

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Funcionalidad del nodo WebRTC en **VIVAit Call**

Fecha : xx de xxxxxx de 2022	Número de revisión: Versión 1
Objeto del documento : Descripción del nodo WebRTC en VIVAit Call	
Actores (empresas):	
<ul style="list-style-type: none"> • MDTEL 	

1. INTRODUCCIÓN.....	1
2. ARQUITECTURA.....	2
3. INSTALACIÓN Y CONFIGURACIÓN.....	4
3.1 INSTALACIÓN DEL REPOSITORIO.....	
3.1.1 Opción 1.- Agregar repositorio web	4
3.1.2 Opción 2.- Agregar repositorio mediante un pendrive.....	5
3.2.3 Configuración de Jitsi.....	5
3.2	10
3.3	10
4. COMPROBACIONES.....	11
5. DIAGNÓSTICOS.....	11

1. Introducción

Este documento tiene como objetivo definir el nodo webRTC de **VIVAit Call** , sus funcionalidades principales , arquitectura , piezas fundamentales , instalación , configuración y diagnósticos.

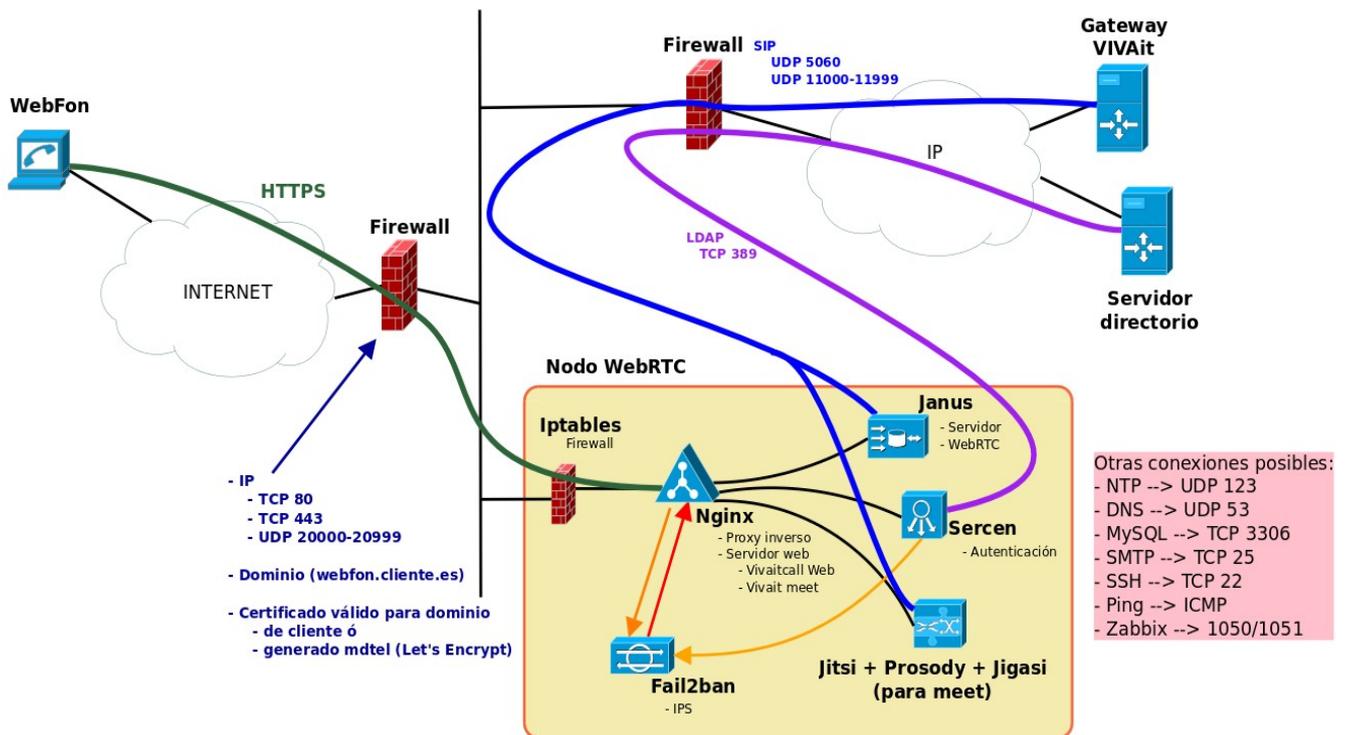
El nodo Webrtc es el nodo donde se dan de alta los servicios necesarios para la funcionalidad multidispositivo, como son: serCen, janus, nginx, FonBo, seguridad y certificados, entre otros.

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



2.Arquitectura de WebRTC

La arquitectura de WebRTC en **VIVAit** Call es la siguiente:



Componentes Principales:

- **NGINX:** Es un servidor web de código abierto que, desde su éxito inicial como servidor web, ahora también es usado como proxy inverso, cache de HTTP, y balanceador de carga.
- **SERCEN:** Sirve para identificar a los usuarios y garantizar que los mismos sean quienes dicen ser.

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



- **JANUS**: Janus es un servidor WebRTC concebido para ser de propósito general. Como tal, no proporciona ninguna funcionalidad más que implementar los medios para configurar una comunicación de medios WebRTC con un navegador, intercambiar mensajes JSON con él y transmitir RTP / RTCP y mensajes entre navegadores y la lógica de la aplicación del lado del servidor a los que están apegados.
- **IPTABLES**: Es un programa que se encarga de filtrar los paquetes de red , es decir , es la parte que se encarga de determinar qué paquetes de datos queremos que lleguen hasta el servidor y cuáles no.
- **FAIL2BAN**: Es una aplicación de Linux que permite evitar accesos no autorizados al servidor. Funciona bloqueando o baneando las IP que realicen varios intentos de acceso incorrectos al servidor.
- **CLIENTE**: El cliente debe de proporcionar una ip pública , un dns para esa ip y un certificado válido.

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



3.Instalación y configuración del NodoRTC en VIVAit_Meet 1.0

3.1 Instalación del repositorio

Existen dos modos de agregar el repositorio que nos permite instalar los diferentes paquetes existentes para la instalación de Vivait-Meet: por web o mediante un pendrive. La instalación por web solo es válida si la máquina se monta en la red de MDtel ya que el repositorio es interno a dicha red.

3.1.1 Opción 1.- agregar repositorio web



Procedimiento solo válido en instalaciones en red de Mdtel

- Después de reiniciar y logarnos con la cuenta de usuario creada pasos atrás, añadimos el repositorio donde están los paquetes de instalación de MDtel.

```
# sudo sh -c "echo 'deb [trusted=yes] http://172.25.128.48/ repositorio_VIVAit_Meet_1.0/'  
>> /etc/apt/sources.list.d/repoMDtel.list"
```

Comprobar con el comando `cat` tras realizar el comando de añadir el repositorio al fichero `repoMDtel.list`

- Deshabilitar el proxy para el acceso a la máquina donde está cargado el repositorio, que está en la red interna.

```
# export no_proxy="172.25.128.48"
```

- Y actualizamos la lista de repositorios.

```
Sudo apt update
```

```
Sudo apt upgrade
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



3.1.2 Opción 2.- agregar repositorio mediante un pendrive

- Introducimos el pendrive y procedemos a montarlo en el sistema operativo.
- Mediante el comando anterior vemos las diferentes particiones del disco duro y en que rutas están. También nos permite localizar donde está nuestro pendrive, en nuestro caso está en `/dev/sdb1`

```
# sudo fdisk -l
```

```
Dispositivo Inicio Comienzo Fin Bloques Id Sistema
/dev/sdb1 * 62 15620279 7810109 c W95 FAT32 (LBA)
```

- Lo montamos en el directorio `/mnt`

```
# sudo mount /dev/sdb1 /mnt
```

- Añadimos el repositorio

```
# sudo sh -c "echo 'deb file:/mnt repositorio_VIVAit_Meet_1.0' >>
/etc/apt/sources.list.d/repoMDtel.list"
```

- **CASO DE EXISTENCIA DE PROXY:** Si tenemos un proxy debemos añadirlo para acceder a internet.

```
# export http_proxy="http://IP_proxy:puerto"
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



- Y actualizamos la lista de repositorios.

```
# sudo apt-get update
# sudo apt-get upgrade
# sudo apt-get dist-upgrade
```

- Desmontamos el pendrive

```
# sudo umount /mnt
```

3.1.3 Configuración de Jitsi

- Introducimos el comando: `apt install jitsi-meet`

```
apt install jitsi-meet
```

Luego la instalación lanzará un asistente que preguntará el hostname que usaremos.

El nombre de host del sistema tiene que coincidir con el nombre del dominio que se quiere usar en su instancia de Jitsi Meet, este resolverá ese nombre de host con la IP del host local. Jitsi Meet utiliza estos dos ajustes al instalar y generar sus archivos de configuración.

Tienen que ser parecido a una URL que se introducirá posteriormente para acceder al webfon.

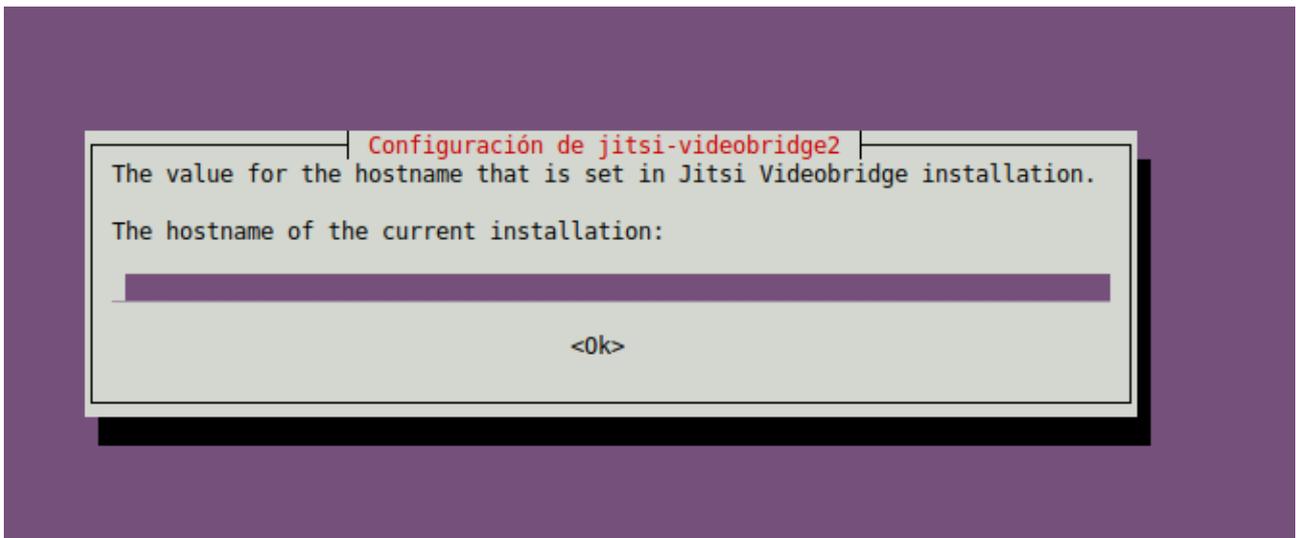
Ejemplos de dos nombres de dominio usados en MDtel:

- El nombre de dominio de MDtel es `www.mdtel.es`
- El nombre de dominio del webfon de homologación es `labmeet.mdnova.local`

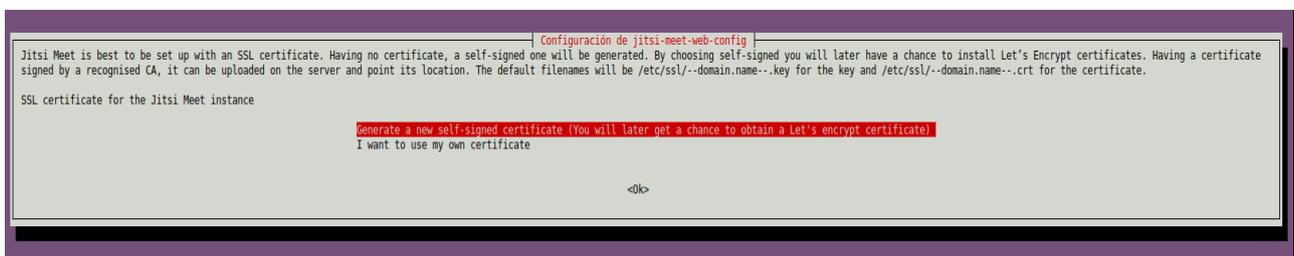
Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



- Introducimos el nombre de dominio de la máquina



- Generamos certificados nuevos (siempre elegir generar certificados nuevos)



Si tenemos certificados del cliente sustituimos los que ha creado en `/etc/jitsi/meet` el `.cert` y el `.key` por los del cliente

- Instalar jigasi con el comando : `apt install jigasi`

```
apt install jigasi
```

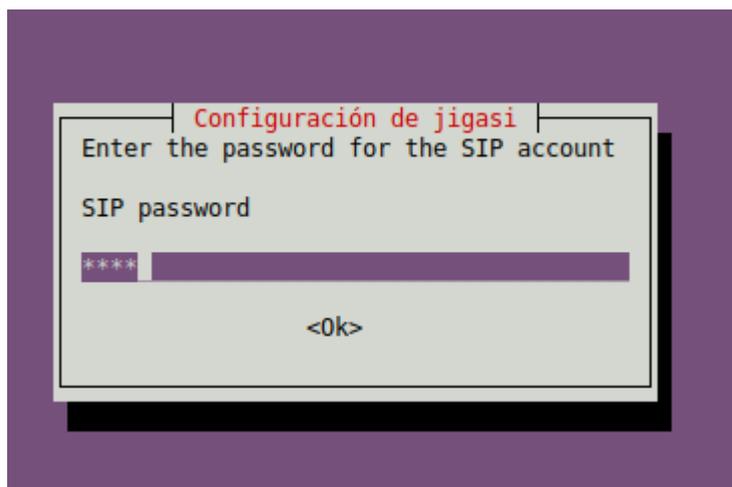
Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



- Meter el peer donde se registrará (EXTENSION@IP_ASTERISK (al no usarse aún el vivait-meet en los clientes esta extensión puede ser inventada (ficticia). Pero si existiese el meet habría que poner una extensión que estuviese creada de verdad en el asterisk). El ver en el asterisk si la extensión se ha registrado solo se vera si se emplea extensión no ficticia y predefinida en el vivait-call (no implica en el caso de solo instalación de webfon).



- Meter la clave del peer



Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



- Una vez completada la instalación tendríamos que ver en el asterisk que el jigasi se ha registrado en la extensión

> Saved useragent "Jigasi1.1.166-g929a439Linux" for peer 4200
 [Apr 5 11:29:09] NOTICE[2133]: chan_sip.c:24540 handle_response_peerpoke: Peer '4200' is now Reachable. (149ms / 2000ms)

3.1.3 Opción 3.- subir los repositorios a la máquina y configurar los diferentes elementos.

Instalación de paquetes

Paso	Instalar paquete nginx-full
Comando	<code>apt install nginx-full ngrep screen unzip net-tools dnstools iptraf-ng</code>
Resultado esperado	<pre>root@PC: ~# ssh root@192.168.1.100 -i /home/sat/repositorio_VIVAit_Meet_1.0# apt install nginx-full ngrep screen unzip net-tools dnstools iptraf-ng Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho unzip ya está en su versión más reciente (6.0-2Subuntul), fijado unzip como instalado manualmente. ngrep ya está en su versión más reciente (1.47+ds1-2).</pre>

Paso	Instalar paquete libmicrohttpd-dev libjansson-dev
Comando	<code>apt install libmicrohttpd-dev libjansson-dev</code>
Resultado esperado	<pre>root@PC: ~# ssh root@192.168.1.100 -i /home/sat/repositorio_VIVAit_Meet_1.0# apt install libmicrohttpd-dev libjansson-dev Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho libjansson-dev ya está en su versión más reciente (2.12-1build1), fijado libjansson-dev como instalado manualmente. libmicrohttpd-dev ya está en su versión más reciente (0.9.66-1), fijado libmicrohttpd-dev como instalado manualmente. 0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 7 no actualizados.</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Instalar paquete lua-lpty libconfig-dev
Comando	<code>apt install lua-lpty libconfig-dev</code>
Resultado esperado	<pre> root@sat:~# cd /home/sat/repositorio_VIVait_Meet_1.0# apt install lua-lpty libconfig-dev Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho libconfig-dev ya está en su versión más reciente (1.5-0.4build1). fijado libconfig-dev como instalado manualmente. Se instalarán los siguientes paquetes NUEVOS: lua-lpty 0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 7 no actualizados. Se necesita descargar 9,744 B de archivos. Se utilizarán 67,6 kB de espacio de disco adicional después de esta operación. ¿Desea continuar? [S/n] s </pre>

Paso	Instalar paquete libsofia-sip-ua-dev libglib2.0-dev libldap2-dev
Comando	<code>apt install libsofia-sip-ua-dev libglib2.0-dev libldap2-dev</code>
Resultado esperado	<pre> root@sat:~# cd /home/sat/repositorio_VIVait_Meet_1.0# apt install libsofia-sip-ua-dev libglib2.0-dev libldap2-dev Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes adicionales: libblkid-dev libffi-dev libglib2.0-dev-bin libmount-dev libpcre2-32-0 libpcre2-16-0 libpcre2-32-0 libpcre2-dev libpcre2-posix2 libpcre2-ua0 uid-dev Paquetes sugeridos: libgirepository1.0-dev libglib2.0-doc libxml2-utils sofia-sip-doc Se instalarán los siguientes paquetes NUEVOS: libblkid-dev libffi-dev libglib2.0-dev-bin libldap2-dev libmount-dev libpcre2-16-0 libpcre2-32-0 libpcre2-ua0 uid-dev libsofia-sip-ua-dev 0 actualizados, 19 nuevos se instalarán, 0 para eliminar y 7 no actualizados. Se necesita descargar 5,956 kB de archivos. Se utilizarán 31,4 MB de espacio de disco adicional después de esta operación. ¿Desea continuar? [S/n] s </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Instalar paquete libopus-dev libogg-dev gengetopt
Comando	<code>apt install libopus-dev libogg-dev gengetopt</code>
Resultado esperado	<pre> /home/sat/repositorio_VIVAit_Meet_1.0# apt install libopus-dev libogg-dev gengetopt Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes NUEVOS: gengetopt libogg-dev libopus-dev 0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 7 no actualizados. Se necesita descargar 557 kB de archivos. Se utilizarán 2.020 kB de espacio de disco adicional después de esta operación. Des:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 gengetopt amd64 2.23+dfsg1-1 [159 kB] Des:2 http://es.archive.ubuntu.com/ubuntu focal/main amd64 libogg-dev amd64 1.3.4-0ubuntu1 [161 kB] Des:3 http://es.archive.ubuntu.com/ubuntu focal/main amd64 libopus-dev amd64 1.3.1-0ubuntu1 [236 kB] Descargados 557 kB en 0s (2.060 kB/s) Seleccionando el paquete gengetopt previamente no seleccionado. </pre>

Paso	Instalar paquete libavutil-dev libavformat-dev libavcodec-dev
Comando	<code>apt install libavutil-dev libavformat-dev libavcodec-dev</code>
Resultado esperado	<pre> /home/sat/repositorio_VIVAit_Meet_1.0# apt install libavutil-dev libavformat-dev libavcodec-dev Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes adicionales: libswresample-dev Se instalarán los siguientes paquetes NUEVOS: libavcodec-dev libavformat-dev libavutil-dev libswresample-dev 0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 7 no actualizados. Se necesita descargar 7.033 kB de archivos. Se utilizarán 29,2 MB de espacio de disco adicional después de esta operación. ¿Desea continuar? [S/n] s </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Instalar paquete libwebsockets-dev libusrctp-dev
Comando	<code>apt install libwebsockets-dev libusrctp-dev</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:~/home/sat/repositorio_VIVAit_Meet_1.0# apt install libwebsockets-dev libusrctp-dev Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes adicionales: libcap-dev libev-dev libev4 libusrctp1 libuv1-dev libwebsockets15 Se instalarán los siguientes paquetes NUEVOS: libcap-dev libev-dev libev4 libusrctp-dev libusrctp1 libuv1-dev libwebsockets-dev libwebsockets15 0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 7 no actualizados. Se necesita descargar 1.331 kB de archivos. Se utilizarán 4.984 kB de espacio de disco adicional después de esta operación. ¿Desea continuar? [S/n] s </pre>

Configuración de los diferentes elementos

El primer paso es subir los archivos que se necesitan a la máquina. No es necesario subirlos a una carpeta específica (esos archivos se moverán a otros directorios).

Configuración de libnice

Paso	Entrar en el directorio:
Comando	<code>cd /root/instal/usr/lib/x86_64-linux-gnu</code>
Resultado esperado	<pre> :~# cd /usr/lib/x86_64-linux-gnu/ :/usr/lib/x86_64-linux-gnu# </pre>

Paso	Cambiar nombre del fichero /usr/lib/x86_64-linux-gnu
Comando	<code>mv -vi /root/instal/usr/lib/x86_64-linux-gnu/libnice.so.10.11.0 /usr/lib/x86_64-linux-gnu/</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/usr/lib/x86_64-linux-gnu/libnice.so.10.11.0 /usr/lib/x86_64-linux-gnu/ renamed '/root/instal/usr/lib/x86_64-linux-gnu/libnice.so.10.11.0' -> '/usr/lib/x86_64-linux-gnu/libnice.so.10.11.0' </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Entrar en el directorio:
Comando	<code>cd /usr/lib/x86_64-linux-gnu/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# cd /usr/lib/x86_64-linux-gnu/ root@VC-WebP-AytoArganda-MAD-02:/usr/lib/x86_64-linux-gnu#</pre>

Paso	Crear enlaces simbólicos
Comando	<code>ln -svi libnice.so.10.11.0 libnice.so.10</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/x86_64-linux-gnu# ln -svi libnice.so.10.11.0 libnice.so.10 'libnice.so.10' -> 'libnice.so.10.11.0'</pre>

Paso	Crear enlaces simbólicos
Comando	<code>ln -svi libnice.so.10 libnice.so</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/x86_64-linux-gnu# ln -svi libnice.so.10 libnice.so 'libnice.so' -> 'libnice.so.10'</pre>

Paso	Verificar los enlaces simbólicos
Comando	<code>ls -ltr</code>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Configuración en directorio /var/www

Paso	Entrar en el directorio /www
Comando	<code>cd /var/www</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/x86_64-linux-gnu# cd /var/www root@VC-WebP-AytoArganda-MAD-02:/var/www#</pre>

Paso	Eliminar la carpeta html
Comando	<code>rm -R html</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/var/www# rm -R html/ root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# ls -l total 0</pre>

Paso	Mover fichero html a /www
Comando	<code>mv -vi /root/instal/var/www/html</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/var/www# mv -vi /root/instal/var/www/html . renamed '/root/instal/var/www/html' -> './html' root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# root@VC-WebP-AytoArganda-MAD-02:/var/www# ls -l total 4 drwxr-xr-x 2 root root 4096 feb 1 14:08 html</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Mover carpeta vivait a /www
Comando	<code>mv -vi /root/instal/var/www/vivait</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/var/www# mv -vi /root/instal/var/www/vivait . renamed '/root/instal/var/www/vivait' -> './vivait'</pre>

Paso	Crear directorio Mdtel
Comando	<code>mkdir /etc/Mdtel/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mkdir /etc/Mdtel root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Configuración de SerCen

Paso	Crear el grupo de sercen
Comando	<code>addgroup --system --gid 990 sercen</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# addgroup --system --gid 990 sercen Adding group 'sercen' (GID 990) ... Done.</pre>

Paso	Crear el usuario sercen
Comando	<code>sudo adduser --system --shell /usr/sbin/nologin --uid 990 --gid 990 --home /nonexistent --no-create-home sercen</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# adduser --system --shell /usr/sbin/nologin --uid 990 --gid 990 --home /nonexistent --no-create-home sercen Warning: The home dir /nonexistent you specified can't be accessed: No such file or directory Adding system user 'sercen' (UID 990) ... Adding new user 'sercen' (UID 990) with group 'sercen' ... Not creating home directory '/nonexistent'.</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Mover el fichero serCen a /etc/sbin
Comando	<code>mv -vi /instal/SerCen/usr/sbin/serCen /usr/sbin/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/serCen/usr/sbin/serCen /usr/sbin/ renamed '/root/instal/serCen/usr/sbin/serCen' -> '/usr/sbin/serCen'</pre>

Paso	Mover el fichero serCen a /etc/init.d
Comando	<code>mv -vi /instal/SerCen/etc/init.d/serCen /etc/init.d/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/serCen/etc/init.d/serCen /etc/init.d/ renamed '/root/instal/serCen/etc/init.d/serCen' -> '/etc/init.d/serCen'</pre>

Paso	Mover el fichero serCen a /etc/logrotate.d
Comando	<code>mv -vi /instal/SerCen/etc/logrotate.d/serCen /etc/logrotate.d/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/serCen/etc/logrotate.d/serCen /etc/logrotate.d/ renamed '/root/instal/serCen/etc/logrotate.d/serCen' -> '/etc/logrotate.d/serCen'</pre>

Paso	Mover el fichero serCen.conf a /etc/Mdtel/
Comando	<code>mv -vi /instal/SerCen/etc/Mdtel/serCen.conf /etc/Mdtel/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/serCen/etc/Mdtel/serCen.conf /etc/Mdtel/ renamed '/root/instal/serCen/etc/Mdtel/serCen.conf' -> '/etc/Mdtel/serCen.conf'</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Entrar en el directorio /etc/rc2.d
Comando	<code>cd /etc/rc2.d</code>
Resultado esperado	<pre>rc0.d/ rc1.d/ rc2.d/ rc3.d/ rc4.d/ rc5.d/ rc6.d/ rcS.d/ root@VC-WebP-AytoArganda-MAD-02:~# cd /etc/rc2.d/</pre>

Paso	Crear enlace simbolico de arranque
Comando	<code>ln -s ../init.d/serCen S10serCen</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/rc2.d# ln -s ../init.d/serCen S10serCen</pre>

Paso	Dar permisos de ejecución a /usr/sbin/serCen
Comando	<code>chmod +x serCen</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/sbin# chmod +x serCen root@VC-WebP-AytoArganda-MAD-02:/usr/sbin#</pre>

Paso	Dar permisos de ejecución a /etc/init.d/serCen
Comando	<code>chmod +x serCen</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# chmod +x serCen root@VC-WebP-AytoArganda-MAD-02:/etc/init.d#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero SerCen.conf

Hay que revisar ciertos parámetros y modificar los que hagan falta dependiendo de las características del cliente.

Paso	Revisar y modificar el fichero /etc/MDtel/serCen.conf
Comando	<code>vi /etc/MDtel/serCen.conf</code>

En el fichero se tienen que comprobar y o modificar los siguientes parámetros:

```
smtps_usa = false
smtp_host = "correoejemplo.mdnova.local"
smtp_puerto = 0
smtp_usuario = ""
smtp_clave = ""
```

En la líneas de f1factor_xx si se pone una ip , no pide pin de acceso para esa ip . Esta característica depende del cliente (Si el cliente no quiere que se le pida el doble factor habría que poner la red del cliente , si no dejar por defecto en blanco)

Ejemplo:

```
f1factor_00_ip = "172.25.0.0"
f1factor_00_msk = "255.255.0.0"

f1factor_01_ip = ""
f1factor_01_msk = ""
```

Los siguientes parámetros definen el nombre de las salas con posibilidad de acceso telefónico:

```
vivait_meet_prefijo_min = 5
vivait_meet_prefijo = "vivaitcall_"
```

Parámetro VDN para acceder a la sala por telefono:

```
vivait_meet_dnis = "9999"
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Arrancar serCen
Comando	<code>/etc/init.d/serCen start</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# /etc/init.d/serCen start Starting serCen</pre>

Paso	Comprobar que SerCen está arrancado
Comando	<code>/etc/init.d/serCen status</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# /etc/init.d/serCen status serCen is running</pre>

Paso	Comprobar que SerCen está funcionando correctamente
Comando	<code>nc localhost 1125</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# nc localhost 1125 serCen:sis ver='00:01:04' inic='20220202 16:100' alarmas=0 ultAlar='00000000 000000' serCen gmp msg=254/256 buf=256/256 tasa=97/102 serCen tmp uptime=44 (0d 0h 0m 44s) serCen wvs mysql=1 conxNum=0 conxMaxPeriodo=0 serCen wvc numCacheLibre=3 numColaPend=0 serCen wvc numReq=0/0 numGet=0/0 numPost=0/0 numPut=0/0 numDelete=0/0 serCen smt numCacheLibre=5 numColaPend=0 enPeriodo=0/0 numMsj=0/0</pre>

Configuración de Janus

Paso	Crear el grupo de janus
Comando	<code>addgroup --system --gid 991 janus</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# addgroup --system --gid 991 janus Adding group `janus' (GID 991) ... Done.</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Crear el usuario janus
Comando	<code>sudo adduser --system --shell /usr/sbin/nologin --uid 991 --gid 991 --home /nonexistent --no-create-home janus</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# adduser --system --shell /usr/sbin/nologin --uid 991 --gid 991 --home /nonexistent --no-create-home janus Warning: The home dir /nonexistent you specified can't be accessed: No such file or directory Adding system user 'janus' (UID 991) ... Adding new user 'janus' (UID 991) with group 'janus' ...</pre>

Paso	Mover scripts a /root
Comando	<code>mv -vi /root/intsal/scripts /root/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/scripts /root/ renamed '/root/instal/scripts' -> '/root/scripts'</pre>

Paso	Mover vivait-meet/opt a /opt/
Comando	<code>mv -vi /instal/vivait-meet/opt/ /opt/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/vivait-meet/opt /opt/ renamed '/root/instal/vivait-meet/opt' -> '/opt/opt'</pre>

Paso	Mover janus a /etc/init.d
Comando	<code>mv -vi /instal/janus/etc/init.d/janus /etc/init.d/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/etc/init.d/janus /etc/init.d/ renamed '/root/instal/janus/etc/init.d/janus' -> '/etc/init.d/janus'</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Mover janus a /etc/
Comando	<code>mv -vi /instal/janus/etc/janus /etc/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/etc/janus /etc/ renamed '/root/instal/janus/etc/janus' -> '/etc/janus'</pre>

Paso	Mover janus a /etc/logrotate.d
Comando	<code>mv -vi /instal/janus/etc/logrotate.d/janus /etc/logrotate.d/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/etc/logrotate.d/janus /etc/logrotate.d/ renamed '/root/instal/janus/etc/logrotate.d/janus' -> '/etc/logrotate.d/janus'</pre>

Paso	Mover lib a /usr/lib
Comando	<code>mv -vi /instal/janus/usr/lib/ /usr/lib/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/usr/lib /usr/lib/ renamed '/root/instal/janus/usr/lib' -> '/usr/lib/lib'</pre>

Paso	Mover janus a /usr/sbin
Comando	<code>mv -vi /instal/janus/usr/sbin/janus /usr/sbin/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/usr/sbin/janus /usr/sbin/ renamed '/root/instal/janus/usr/sbin/janus' -> '/usr/sbin/janus'</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Mover safe_janus a /usr/sbin
Comando	<code>mv -vi /instal/janus/usr/sbin/safe_janus /usr/sbin/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/init.d# mv -vi /root/instal/janus/usr/sbin/janus /usr/sbin/ renamed '/root/instal/janus/usr/sbin/janus' -> '/usr/sbin/janus'</pre>

Paso	Dar permisos de ejecución /usr/sbin/janus
Comando	<code>chmod +x janus</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/sbin# chmod +x janus root@VC-WebP-AytoArganda-MAD-02:/usr/sbin#</pre>

Paso	Dar permisos de ejecución /usr/sbin/janus
Comando	<code>chmod +x safe_janus</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/sbin# chmod +x safe_janus root@VC-WebP-AytoArganda-MAD-02:/usr/sbin#</pre>

Paso	Entrar en el directorio /etc/rc2.d
Comando	<code>cd /etc/rc2.d</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/sbin# cd /etc/rc2.d/ root@VC-WebP-AytoArganda-MAD-02:/etc/rc2.d#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Crear enlace simbólico entre dos ficheros
Comando	<code>ln -s ../init.d/janus S10janus</code>
Resultado esperado	<pre>root@VC-VebP-AytoArganda-MAD-02:/etc/rc2.d# ln -s ../init.d/janus S10janus root@VC-VebP-AytoArganda-MAD-02:/etc/rc2.d#</pre>

Modificar el fichero janus.jcfg

Hay que revisar ciertos parámetros y modificar los que hagan falta dependiendo de las características del cliente.

Paso	Revisar y modificar el fichero /etc/janus.jcfg
Comando	<code>vi /etc/janus/janus.jcfg</code>

En el fichero se tienen que comprobar y o modificar los siguientes parámetros:

`server_name = "labmeet.mdnova.local"` → Nombre de dominio del servidor

```
certificates: {
  # dtls
  cert_pem = "" → Dejar en blanco
  cert_key = "" → Dejar en blanco
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero janus.consola.jcfg

Paso	Modificar el fichero /etc/janus/janus.consola.jcfg
Comando	<code>vi /etc/janus/janus.consola.jcfg</code>

REVISAR:

server_name = "labmeet.mdnova.local" → Nombre de dominio del servidor

```
certificates: {  
  # dtls  
  cert_pem = "" → Dejar en blanco  
  cert_key = "" → Dejar en blanco
```

Modificar el fichero janus.transport.http.jcfg

Paso	Modificar el fichero janus.transport.http.jcfg
Comando	<code>vi /etc/janus/janus.transport.http.jcfg</code>

REVISAR:

```
cert_pem = "" → Dejar en blanco  
cert_key = "" → Dejar en blanco
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero janus.consola.jcfg

Paso	Modificar el fichero janus.transport.websockets.jcfg
Comando	<code>vi /etc/janus/janus.transport.websockets.jcfg</code>

REVISAR:

cert_pem = "" → Dejar en blanco

cert_key = "" → Dejar en blanco

Modificar el fichero vivait.plugin.webfon.jcfg

Paso	Modificar el fichero vivait.plugin.webfon.jcfg
Comando	<code>vi /etc/janus/vivait.plugin.webfon.jcfg</code>

REVISAR:

local_nodo_id = 4 → ID NODO DE LA BASE DE DATOS EN LA QUE ESTE CREADO EL WEBPHONE *****

colas_limpiar_siempre = false → SI SE TRABAJA CON POOL DE CONEXIONES a true

local_ip = "172.25.0.22" → IP PRIVADA RED DE VOZ

max_digi_llam_sal = 10 → NUMERO MAXIMO DE DIGITOS EN LLAMADAS SALIENTES DE LA EXTENSION



Se configura max_digi_llam_sal porque son pequeños mecanismos de seguridad por si un cliente solo va a hacer llamadas nacionales , para evitar que no haga llamadas internacionales.

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Parar el servicio janus
Comando	<code>/etc/init.d/janus stop</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivaIt# /etc/init.d/janus stop Stopping janus: janus.</pre>

Paso	Arrancar janus
Comando	<code>/etc/init.d/janus start</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/rc2.d# /etc/init.d/janus start Starting janus: janus.</pre>

Paso	Comprobar que janus funciona correctamente
Comando	<code>ps aux grep janus</code>
Resultado esperado	<pre>Stopping janus: janus. root@VC-WebP-AytoArganda-MAD-02:~/install-vebfon/janus/usr/sbin# ps aux grep janus root 3111121 0.0 0.0 6892 1708 ? S 10:43 0:00 /bin/bash /usr/sbin/safe_janus root 3111128 0.0 0.0 7996 3260 ? S 10:43 0:00 runuser -u janus -g janus -- nice -n 0 /usr/sbin/janus --pid-file=/var/run/janus/janus.pid --configs-folder=/etc/janus --log-file=/var/log/janus/janus.log janus 3111129 0.6 0.2 1106928 23284 ? S1 10:43 0:00 /usr/sbin/janus --pid-file=/var/run/janus/janus.pid --configs-folder=/etc/janus --log-file=/var/log/janus/janus.log root 3111154 0.0 0.0 6432 672 pts/1 S+ 10:43 0:00 grep --color=auto janus</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Configuración de NGINX

Paso	Entrar en el directorio /etc/nginx/sites-available
Comando	<code>cd /etc/nginx/sites-avaiable/</code>

Paso	Renombrar el fichero /etc/nginx/sites-available/webphone.ejemplo.com.conf
Comando	<code>mv -vi /etc/nginx/sites-available/webphone."".".conf /etc/nginx/sites-available/webphone."".".conf.orig</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait# mv -vi /etc/nginx/sites-available/webphone.ayto-arganda.es.conf /etc/nginx/sites-available/webphone.ayto-arganda.es.conf.orig renamed '/etc/nginx/sites-available/webphone.ayto-arganda.es.conf' -> '/etc/nginx/sites-available/webphone.ayto-arganda.es.conf.orig'</pre>

Paso	Verificar que se ha renombrado el fichero
Comando	<code>ls -l /etc/nginx/sites-available/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait# ls -l /etc/nginx/sites-available/ total 12 -rw-r--r-- 1 root root 2416 mar 26 2020 default -rw-r--r-- 1 root root 4113 feb 2 09:32 webphone.ayto-arganda.es.conf.orig root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Mover el fichero root/install/nginx/etc/nginx/sites-avaliabile
Comando	<code>mv -vi /root/instal/nginx/etc/nginx/sites-avaliabile/* /etc/nginx/sites-avaliabile/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait# mv -vi /root/instal/nginx/etc/nginx/sites-avaliabile/* /etc/nginx/sites-avaliabile/ renamed '/root/instal/nginx/etc/nginx/sites-avaliabile/labmeet.mdnova.local.conf' -> '/etc/nginx/sites-avaliabile/labmeet.mdnova.local.conf'</pre>

Paso	Renombrar fichero /etc/nginx/sites-avaliabile/labmeet.mdnova.local.conf
Comando	<code>mv labmeet.mdnova.local.conf webphone.zonaejemplo.conf</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait# mv /etc/nginx/sites-avaliabile/labmeet.mdnova.local.conf /etc/nginx/sites-avaliabile/webphone.ayto-arganda.es.conf root@VC-WebP-AytoArganda-MAD-02:/usr/lib/vivait#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero webphone.zonaejemplo.com.conf

Paso	Modificar fichero /etc/nginx/sites-available/webphone.zonaejemplo.com.conf
Comando	<code>vi webphone.zonaejemplo.com.conf</code>



Buscar en el fichero las líneas que aparezca labmeet.mdnova.local y modificar el nombre con el del servidor de dominio.

`server_name = "labmeet.mdnova.local"` → Nombre de dominio del servidor

`ssl_certificate /etc/jitsi/meet/labmeet.mdnova.local.crt` → Modificar el nombre del certificado

`ssl_certificate_key /etc/jitsi/meet/labmeet.mdnova.local.key;` → Modificar el nombre del certificado

`alias /etc/jitsi/meet/labmeet.mdnova.local-config.js;` → Modificar el nombre a NombreDominioServidor .config.js

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Instalación y configuración del certificado

Un certificado digital no es más que una cadena de bits con la clave pública y una serie de atributos, todo, firmado digitalmente por una autoridad de certificación (CA) que actúa de garante de la información que contiene. Cuando la información ha sido verificada por la CA, utiliza su clave privada para firmar digitalmente el certificado emitido, lo que proporciona confianza a quien lo recibe.

La llave privada es un archivo electrónico con extensión KEY. Este mecanismo se compone de un software que sirve para el desarrollo de mecanismos de encriptación como los cifrados.

Existen diferentes extensiones en los certificados , estos pueden ser :

- .pfx: es la copia de seguridad con clave privada de un certificado (exportado desde Internet Explorer).
- .p12: es la copia de seguridad con clave privada de un certificado (exportado desde Firefox).
- .cer: es un formato de exportación de clave pública desde Internet Explorer, puede ser en formato DER o formato PEM (Base64)
- .crt: es un formato de exportación de clave pública desde Mozilla firefox. Es en formato PEM (Base 64).

Es importante tener en cuenta que en cuanto a los certificados SSL/TLS, no importa la extensión del archivo . El certificado SSL/TLS puede estar colocado en forma textual que predomina (linux y apache, unix y otros servidores) o en forma binaria (Java, Microsoft Server).

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Dependiendo del cliente , la forma de instalar y configurar el certificado puede variar. A continuación se muestran los pasos para configurar un certificado con extensión .pfx :

Lo primero es copiar los certificados y copiarlos en una carpeta de la máquina.

Paso	Generar clave.key
Comando	<code>openssl pkcs12 -in CertWebphone.pfx -nocerts -out Clave.key</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:~# openssl pkcs12 -in CertWebPhone.pfx -nocerts -out Clave.key Enter Import Password: Enter PEM pass phrase: Verifying - Enter PEM pass phrase: </pre>

Paso	Generar certificado.crt
Comando	<code>openssl pkcs12 -in CertWebphone.pfx -cicerts -nokeys -out Certificado.crt</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:~# openssl pkcs12 -in CertWebPhone.pfx -cicerts -nokeys -out Certificado.crt Enter Import Password: root@VC-WebP-AytoArganda-MAD-02:~# </pre>

Paso	Generar certificado.crt
Comando	<code>openssl rsa -in webphone.ejemplo.es.key -out webphone.ejemplo.es.limpia.key</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# openssl rsa -in webphone.ayto-arganda.es.key -out webphone.ayto-arganda.es.limpia.key Enter pass phrase for webphone.ayto-arganda.es.key: writing RSA key </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Copiar los certificados a /etc/jitsi/meet/
Comando	<code>cp Certificado.crt /etc/jitsi/meet/</code> <code>cp clave.key /etc/jitsi/meet/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# cp Certificado.crt /etc/jitsi/meet/ root@VC-WebP-AytoArganda-MAD-02:~# root@VC-WebP-AytoArganda-MAD-02:~# cp Clave.key /etc/jitsi/meet/ root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Paso	Entrar en el directorio /etc/jitsi/meet
Comando	<code>cd /etc/jitsi/meet</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# cd /etc/jitsi/meet/ root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# ls -l total 44 -rw----- 1 root root 2517 feb 2 11:00 Certificado.crt -rw----- 1 root root 2067 feb 2 11:00 Clave.key -rw-r--r-- 1 root root 27605 feb 2 09:32 webphone.ayto-arganda.es-config.js -rw-r--r-- 1 root root 2143 feb 2 09:32 webphone.ayto-arganda.es.crt -rw----- 1 root root 3272 feb 2 09:32 webphone.ayto-arganda.es.key</pre>

Paso	Renombrar webphone.ejemplo.es.crt
Comando	<code>mv webphone.ejemplo.es.crt webphone.ejemplo.es.crt.orig</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv webphone.ayto-arganda.es.crt webphone.ayto-arganda.es.crt.orig root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Renombrar webphone.ejemplo.es.key
Comando	<code>mv webphone.ejemplo.es.key webphone.ejemplo.es.key.orig</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv webphone.ayto-arganda.es.key webphone.ayto-arganda.es.key.orig root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Renombrar clave.key a webphone.ejemplo.es.key
Comando	<code>mv clave.key webphone.ejemplo.es.key</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv Clave.key webphone.ayto-arganda.es.key root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Renombrar Certificado.crt a webphone.ejemplo.es.crt
Comando	<code>mv Certificado.crt webphone.ejemplo.es.crt</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv Certificado.crt webphone.ayto-arganda.es.crt root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Renombrar Certificado.crt a webphone.ejemplo.es.crt
Comando	<code>mv webphone.ejemplo.es.key webphone.ejemplo.es.key.cifrada</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv webphone.ayto-arganda.es.key webphone.ayto-arganda.es.key.cifrada root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Renombrar Certificado.crt a webphone.ejemplo.es.crt
Comando	<code>mv webphone.ejemplo.es.limpia.key webphone.ejemplo.es.key</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv webphone.ayto-arganda.es.limpia.key webphone.ayto-arganda.es.key root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Cambiar permisos a webphone.ejemplo.es.key y webphone.ejemplo.es.crt
Comando	<code>chmod 644 webphone.ejemplo.es.crt</code> <code>chmod 644 webphone.ejemplo.es.key</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# chmod 644 webphone.ayto-arganda.es.crt root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# chmod 644 webphone.ayto-arganda.es.key root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Comprobar si hay algún error del nginx
Comando	<code>cat /var/log/nginx/error.log</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# cat /var/log/nginx/error.log 2022/02/02 09:32:18 [notice] 3851#3851: signal process started 2022/02/02 11:03:19 [emerg] 37669#37669: master: load certificate key "/etc/jitsi/meet/webphone.ayto-arganda.es.key": PEM_read_bio_PrivateKey() failed (SSL: error:30071068:PEM routines:PEM_read_bio_PrivateKey:processing error:while reading strings error:30916406:PEM routines:PEM_def_callback:problem getting password error:30970068:PEM routines:PEM_read_bio_PrivateKey:bad password read) </pre>

Configuración de Prosody

Paso	Renombrar el fichero “labmeet.mdnova.local.cfg.lua”
Comando	<code>mv -vi /etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua labmeet.mdnova.local.cfg.lua.orig</code>
Resultado esperado	<pre> example.com.cfg.lua localhost.cfg.lua webphone.ayto-arganda.es.cfg.lua root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv -vi /etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua /etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua.orig renamed '/etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua' -> '/etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua.orig' root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# </pre>

Paso	Mover el fichero “labmeet.mdnova.local.cfg.lua”
Comando	<code>mv -vi /instal/prosody/etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua /etc/prosody/conf.avail/</code>
Resultado esperado	<pre> root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv -vi /root/instal/prosody/etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua /etc/prosody/conf.avail/ renamed '/root/instal/prosody/etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua' -> '/etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua' root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Renombrar el fichero labmeet.mdnova.local.cfg.lua
Comando	<code>mv /etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua webphone.zona-ejemplo.com.cfg.lua</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv /etc/prosody/conf.avail/labmeet.mdnova.local.cfg.lua /etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Modificar el fichero webphone.zona-ejemplo.com.cfg.lua

Cambiar todo aquel certificado y nombre de dominio por el nuestro

Paso	Modificar fichero webphone.zona-ejemplo.com.cfg.lua
Comando	<code>vi webphone.zona-ejemplo.com.cfg.lua</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# vi /etc/prosody/conf.avail/webphone.ayto-arganda.es.cfg.lua</pre>



Buscar en el fichero las líneas que aparezca labmeet.mdnova.local y modificar el nombre con el del servidor de dominio.

`server_name = "labmeet.mdnova.local"` → Nombre de dominio del servidor

`ssl_certificate /etc/jitsi/meet/labmeet.mdnova.local.crt` → Modificar el nombre del certificado

`ssl_certificate_key /etc/jitsi/meet/labmeet.mdnova.local.key;` → Modificar el nombre del certificado

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Copiar contenido del fichero webphone.zona-ejemplo.com.cfg.lua.orig
Comando	<code>vi webphone.zona-ejemplo.com.cfg.lua.orig</code>
Resultado esperado	

En el fichero **webphone.zona-ejemplo.com.cfg.lua.orig** , hay que copiar el contenido que esta entre las comillas de (turncredentials_secret) y despues pegarlo en el otro fichero modificado en el paso anterior(fichero : **webphone.zona-ejemplo.com.cfg.lua**):

```
turncredentials_secret = "xxxHDGLDJdWcY6l";
```

Paso	Reiniciar prosody
Comando	<code>systemctl restart prosody.service</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# systemctl restart prosody.service root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Paso	Comprobar que prosody funciona correctamente
Comando	<code>ps -aux grep prosody</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# ps -aux grep prosody prosody 38105 0.8 0.4 24208 17776 ? Ss 11:32 0:00 lua5.2 /usr/bin/prosody root 38181 0.0 0.0 6432 736 pts/1 S+ 11:32 0:00 grep --color=auto prosody root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Configuración de Jicofo

Paso	Renombrar el fichero sip-communicator.properties.orig
Comando	<code>mv -vi /etc/jitsi/jicofo/sip-communicator.properties /etc/jitsi/jicofo/sip-communicator.properties.orig</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /etc/jitsi/jicofo/sip-communicator.properties /etc/jitsi/jicofo/sip-communicator.properties.orig renamed '/etc/jitsi/jicofo/sip-communicator.properties' -> '/etc/jitsi/jicofo/sip-communicator.properties.orig' root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Paso	Mover el fichero sip-communicator.properties
Comando	<code>mv -vi /instal/jitsi/etc/jitsi/jicofo/sip-communicator.properties /etc/jitsi/jicofo/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/jitsi/etc/jitsi/jicofo/sip-communicator.properties /etc/jitsi/jicofo/ renamed '/root/instal/jitsi/etc/jitsi/jicofo/sip-communicator.properties' -> '/etc/jitsi/jicofo/sip-communicator.properties' root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero sip-communicator.properties

Cambiar todo aquel certificado y nombre de dominio por el nuestro

Paso	Modificar fichero <code>/etc/jitsi/jicofo/sip-communicator.properties</code>
Comando	<code>vi sip-communicator.properties</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mv -vi /root/instal/jitsi/etc/jitsi/jicofo/sip-communicator.properties</pre>

REVISAR:

Poner el nombre de dominio (ejemplo : labmeet.mdnova.local):

org.jitsi.jicofo.BRIDGE_MUC=JvbBrewery@internal.auth.labmeet.mdnova.local

org.jitsi.jicofo.auth.URL=XMPP:labmeet.mdnova.local

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Configuración de Jitsi/meet

Paso	Entrar en el directorio /etc/jitsi/meet
Comando	<code>cd /etc/jitsi/meet</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# cd /etc/jitsi/meet/ root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Renombrar el fichero /etc/jitsi/meet/labmeet.mdnova.local-config.js
Comando	<code>mv labmeet.mdnova.local-config.js labmeet.mdnova.local-config.js.orig</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv webphone.ayto-arganda.es-config.js webphone.ayto-arganda.es-config.js.orig root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Paso	Mover el fichero /root/instal/jitsi/etc/jitsi/meet/labmeet.mdnova.local-config.js
Comando	<code>mv -vi /root/instal/jitsi/etc/jitsi/meet/labmeet.mdnova.local-config.js /etc/jitsi/meet/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv -vi /root/instal/jitsi/etc/jitsi/meet/labmeet.mdnova.local-config.js /etc/jitsi/meet/ renamed '/root/instal/jitsi/etc/jitsi/meet/labmeet.mdnova.local-config.js' -> '/etc/jitsi/meet/labmeet.mdnova.local-config.js' root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Renombrar el fichero labmeet.mdnova.local-config.js
Comando	<code>mv labmeet.mdnova.local-config.js webphone.zonaejemplo.com-config.js</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet# mv labmeet.mdnova.local-config.js webphone.ayto-arganda.es-config.js root@VC-WebP-AytoArganda-MAD-02:/etc/jitsi/meet#</pre>

Modificar el fichero sip-communicator.properties

Copiar el contenido que esta entre comillas en la línea "password" para pegarlo en el fichero sip-communicator.properties.

Paso	Copiar el contenido del fichero jigasi.dat
Comando	<code>vi var/lib/prosody/auth%2elabmeet%2emdnova%2elocal/accounts/jigasi.dat</code>

Ejemplo:

```
return {
    ["password"] = "tszqgi0IMCU40KsT";
};
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Pegar el contenido password del fichero jigasi.dat a /etc/jitsi/jigasi/sip-communicator.properties
Comando	<code>vi /etc/jitsi/jigasi/sip-communicator.properties</code>

En el fichero sip-communicator.properties , primero se tiene que descomentar y modificar las tres líneas siguientes:

org.jitsi.jigasi.xmpp.acc.USER_ID=jigasi@auth.webphone.ejemplo.es → Poner después de auth. el nombre de dominio.

org.jitsi.jigasi.xmpp.acc.PASS=xxxxxxxxxxxxxxxxxxxxxxxx → Pegar la “password” del fichero anterior.

org.jitsi.jigasi.xmpp.acc.ANONYMOUS_AUTH=false → Dejar en false

Ejemplo:

```
# If you want jigasi to perform authenticated login instead of anonymous login
# to the XMPP server, you can set the following properties.
org.jitsi.jigasi.xmpp.acc.USER_ID=jigasi@auth.webphone. es
org.jitsi.jigasi.xmpp.acc.PASS=
org.jitsi.jigasi.xmpp.acc.ANONYMOUS_AUTH=false
```

Comentar con # al principio de la línea:

```
net.java.sip.communicator.impl.protocol.jabber.acc-xmpp-1.BOSH_URL_PATTERN=https://(host)(subdomain)/http-bind?room=(roomName)
```

Ejemplo:

```
#net.java.sip.communicator.impl.protocol.jabber.acc-xmpp-1.BOSH_URL_PATTERN=https://(host)(subdomain)/http-bind?room=(roomName)
net.java.sip.communicator.impl.protocol.jabber.acc-xmpp-1.DOMAIN_BASE=webphone.ayto-arganda.es
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Descomentar la línea:

```
net.java.sip.communicator.service.gui.ALWAYS_TRUST_MODE_ENABLED=true
```

Ejemplo:

```
# Activate this property if you are using self-signed certificates or other
# type of non-trusted certificates. In this mode your service trust in the
# remote certificates always.
net.java.sip.communicator.service.gui.ALWAYS_TRUST_MODE_ENABLED=true
```

Descomentar la línea y cambiar **siptest** por **vivaitcall** :

```
org.jitsi.jitsi.DEFAULT_JVB_ROOM_NAME=sivaitcall@conference.webphone.
ejemplo.es
```

Ejemplo:

```
# Name of default JVB room that will be joined if no special header is included
# in SIP invite
org.jitsi.jigasi.DEFAULT_JVB_ROOM_NAME=vivaitcall@conference.webphone.ayto-arganda.es
```

Paso	Reiniciar la máquina
Comando	<code>reboot</code>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



3.4 Configuración de firewall (iptables) .

Dependiendo de la arquitectura del cliente puede tener una configuración u otra.

Un **firewall**, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

Las **reglas de entrada** filtran el tráfico que pasa de la red al equipo local en función de las condiciones de filtrado especificadas en la regla. Por el contrario, las **reglas de salida** filtran el tráfico que pasa del equipo local a la red en función de las condiciones de filtrado especificadas en la regla.

Iptables es un módulo del núcleo de Linux que se encarga de filtrar los paquetes de red, es decir, es la parte que se encarga de determinar qué paquetes de datos queremos que lleguen hasta el servidor y cuáles no. Iptables gestiona, mantiene e inspecciona las reglas de filtrado de paquetes IPv4 a través de tablas. Estas tablas clasifican y organizan las reglas de acuerdo al tipo de decisiones que se deben tomar sobre los paquetes.

El primer paso es obtener los ficheros(**.sh , firewall**) y copiarlos en la máquina. Después hay que crear la carpeta firewall en **/etc** .

firewall.sh -> Contiene todas las reglas iptables, **NO TOCAR**

vars.sh -> Fichero donde se configura la red del cliente así como las interfaces públicas y privadas de la máquina.

Paso	Crear la carpeta /etc/firewall
Comando	<code>mkdir /etc/firewall</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:~# mkdir /etc/firewall root@VC-WebP-AytoArganda-MAD-02:~#</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Entrar en el directorio /etc/firewall
Comando	<code>cd /etc/firewall/</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc# cd firewall/ root@VC-WebP-AytoArganda-MAD-02:/etc/firewall#</pre>

Paso	Mover los ficheros .sh a /etc/firewall
Comando	<code>mv -vi /carpetaorigen/*.sh .</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# mv -vi /home/sat/*.sh . renamed '/home/sat/firewall.sh' -> './firewall.sh' renamed '/home/sat/vars.sh' -> './vars.sh'</pre>

*La carpeta origen es dónde se han copiado los ficheros a la máquina.

Paso	Poner permisos de ejecución a los ficheros .sh
Comando	<code>chmod +x *.sh</code>
Resultado esperado	<pre>root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# chmod +x * root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# root@VC-WebP-AytoArganda-MAD-02:/etc/firewall# ls -l total 8 -rwxr-xr-x 1 root root 1322 feb 2 12:04 firewall.sh -rwxr-xr-x 1 root root 75 feb 2 12:01 varsh.sh</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Poner permisos de ejecución a los ficheros .sh
Comando	<code>chown root:root *.sh</code>
Resultado esperado	<pre> root@VC-WEB-202aFrance-VIG0-02:/etc/firewall# chown root:root *.sh root@VC-WEB-202aFrance-VIG0-02:/etc/firewall# ls -l total 8 -rwxr-xr-x 1 root root 2034 ene 18 11:33 firewall.sh -rwxr-xr-x 1 root root 171 ene 18 11:33 vars.sh </pre>

Paso	Editar el fichero /etc/firewall/vars.sh
Comando	<code>vi vars.sh</code>
Resultado esperado	

Copiar el contenido que está debajo y copiarlo en el fichero vars.sh

```
#!/bin/bash
```

```

export ETH_LAN=ens3
export IP_LAN=172.25.128.253
export RED_LAN=172.25.0.0/23
export ETH_DMZ=ens7
export IP_DMZ=89.140.51.149
export RED_DMZ=89.140.51.144/29

```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Editar el fichero firewall.sh
Comando	<code>vi firewall.sh</code>

Copiar el contenido que está debajo y copiarlo en el fichero firewall.sh

```
#!/bin/bash

DIR=$(dirname "$0")

. ${DIR}/vars.sh

# Se inician las cadenas
iptables -t filter -F
iptables -t filter -X
iptables -t nat -F
iptables -t nat -X

### INPUT
iptables -P INPUT ACCEPT

# DMZ filtrada
# privadas no
iptables -A INPUT -i $ETH_DMZ -s 192.168.0.0/16 -j DROP
iptables -A INPUT -i $ETH_DMZ -s 172.16.0.0/12 -j DROP
iptables -A INPUT -i $ETH_DMZ -s 10.0.0.0/8 -j DROP
# otras ip publicas no valen para RTP
# iptables -A INPUT -i $ETH_DMZ -s 213.97.161.214 -p udp -j DROP
# web
iptables -A INPUT -i $ETH_DMZ -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i $ETH_DMZ -p tcp --dport 443 -j ACCEPT
# rtp / udp (jitsi videobridge)
iptables -A INPUT -i $ETH_DMZ -p udp --dport 10000 -j ACCEPT
# rtp / udp (/etc/janus/janus.cfg)
iptables -A INPUT -i $ETH_DMZ -p udp --dport 20000:20999 -j ACCEPT
# turn
# iptables -A INPUT -i $ETH_DMZ -p tcp --dport 3478 -j ACCEPT
# iptables -A INPUT -i $ETH_DMZ -p tcp --dport 5349 -j ACCEPT
# iptables -A INPUT -i $ETH_DMZ -p udp --dport 60000:60099 -j ACCEPT
# xmpp
# iptables -A INPUT -i $ETH_DMZ -p tcp --dport 5222 -j ACCEPT
# acme
iptables -A INPUT -i $ETH_DMZ -p tcp --sport 443 -m state --state
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



```

RELATED,ESTABLISHED -j ACCEPT
# stun STUN_MAPPING_HARVESTER_ADDRESSES en /etc/jitsi/videobridge/sip-
communicator.properties
iptables -A INPUT -i $ETH_DMZ -p udp --sport 443 -m state --state
RELATED,ESTABLISHED -j ACCEPT
# icmp pruebas
iptables -A INPUT -i $ETH_DMZ -p icmp -s 213.97.161.214 -j ACCEPT
iptables -A INPUT -i $ETH_DMZ -p icmp --icmp-type 0 -j ACCEPT
# iperf3
iptables -A INPUT -i $ETH_DMZ -p tcp --dport 4444 -j ACCEPT
# resto
iptables -A INPUT -i $ETH_DMZ -j DROP

### OUTPUT
iptables -P OUTPUT ACCEPT
# otras ip publicas no valen para RTP
# iptables -A OUTPUT -o $ETH_DMZ -d 213.97.161.214 -p udp -j DROP
# no se permiten salidas con ip cruzadas
iptables -A OUTPUT -o $ETH_LAN -s $RED_DMZ -j DROP
iptables -A OUTPUT -o $ETH_DMZ -s $RED_LAN -j DROP

### FORWARD
iptables -P FORWARD ACCEPT
iptables -A FORWARD -i $ETH_DMZ -j DROP
iptables -A FORWARD -o $ETH_DMZ -j DROP
~

```

Paso	Mover el fichero firewall a /etc/init.d
Comando	<code>mv -vi /carpetaorigen/ /etc/init.d/</code>
Resultado esperado	

Paso	Entrar en el directorio /etc/init.d
Comando	<code>cd /etc/init.d</code>
Resultado esperado	

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Poner permisos de ejecución a al fichero firewall
Comando	<pre>chmod +x firewall chown root:root firewall</pre>
Resultado esperado	<pre>root@PC-WEB-ZonaFranca-VIG0-02:/etc/init.d# chown root:root firewall root@PC-WEB-ZonaFranca-VIG0-02:/etc/init.d# chmod +x firewall</pre>

Paso	Entrar en el directorio /etc/rc2.d
Comando	<pre>cd /etc/rc2.d/</pre>
Resultado esperado	<pre>root@PC-WEB-ZonaFranca-VIG0-02:/etc/init.d# cd /etc/rc2.d/</pre>

Paso	Crear enlace simbólico
Comando	<pre>ln -s ../init.d/firewall s10firewall</pre>
Resultado esperado	<pre>root@PC-WEB-ZonaFranca-VIG0-02:/etc/rc2.d# ln -s ../init.d/firewall s10firewall</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



3.5 Instalación y configuración de fail2ban .

Paso	Instalar fail2ban
Comando	<code>apt install fail2ban</code>
Resultado esperado	<pre> root@VVC-WebP-AytoArganda-MAD-02:/etc/init.d# apt-get install fail2ban Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes adicionales: python3-pyinotify whois Paquetes sugeridos: mailx monit python-pyinotify-doc Se instalarán los siguientes paquetes NUEVOS: fail2ban python3-pyinotify whois 0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados. Se necesita descargar 444 kB de archivos. Se utilizarán 2,400 kB de espacio de disco después de esta operación. ¿Desea continuar? [S/n] s </pre>

Paso	Entrar en el directorio /etc/fail2ban
Comando	<code>cd /etc/fail2ban/</code>
Resultado esperado	<pre> root@VVC-Web-ZonaFranca-VIG0-02:/etc/firewall# cd /etc/fail2ban/ root@VVC-Web-ZonaFranca-VIG0-02:/etc/fail2ban# ls -l total 64 drwxr-xr-x 2 root root 4096 ene 18 11:45 action.d -rw-r--r-- 1 root root 2817 ene 11 2020 fail2ban.conf drwxr-xr-x 2 root root 4096 mar 2 2020 fail2ban.d drwxr-xr-x 3 root root 4096 ene 18 11:45 filter.d -rw-r--r-- 1 root root 25740 ene 11 2020 jail.conf drwxr-xr-x 2 root root 4096 ene 18 11:45 jail.d -rw-r--r-- 1 root root 645 ene 11 2020 paths-arch.conf -rw-r--r-- 1 root root 2827 ene 11 2020 paths-common.conf -rw-r--r-- 1 root root 573 ene 11 2020 paths-debian.conf -rw-r--r-- 1 root root 738 ene 11 2020 paths-opensuse.conf root@VVC-Web-ZonaFranca-VIG0-02:/etc/fail2ban# mv jail.conf jail. </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Hacer una copia de seguridad del fichero jail.conf
Comando	<code>mv jail.conf jail.conf.orig</code>
Resultado esperado	<pre>root@VC-WEB-2024franca-V100-02:/etc/fail2ban# mv jail.conf jail.conf.orig root@VC-WEB-2024franca-V100-02:/etc/fail2ban# █</pre>

Paso	Copiar el fichero jail.conf.orig a jail.conf
Comando	<code>cp jail.conf.orig jail.conf</code>
Resultado esperado	<pre>root@VC-WEB-2024franca-V100-02:/etc/fail2ban# cp jail.conf.orig jail.conf root@VC-WEB-2024franca-V100-02:/etc/fail2ban# █</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero jail.conf

Paso	Editar el fichero jail.conf
Comando	<code>vi /etc/fail2ban/jail.conf</code>

En el fichero jail.conf , hay que editar las siguientes líneas :

Se configura la línea de **ignoreip** si no se quiere banear a las ip que estén dentro de la red del cliente.(Comentar la línea con **#wkwignoreip** y añadirla abajo para modificarla)

```
ignoreip = 127.0.0.1/8 ::1 redcliente
```

Ejemplo:

```
# wkw ignoreip = 127.0.0.1/8 ::1
ignoreip = 127.0.0.1/8 ::1 172.20.0.0/16
```

Se configura la línea de **bantime** para poner el tiempo de baneo.
(Comentar la línea con **#wkwbantime** y añadirla abajo para modificarla)

```
#wkwbantime
bantime = 15 m
```

Se configura la línea de **Usedns** poniendo un no .
(Comentar la línea con **#wkwUsedns** y añadirla abajo para modificarla)

```
#wkw Usedns = warn
usedns = no
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Entrar en el directorio jail.d
Comando	<code>cd jail.d/</code>
Resultado esperado	<pre>root@VC-WEB-IonaFrance-V100-02:/etc/fail2ban# cd jail.d/ root@VC-WEB-IonaFrance-V100-02:/etc/fail2ban/jail.d# ls -l total 4 -rw-r--r-- 1 root root 22 mar 2 2020 defaults-debian.conf</pre>

Paso	Hacer una copia de seguridad del fichero defaults-debian.conf
Comando	<code>mv -vi defaults-debian.conf defaults-debian.conf.orig</code>
Resultado esperado	<pre>root@VC-WEB-IonaFrance-V100-02:/etc/fail2ban/jail.d# mv -vi defaults-debian.conf defaults-debian.conf.orig renamed 'defaults-debian.conf' -> 'defaults-debian.conf.orig'</pre>

Paso	Hacer una copia de seguridad del fichero defaults-debian.conf
Comando	<code>cp -vi defaults-debian.conf.orig defaults-debian.conf</code>
Resultado esperado	<pre>root@VC-WEB-IonaFrance-V100-02:/etc/fail2ban/jail.d# cp defaults-debian.conf.orig defaults-debian.conf root@VC-WEB-IonaFrance-V100-02:/etc/fail2ban/jail.d# █</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero defaults-debian.conf

Paso	Editar el fichero defaults-debian.conf
Comando	<code>vi defaults-debian.conf</code>

En el fichero defaults-debian.conf hay que poner la palabra "true".

```
[sshd]
enabled = true
```

Paso	Entrar en el directorio action
Comando	<code>cd /etc/fail2ban/action</code>
Resultado esperado	<pre>root@VC-WEB-Ismafranca-V100-02:/etc/fail2ban/jail.d# cd .. root@VC-WEB-Ismafranca-V100-02:/etc/fail2ban# cd action.d/ root@VC-WEB-Ismafranca-V100-02:/etc/fail2ban/action.d# █</pre>

Paso	Hacer una copia de seguridad del fichero iptables-common.conf
Comando	<code>mv -vi iptables-common.conf iptables-common.conf.orig</code>
Resultado esperado	<pre>root@VC-WEB-Ismafranca-V100-02:/etc/fail2ban/action.d# mv -vi iptables-common.conf iptables-common.conf.orig renamed 'iptables-common.conf' -> 'iptables-common.conf.orig'</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Hacer una copia de seguridad del fichero iptables-common.conf
Comando	<code>cp iptables-common.conf.orig iptables-common.conf</code>
Resultado esperado	

Modificar el fichero iptables-common.conf

Paso	Editar el fichero iptables-common.conf
Comando	<code>vi iptables-common.conf</code>

Se configura la línea de **blocktype** para poner la palabra "DROP"
(Comentar la línea con #wkwbantime y añadirla abajo para modificarla)

```
#wkw blocktype = REJECT --reject-with icmp6-port-unreachable
blocktype = DROP
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero serCen.conf

Paso	Editar el fichero serCen.conf
Comando	<code>vi /etc/fail2ban/jail.d/serCen.conf</code>

Copiar el contenido que está debajo y copiarlo en el fichero serCen.conf

```
[serCen]
enabled = true
port = 80,443
protocol = tcp
filter = serCen
blocktype = DROP
action = %(action_)s[blocktype=%(blocktype)s]
logpath = /var/log/serCen/serCen.log
bantime = 900
findtime = 600
maxretry = 10
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero vivait.conf

Paso	Editar el fichero vivait.conf
Comando	<code>vi /etc/fail2ban/jail.d/vivait.conf</code>

Copiar el contenido que está debajo y copiarlo en el fichero vivait.conf

```
[vivait-janus]
enabled = true
port = 80,443
filter = vivait-janus
blocktype = DROP
action = %(action_)s[blocktype=%(blocktype)s]
logpath = /var/log/janus/janus.log
bantime = 900
findtime = 600
maxretry = 10
```

```
[vivait-nginx]
enabled = true
port = 80,443
filter = vivait-nginx
blocktype = DROP
action = %(action_)s[blocktype=%(blocktype)s]
logpath = /var/log/nginx/access.log
# hay bastantes falsos positivos
bantime = 900
findtime = 600
maxretry = 100
```

~

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero vivait-janus.conf

Paso	Editar el fichero vivait-janus.conf
Comando	<code>vi /etc/fail2ban/filter.d/vivait-janus.conf</code>

Copiar el contenido que está debajo y copiarlo en el fichero vivait-janus.conf

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = janus
failregex = TRUCO_KO \[<HOST>\]
ignoreregex =

~
```

Paso	Renombrar el fichero vivait-apache.conf a vivait-nginx.conf
Comando	<code>mv -vi /etc/fail2ban/filter.d/vivait-apache.conf vivait-nginx.conf</code>
Resultado esperado	

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero vivait-nginx.conf

Paso	Editar el fichero vivait-nginx.conf
Comando	<code>vi /etc/fail2ban/filter.d/vivait-nginx.conf</code>

Copiar el contenido que está debajo y copiarlo en el fichero vivait-nginx.conf

[INCLUDES]

before = botsearch-common.conf

[Definition]

_daemon = nginx

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD|CONNECT) \/?\S* \S+\\" .+\$

```
ignoreregex = ^<HOST> \-.*\http-bind\?.*\\" 200
               ^<HOST> \-.*\janus\/?.*\\" (200|304)
               ^<HOST> \-.*\webfon2\/?.*\\" (200|304)
               ^<HOST> \-.*\webrtc-test\/?.*\\" (200|304)
               ^<HOST> \-.*\Vivait-FonB0\/?.*\\" (200|304)
               ^<HOST> \-.*\css\?.*\\" (200|304)
               ^<HOST> \-.*\images\?.*\\" (200|304)
               ^<HOST> \-.*\lang\?.*\\" (200|304)
               ^<HOST> \-.*\libs\?.*\\" (200|304)
               ^<HOST> \-.*\fonts\?.*\\" (200|304)
               ^<HOST> \-.*\static\?.*\\" (200|304)
```

~
~

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Cambiar nombre del fichero vivait-apache.conf a vivait-nginx.conf

Paso	Entrar en el directorio /etc/fail2ban/filter.d/
Comando	<code>cd /etc/fail2ban/filter.d</code>
Resultado esperado	<pre>root@VC-VEB-Sosafranca-VIG-02:/etc/fail2ban/jail.d# cd .. root@VC-VEB-Sosafranca-VIG-02:/etc/fail2ban# cd filter.d/ root@VC-VEB-Sosafranca-VIG-02:/etc/fail2ban/filter.d# █</pre>

Paso	Cambiar nombre del fichero vivait-apache.conf a vivait-nginx.conf
Comando	<code>mv -vi vivait-apache.conf vivait-nginx.conf</code>
Resultado esperado	<pre>root@VC-VEB-Sosafranca-VIG-02:/etc/fail2ban/filter.d# mv -vi vivait-apache.conf vivait-nginx.conf renamed 'vivait-apache.conf' -> 'vivait-nginx.conf'</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Modificar el fichero vivait-nginx.conf

Paso	Modificar fichero /etc/fail2ban/filter.d/vivait-nginx.conf
Comando	<code>vi vivait-nginx.conf</code>

Copiar el contenido que está debajo y copiarlo en el fichero vivait-nginx.conf

[INCLUDES]

before = botsearch-common.conf

[Definition]

_daemon = nginx

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD|CONNECT) \/?\S* \S+\\" .+&

```
ignoreregex = ^<HOST> \-.*\http-bind\?.*\\" 200
              ^<HOST> \-.*\janus\/?.*\\" (200|304)
              ^<HOST> \-.*\webfon2\/?.*\\" (200|304)
              ^<HOST> \-.*\webrtc-test\/?.*\\" (200|304)
              ^<HOST> \-.*\Vivait-FonB0\/?.*\\" (200|304)
              ^<HOST> \-.*\css\?.*\\" (200|304)
              ^<HOST> \-.*\images\?.*\\" (200|304)
              ^<HOST> \-.*\lang\?.*\\" (200|304)
              ^<HOST> \-.*\libs\?.*\\" (200|304)
              ^<HOST> \-.*\fonts\?.*\\" (200|304)
              ^<HOST> \-.*\static\?.*\\" (200|304)
```

~
~

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Iniciar fail2ban

Paso	Iniciar fail2ban
Comando	<code>/etc/init.d/fail2ban start</code>
Resultado esperado	<pre>root@VC-WEB-ZonaFranca-V100-02:/etc/fail2ban/filter.d# /etc/init.d/fail2ban start Starting fail2ban (via systemctl): fail2ban.service.</pre>

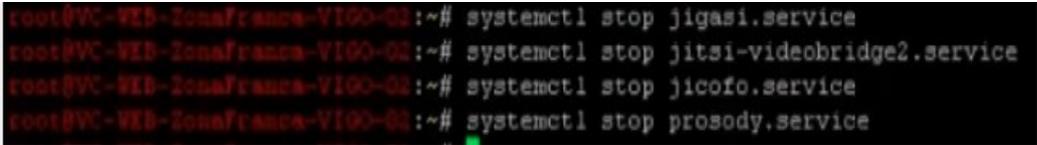
Paso	Comprobar que fail2ban funciona correctamente
Comando	<code>/etc/init.d/fail2ban status</code>
Resultado esperado	<pre>root@VC-WEB-ZonaFranca-V100-02:/etc/fail2ban/filter.d# /etc/init.d/fail2ban status fail2ban.service - Fail2Ban Service Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled) Active: active (running) since Tue 2022-01-18 12:17:49 UTC; 4s ago Docs: man:fail2ban(1) Process: 3118581 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS) Main PID: 3118230 (#2b/server) Tasks: 0 (limit: 9447) Memory: 248.0K CGroup: /system.slice/fail2ban.service └─ 3118230 /usr/bin/python /usr/bin/fail2ban-server --async -b -s /var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid --loglevel INFO --logtarget /var/log/fail2ban.log ene 18 12:17:49 VC-WEB-ZonaFranca-V100-02 systemd[1]: Starting Fail2Ban Service... ene 18 12:17:49 VC-WEB-ZonaFranca-V100-02 systemd[1]: Started Fail2Ban Service. ene 18 12:17:49 VC-WEB-ZonaFranca-V100-02 fail2ban-server[3118582]: 2022-01-18 12:17:49,585 fail2ban [3118582]: ERROR Server already running ene 18 12:17:49 VC-WEB-ZonaFranca-V100-02 fail2ban-server[3118582]: 2022-01-18 12:17:49,586 fail2ban [3118582]: ERROR Async configuration of server failed</pre>

Paso	Reiniciar fail2ban-client
Comando	<code>fail2ban-client restart</code>
Resultado esperado	<pre>root@VC-WEB-ZonaFranca-V100-02:/etc/fail2ban/filter.d# fail2ban-client restart Shutdown successful Server ready</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Parar servicios innecesarios

Paso	Parar servicio jigasi.service Parar servicio jitsi-videobridge2.service Parar servicio jicofo.service Parar servicio systemctl stop prosody.service
Comando	<pre>systemctl stop jigasi.service</pre> <pre>systemctl stop jitsi-videobridge2.service</pre> <pre>systemctl stop jicofo.service</pre> <pre>systemctl stop prosody.service</pre>
Resultado esperado	 <pre>root@VC-VIB-2osafranca-V100-01:~# systemctl stop jigasi.service root@VC-VIB-2osafranca-V100-01:~# systemctl stop jitsi-videobridge2.service root@VC-VIB-2osafranca-V100-01:~# systemctl stop jicofo.service root@VC-VIB-2osafranca-V100-01:~# systemctl stop prosody.service</pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Deshabilitar servicios

Paso	Deshabilitar arranque del servicio jigasi.service Deshabilitar arranque del servicio jitsi-videobridge2.service Deshabilitar arranque del servicio jicofo.service Deshabilitar arranque del servicio prosody.service
Comando	<pre>systemctl disable jigasi.service</pre> <pre>systemctl disable jitsi-videobridge2.service</pre> <pre>systemctl disable jicofo.service</pre> <pre>systemctl disable prosody.service</pre>
Resultado esperado	<pre>root@VC-WEB-2024franco-V100-Q2:~# systemctl disable prosody.service Synchronizing state of prosody.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /lib/systemd/systemd-sysv-install disable prosody Removed /etc/systemd/system/multi-user.target.wants/prosody.service. root@VC-WEB-2024franco-V100-Q2:~# systemctl disable jigasi.service Synchronizing state of jigasi.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /lib/systemd/systemd-sysv-install disable jigasi Removed /etc/systemd/system/multi-user.target.wants/jigasi.service. root@VC-WEB-2024franco-V100-Q2:~# systemctl disable jitsi-videobridge2.service Synchronizing state of jitsi-videobridge2.service with SysV service script with /lib/systemd/systemd-sysv-install. Executing: /lib/systemd/systemd-sysv-install disable jitsi-videobridge2 Removed /etc/systemd/system/multi-user.target.wants/jitsi-videobridge2.service. root@VC-WEB-2024franco-V100-Q2:~# systemctl disable jicofo.service jicofo.service is not a native service, redirecting to systemd-sysv-install. Executing: /lib/systemd/systemd-sysv-install disable jicofo</pre>

Paso	Reiniciar la máquina
Comando	<pre>reboot</pre>

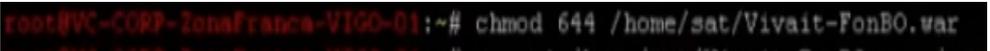
Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



3.5 Subir FonBo.war a Tomcat .

Subir el archivo Vivait-FonBo.war a la máquina de Tomcat . Poner el archivo en una carpeta como por ejemplo /home/sat (Después se moverá ese archivo a otra carpeta)

Paso	Cambiar los permisos del archivo Vivait-FonBo.war
Comando	<code>chown root:root /home/sat/Vivait-FonBo.war</code>
Resultado esperado	

Paso	Cambiar los permisos del archivo FonBo.war
Comando	<code>chmod 644 /home/sat/Vivait-FonBo.war</code>
Resultado esperado	

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Paso	Renombrar el archivo Vivait-FonBo.war
Comando	<code>mv Vivait-FonBo.war Vivait-Fonbo.war.orig</code>
Resultado esperado	<pre> root@VC-CORP-IonaFrance-VIGG-01:/var/lib/tomcat9/webapps# mv Vivait-FonBO.war Vivait-FonBO.war.orig root@VC-CORP-IonaFrance-VIGG-01:/var/lib/tomcat9/webapps# ls -l total 223156 drwxr-x--- 4 tomcat tomcat 4096 dic 14 12:18 CargaContactos -rw-r--r-- 1 root root 815667 jun 21 2021 CargaContactos.war drwxr-x--- 4 tomcat tomcat 4096 dic 14 12:18 ChatWebService -rw-r--r-- 1 root root 4616533 jun 7 2021 ChatWebService.war drwxr-x--- 4 tomcat tomcat 4096 dic 14 12:18 ClicktoCall -rw-r--r-- 1 root root 1965800 jun 7 2021 ClicktoCall.war drwxr-x--- 4 tomcat tomcat 4096 dic 14 12:18 GeneraConf -rw-r--r-- 1 root root 3744355 jun 25 2021 GeneraConf.war drwxr-xr-x 3 root root 4096 dic 13 13:49 ROOT drwxr-x--- 12 tomcat tomcat 4096 dic 14 12:18 Vivait-Call -rw-r--r-- 1 root root 27053953 jun 7 2021 Vivait-Call.war -rw-r--r-- 1 root root 49956505 jun 7 2021 Vivait-FonBO.war.orig drwxr-x--- 6 tomcat tomcat 4096 dic 14 12:18 Vivait-Supervisor -rw-r--r-- 1 root root 60016834 jun 7 2021 Vivait-Supervisor.war drwxr-x--- 6 tomcat tomcat 4096 dic 13 13:50 Vivait-Tracker -rw-r--r-- 1 root root 19535940 jun 7 2021 Vivait-Tracker.war drwxr-x--- 11 tomcat tomcat 4096 dic 14 12:18 Vivait-Usuario -rw-r--r-- 1 root root 60034523 jun 7 2021 Vivait-Usuario.war drwxr-x--- 4 tomcat tomcat 4096 dic 14 12:18 WSActualizaXML -rw-r--r-- 1 root root 708836 jun 7 2021 WSActualizaXML.war </pre>

Paso	Mover el archivo FonBo.war a var/lib/tomcat9/webapps/
Comando	<code>mv -vi /home/sat/Vivait-FonBo.war /var/lib/tomcat9/webapps/</code>
Resultado esperado	<pre> root@VC-CORP-IonaFrance-VIGG-01:~# mv -vi /home/sat/Vivait-FonBO.war /var/lib/tomcat9/webapps/ </pre>

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Proteger Nginx con Let's Encrypt

Obtener un certificado SSL

Certbot ofrece varias alternativas para obtener certificados SSL a través de complementos. El complemento de Nginx se encargará de reconfigurar Nginx y volver a cargar la configuración cuando sea necesario. Para utilizar este complemento, escriba lo siguiente (sustituyendo example.com por el nombre de dominio de la maquina. Dicho nombre **a de resolverse desde internet**):

- `sudo certbot --nginx -d example.com -d www.example.com`

Esto ejecuta certbot con el complemento --nginx, usando -d para especificar los nombres de dominio para los que queremos que el certificado sea válido.

Si es la primera vez que ejecuta certbot, se le pedirá que ingrese una dirección de correo electrónico y que acepte las condiciones de servicio. Después de esto, certbot se comunicará con el servidor de Let's Encrypt y realizará una comprobación a fin de verificar que usted controle el dominio para el cual solicite un certificado.

Si la comprobación se realiza correctamente, certbot le preguntará cómo desea configurar sus ajustes de HTTPS:

Output

```
Please choose whether or not to redirect HTTP traffic to HTTPS,
removing HTTP access.
```

```
- - - - -
```

```
1: No redirect - Make no further changes to the webserver configuration.
```

```
2: Redirect - Make all requests redirect to secure HTTPS access.
```

```
Choose this for
new sites, or if you're confident your site works on HTTPS. You
can undo this
change by editing your web server's configuration.
```

```
- - - - -
```

```
Select the appropriate number [1-2] then [enter] (press 'c' to
cancel):
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Seleccione su elección y luego ENTER. La configuración se actualizará y Nginx se volverá a cargar para aplicar los ajustes nuevos. certbot concluirá con un mensaje que le indicará que el proceso tuvo éxito e indicará la ubicación de almacenamiento de sus certificados:

Output

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/example.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/example.com/privkey.pem
Your cert will expire on 2020-08-18. To obtain a new or tweaked version of this certificate in the future, simply run certbot again
with the "certonly" option. To non-interactively renew *all* of your certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>

Donating to EFF: <https://eff.org/donate-le>

Así, sus certificados se quedarán descargados, instalados y cargados. Intente volver a cargar su sitio web utilizando https:// y observe el indicador de seguridad de su navegador. Debería indicar que el sitio cuenta con la protección correcta, en general, con un ícono de un candado. Si prueba su servidor utilizando [SSL Labs Server Test](#), obtendrá una calificación **A**.

Terminaremos con una prueba del proceso de renovación.

Verificar la renovación automática de Certbot

Los certificados de Let's Encrypt son válidos únicamente por noventa días. El propósito de esto es incentivar a los usuarios a automatizar sus procesos de renovación de certificados. El paquete certbot que instalamos se ocupa de esto por nosotros añadiendo un temporizador systemd que se ejecutará dos veces al día y renovará automáticamente cualquier certificado que vaya a vencer en los próximos 30 días.

Puede consultar el estado del temporizador con systemctl:

```
sudo systemctl status certbot.timer
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Output

```
certbot.timer - Run certbot twice daily
Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
Active: active (waiting) since Mon 2020-05-04 20:04:36 UTC; 2 weeks 1 days ago
Trigger: Thu 2020-05-21 05:22:32 UTC; 9h left
Triggers: certbot.service
```

Para probar el proceso de renovación, puede hacer un simulacro con certbot:

```
sudo certbot renew --dry-run
```

Si no ve errores, estará listo. Cuando sea necesario, Certbot renovará sus certificados y volverá a cargar Nginx para registrar los cambios. Si el proceso de renovación automática falla, Let's Encrypt enviará un mensaje a la dirección de correo electrónico que especificó en el que se le advertirá cuándo se aproxime la fecha de vencimiento de sus certificados.

3.6 Crear script escobatoken.pl

Crear el archivo escobaToken.pl en /usr/local/sbin

Este script sera el encargado de borrar los registros de token de la base de datos que son ya inservibles, haciendo así la tabla mas manejable.

El contenido del script:

```
#!/usr/bin/perl

use DBI;
use strict;
use warnings;
use Getopt::Long;
use Log::Log4perl;
#use Switch;

use feature qw/switch/;

no warnings 'uninitialized';
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



```

# Inicializamos el log
#
my $log_conf = q(
    log4perl.rootLogger          = DEBUG, LOG1
    log4perl.appender.LOG1      = Log::Log4perl::Appender::File
    log4perl.appender.LOG1.filename = /var/log/escobaToken.log
    log4perl.appender.LOG1.mode   = append
    log4perl.appender.LOG1.layout = Log::Log4perl::Layout::atternLayout
    log4perl.appender.LOG1.layout.ConversionPattern = %d %p %m %n
);
Log::Log4perl::init(\$log_conf);

my $logger = Log::Log4perl->get_logger();

my $filas=1;
my $totFilas=0;
my $dbh;
my $sth;
my $query;
my $res;

# Lee los parámetros en una variable rh_params
my $rh_params = {};
#s Cadena obligatoria
#s Cadena opcional
#i Entero obligatorio
#i Entero opcional
GetOptions($rh_params,
    'hDB=s',
    'ayuda',
);

# Si se ha especificado el parámetro 'ayuda', imprimir la ayuda y abandonar
$rh_params->{ayuda} && imprime_ayuda( 0 );

unless (defined $rh_params->{hDB})
{
    $logger->logdie("ERROR: Falta param --hDB");
    imprime_ayuda(1);
}

sub imprime_ayuda {
    my $exit_status = shift;

    print <<"END"

    Uso: escobamcan.pl [parametros]

    Lee un fichero y genera un informe
    Todos los parámetros son obligatorios si no se indica lo contrario:

        --hDB: Servidor BD Nimitz a la que conectarse

```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



--ayuda: imprime esta ayuda (opcional)

```

END
;
    exit $exit_status;
}

#Datos de la conexión
my $db="nimitz";
my $host=$rh_params->{hDB};
my $port="3306";
my $userid="root";
my $passwd="ivivamysql";
my $connectionInfo="DBI:mysql:database=$db;$host:$port";

sub handle_error {
    my $message = shift;
    $logger->error("Error al conectar a $host: $message");
    exit;
}

# Realizamos la conexión a la base de datos
$dbh = DBI->connect($connectionInfo,$userid,$passwd) or handle_error(DBI->errstr);

# Empieza el programa
$logger->info("Conectado a la base de datos $host:$db");

#Desactivamos la copia a la réplica
$query = "set SQL_LOG_BIN=0";
$sth = $dbh->prepare($query);
$res = $sth->execute();

$logger->info("Borrando tabla DAT_TOKENS");

$query = "DELETE FROM DAT_TOKENS WHERE (D_HORA_FIN < DATE_SUB(now(), INTERVAL
15 DAY)) OR ((D_HORA_INICIO < DATE_SUB(now(), INTERVAL 15 DAY)) AND
(E_TOKEN_ESTADO<>200)) LIMIT 100";

$logger->info("Query: $query");

while($filas>0)
{
    # Primero hay que "preparar" el query
    $sth = $dbh->prepare($query);

    # Ejecutamos el query
    $filas = $sth->execute();

    if (defined $filas)
    {
        $totFilas = $totFilas + $filas;
    }
}

```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



```
        }
        else
        {
            $logger->warn("Error al borrar de DAT_TOKEN");
        }
    }
    $logger->info("Ejecutada query: $query");
    $filas=1;
    $logger->info("Filas borradas: $totFilas");
    $totFilas=0;

    #Activamos la copia a la réplica
    $query = "set SQL_LOG_BIN=1";
    $sth = $dbh->prepare($query);
    $res = $sth->execute();

    $sth->finish();
    $logger->info("Borrado finalizado");
    $dbh->disconnect;
```

4. COMPROBACIONES

Logrotate.d y cron.d

Comprobar que todos los ficheros que están contenidos en el `logrotate.d` y `cron.d` estén descomentadas sus líneas para que los logs roten y se ejecuten las tareas de forma correcta.

Grabaciones

Para que funcione las grabaciones hace falta ejecutar un ssh desde el usuario vivait de la máquina que corre el recordCentral con destino el usuarioSSH que está puesto en el nodo en el portal de administración.

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Ramdisk

Solo válido nodos que tengan la propiedad de grabar, es decir, todas menos el ACD ya que no posee un dialplan para la grabación.

En `/etc/cron.d/ramDisk`, descomentar la línea:

```
#@reboot root mount -t tmpfs -o  
size=2000M,nr_inodes=10k,mode=0777,uid=asterisk,gid=asterisk tmpfs  
/var/spool/asterisk/monitor
```

Y ajustar el tamaño (size) a la mitad del valor de la RAM de la máquina.

Certbot

Comprobar que certbot funciona correctamente usando el comando `systemctl status certbot.timer`

```
root@VC-WEB-ZonaFranca-VIGO-02:~# systemctl status certbot.timer
● certbot.timer - Run certbot twice daily
   Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
   Active: active (waiting) since Fri 2022-02-04 13:32:32 CET; 5 days ago
   Trigger: Thu 2022-02-10 21:32:36 CET; 12h left
   Triggers: ● certbot.service

feb 04 13:32:32 VC-WEB-ZonaFranca-VIGO-02 systemd[1]: Started Run certbot twice daily.
root@VC-WEB-ZonaFranca-VIGO-02:~# █
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



5.DIAGNÓSTICOS

Herramientas de diagnóstico

Para listar los certificados gestionados por Let's Encrypt

```
sudo certbot-auto certificates
```

Renovar un certificado:

```
sudo certbot-auto renew --cert-name example.org --force-renewal
```

Expedir un nuevo certificado

```
sudo certbot-auto certonly --webroot -w /var/www/example.org -d  
exa
```

Listado de información de serCen

```
nc localhost 1125
```

Error de webfon al recibir una llamada

Se ha detectado un error en el webfon, al recibir una llamada con caller id num vacío muestra el de la llamada anterior. Para resolver este fallo basta con cambiar el plugin `/usr/lib/vivait/plugins/vivait_webfon_plugin.so`

Antes de hacer el cambio se ha de parar janus (`/etc/init.d/janus stop`).

Renombrar el antiguo a `.orig` antes de poner el nuevo. Comprobar que una vez puesto el nuevo plugin tienen los mismos permisos que el `.orig`. Una vez hecho esto arrancar el janus (`/etc/init.d/janus start`)

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



Error de envío de correo desde serCen

Error:	Desde la máquina se envían correos desde el prompt y no hay problemas, fail2ban también envía correos , solo falla cuando se envía desde el serCen.
Log de serCen:	SMT funEnviarTexto code='64/Requested SSL level failed' servidor='10.60.6.86' usuario='vivait'
Solución:	El servidor de correo de cliente no acepta el cifrado ssl (que en la versión anterior estaba forzada) . En la nueva versión no es obligatorio.

Script para enviar correo desde línea comandos

Este script sirve para enviar un correo desde el terminal . En el script se tiene que modificar (FROM , TO , IP , PUERTO Y CLAVE) .

Script:

```
#!/bin/bash
```

```
FROM=""
```

```
TO=""
```

```
ASUNTO="Pruebas de correo para '${TO}' desde '${FROM}'"
```

```
URL="smtp://IP:PUERTO"
```

```
USU=""
```

```
CLV=""
```

```
TMP=$(mktemp /tmp/tmp.XXXXXX)
```

```
echo -ne "From: <${FROM}>\r\n" >${TMP}
```

```
echo -ne "To: <${TO}>\r\n" >>${TMP}
```

```
echo -ne "Subject: ${ASUNTO}\r\n" >>${TMP}
```

Autor: xxxxx	Asunto: xxxxx
Revisado: xxxxxxx	Fecha: xx de xxxx de 20xx



```
echo -ne "\r\n" >>${TMP}
echo -ne "Esto es un mensaje de pruebas:\r\n" >>${TMP}
echo -ne "Desde: ${FROM}\r\n" >>${TMP}
echo -ne "Para: ${TO}\r\n" >>${TMP}
echo -ne "Asunto: ${ASUNTO}\r\n" >>${TMP}
echo -ne "Url: ${URL}\r\n" >>${TMP}
echo -ne "Usuario: ${USU}\r\n" >>${TMP}
echo -ne "Archivo: ${TMP}\r\n" >>${TMP}
```

```
cat >"${TMP}" <<EOF
From: <${FROM}>
To: <${TO}>
Subject: ${ASUNTO}
```

```
Esto es un mensaje de pruebas:
Desde: ${FROM}
Para: ${TO}
Asunto: ${ASUNTO}
Url: ${URL}
Usuario: ${USU}
Archivo: ${TMP}
EOF
```

```
curl -v "${URL}" \
--verbose \
--insecure \
--ssl \
--user "${USU}:${CLV}" \
--mail-from "${FROM}" \
--mail-rcpt "${TO}" \
--upload-file "${TMP}"
```

```
echo "Archivo temporal: ${TMP}"
rm -v "${TMP}"
```