

**ACTIVIDAD 11: VoIP AWS UD**



**UNIVERSIDAD DISTRITAL  
FRANCISCO JOSÉ DE CALDAS**

**KEVIN NICOLÁS SIERRA GONZÁLEZ 20182020151**

**LUIS MIGUEL POLO 20182020158**

**YEISON ALEXANDER FARFAN PERALTA 20201020138**

**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**

**INGENIERÍA DE SISTEMAS**

**TELEINFORMATICA I**

**ANDRES ALEXANDER RODRIGUEZ FONSECA**

**2024-III**

## Objetivos

- Implementar servicios en la nube
- Implementar un servidor Asterisk

## Materiales

- Computador personal con acceso a Internet
- Cuenta activa en AWS EC2 (elastic compute cloud)

## Procedimiento

Desde la consola de AWS específicamente en el servicio EC2 (Echange Compute Cloud) se crea un grupo de seguridad, el cual fue denominado inicialmente como ServicioNubeKLY

EC2 > Grupos de seguridad > sg-0a4eba53661db19b5

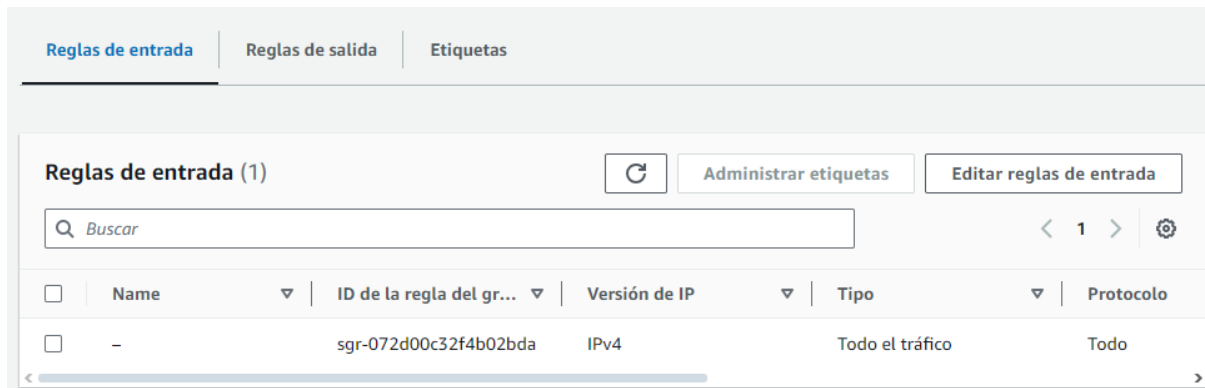
### sg-0a4eba53661db19b5 - ServicioNubeKLY

Acciones ▼

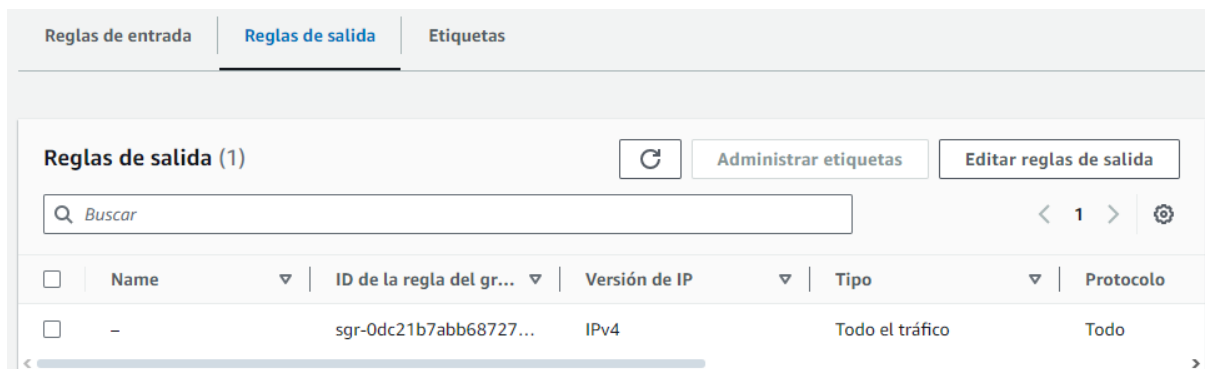
**Detalles**

Nombre del grupo de seguridad ServicioNubeKLY	ID del grupo de seguridad sg-0a4eba53661db19b5	Descripción VoIP	ID de la VPC <a href="#">vpc-032c840bd565ee10f</a>
Propietario 361769595033	Número de reglas de entrada 1 Entrada de permiso	Número de reglas de salida 1 Entrada de permiso	

Se establece las reglas de entrada para permitir el tráfico entrante, donde se permite todo el tráfico, es decir, hacia el servidor, con la versión IPv4



Se establece las reglas de salida donde se permite todo el tráfico, con la versión IPv4



## Proceso de creación de la instancia por medio de la distribución CentOS

Se busca CentOS por medio del siguiente enlace:

ProComputers CentOS-7.9-x86\_64-Minimal-8GiB-HVM-20240203\_142453-b4e1cdfa-6b17-40cf-a9d8-8cfae972ea84

Esta versión es accesible de manera gratuita

✕
▼

**AMI de inicio rápido (0)**  
 AMI de uso común

**Mis AMI (0)**  
 Creado por mí

**AMI de AWS Marketplace (6822)**  
 AWS y AMI de terceros de confianza

**AMI de la comunidad (1)**  
 Publicadas por cualquiera

☐ Gentoo  
☐ macOS  
☐ openSUSE  
☐ Otros sistemas Linux  
☐ Red Hat  
☐ SUSE Linux  
☐ Ubuntu  
**▼ Windows**  
☐ Todos los de Windows

**Proveedor verificado**

**ProComputers CentOS-7.9-x86\_64-Minimal-8GiB-HVM-20240203\_142453-b4e1cdfa-6b17-40cf-a9d8-8cfae972ea84**  
 ami-070fe26fce9a5f8fb  
 CentOS 7 Minimal Install Golden AMI Template (CentOS Linux 7.9) (CentOS 7.9) (centos7)  
 OwnerAlias: aws-marketplace    Plataforma: Cent OS  
 Arquitectura: x86\_64    Propietario: 679593333241  
 Fecha de publicación: 2024-02-03  
 Tipo de dispositivo raíz: ebs    Virtualización: hvm  
 Activado para ENA: Sí

**Seleccionar**

La instancia por crear es montada dentro del servidor t2.small ya que es un servicio moderado y gratuito, esta instancia se nombra como: ServerVoIP.

Es necesario antes de crear la instancia, crear el par de claves del algoritmo RSA: la clave pública y la clave privada. El fichero a generar (donde contendrá el par de claves) tendrá la extensión .ppk

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

**Tipo de par de claves**

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

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

**Formato de archivo de clave privada**

☐ .pem  
 Para usar con OpenSSH

☒ .ppk  
 Para usar con PuTTY

Cuando se le solicite, almacene la clave privada en un lugar seguro y accesible del equipo. **Lo necesitará más adelante para conectarse a la instancia.** [Más](#)

Cancelar

Crear par de claves

Después el fichero es descargado al oprimir “crear par de claves”

Luego se selecciona el grupo de seguridad creado anteriormente: ServicioNubeKLY

▼ Configuraciones de red

Información

Editar

Red

Información

vpc-032c840bd565ee10f

Subred

Información

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública

Información

Habilitar

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

Firewall (grupos de seguridad)

Información

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☐ Crear grupo de seguridad

☒ Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes

Información

Seleccionar grupos de seguridad

▼

Compare reglas de

La instancia ahora es creada al oprimirse “Lanzar Instancias”

✓ Correcto

El lanzamiento de la instancia se inició correctamente (i-068b9c5918d7d3042)

► Registro de lanzamiento

Pasos siguientes

Crear alertas de uso del nivel gratuito y facturación

Para administrar los costos y evitar facturas sorpresa, configure las notificaciones por correo electrónico para los umbrales de uso del nivel gratuito y facturación.

Crear alertas de facturación

🔗

Conectarse a la instancia

Una vez que la instancia esté en ejecución, inicie sesión en ella desde el equipo local.

Conectarse a la instancia

🔗

Más información

🔗

Conectar una base de datos de RDS

Configure la conexión entre una instancia de EC2 y una base de datos para permitir el flujo de tráfico entre ellas.

Conectar una base de datos de RDS

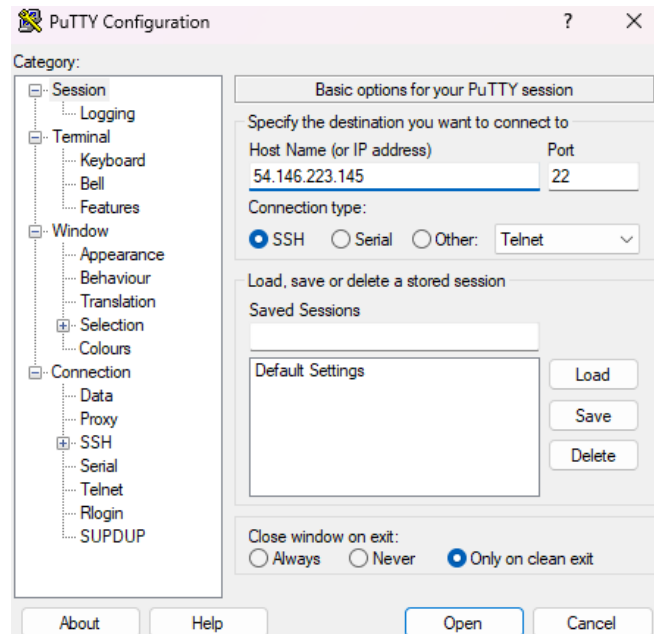
🔗

La instancia creada ServerVoIP puede verse en el listado de instancias, y estado de “En ejecución” y genera una dirección pública (servidor) y privada

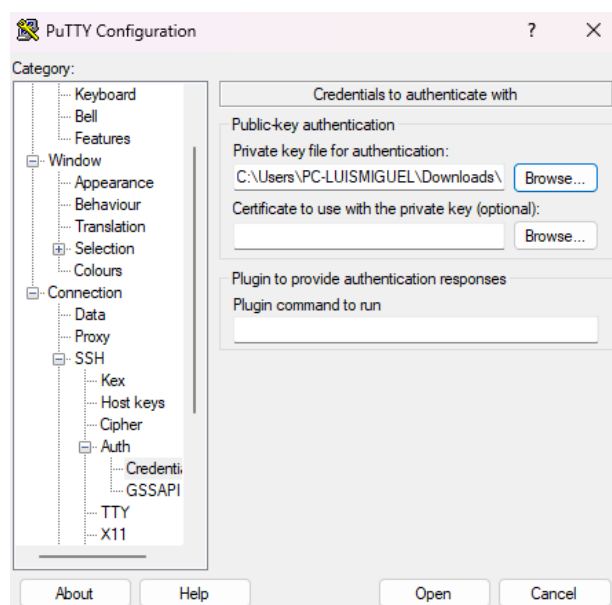
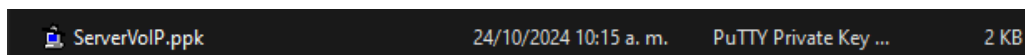
Instancias (1/1) Información							
Última actualización Hace less than a minute		Conectar	Estado de la instancia ▼	Acciones ▼	Lanzar instancias ▼		
<input type="text" value="Buscar Instancia por atributo o etiqueta (case-sensitive)"/>				Todos los estados ▼		< 1 > ⚙	
✓	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al	Zona
✓	ServerVoIP	i-09806a9055aa874e1	✓ En ejecución 🔍	t2.small	🕒 Inicializando	Ver alarmas +	us-e

Se instala PuTTY que es un cliente SSH o Telnet, para hacer una conexión remota como se muestra a continuación.

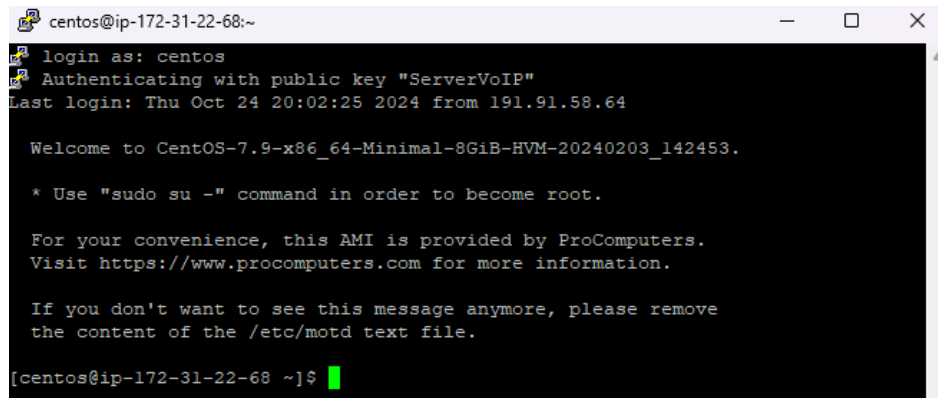
Se coloca la dirección pública del servidor dentro de la categoría “Session” de la interfaz de configuración PuTTY, que en este caso es 54.146.223.145, y se establece el tipo de conexión como SSH.



Luego se ubica a la siguiente ruta dentro de la interfaz de la configuración de PuTTY: Connection>SSH>Auth>Credentials. Y se coloca el fichero .ppk (serverVoIP) dentro del campo de “Archivo de la clave privada para autenticación” y se le da abrir



Al oprimir el botón “Open” (abrir) aparece una terminal o CLI proporcionado por PuTTY. Y aparecerá un campo para logearse como “login as” donde se coloca “centos”, la distribución elegida.



```
centos@ip-172-31-22-68:~
login as: centos
Authenticating with public key "ServerVoIP"
Last login: Thu Oct 24 20:02:25 2024 from 191.91.58.64

Welcome to CentOS-7.9-x86_64-Minimal-8GiB-HVM-20240203_142453.

* Use "sudo su -" command in order to become root.

For your convenience, this AMI is provided by ProComputers.
Visit https://www.procomputers.com for more information.

If you don't want to see this message anymore, please remove
the content of the /etc/motd text file.

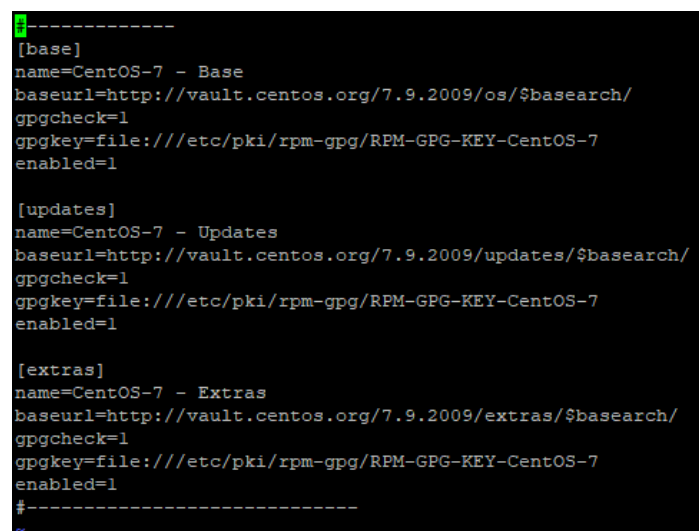
[centos@ip-172-31-22-68 ~]$
```

Se accede a la siguiente ruta para configurar centOS, ya que es necesario modificarlo para cambiar sus repositorios a versiones anteriores

```
[centos@ip-172-31-22-68 ~]# sudo vi /etc/yum.repos.d/CentOS-Base.repo
```

```
[root@ip-172-31-22-68 asterisk-20.10.0]# cd
[root@ip-172-31-22-68 ~]# sudo vi /etc/yum.repos.d/CentOS-Base.repo
```

Adentro del repositorio, se elimina todo lo que está en comentario, y se coloca la siguiente configuración



```
~
[base]
name=CentOS-7 - Base
baseurl=http://vault.centos.org/7.9.2009/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1

[updates]
name=CentOS-7 - Updates
baseurl=http://vault.centos.org/7.9.2009/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1

[extras]
name=CentOS-7 - Extras
baseurl=http://vault.centos.org/7.9.2009/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
#~
~
```

Se instala algunas actualizaciones y complementos. Luego se desactiva el Security-Exchange Linux (SELinux) para permitir acceso con el siguiente comando:

vi /etc/selinux/config

Para esto se cambia el estado “enforcing” a “disabled”

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are protected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Se descarga Asterisk en el siguiente repositorio

<https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20.10.0.tar.gz>

```
[root@ip-172-31-92-4 src]# wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20.10.0.tar.gz
--2024-10-22 03:53:10-- https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20.10.0.tar.gz
Resolving downloads.asterisk.org (downloads.asterisk.org)... 165.22.184.19, 2604:a880:400:d0::14:9001
Connecting to downloads.asterisk.org (downloads.asterisk.org)|165.22.184.19|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28309321 (27M) [application/octet-stream]
Saving to: 'asterisk-20.10.0.tar.gz'

100%[=====>] 28,309,321  40.4MB/s  in 0.7s

2024-10-22 03:53:11 (40.4 MB/s) - 'asterisk-20.10.0.tar.gz' saved [28309321/28309321]
```

Se descomprime el repositorio descargando:

```
[root@ip-172-31-92-4 src]# tar -zxvf asterisk-20.10.0.tar.gz
asterisk-20.10.0/
asterisk-20.10.0/.cleancount
asterisk-20.10.0/.gitignore
asterisk-20.10.0/.lastclean
asterisk-20.10.0/.version
asterisk-20.10.0/BSDmakefile
asterisk-20.10.0/BUGS
asterisk-20.10.0/CHANGES.md
asterisk-20.10.0/COPYING
asterisk-20.10.0/CREDITS
asterisk-20.10.0/ChangeLogs/
asterisk-20.10.0/ChangeLogs/ChangeLog-20.10.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.3.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.3.1.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.4.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.5.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.5.1.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.5.2.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.6.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.7.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.8.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.8.1.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.9.0.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.9.1.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.9.2.md
asterisk-20.10.0/ChangeLogs/ChangeLog-20.9.3.md
asterisk-20.10.0/ChangeLogs/historical/
asterisk-20.10.0/ChangeLogs/historical/CHANGES
asterisk-20.10.0/ChangeLogs/historical/ChangeLog
asterisk-20.10.0/LICENSE
asterisk-20.10.0/Makefile
asterisk-20.10.0/Makefile.moddir_rules
asterisk-20.10.0/Makefile.rules
asterisk-20.10.0/README-SERIOUSLY.bestpractices.md
asterisk-20.10.0/README-addons.txt
asterisk-20.10.0/README.md
asterisk-20.10.0/SECURITY.md
asterisk-20.10.0/Zaptel-to-DAHDI.txt
asterisk-20.10.0/addons/
asterisk-20.10.0/addons/.gitignore
asterisk-20.10.0/addons/Makefile
asterisk-20.10.0/addons/chan_mobile.c
```

Se sitúa a la carpeta de Asterisk versión 20.10.0 con el siguiente comando

```
#cd asterisk-20.10.0
```

Luego se listan sus elementos con el comando “ls”



```
[root@ip-172-31-22-68 asterisk-20.10.0]# ls
addons          configure.ac      menuselect.makeopts
agi             contrib          menuselect-tree
apps            COPYING          missing
autoconf        CREDITS          mkinstalldirs
bootstrap.sh    default.exports  pbx
bridges         defaults.h       phoneprov
BSDmakefile     doc              README-addons.txt
BUGS            formats          README.md
build_tools     funcs            README-SERIOUSLY.bestpractices.md
cdr             images           res
cel             include          rest-api
ChangeLogs      install-sh       rest-api-templates
CHANGES.md     LICENSE          sample.call
channels        main              SECURITY.md
codecs          Makefile          sounds
config.guess     Makefile.moddir_rules  static-http
config.log       Makefile.rules   tests
configs          makeopts         third-party
config.status    makeopts.in      utils
config.sub       menuselect       Zaptel-to-DAHDI.txt
configure        menuselect.makedeps
```

Se instala Asterisk con los comandos

```
#sudo contrib/scripts/install_prereq install
```

```
#./configure --libdir=/usr/lib64 --with-jansson-bundled
```

```

configure: Menumelect build configuration successfully completed

$$$$$$$$$$$$$$$$$=..
      .$7$7..      .7$$7:..
    .$$:..      ,.$7.7
      .$.7.      7$$$$      .$$77
    ..$$..      $$$$$      .$$$7
    ..7$ .?.. $$$$$ .?.. 7$$$..
    $.$. .$$$7. $$$7. 7$$$.. $$$..
    .777.. $$$$$$77$7$77$7$7$7.. $$$..
    $$$~ .7$$$$$$$$$$$$$$7. $$$..
    .$.7 .7$$$$$$$$7: ?$$$..
    $$$ ?7$$$$$$$$$$I .$$$7
    $$$ .7$$$$$$$$$$$$$$ :$$$..
    $$$ $$$$$$7$$$$$$$$$$$$ .$$$..
    $$$ $$$ 7$$$7 .$$$ .$$$..
    $$$ $$$$ $$$$7 .$$$..
    7$$$7 7$$$ 7$$$
    $$$$ $$$$
    $$$7. $$ (TM)
    $$$$$$. .7$$$$$$ $$
    $$$$$$$$$$7$$$$$$$$$. $$$$$$
    $$$$$$$$$$$$$$.

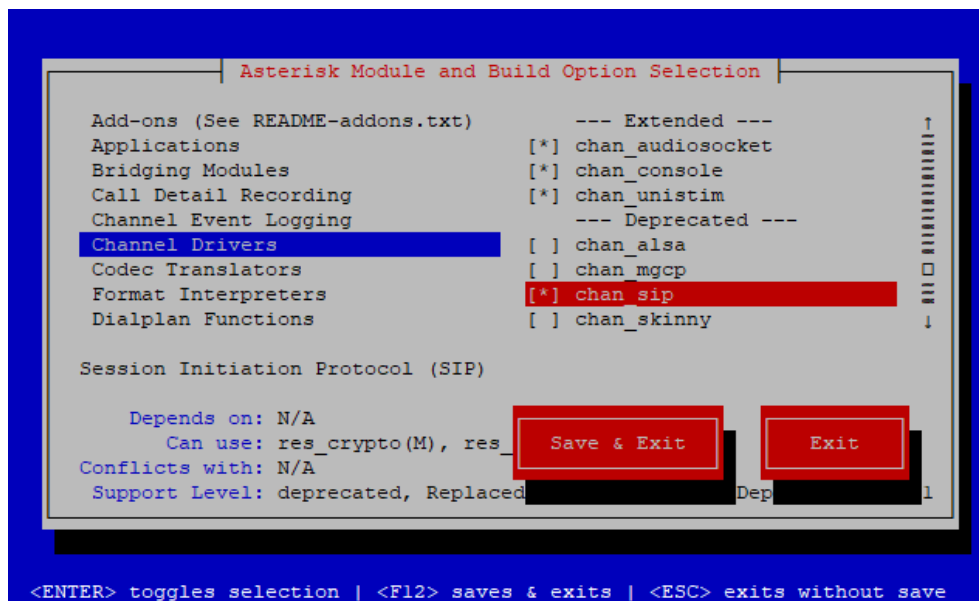
configure: Package configured for:
configure: OS type : linux-gnu
configure: Host CPU : x86_64
configure: build-cpu:vendor:os: x86_64 : pc : linux-gnu :
configure: host-cpu:vendor:os: x86_64 : pc : linux-gnu :
[root@ip-172-31-92-4 asterisk-20.10.0]#

```

Se carga la configuración y se activa el protocolo SIP con el siguiente comando

```
#make menuselect && make && sudo make install && make samples && make config
```

Y se despliega la siguiente interfaz



Para guardar la configuración anterior se hace lo siguiente:

Channel Drivers > Chan\_SIP y presionar Enter, luego Save & Exit

Se activa el servicio de Asterisk y se accede a la consola

```
[root@ip-172-31-22-68 asterisk-20.10.0]# service asterisk start
Starting asterisk (via systemctl): [ OK ]
[root@ip-172-31-22-68 asterisk-20.10.0]# asterisk -r
Asterisk 20.10.0, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 20.10.0 currently running on ip-172-31-22-68 (pid = 912)
ip-172-31-22-68*CLI>
```

Se utiliza el comando sip show peers para listar las extensiones por VoIP creadas, pero no muestra debido a que aún no se han creado.

Para configurar el protocolo SIP se accede al siguiente fichero, con el siguiente comando

```
# vi /etc/asterisk/modules.conf
```

Y se coloca en comentario la línea: ;noload=chan\_sip.so

```
;
noload = res_hep.so
noload = res_hep_pjsip.so
noload = res_hep_rtcp.so
;
; Do not load chan_sip by default, it may conflict with res_pjsip.
;noload = chan_sip.so
;
; Load one of the voicemail modules as they are mutually exclusive.
; By default, load app_voicemail only (automatically).
;
;noload = app_voicemail.so
noload = app_voicemail_imap.so
;noload = app_voicemail_odb.so
```

Se reinicia el servicio con el comando:

```
#service asterisk restart
```

Y el comando:

```
Asterisk -r
```

Ahora se accede al siguiente fichero para crear y configurar las extensiones VoIP

```
[root@ip-172-31-22-68 asterisk-20.10.0]# vi /etc/asterisk/sip.conf
```

Se introduce las siguientes líneas en consola definiéndose la ip pública y privada de la instancia; los números de las extensiones: 101 y 102 respectivamente; cuya contraseña para cada una es secret=123456

Debido a que se cambia la instancia por otra, esto por razones de errores de instalación de un repositorio la dirección ip pública cambia siendo ahora 54.146.233.145 y el grupo de seguridad se denomina ahora ServicioNubeKLY

```
[general]
context=internal
nat=force_rport,comedia ; Manejar dispositivos detrás de NAT
externip= 54.146.233.145 ; Ip publica de la instancia
localnet=172.31.22.68/255.255.240.0 ; Ip privada de la instancia
realm= 54.146.233.145 ; Ip publica de la instancia
rtpstart=10000
rtpend=20000
canreinvite=no ;Asterisk maneja el flujo de audio (RTP)

[101]
type=friend
host=dynamic
secret=123456
context=internal
disallow=all
allow=all
allow=ulaw
allow=alaw
allow=GSM

[102]
type=friend
host=dynamic
secret=123456
context=internal
disallow=all
allow=all
allow=all
allow=ulaw
allow=alaw
allow=gsm
```

Se rebootea la máquina virtual con el comando #reboot y se reincida el servicio de Asterisk

```
[root@ip-172-31-22-68 asterisk-20.10.0]# asterisk -r
Asterisk 20.10.0, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 20.10.0 currently running on ip-172-31-22-68 (pid = 908)
```

Se recarga el servicio SIP, ahora mostrando las extensiones anteriormente creadas y sus características

```

ip-172-31-22-68*CLI> sip reload
ip-172-31-22-68*CLI> sip show peers
Name/username      Host                               Dyn Forcerport
Comedia    ACL Port      Status      Description
101/101                200.118.60.193      D  Auto (No)
No          3491          Unmonitored
102/102                191.91.58.64        D  Auto (No)
No          42593         Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 2 online, 0 offline]

```

## Creación del marcado Dial Plan

Se accede al siguiente fichero para agregar las extensiones y configurar el Dial Plan

```
[root@ip-172-31-22-68 asterisk-20.10.0]# vi /etc/asterisk/extensions.conf
```

Se configura el Dial Plan añadiendo al fichero:

```
[internal]
```

```
exten => 101,1,Dial(SIP/101)
```

```
exten => 102,1,Dial(SIP/102)
```

```

;exten => 6882,1,noOp()
;    same => n,Answer()
;    same => n,PJSIPNotify(,4Event=0
;    same => n,Wait(1)
;    same => n,Hangup()

[internal]
exten => 101,1,Dial(SIP/101)
exten => 102,1,Dial(SIP/102)

```

Por último, se recarga el servicio de Dial Plan con el siguiente comando

```
[root@ip-172-31-22-68 asterisk-20.10.0]# sudo asterisk -rx "dialplan reload"
Dialplan reloaded.
```

## Prueba de funcionamiento

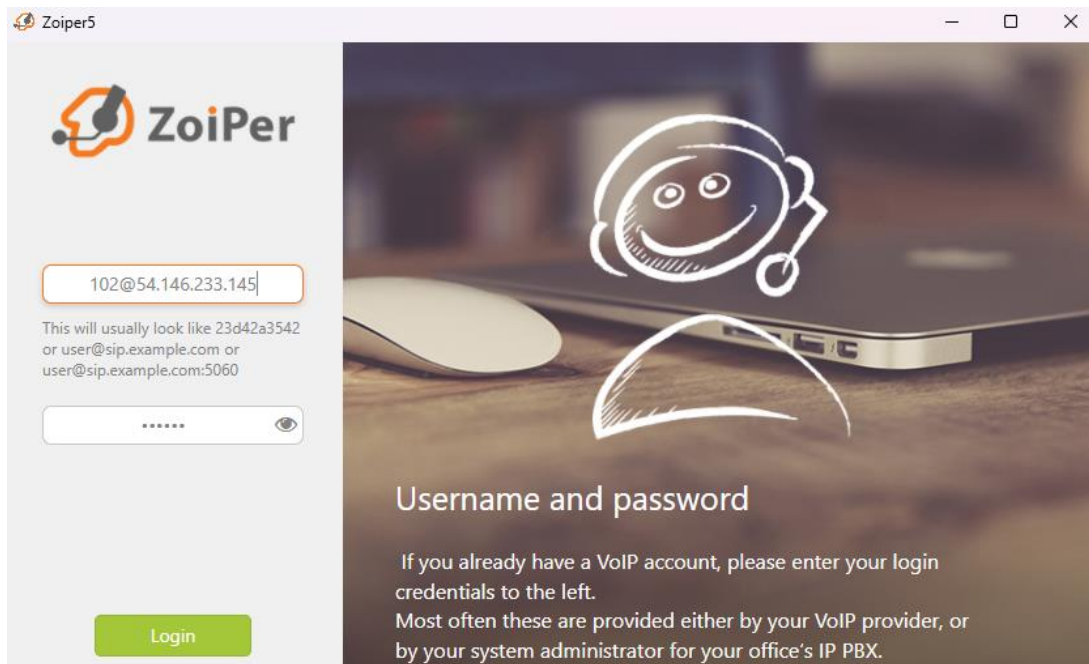
Se descarga e instala el software Zoiper tanto en el pc como en dispositivos móviles que proporciona el servicio de VoIP y marcación a través de extensiones

En el PC, después de instalado Zoiper, se hace un logueo con las siguientes credenciales:

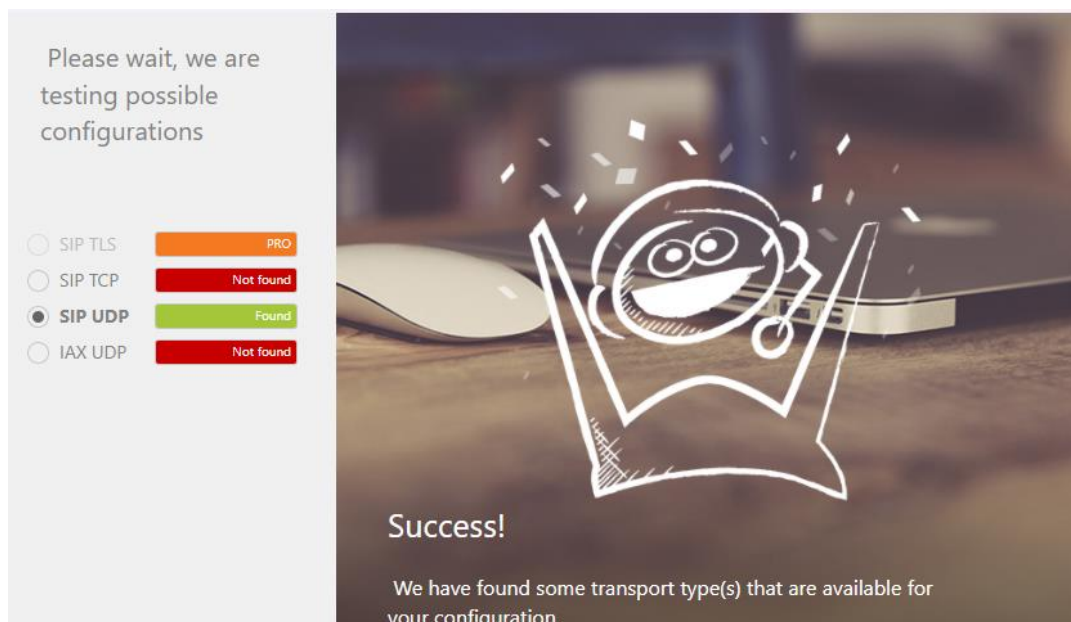
**Nombre de usuario:** [102@54.146.233.145](mailto:102@54.146.233.145)

**Contraseña:** 123456

Donde 102 será la extensión que tendrá el host y 54.146.233.145 la dirección de la ip pública del servidor



Luego después del logueo se despliega varios tipos de configuraciones de transporte, es decir de la transmisión en las llamadas, por medio del protocolo SIP, donde SIP UDP será el protocolo de transporte predeterminado

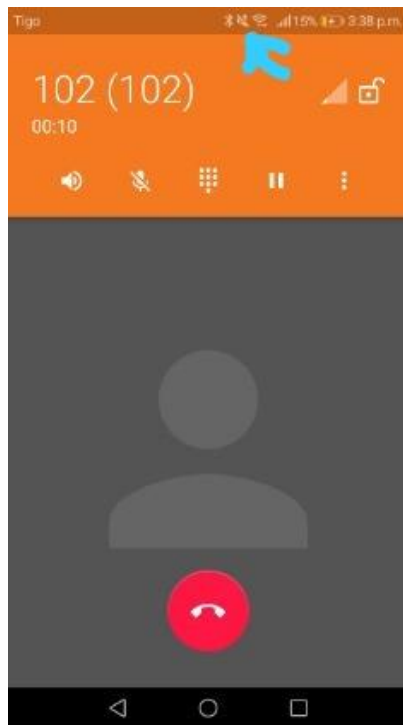


## Realización de llamadas

Se prueba el servicio de VoIP marcando a las extensiones anteriormente configuradas

### Llamada hacia la extensión 102:

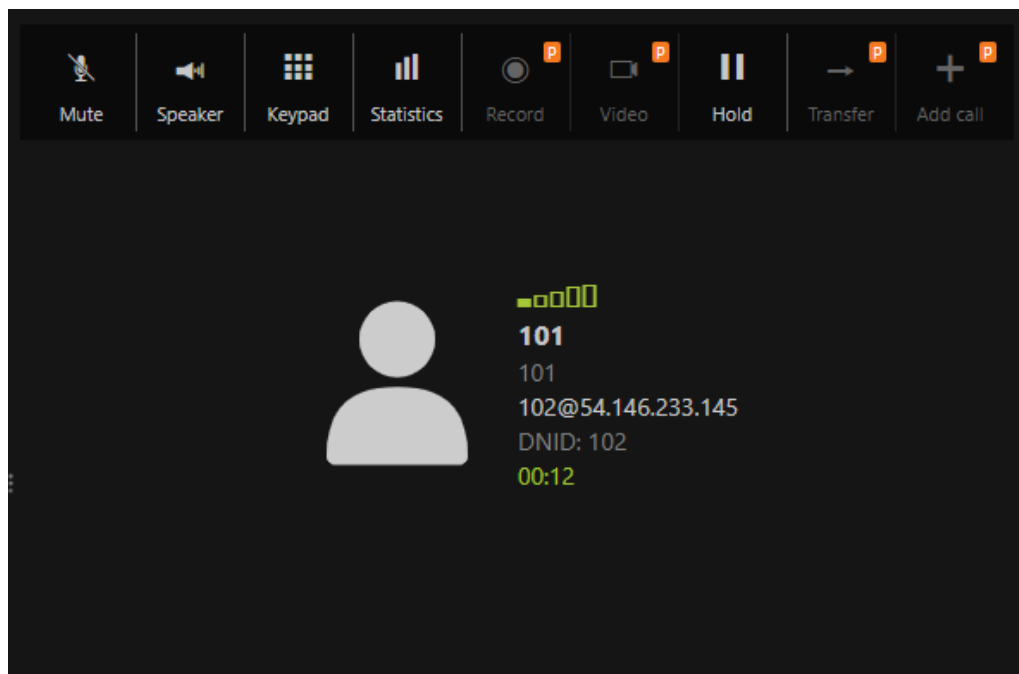
Desde la extensión 101 hacia la extensión 102



Por defecto la aplicación móvil Zoiper version IAX mutea o silencia la llamada al iniciarse.


### **Recepción de la llamada por la extensión 102:**



Se recibe la llamada a través del PC por medio de la extensión 101





### **Historial de las llamadas de la extensión 102:**

Se muestra el historial de llamadas a través del PC desde la extensión 102 hacia la extensión 101:




101











---

Today


Call to **Phone (101)**, rejected.  
Busy Here (code: 486)
3:27 PM 


Call from **Phone (101)**, answered.  
Account: 102@54.146.233.145  
Number: 101  
Duration: 00:09  
Call quality: Excellent  
Local codecs: G.711 mu-law, remote codecs: None
3:39 PM 


Call from **Phone (101)**, answered.
3:40 PM 

## Registro de actividad por consola

Las transmisiones VoIP entre las extensiones 101 y 102 se muestran en consola, se evidencia que hay una advertencia en el proceso de transmisión debido que hay problema de comunicación en las llamadas lo que deben retransmitirse algunos paquetes

```

Packet timed out after 31999ms with no response
[Oct 24 20:40:06] WARNING[986]: chan_sip.c:4177 retrans_pkt: Hanging up call Mly
a7qfOHpBu0CsuQx8aBg.. - no reply to our critical packet (see https://wiki.asteri
sk.org/wiki/display/AST/SIP+Retransmissions).
[Oct 24 20:40:06] WARNING[986][C-00000005]: chan_sip.c:24444 handle_response_inv
ite: Re-invite to non-existing call leg on other UA. SIP dialog '5f8ad4f918d95a4
c6ef57ff702dd5bbc@172.31.22.68:5060'. Giving up.
[Oct 24 20:40:51] WARNING[986]: chan_sip.c:4153 retrans_pkt: Retransmission time
out reached on transmission gkQQF0KaAS2BWQKYb8_iDg.. for seqno 2 (Critical Respo
nse) -- See https://wiki.asterisk.org/wiki/display/AST/SIP+Retransmissions
Packet timed out after 32001ms with no response
[Oct 24 20:40:51] WARNING[986]: chan_sip.c:4177 retrans_pkt: Hanging up call gkQ
QF0KaAS2BWQKYb8_iDg.. - no reply to our critical packet (see https://wiki.asteri
sk.org/wiki/display/AST/SIP+Retransmissions).
[Oct 24 20:40:51] WARNING[986][C-00000006]: chan_sip.c:24444 handle_response_inv
ite: Re-invite to non-existing call leg on other UA. SIP dialog '0308c63a7887952
0458clf0d6534681e@172.31.22.68:5060'. Giving up.
[Oct 24 20:40:51] WARNING[986][C-00000006]: chan_sip.c:24444 handle_response_inv
ite: Re-invite to non-existing call leg on other UA. SIP dialog 'gkQQF0KaAS2BWQK

```

## Análisis y Discusión:

- ¿Cuál es el propósito de Asterisk en un servidor de comunicaciones y cómo interactúa con el protocolo SIP en un entorno basado en CentOS alojado en AWS?

**Rta:**

En un servidor de comunicaciones, el propósito principal de Asterisk es administrar y conectar llamadas telefónicas, ya sea a través de aparatos convencionales o a través de tecnología VoIP. Asterisk proporciona características como el enrutamiento de llamadas, el correo de voz y las conferencias, lo que lo transforma en un instrumento eficiente para gestionar las comunicaciones corporativas de forma adaptable y escalable.

En un ambiente con CentOS en AWS, Asterisk colabora con el protocolo SIP para gestionar las comunicaciones VoIP. SIP es el protocolo estándar empleado para comenzar, cambiar y concluir sesiones de voz y video en tiempo real mediante redes IP. Asterisk utiliza SIP para registrar aparatos, establecer vínculos entre las partes interesadas en comunicarse, discutir las condiciones de la llamada y administrar el tráfico de las comunicaciones de acuerdo a las configuraciones del servidor.

- Describa los pasos principales para configurar Asterisk sobre una distribución CentOS en AWS. ¿Qué desafíos se encontraron y cómo se solucionaron?

**Rta:** Para iniciar una versión de EC2 en AWS, se debe usar CentOS como sistema operativo de base. Es crucial elegir el tamaño del archivo y los recursos apropiados de acuerdo a las demandas del servidor de comunicaciones.

Una vez comenzada la instancia, se requiere ajustar el ambiente instalando actualizaciones y dependencias. Esto conlleva la actualización de los paquetes del sistema a través de yum update y garantizar la instalación de herramientas como wget, gcc y las librerías requeridas para la compilación de Asterisk.

La versión más reciente de Asterisk se puede descargar desde su página web oficial o a través de Wget, descomprimiendo los archivos e instalando el software desde el código original. Esto conlleva la ejecución de un conjunto de comandos como ./configure, make y make install para la compilación e instalación de Asterisk.



Una vez instalado Asterisk, se lleva a cabo la configuración de los archivos vinculados a SIP, usualmente localizados en `/etc/asterisk/sip.conf`, donde se definen las normas para la conexión de los dispositivos VoIP.

Para que Asterisk opere de manera adecuada, es imprescindible establecer las normas de seguridad de la instancia en AWS. Esto conlleva la apertura de puertos en el Grupo de Seguridad, tales como el puerto 5060 para SIP y los puertos 10000-20000 para RTP (Protocolo Real-Time). Finalmente, se llevan a cabo pruebas al configurar dispositivos VoIP y asegurándose de que las llamadas se hayan establecido de manera adecuada.

Uno de los retos habituales al instalar Asterisk en AWS es la adecuada configuración de NAT. Ya que las instancias EC2 generalmente se encuentran detrás de NAT, esto podría generar dificultades con las llamadas VoIP y la transmisión de audio. La respuesta consiste en establecer adecuadamente los parámetros de NAT en `sip.conf`, indicando la dirección pública de la instancia y las redes internas.

- Explicar cómo se configuran las extensiones SIP en Asterisk. ¿Qué consideraciones de seguridad deben tenerse en cuenta al realizar esta configuración?

**Rta:** La configuración de extensiones SIP en Asterisk se lleva a cabo principalmente en el archivo `sip.conf`, en el que se establecen parámetros concretos como el nombre de usuario, la contraseña y los ajustes de red. Cada extensión se establece en una sección concreta, donde se definen parámetros como `host`, que determina si el dispositivo se conecta desde una IP determinada o de cualquier dirección; `secret`, que determina la contraseña; y `context`, que asigna la extensión a un contexto de dialplan específico en el archivo `extensions.conf`. Además, se establecen alternativas como `type`, que determina si la extensión es de tipo amigo, peer o usuario, y `nat`, que facilita la administración de las configuraciones de red si el dispositivo se encuentra detrás de un NAT.

Es crucial la seguridad al establecer extensiones SIP en Asterisk, ya que estos sistemas pueden estar expuestos a ataques como el acceso no permitido y el fraude de llamadas. Para salvaguardar las extensiones, es necesario emplear contraseñas sólidas y exclusivas para cada usuario, evitando combinaciones sencillas que puedan ser detectadas con facilidad por ataques de fuerza bruta. Además, es aconsejable activar el uso de `deny` y `permit` para identificar direcciones IP permitidas y bloquear a las desconocidas. Además, la

implementación de cortafuegos y la restricción de acceso únicamente a las direcciones IP fiables reducen los peligros de intrusión.

- ¿Qué es PJSIP y cuáles son las principales diferencias entre PJSIP y el protocolo SIP tradicional? ¿Por qué se podría preferir usar PJSIP en lugar de SIP en ciertos escenarios?

**Rta:** PJSIP es una serie y biblioteca de programas informáticos que ofrece una versión sofisticada del protocolo SIP para la elaboración de aplicaciones de comunicaciones en tiempo real. En Asterisk, PJSIP funciona como una sustitución y optimización del módulo SIP convencional, proporcionando una arquitectura más contemporánea y adaptable para la administración de las comunicaciones VoIP. PJSIP soporta funciones avanzadas como el control de varios dispositivos por extensión, una integración optimizada con NAT, y una administración eficaz de usuarios, dispositivos y recursos mediante un único archivo de configuración (pjsip.conf), lo que facilita la gestión y el desarrollo del sistema.

Las diferencias fundamentales entre PJSIP y el protocolo SIP clásico (chan\_sip en Asterisk) radican en el desempeño, la adaptabilidad en la configuración y las habilidades para gestionar NAT. Aunque chan\_sip gestiona cada conexión como un proceso único, PJSIP emplea un modelo de subprocesos más eficaz, mejorando la eficiencia y facilitando la gestión de un mayor número de llamadas simultáneas. Adicionalmente, PJSIP tiene la capacidad de administrar varios dispositivos vinculados a una única extensión, lo que resulta beneficioso en situaciones donde el mismo usuario cuenta con varios dispositivos. Otra distinción relevante es la administración de NAT, dado que PJSIP ofrece un respaldo optimizado para manejar configuraciones de NAT complejas, lo que incrementa la estabilidad y la calidad de las llamadas en contextos de red complejos.

- ¿Cómo se puede verificar que las llamadas configuradas a través de SIP en Asterisk están funcionando correctamente? ¿Qué herramientas o comandos de diagnóstico se utilizarían en caso de problemas?

**Rta:** Para confirmar el correcto funcionamiento de las llamadas realizadas a través de SIP en Asterisk, es crucial efectuar pruebas de llamada directas entre

extensiones y a números externos, asegurándose de que el ajuste de la llamada, la calidad del sonido y la estabilidad sean ideales. Además, es posible supervisar los registros en tiempo real, tales como la circulación de paquetes SIP y la reacción del servidor al tratar de conectar una llamada. Esto facilita la detección de posibles inconvenientes en las configuraciones o en la conexión de red.

Si se presentan dificultades, en Asterisk se encuentran diversas herramientas y comandos de diagnóstico que asisten en la detección de la causa. Uno de los comandos clave es `sip show peers`, que presenta una lista de los dispositivos SIP registrados y su estado, lo que permite verificar si están en funcionamiento o están desconectados. También resulta beneficioso el comando `sip show channels`, que especifica las llamadas en curso y asiste en la comprobación de si existen obstáculos o fallos en las conexiones. Para examinar problemas a fondo, `sip set debug on` activa un modo de depuración exhaustivo para el protocolo SIP, mostrando el tráfico de los paquetes SIP, incluyendo los mensajes INVITE, ACK, BYE y otros que son esenciales en la negociación de la conversación.

## **Bibliografía**

[1] M. IP. “Qué es Asterisk y cómo funciona: características, servicios y por qué lo necesitas”. Más IP. Accedido el 27 de octubre de 2024. [En línea]. Disponible: <https://www.masip.es/blog/que-es-asterisk/>

[2] “¿Qué es CentOS?” Red Hat - We make open source technologies for the enterprise. Accedido el 27 de octubre de 2024. [En línea]. Disponible: <https://www.redhat.com/es/topics/linux/what-is-centos>

[3] Equipo editorial de IONOS. “SIP: todo lo que necesitas saber sobre el Session Initiation Protocol”. IONOS Digital Guide. Accedido el 27 de octubre de 2024. [En línea]. Disponible: <https://www.ionos.com/es-us/digitalguide/servidores/know-how/session-initiation-protocol/>