Que se compruebe si algún instalable con el formato: "takserver_<numero>-RELEASE<numero>-all.deb" se ha instalado en el sistema, en caso positivo que salga un mensaje que diga: "El programa takserver_<numero>-numero>-RELEASE<numero>-all.deb se ha instalado el <día, mes año>" Para sobrescribir la instalación ya existente pulsar [INTRO], para descartar pulsar [ESCAPE], si se pulsa la tecla [ESCAPE], nos llevará al menú principal y si pulsa la tecla [INTRO] se ejecutarán automáticamente los siguientes comandos uno detrás de otro pero esperando que se ejecute correctamente el anterior para lanzar el siguiente: ejecutarán automáticamente los siguientes comandos uno detrás de otro pero esperando que se ejecute corr - sudo apt update && apt full-upgrade - y - echo -e "* soft nofile 32768\n* hard nofile 32768" | sudo tee – append /etc/security/limits.conf > /dev/null ntes comandos uno detrás de otro pero esperando que se ejecute correctamente el anterior para lanzar el sigu sudo mkdir -p /etc/apt/keyrings sudo curl https://www.postgresql.org/media/keys/ACCC4CF8.asc—output/etc/apt/keyrings/postgresql.asc apt install -y openjdk-17-jdk add-apt-repository pas-openidk-r/ppa add-apt-repository ppa:ope
 Pulsa INTRO para continuar - Pulsa INTRO para continuar ...
- sudo apt update && apt full-upgrade-y
- update-alternatives -- config java
- Pulsa INTRO para continuar ...
- apt install -y maven gradle
- sudo apt update && apt full-upgrade-y c d /root/takserver - chmod 777 * - Mensaje: "Se han instalado todas las dependencias necesarias correcta - Pulsa INTRO para continuar ... - Puisa in iku para continuar ... - Introduce el nombre del instalable: <instalable> - Se ejecutará el instalable con este comando: sudo apt install ./<instalable> - sudo systemct! daemon-reload - sudo systemct! start takserver sudo systemctl enable takserve - sudo systemct lenable takserver
- Pulsa INTRO para continuar ...
- Mensaje: "Ahora tendrás que modificar 4 parámetros para definir las características de tus futuros certificados dentro del Servidor TAK, tendrás que modificar los siguientes: STATE, CITY, ORGANIZATION y ORGANIZATIONAL_UNIT"
- Pulsa INTRO para continuar ...
- Cuando se haya pulsado INTRO se ejecutará automáticamente el comando siguiente: "sudo nano /opt/tak/certs/cert-metadata.sh" Cuando el documento cert-metadata.sh se cierre se continuará mostrando un mensaje de finalización: "¡Enhorabuena! ya tienes el Servidor TAK instalado, sigue con los pasos del mo principal por orden para personalizarlo completamente." tras esto se redirigirá al menú genérico inicial Que se compruebe si en algún momento se han ejecutado los comandos: "sudo netplan apply" ó "sudo systemcti restart NetworkManager" en caso de que si se hayan ejecutado en algún momento deberña de salir un mensaje que diga: "La configuración de la tarjeta de red, ya se ha realizado" Para sobrescribir la configuración ya existente pulsar [INTRO], para descartar pulsar [ESCAPE], si se pulsa la tecla [ESCAPE], nos llevará al menú principal y si pulsa la tecla [INTRO] se ejecutarán automáticamente los siguientes comandos uno detrás de otro pero esperando que se ejecute correctamente el anterior para lanzar el siguiente: - Se ejecutarán automáticamente los siguientes comandos uno detrás de otro pero esperando que se ejecute correctamente el anterior para lanzar el siguiente:

- Mensaje: "Ahora tendrás que modificar el archivo de configuración de la tarjeta de red de tu ordenador / maquina virtual para que tenga una dirección IPv4 privada estática. Copia el siguiente contenido, pulsa la tecla [INTRO] y pégalo en el documento que se te va a abrir a continuación: version: 2 renderer: NetworkManager ethernets: etnernets:
enp033: # Reemplaza 'eth0' por tu interfaz (suele ser enp0s3)
addresses: [192.168.1.100/24] # IPv4 privada estática para tu ordenador o máquina virtual que albergará al Servidor TAK
gateway4: 192.168.1.1 # IPv4 privada de la puerta de enlace de tu Router de Internet
nameservers: addresses:

- 8.8.8.8 # DNS Primario (Google para evitar fallos)

- 8.8.4.4 # DNS Secundario (Google para evitar fallos)*

- Cuando se muestre el texto a continuación aparecerá este mensaje: Pulse INTRO para continuar... ó ESCAPE para regresar al menú principal

- En caso de apretar la tecla INTRO se ejecutarán automáticamente estos comandos:

- Buscará si existe algún documento dentro del directorio /etc/netplan, si hay algún documento comprobará su nombre, en caso de que su nombre NO sea 00-installer-config.yaml se ejecutará un comando que cambie el nombre del archivo contenido en el directorio /etc/netplan y que se sustituya por 00-installer-config.yaml, una vez que se ha sustituido el nombre se ejecutará este comando automáticamente

- "> netplan/00-installer-config.yaml"

- "sudo nano /etc/netplan/00-installer-config.yaml"

- "sudo nano /etc/netplan/00-installer-config.yaml"

- Cuando se cirre el documento .yaml se ejecutarán estos comandos automáticamente con un intervalo de 2 segundos cada uno: "sudo netplan apply" y "sudo systemcti restart NetworkManager"

- Cuando se haya ejecutado correctamente el último comando automática parecerá un mensaje que diga: "[Enhorabuenal y a tienes la tarjeta de red configurada para tu Servidor TAK, sigue con los pasos del menú principal por orden para personalizarlo completamente." tras esto se redirigirá al menú genérico inicial

Que se compruebe si en algún momento se han ejecutado los comandos: "sudo ufw allow 8089/tcp" ó "sudo ufw allow 8443/tcp" en caso de que si se hayan ejecutado en algún momento deberá de salir un mensaje que diga: "La configuración del firewall "genérico inicial"

Que se compruebe si en algún momento se han ejecutado los comandos: "sudo ufw allow 8089/tcp" ó "sudo ufw allow 8089/tcp" é "sudo ufw allow 8089/tcp" é "sudo ufwa allow 8089/tcp" en caso de que si se hayan ejecutado en algún momento deberá de salir un mensaje que diga: "La configuración del firewall "genérico inicial" tras esto se mensaje que diga: "La configuración del firewall "genér Que se compruebe si en algún momento se han ejecutado los comandos: "sudo ufwa allow 8089/tcp" ó "sudo ufwa allow 8443/tcp" en caso de que si se hayan ejecutado en algún momento deberá de salir un mensaje que diga: "La configuración del firew ha realizado" Para sobrescribir la configuración ya existente pulsar [INTRO], para descartar pulsar [ESCAPE], si se pulsa la tecla [ESCAPE], nos llevará al menú principal y si pulsa la tecla [INTRO] se ejecutarán automáticamente los siguientes comandos un de otro pero esperando que se ejecute correctamente el anterior para lanzar el siguiente: el Firewall Comprobación ₩ Mensaje: "Ahora tendras (- sudo apt-get install ufw - sudo ufw enable - sudo ufw allow 8089/tcp - sudo ufw allow 8443/tcp - sudo ufw status verbose sudo ufw reload Cuando se haya ejecuta do deberá aparecer un mensaje: "¡Enhorabuena! ya tienes los puertos del Firewall configurados (por defecto) para tu Servidor TAK, sigue con los pasos del menú principal por orden para per lo completamente." tras esto se redirigirá al menú genérico inicial Cuando se eliia esta se accederá automáticamente al directorio /opt/tak/certs/files y se mostrarán todos los documentos, sin repetir y sin las extensiones siguientes: ".csr", ".iks", ".kev", ".p12", ".pem", "-trusted.pem" Cuando se elija esta opción aparecerá un mensaje que diga: "Se va a crear el certificado de Autoridad Certificadora" Pulse INTRO para continuar ó ESCAPE para salir del proceso. Si se pulsa INTRO se accederá al directorio /opt/tak/certs y se ejecutará el archivo makeRootCa.sh con esta combinación./ Cuando se elija esta opción aparecerá un mensaje que diga: "Defina que tipo de certificado quiere crear (client o server)" Cuando se haya introducido el <ti>de certificado> saldrá un mensaje que diga: "Introduzca el nombre del certificado que desee crear (si es más de uno sepárelos por una coma)" cuando se haya introducido el <nombre del certificado> se accederá automáticamente a este directorio: /opt/tak/certs/ y se ejecutará el documento makeCert.sh <tipo de certificado> con esta combinación./ Nos llevará al menú genérico inicial Cuando se elija esta opción aparecerá un mensaje que diga: "Indique el nombre del certificado que desea eliminar" Cuando se haya introducido el <nombre del certificado> se comprobará en la carpeta /opt/tak/cert/files si ese certificado existe comprobando la extensión. pem Cuando se haya comprobado saldrá un mensaje que diga: "El certificado indicado existe, se borrará" En este momento se accederá al directorio:/opt/tak/certs/files y se ejecutará el comando rm -r <nombre del certificado> en las extensiones siguientes: ".csr", ".jks", ".key", ".p12", ".pem", "-trusted.pem" [7.1] Agrega Cuando se seleccione esta opción se nos pedirá ingresar un certificado que deberá validarse su existencia en el /opt/tak/certs/files con <nombre del certif En caso de que el certificado exista aparecerá otro submenú siguiente comando: /opt/tak/utils/UserManager.jar Comprobación [7.1.1] Grupo de Adr [7.1.1] Grupo de Admir one esta opción nos aparecerán un seleccionable [Entrada, Salida o Amb Cuando se seleccione esta opción nos aparecerán un seleccionable [Entrada, Salida o Ambas], para que el si se escribe:

- Entrada, se ejecute este comando: java jar /opt/tak/utils/UserManager.jar certmod - ig<a href="ig/opt/tak/certs/files/<nombre del certificado>-pem">nombre del grupo indicado>/opt/tak/certs/files/<nombre del certificado>-pem og/opt/tak/certs/files/<nombre del certificado>-pem">nombre del certificado>-pem

- Ambos, se ejecute este comando: java -jar /opt/tak/tils/JserManager.jar certmod - g/opt/tak/certs/files/<nombre del certificado>-pem">nombre del grupo indicado>/opt/tak/certs/files/<nombre del certificado>-pem">nombre del grupo indicado>-pem /opt/tak/certs/files/<nombre del certificado>-pem Nos llevará al menú anterior uando se seleccione esta opción se nos pedirá ingresar un nombre de certificado que deberá validarse su existencia en el directorio /opt/tak/certs/files con <nombre del certificado>.pem En caso de que el certificado exista nos indicará que introduzcamos el grupo para desasignar al certificado, en caso de que el usuario indicado esté en el grupo indicado esto se comprobará con el comando: java -jar /opt/tak/utils/UserManager.jar certmod -g<nombre del rupo indicado>/opt/tak/certs/files/cnombre del certificado>.pem y si la respuesta es correcta se ejicarán estos comandos automáticamente:
- sudo java -jar /opt/tak/utils/UserManager.jar certmod -g (grupo indicado> /opt/tak/certs/files/<nombre del certificado>.pem
- sudo java -jar /opt/tak/utils/UserManager.jar certmod -g <grupo indicado>/opt/tak/certs/files/<nombre del certificado>.pem Cuando se seleccione esta opción aparecerá el siguiente cuadro de texto:
"Administración por WebTAK > https://<dirección IPv4>:8443/webtak/index.html
Administración por Metrics Dashboards > https://<dirección IPv>:8443/Matri/metrics/index.html#!/" [9] Salir Mensaje de despedida y cierre del script