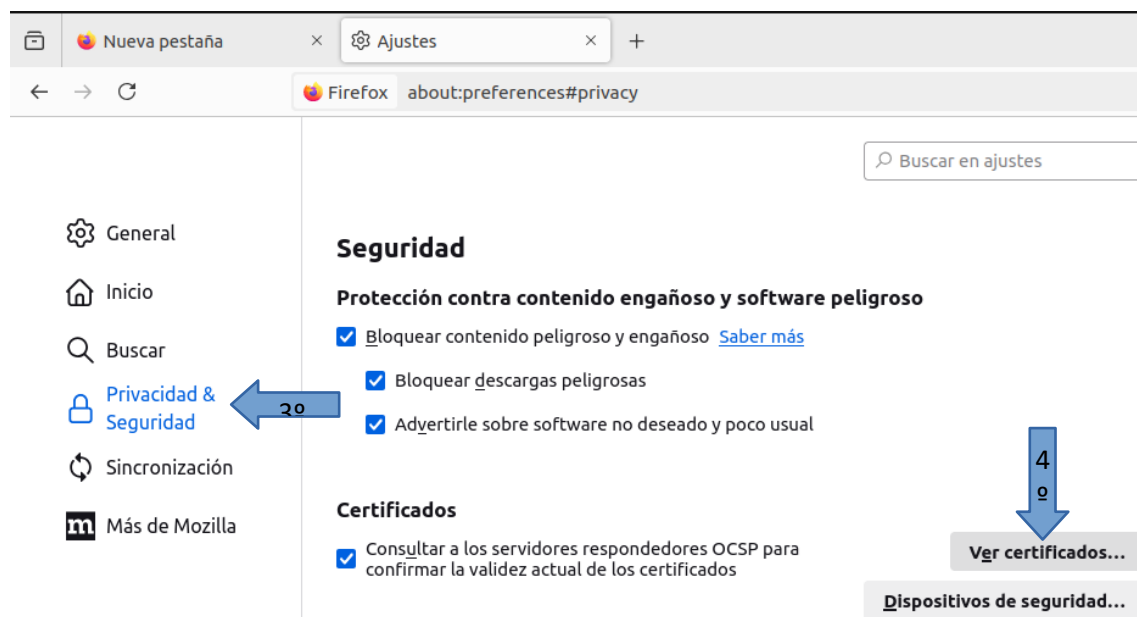
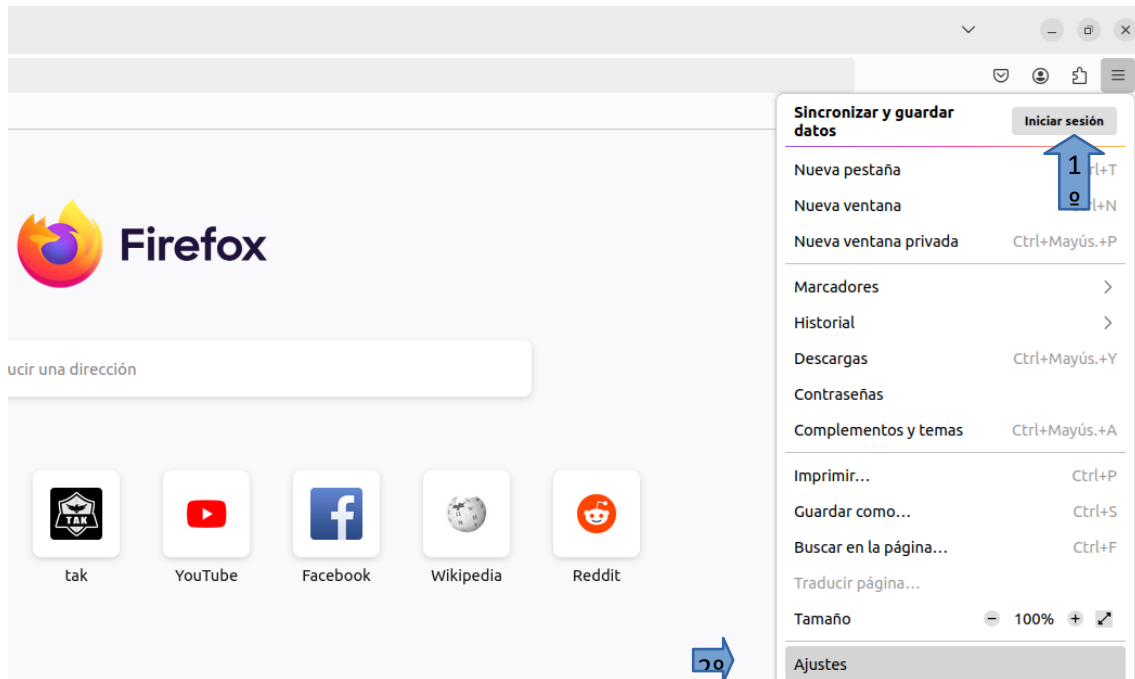
25.- Acceder al repositorio de los certificados

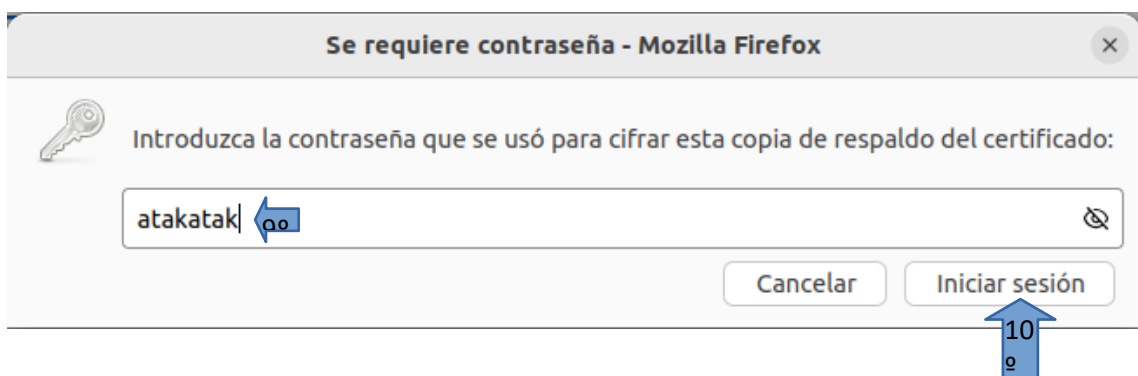
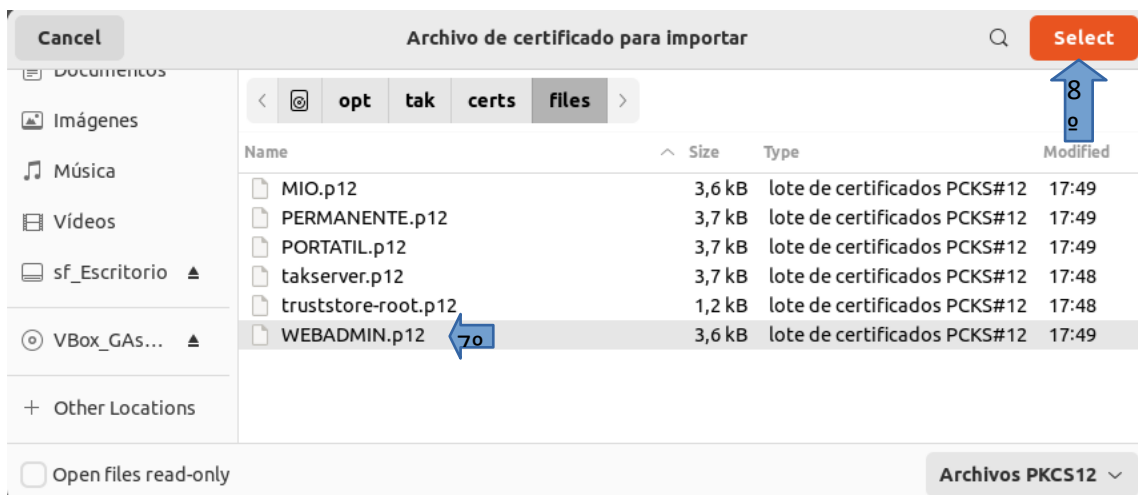
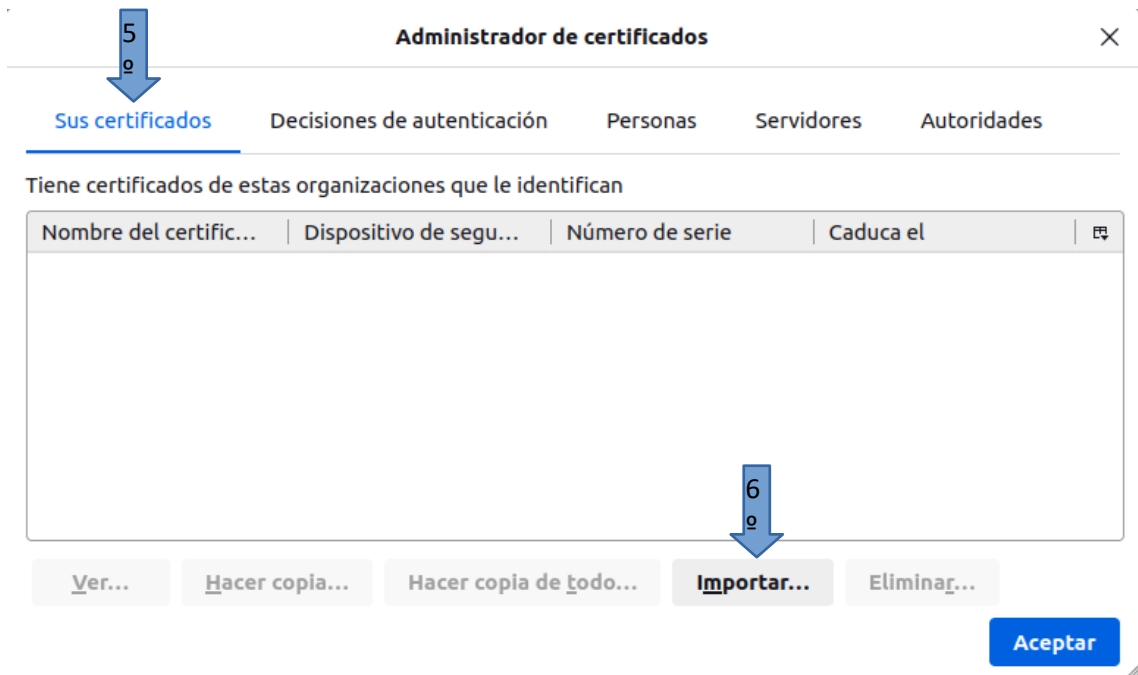
cd /opt/tak/certs/files

26.- Otorgar privilegios de lectura, escritura y edición al certificado de administración por web (WEBADMIN.p12)

sudo chmod 777 WEBADMIN.p12

27.- Introducir el certificado de administración web al buscador FIREFOX, siguiendo las siguientes fotografías:





Administrador de certificados

Sus certificados

Decisiones de autenticación

Personas

Servidores

Autoridades

Tiene certificados de estas organizaciones que le identifican

Nombre del certific...	Dispositivo de segu...	Número de serie	Caduca el	
▼ BCG-COMGEMEL				
WEBADMIN	Disp. software de segu...	0F:12:43:CF:45:07:42:6...	6 de agosto de 2026	

Ver...

Hacer copia...

Hacer copia de todo...

Importar...

Eliminar...

11

Aceptar

Administrador de certificados

Sus certificados

Decisiones de autenticación

Personas

Servidores

Autoridades

Tiene certificados guardados que identifican estas autoridades de certificación

Nombre del certificado	Dispositivo de seguridad	
Baltimore CyberTrust Root	Builtin Object Token	
▼ BCG-COMGEMEL		
ADMIN	Disp. software de seguridad	
▼ BEIJING CERTIFICATE AUTHORITY		
BJCA Global Root CA2	Builtin Object Token	
BJCA Global Root CA1	Builtin Object Token	

Ver...

Editar confianza...

Importar...

Exportar...

Eliminar o dejar de conf...

12

14

Aceptar

Editar configuración de confianza de la CA

El certificado "ADMIN" representa a una autoridad certificadora.

Editar configuraciones de confianza:

☒

 Este certificado puede identificar sitios web.

☒

 Este certificado puede identificar a los usuarios de correo.

Cancelar

Aceptar

Una vez realizados estos pasos a través de las imágenes se procede a la administración vía Web. Por lo que antes de todo necesitamos saber la dirección Ipv4 privada de la máquina virtual del TAKSERVER

ifconfig

nos mostrará las direcciones y estados de las diferentes tarjetas de red, nosotros nos fijaremos en la siguiente:

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 192.168.1.108 netmask 255.255.255.0 broadcast 192.168.1.255
```

```
inet6 fe80::a00:27ff:feac:5a56 prefixlen 64 scopeid 0x20<link>
```

```
ether 08:00:27:ac:5a:56 txqueuelen 1000 (Ethernet)
```

```
RX packets 8679 bytes 5865366 (5.8 MB)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
```

```
TX packets 5654 bytes 843756 (843.7 KB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

La dirección IPV4 privada de la máquina virtual del TAKSERVER es 192.168.1.108

Paso Intermedio

Es **fundamental** que las reglas del Firewall que se han configurado previamente (Pasos 20 a 24) se configuren en el Router de Acceso Wi-Fi particular para tener un correcto *forwarding* de paquetes.

A continuación se mostrarán una serie de imágenes de como se configuran los puertos en el Wi-Fi particular (cada empresa tiene una disposición de los menus diferente)

configuración del firewall

192.168.1.1/index.htm

Livebox Fibra

mi red local

Wi-Fi

mis archivos

mi teléfono

información y diagnóstico

configuración avanzada

configuración de la red

configuración del firewall

configuración del Wi-Fi

acceso remoto al router

administración

servidor de impresión

configuración avanzada > configuración del firewall

Firewall

Configurar el firewall.

Puedes configurar el nivel de protección del Livebox. El nivel por defecto (medio) es el recomendado ya que garantiza que todos tus servicios funcionen y tu red esté protegida.

Elegir el nivel de seguridad

☐ bajo


El firewall no filtra nada. Ten cuidado, este nivel está reservado para usuarios avanzados para los que la seguridad no es una prioridad. Ten en cuenta también que, incluso en este modo, no se permitirá una conexión iniciada desde Internet si no se ha creado una regla NAT/PAT ad-hoc para ello.

☐ medio

El firewall descarta todas las conexiones entrantes. Se permite el tráfico saliente excepto los servicios de Netbios. Este es el modo recomendado.

☐ alto

El firewall permite la salida de los servicios estándar (www, ftp, correo, noticias...) y descarta conexiones entrantes inesperadas. Se recomienda esta configuración para tener un nivel de seguridad máximo. Atención: es incompatible con ciertos servicios.



Algunas aplicaciones (Mensajería, aplicaciones P2P, juegos, etc.) que dependen de NAT-transversal, activados automáticamente por UPnP IGD, ya no funcionarán correctamente.

☒ personalizado

Este perfil te permite personalizar tu firewall. De este modo, puedes definir algunas reglas de filtrado específicas. (Reservado para usuarios expertos).

personalizado

configuración del firewall

192.168.1.1/index.htm

Livebox Fibra

mi red local

Wi-Fi

mis archivos

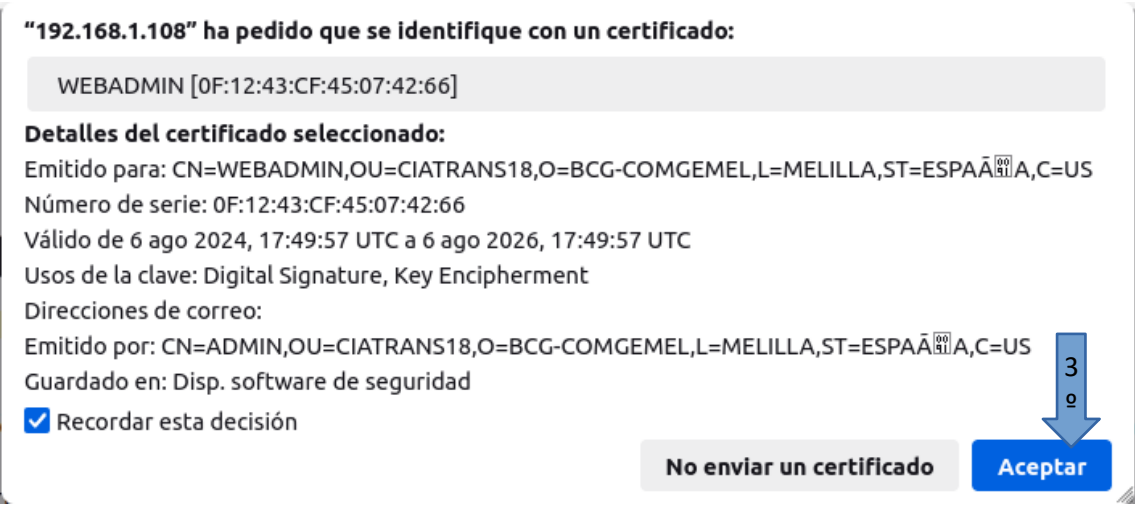
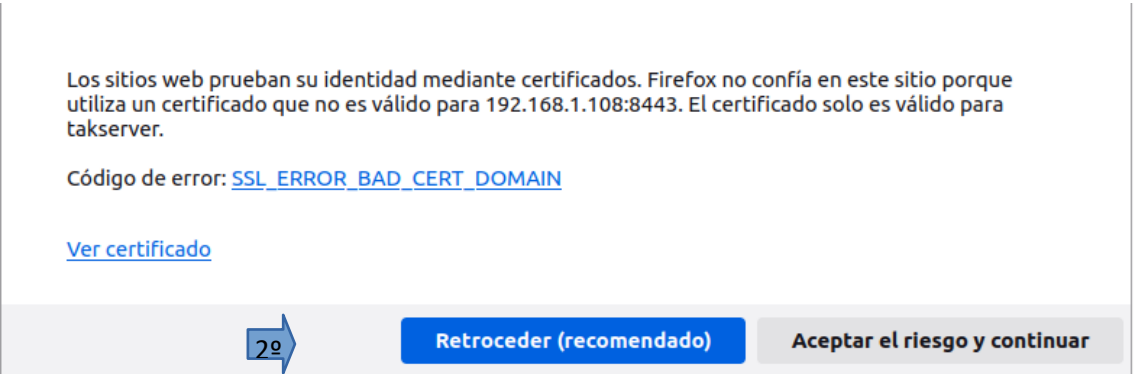
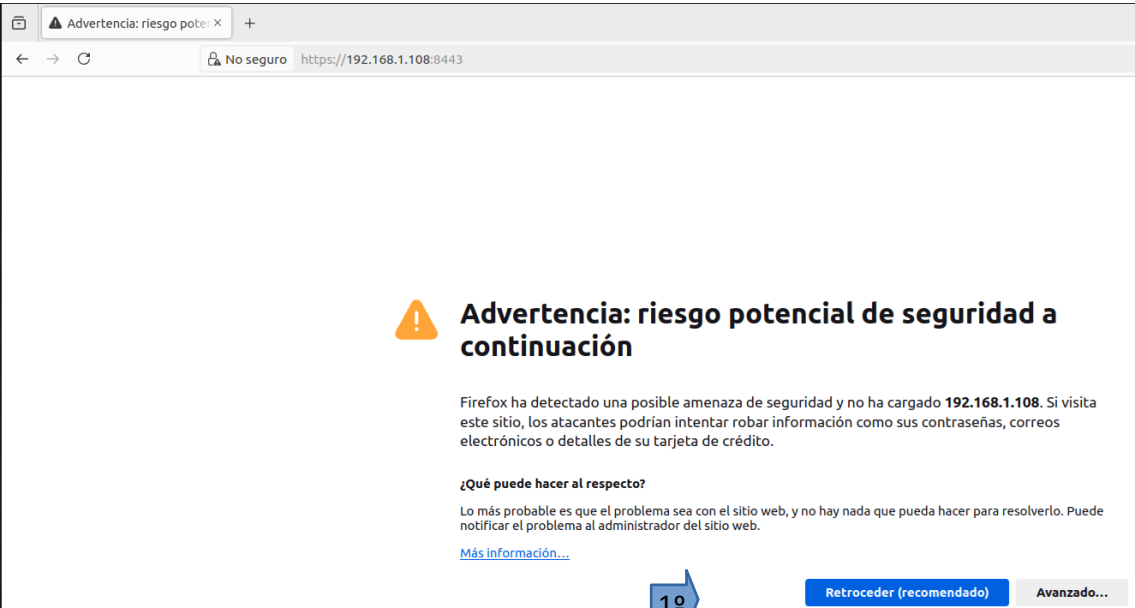
mi teléfono

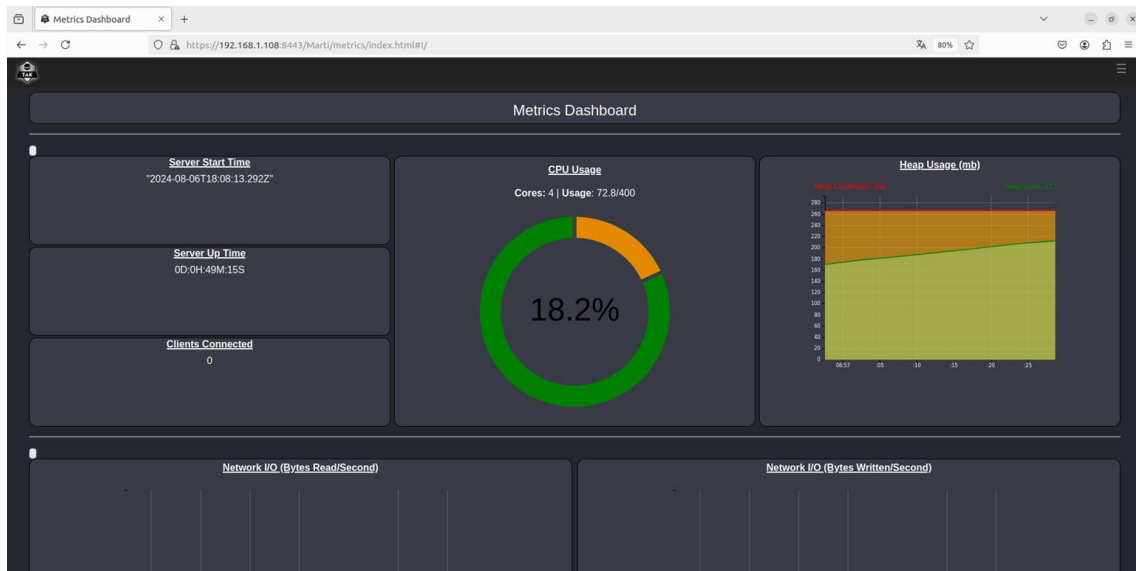
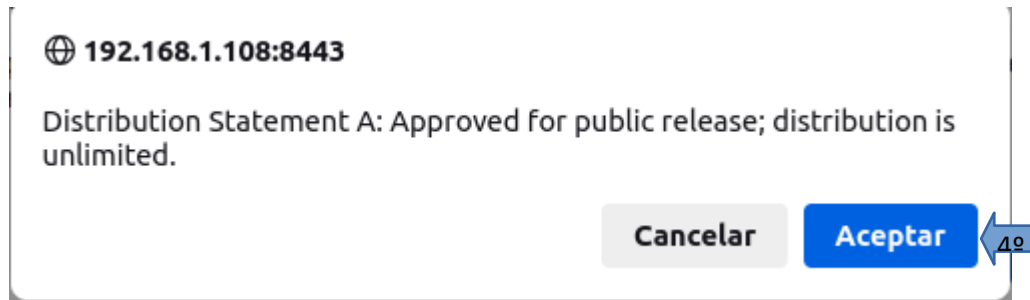
información y diagnóstico

configuración avanzada

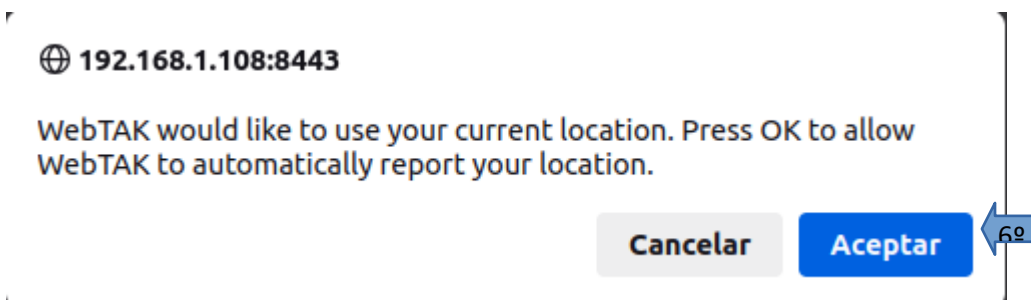
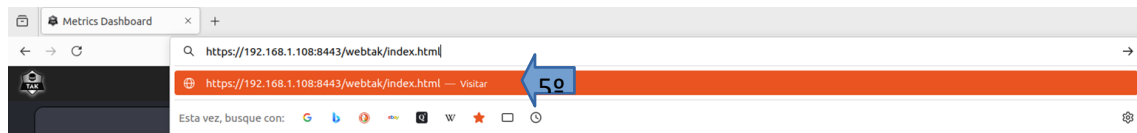
SMTPAuth	TCP						587	aceptar	<div>borrar</div>
SMTP	TCP						25	aceptar	<div>borrar</div>
FTP	ambos						20:21	aceptar	<div>borrar</div>
SSH	TCP						22	aceptar	<div>borrar</div>
NTP	UDP						123	aceptar	<div>borrar</div>
NNTP	TCP						119	aceptar	<div>borrar</div>
NNTPS	TCP						563	aceptar	<div>borrar</div>
DNS	ambos						53	aceptar	<div>borrar</div>
IMAP	TCP						143	aceptar	<div>borrar</div>
IMAPS	TCP						993	aceptar	<div>borrar</div>
STUN	UDP						3478	aceptar	<div>borrar</div>
IRC	TCP						6666:6667	aceptar	<div>borrar</div>
mDNS	UDP						5353	aceptar	<div>borrar</div>
UPnP	UDP						1900	aceptar	<div>borrar</div>
TAK v5.2	TCP	192.168.1.108	255.255.255.0	8089	192.168.1.1	255.255.255.0	8089	aceptar	<div>borrar</div>
TAK v5.2	TCP	192.168.1.108	255.255.255.0	8443	192.168.1.1	255.255.255.0	8443	aceptar	<div>borrar</div>

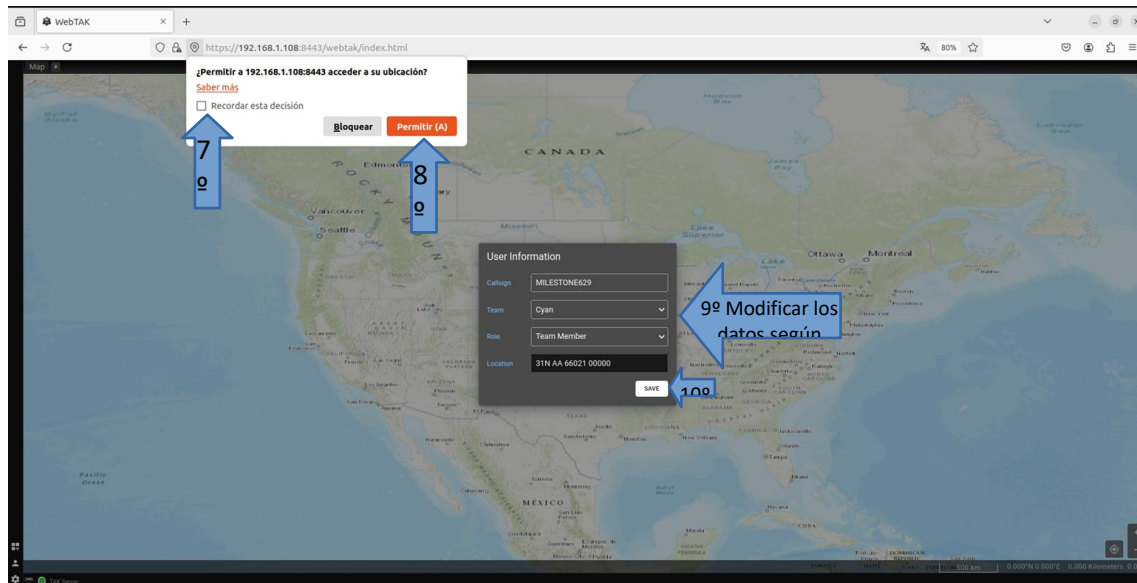
Ahora si, una vez hecho esto lo tenemos todo listo para la administración vía Web, siguiendo las instrucciones de las siguientes imágenes:





Si lo que queremos es abrir el mapa de situación haríamos lo siguiente:





El resultado quedaría tal que así:

