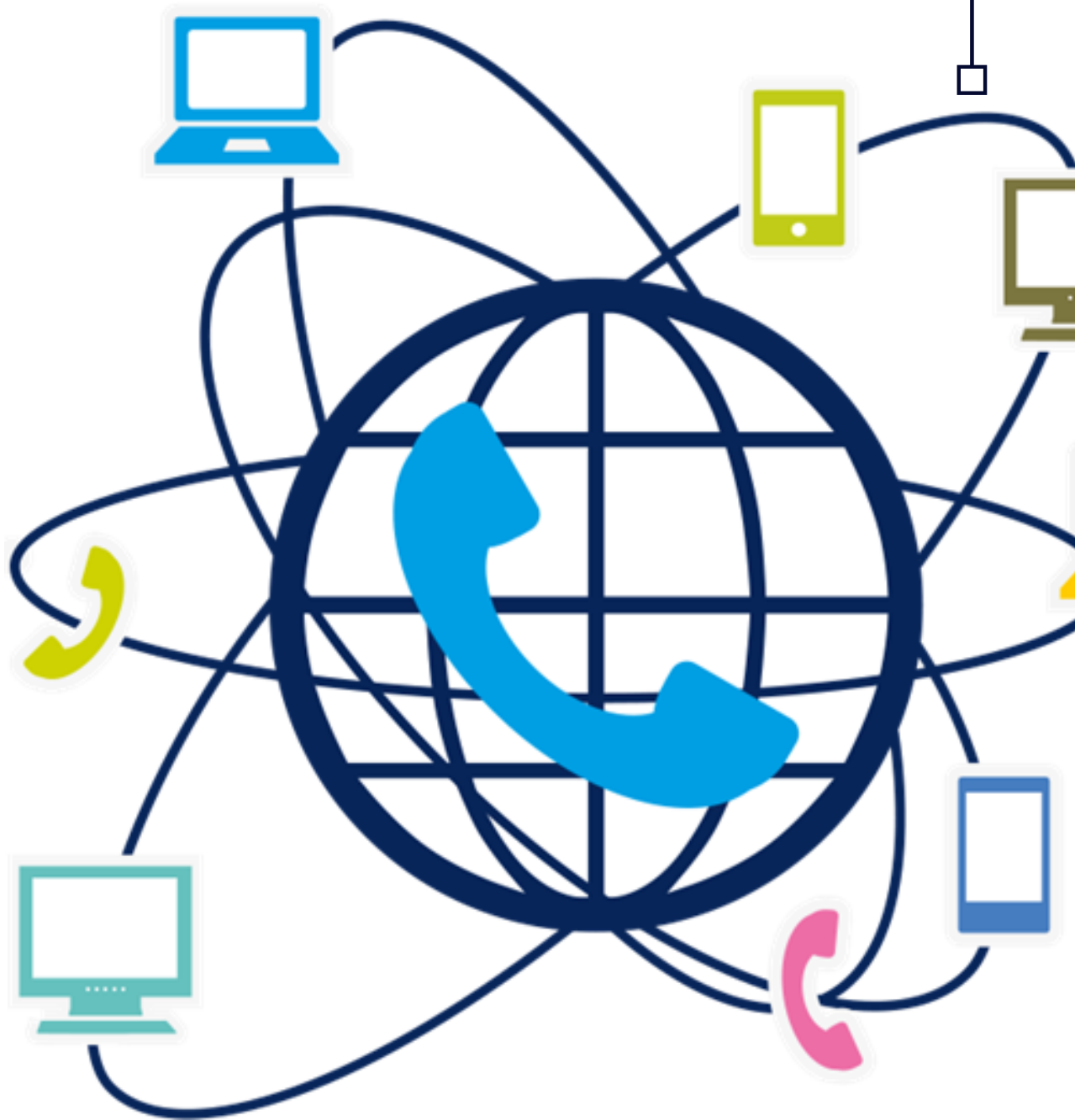


14/08/2021

Proyecto Final

Monitero VOIP con Nagios (SNMP y NRPE)



Administración de Redes

Alumnos:

Fuentes Díaz Alan Abner
Gómez Trejo Gustavo Ali
Hernández Escobar Oswaldo

Mancilla Checa Luis Enrique
Méndez Cabrera Ana Belem

Índice

Apartado 1

Introducción

Apartado 2

Planteamiento

Apartado 3

Desarrollo

Apartado 4

Conclusiones

Apartado 5

Referencias

Introducción

Voice Over Internet Protocol (VoIP)

Es una tecnología que permite enviar voz y realizar sesiones multimedia como streamings a través del protocolo de internet. Implementar este servicio representa muchos beneficios, como la reducción de gastos mensuales de teléfono, aumento de movilidad y productividad, entre otros.

Session Initial Protocol (SIP)

Es utilizado junto con VoIP, este permite establecer una sesión entre 2 o más participantes, modificar la sesión y eventualmente, terminar dicha sesión. Es un protocolo importante, ya que es un estándar abierto, por lo tanto, ha generado interés en el mercado de la telefonía.

User Datagram Protocol (UDP)

Para aprovechar la tecnología de VoIP es recomendable hacer uso del Protocolo de Datagramas de Usuario (UDP), ya que no está orientado a conexión, por lo tanto, es adecuado para llamadas de voz y streamings, puesto que no es necesario que lleguen todos los paquetes de datos, esto representa una comunicación más efectiva.



Es un sistema operativo de software libre y código abierto. Es una distribución de Linux basada en Debian. Puede utilizarse en ordenadores y servidores cuyas principales características son:

- Facilidad de manejo
- Actualizaciones frecuentes
- Facilidad de instalación del sistema
- Búsqueda e instalación de programas robusta y fácil al basarse en paquetes.
- Libertad de uso y distribución.

Introducción

Asterisk



Asterisk es el líder mundial en plataformas de telefonía de código abierto. Asterisk es un software que puede convertir un ordenador de propósito general en un sofisticado servidor de comunicaciones VoIP. Es un sistema de centralita IP utilizado por empresas de todos los tamaños para mejorar su comunicación, incluyendo a Google, Yahoo, IBM, e incluso el Ejército de EE.UU.

Se puede conectar un número determinado de teléfonos para hacer llamadas entre sí dentro de una misma organización e incluso acceder a comunicaciones fuera de la misma a la PSTN o conectando a un proveedor de VoIP o bien a una RDSI tanto básicos como primarios.

Nagios



Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Introducción



Zoiper es un software multiplataforma (funciona con Windows, Linux, MAC, iPod Touch, iPad, iPhone, tablets y Android), diseñado para trabajar con sus sistemas de comunicación IP basado en el protocolo SIP.

Entre las características que podemos encontrar en esta aplicación podemos destacar:

- Audio / Video Conferencia
- Chat / Mensajería
- Gestión de contactos
- Gestión de fax

Planteamiento (Políticas a implementar)

Política de Seguridad de las comunicaciones

Estas nos ayudan a asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. Para ello se debe implementar una seguridad de red con medidas y características adecuadas. Las cuales incluyan las siguientes características de seguridad:

- Autenticación, cifrado y controles de conexión de red.
- Parámetros técnicos necesarios para realizar una conexión segura con los servicios de red, de acuerdo con las reglas de seguridad y conexión de red como: firewall, VPN e IDS / IPS.
- Procedimientos para restringir el acceso a los servicios de red o aplicaciones, cuando sea necesario.
- Implementar controles para garantizar la seguridad de la información en las redes y la protección de servicios conectados de acceso no autorizado. En particular, deben tenerse en cuenta los siguientes elementos:
- Establecer responsabilidades y procedimientos para la gestión de equipos de red.
- Establecerse controles especiales para salvaguardar la confidencialidad e integridad de los datos que se transmiten.
- Para redes públicas o redes inalámbricas: Se debe aplicar un registro y monitoreo apropiados para permitir el registro y detección de acciones que puedan afectar o sean relevantes para la seguridad de la información.



Planteamiento (Políticas a implementar)

Política de Seguridad de la información

Una política de seguridad de la información (ISP) establece reglas y procesos para los miembros de la fuerza laboral, creando un estándar sobre el uso aceptable de la tecnología de la información de la organización, incluidas las redes y aplicaciones para proteger la confidencialidad, integridad y disponibilidad de los datos.

Los ISP establecen reglas formalizadas para garantizar que la empresa tenga una serie de controles en torno a los tres principios de seguridad de la información: confidencialidad, integridad y disponibilidad.

1. Propósito.- Primero, indique el propósito de la política, que puede ser:

- Cree un enfoque general para la seguridad de la información.
- Detecte y evite las brechas de seguridad de la información, como el uso indebido de redes, datos, aplicaciones y sistemas informáticos.
- Mantener la reputación de la organización y cumplir con las responsabilidades éticas y legales.
- Respete los derechos del cliente, incluida la forma de reaccionar ante consultas y quejas sobre incumplimiento.

2. Público

- Defina la audiencia a la que se aplica la política de seguridad de la información. También puede especificar qué audiencias están fuera del alcance de la política (por ejemplo, el personal de otra unidad de negocios que administra la seguridad por separado puede no estar en el alcance de la política).

Planteamiento (Políticas a implementar)

Política de Seguridad de la información

3. Objetivos de seguridad de la información

- Guíe a su equipo de gestión para que llegue a un acuerdo sobre objetivos bien definidos de estrategia y seguridad. La seguridad de la información se centra en tres objetivos principales:
 - Confidencialidad: solo las personas con autorización pueden acceder a los datos y a los activos de información.
 - Integridad: los datos deben estar intactos, ser precisos y completos, y los sistemas de TI deben mantenerse operativos.
 - Disponibilidad: los usuarios deben poder acceder a la información o los sistemas cuando sea necesario.

4. Política de autoridad y control de acceso

- Patrón jerárquico: un gerente senior puede tener la autoridad para decidir qué datos se pueden compartir y con quién. La política de seguridad puede tener diferentes términos para un alto directivo frente a un empleado subalterno. La política debe describir el nivel de autoridad sobre los datos y los sistemas de TI para cada función organizacional.
- Política de seguridad de la red: los usuarios solo pueden acceder a las redes y servidores de la empresa a través de inicios de sesión únicos que exigen autenticación, incluidas contraseñas, datos biométricos, tarjetas de identificación o tokens. Debe monitorear todos los sistemas y registrar todos los intentos de inicio de sesión.

Planteamiento (Políticas a implementar)

Política de Seguridad de la información

5. Clasificación de datos

- La política debe clasificar los datos en categorías, que pueden incluir "ultrasecreto", "secreto", "confidencial" y "público". Su objetivo al clasificar los datos es:
 - Para garantizar que las personas con niveles de autorización más bajos no puedan acceder a los datos confidenciales.
 - Para proteger datos muy importantes y evitar medidas de seguridad innecesarias para datos sin importancia.

6. Soporte de datos y operaciones

- Regulaciones de protección de datos: los sistemas que almacenan datos personales u otros datos confidenciales deben protegerse de acuerdo con los estándares organizacionales, las mejores prácticas, los estándares de cumplimiento de la industria y las regulaciones relevantes. La mayoría de los estándares de seguridad requieren, como mínimo, cifrado, un cortafuegos y protección antimalware.
- Copia de seguridad de datos: cifre la copia de seguridad de datos de acuerdo con las mejores prácticas de la industria. Almacene de forma segura los medios de copia de seguridad o mueva la copia de seguridad a un almacenamiento seguro en la nube.
- Movimiento de datos: solo transfiera datos a través de protocolos seguros. Cifre cualquier información copiada a dispositivos portátiles o transmitida a través de una red pública.

Planteamiento (Políticas a implementar)

Política de Seguridad de la información

7. Comportamiento y conciencia de seguridad

- Comparta las políticas de seguridad de TI con su personal. Realice sesiones de capacitación para informar a los empleados sobre sus procedimientos y mecanismos de seguridad, incluidas las medidas de protección de datos, las medidas de protección de acceso y la clasificación de datos confidenciales.
- Ingeniería social: haga especial hincapié en los peligros de los ataques de ingeniería social (como los correos electrónicos de phishing). Haga que los empleados sean responsables de advertir, prevenir y denunciar tales ataques.
- Política de escritorio limpio: asegure las computadoras portátiles con un candado de cable. Triture los documentos que ya no necesite. Mantenga las áreas de la impresora limpias para que los documentos no caigan en las manos equivocadas.
- Política de uso aceptable de Internet: defina cómo se debe restringir Internet. ¿Permiten YouTube, sitios web de redes sociales, etc.? Bloquea sitios web no deseados mediante un proxy.

8. Responsabilidades, derechos y deberes del personal

- Designar personal para llevar a cabo revisiones de acceso de usuarios, educación, gestión de cambios, gestión de incidentes, implementación y actualizaciones periódicas de la política de seguridad. Las responsabilidades deben definirse claramente como parte de la política de seguridad.



Planteamiento (¿Cómo se llevará a la práctica)

Para poder implementar las políticas explicadas anteriormente se montará un servidor de Asterisk en una máquina virtual de Ubuntu, en dicho servidor se lleva a cabo la creación y configuración completa de los usuarios.

Los usuarios serán las extensiones con las cuales se establecerá la comunicación, para ellos se crea un nombre de la extensión y posteriormente se le configura una contraseña para poder tener un control de acceso restringido con estos usuarios.

Otras configuraciones a destacar son los protocolos de comunicación tanto del usuario como en la forma en la que se realiza el envío de información. Dichos protocolos son SIP y UDP de los cuales ya se hablo anteriormente dentro de este documento.

Con el uso de Zoiper vamos a logear a las extensiones que se crearon asignándoles la IP de la computadora (en este caso de la máquina virtual) para que se puedan comunicar entre ambas extensiones, para que posteriormente Asterisk les destine una IP distinta pero que pertenece al mismo segmento de red que IP de la máquina virtual.

Y con la herramienta Nagios se implementará la monitorización tanto de la máquina virtual como de las llamadas por medio del protocolo SNMP (que es un protocolo de administración y monitorización de red) y NRPE (que es un agente de Nagios que realiza una monitorización activa de los recursos).



Desarrollo

Primero iniciamos con la instalación de Asterisk en ubuntu con el comando

```
sudo apt-get install asterisk
```

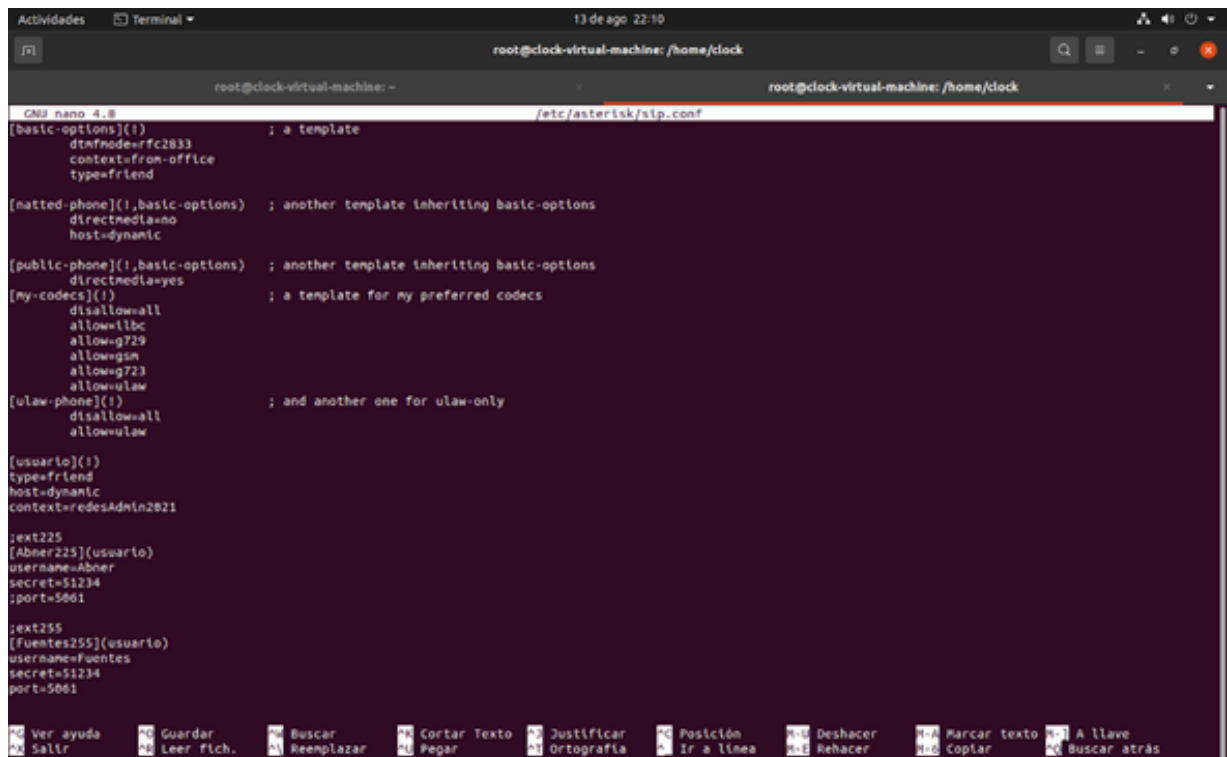
Se pone el siguiente comando para visualizar la versión de Asterisk instalada :

```
root@clock-virtual-machine:/home/clock# asterisk -V
Asterisk 16.2.1~dfsg-2ubuntu1
root@clock-virtual-machine:/home/clock#
```

Ingresamos al archivo de configuración "sip", para dar de alta a los usuarios mediante el comando:

```
nano /etc/asterisk/sip.conf
```

Poniendo el "username", la contraseña que es "secret" y el puerto. Aquí es donde se da una de las configuraciones importantes sobre seguridad ya que se le agrega la contraseña para la extensión, lo cual nos ayuda a restringir el acceso para otras personas y hace más seguro el canal.



```
root@clock-virtual-machine: /home/clock
root@clock-virtual-machine: /home/clock
root@clock-virtual-machine: /home/clock
/etc/asterisk/sip.conf

[basic-options]({}) ; a template
    dtmfmode=rfc2833
    context=from-office
    type=friend

[natted-phone]({},basic-options) ; another template inheriting basic-options
    directmedia=no
    host=dynamic

[public-phone]({},basic-options) ; another template inheriting basic-options
    directmedia=yes

[my-codecs]({}) ; a template for my preferred codecs
    disallow=all
    allow=ilbc
    allow=g729
    allow=gsn
    allow=g723
    allow=ulaw

[ulaw-phone]({}) ; and another one for ulaw-only
    disallow=all
    allow=ulaw

[userlo]({})
    type=friend
    host=dynamic
    context=redesAdmin2021

;ext225
;[Abner225](userlo)
;username=Abner
;secret=$1234
;port=5061

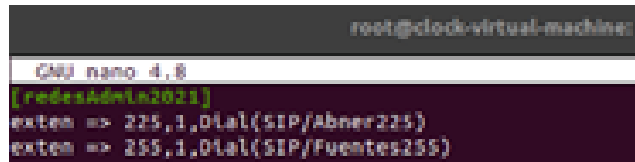
;ext255
;[Fuentes255](userlo)
;username=Fuentes
;secret=$1234
;port=5061

Ver ayuda Guardar Buscar Cortar Texto Justificar Posición Deshacer Marcar texto A llave
Salir Leer fich. Reemplazar Pegar Ortografía Ir a línea Rehacer Copiar Buscar atrás
```

Desarrollo

Después una vez dada de alta los usuarios lo que hicimos fue pasarle el contexto por el cual van a ser la llamada esto con la modificación de extensiones (extensions.conf) mediante el comando:

```
nano /etc/asterisk/extensions.conf
```

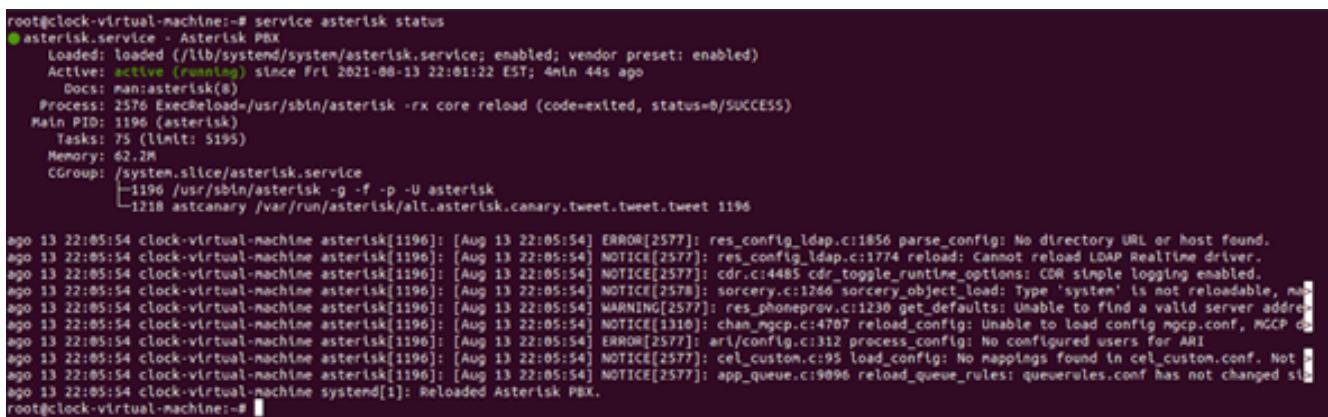


```
root@clock-virtual-machine: ~  
GNU nano 4.8  
[redesAdmin2021]  
exten => 225,1,Dial(SIP/abner225)  
exten => 255,1,Dial(SIP/Puentes255)
```

En la parte mostrada por la imagen anterior se tiene otra configuración importante, en donde colocamos el contexto para la llamada que es "redesAdmin2021" que nos ayudará a establecer la llamada entre ambas extensiones y por supuesto también se indica que se comunicarán por medio de Dial y SIP que son características para el tipo de comunicación segura que llevarán ambas extensiones.

Una vez finalizado dar de alta a los usuarios y las extensiones, proseguimos a revisar el estado del servicio de asterisk, mediante el comando de:

```
service asterisk status
```



```
root@clock-virtual-machine:~# service asterisk status  
● asterisk.service - Asterisk PBX  
   Loaded: loaded (/lib/systemd/system/asterisk.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2021-08-13 22:01:22 EST; 4min 44s ago  
     Docs: man:asterisk(8)  
  Process: 2576 ExecReload=/usr/sbin/asterisk -rx core reload (code=exited, status=0/SUCCESS)  
 Main PID: 1196 (asterisk)  
    Tasks: 75 (limit: 5195)  
   Memory: 62.2M  
    CGroup: /system.slice/asterisk.service  
            └─1196 /usr/sbin/asterisk -g -f -p -U asterisk  
              1218 astcanary /var/run/asterisk/alt.asterisk.canary.tweet.tweet.tweet 1196  
  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] ERROR[2577]: res_config_ldap.c:1856 parse_config: No directory URL or host found.  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[2577]: res_config_ldap.c:1774 reload: Cannot reload LDAP Realtime driver.  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[2577]: cdr.c:4485 cdr_toggle_runtime_options: CDR simple logging enabled.  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[2578]: sorcery.c:1266 sorcery_object_load: Type 'system' is not reloadable, ma  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] WARNING[2577]: res_phoneprov.c:1230 get_defaults: Unable to find a valid server addre  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[1310]: chan_mgcp.c:4707 reload_config: Unable to load config mgcp.conf, MGCP co  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] ERROR[2577]: ari/config.c:312 process_config: No configured users for ARI  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[2577]: cel_custom.c:95 load_config: No mappings found in cel_custom.conf. Not  
ago 13 22:05:54 clock-virtual-machine asterisk[1196]: [Aug 13 22:05:54] NOTICE[2577]: app_queue.c:9096 reload_queue_rules: queuerules.conf has not changed si  
ago 13 22:05:54 clock-virtual-machine systemd[1]: Reloaded Asterisk PBX.  
root@clock-virtual-machine:~#
```

Como se aprecia en la imagen anterior el estado del servicio asterisk esta corriendo y funcionando correctamente, entonces se puede continuar con el desarrollo

Desarrollo

Para ingresar a la consola de asterisk es con el comando:

asterisk -rvvvvvvvvvv

Mientras mas "v" le demos nos dará esta mas información (ya que es v de verbose). La información que nos detallan la letra "v" será sobre las notificación de ingresos de llamadas, rechazos de llamadas, conexiones de las extensiones, entre otras cuestiones.

```
root@clock-virtual-machine:~# asterisk -rvvvvvvvvvvvvvvvv
Asterisk 16.2.1-dfsg-2ubuntu1, Copyright (C) 1999 - 2018, Digium, Inc. 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 16.2.1-dfsg-2ubuntu1 currently running on clock-virtual-machine (pid = 1196)
clock-virtual-machine*CLI>
```

Con el siguiente comando se puede visualizar a los usuarios que ya se crearon anteriormente:

```
sip show users
```

La información que se nos muestra es el nombre de usuario, la contraseña y el contexto (recordemos que la dicha información se configuro anteriormente y nos ayuda a mantener la seguridad de la inromación y el canal de comunicación).

```
root@clock-virtual-machine:~# asterisk -rvvvvvvvvvvvvvvvvvvvv
Asterisk 16.2.1-dfsg-2ubuntu1, Copyright (C) 1999 - 2018, Digium, Inc. 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 16.2.1-dfsg-2ubuntu1 currently running on clock-virtual-machine (pid = 1196)
clock-virtual-machine*CLI> sip show users
Username                Secret      Accountcode    Def.Context     ACL   Forcerport
Fuentes255              51234      redAdmin2021   No               No
Abner225                51234      redAdmin2021   No               No
clock-virtual-machine*CLI>
```


Desarrollo

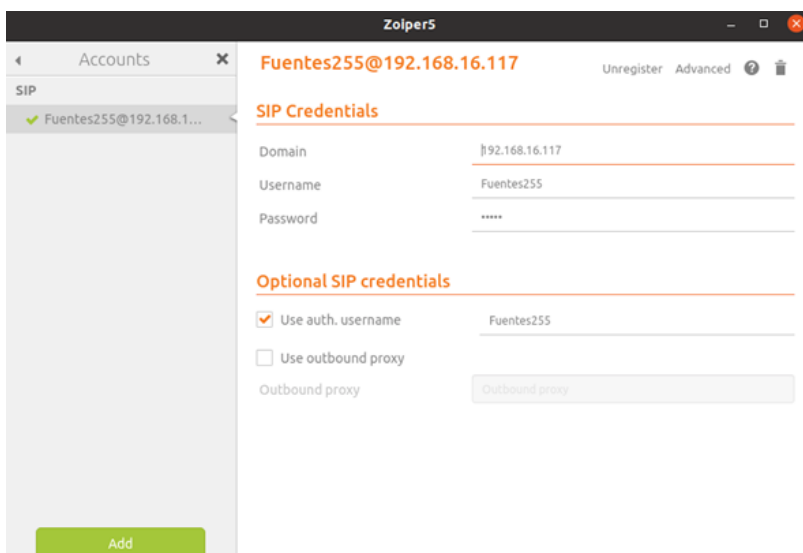
Lo anterior se logra una vez que se dan de alta los usuarios en la aplicación Zoiper. En donde solo basta con ingresar el nombre de la extensión de la siguiente forma:

"nombreExtension@192.x.x.x"

La IP que se asigna aquí es la que nos proporciona la máquina virtual de ubuntu. Una vez hecho eso se pide una IP la cual se pone automaticamente cuando ya se hizo lo anterior. Posteriormente se nos pide rellenar una casilla y volver a poner el nombre de la extensión de la siguiente forma:

"nombreExtension"

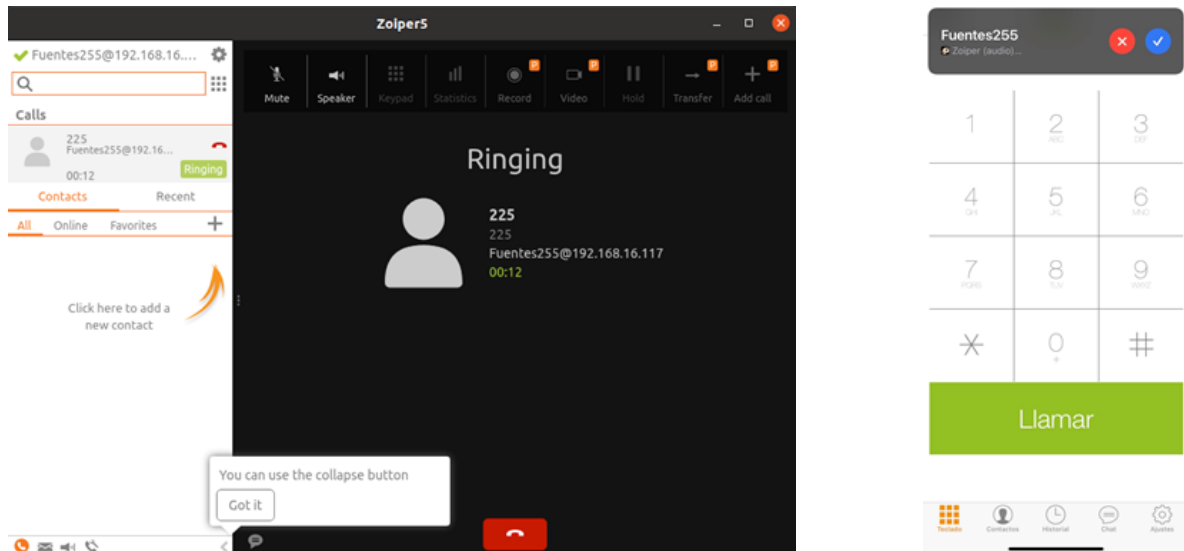
Y por último se nos muestran los 4 servicios posibles a los cuales se va a conectar la extensión, en este caso debe conectarse por UDP. Entonces dicho servicio aparece con una barrita verde, lo seleccionamos y listo se nos mostrará el registro exitoso. Tal y como se puede observar a continuación:



NOTA: La imagen de la izquierda corresponde a la extensión de la máquina virtual y la imagen de la derecha corresponde a la extensión del celular

Desarrollo

Una vez que se logro lo anterior, se procederá a realizar una llamada de prueba para poder registrar si ambas extensiones pueden comunicarse de manera segura entre si.



Como se visualiza en las imágenes anteriores ambos dispositivos se pueden comunicar entre si. Esto quiere decir que se configuro todo lo anterior. Otra cosa a destacar es como en la consola de asterisk se visualiza la notificación de la llamada, la cual se muestra a continuación:

```
root@clock-virtual-machine: ~
-- Registered SIP 'Abner225' at 192.168.16.111:51330
[Aug 13 22:13:59] NOTICE[1326]: chan_sip.c:24884 handle_response_peerpoke: Peer 'Abner225' is now Reachable. (32ns / 2000ms)
-- Using SIP RTP CoS mark 5
  > 0x7f18ec02a4c0 -- Strict RTP learning after remote address set to: 192.168.16.111:56704
-- Executing [255@redesAdmin2021:1] Dial("SIP/Abner225-00000000", "SIP/Fuentes255") in new stack
-- Using SIP RTP CoS mark 5
-- Called SIP/Fuentes255
-- SIP/Fuentes255-00000001 is ringing
-- Spawn extension (redesAdmin2021, 255, 1) exited non-zero on 'SIP/Abner225-00000000'
-- Using SIP RTP CoS mark 5
  > 0x7f18ec029ca0 -- Strict RTP learning after remote address set to: 192.168.16.117:8000
-- Executing [225@redesAdmin2021:1] Dial("SIP/Fuentes255-00000002", "SIP/Abner225") in new stack
-- Using SIP RTP CoS mark 5
-- Called SIP/Abner225
-- SIP/Abner225-00000003 is ringing
-- SIP/Abner225-00000003 is ringing
-- Spawn extension (redesAdmin2021, 225, 1) exited non-zero on 'SIP/Fuentes255-00000002'
clock-virtual-machine*CLI>
```

Desarrollo

Ya comprobado lo anterior, se instalará el agente NRPE de Nagios en la máquina virtual de Ubuntu para poder realizar la monitorización.

```
root@clock-virtual-machine: /tmp/linux-nrpe-agent

### ::1                                     ###
###                                     ###
### If you would like to change this list, enter all IP addresses to allow, ###
### separated by SPACES only, and then press Enter.                         ###
### (Put the address(es) of your Nagios XI servers(s) here.)                 ###
###                                     ###
#####

Allow from: 192.168.16.119
xinetd.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable xinetd
Subcomponents installed OK
RESULT=0

#####
###                                     ###
### Nagios XI Linux Agent Installation Complete!                             ###
###                                     ###
#####

If you experience any problems, please attach the file install.log that was just
created to any support requests.

root@clock-virtual-machine: /tmp/linux-nrpe-agent#
```

Ya instalado el agente NRPE, se creará la máquina virtual de Nagios Xi. Esta máquina ya viene configurada y por consecuencia solo se procederá a la creación de un usuario en la página web de Nagios Xi para poder entrar a la monitorización



Desarrollo

En las siguientes imágenes observamos la creación del usuario en la página web de Nagios y el mensaje de instalación completa. De esta manera podemos continuar para realizar la monitorización:

The screenshot shows the Nagios XI Installation page. The browser address bar displays '192.168.16.116'. The page title is 'Nagios XI Installation'. Below the title, it says 'Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.'

Admin Account Settings

Username: nagiosadmin
Password: admin123
Full Name: Nagios Administrator
Email Address: root@localhost

Admin Notification Settings

☐ Send this account email notifications [Advanced email notification settings](#)

[< Back](#) [Finish Install](#)

The screenshot shows the Nagios XI Installation page after successful installation. The browser address bar displays '192.168.16.116/nagiosxi/install.php'. The page title is 'Nagios XI Installer'.

Instalacion completa

¡Felicidades! usted ha instalado exitosamente nagios xi. Ahora puede iniciar sesión en nagios xi usando las siguientes credenciales.

Usuario: nagiosadmin
Contraseña: admin123

[Iniciar sesión en nagios xi >](#)

Una vez dentro se nos mostrará una página como la siguiente. Dicha página es la principal del servidor de Nagios para la monitorización, junto con otros servicios y herramientas.

The screenshot shows the Nagios XI Home Dashboard. The browser address bar displays '192.168.16.116/nagiosxi/index.php'. The page title is 'Nagios XI'. The dashboard includes a sidebar with navigation links, a main content area with various monitoring metrics, and a footer with copyright information.

Home Dashboard

Guía de Inicio

- **Cambiar las configuraciones de su cuenta**
Cambiar la contraseña de la cuenta y las preferencias generales.
- **Cambiar las configuraciones de su agente**
Cambiar cómo y cuándo recibir notificaciones de alerta.
- **Configurar monitoreo básico**
Agregar o modificar elementos a monitorear con la UI de utilizar asistentes.

Resumen del Estado del Host

Arriba	Abajo	Instalizable	Pendiente
0	0	0	0
No controlado	Problemas	Alerta	
0	0	1	

Última actualización: 2021-09-09 12:44:00

Resumen del Estado del Servicio

Ok	Advertencia	Desconocido	Crítico	Pendiente
0	0	0	0	0
No controlado	Problemas	Alerta		
0	0	0	12	

Última actualización: 2021-09-09 12:44:00

Tareas Administrativas

Tarea

Tareas de configuración inicial:

- **Cambiar configuraciones básicas del host**
Configure los parámetros básicos para su sistema XI.

Estamos para ayudarle!!!

Nuestros técnicos expertos están encantados de ayudarle con cualquier pregunta o problema que pueda tener cada vez Nagios en marcha.

[Paso de soporte / Paso de soporte al cliente](#)

[Recursos de ayuda](#)

[Centro de soporte de Nagios para clientes](#)

[Soporte telefónico del cliente +1 851-254-9102 Ext. 4](#)

iniciar la supervisión ahora

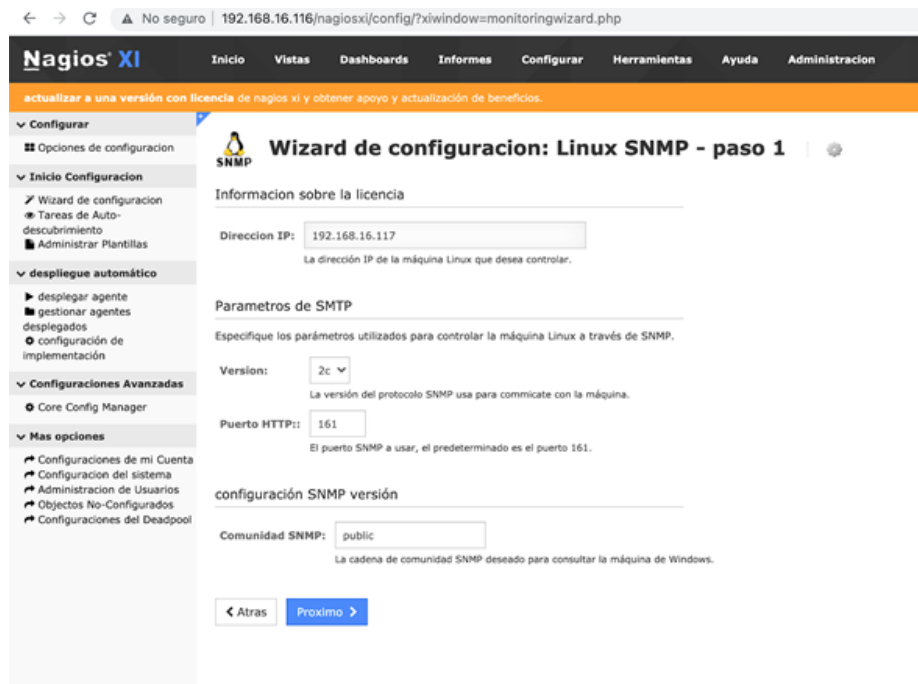
[agregar un sistema de configuración](#)

Nagios XI 5.6.4 • [Chequear actualizaciones](#)

Agencia de: 1 Legal • Copyright © 2008-2021 Nagios Enterprises, LLC

Desarrollo

Posteriormente ingresamos a la herramienta de monitorización "Linux SNMP", la cual mediante ese protocolo trabajará en la máquina virtual de Ubuntu para poder monitorizar algunos aspectos de la misma, para esto bastará con realizar lo que sigue:



The screenshot shows the Nagios XI web interface. The top navigation bar includes links for Inicio, Vistas, Dashboards, Informes, Configurar, Herramientas, Ayuda, and Administracion. A sidebar on the left contains a tree view with categories like Configurar, Inicio Configuración, despliegue automático, Configuraciones Avanzadas, and Mas opciones. The main content area is titled "Wizard de configuracion: Linux SNMP - paso 1". It contains three sections: "Informacion sobre la licencia" with a "Direccion IP:" field set to "192.168.16.117"; "Parametros de SMTP" with "Version:" set to "2c" and "Puerto HTTP:" set to "161"; and "configuración SNMP versión" with "Comunidad SNMP:" set to "public". Navigation buttons "Atras" and "Proximo" are at the bottom.

La IP que se agrega en la imagen anterior es la que le corresponder a la máquina virtual de Ubuntu, ya que es el dispositivo en donde se realizará la monitorización. Posteriormente una vez terminado eso, se procede a realizar la monitorización por NRPE, la cual es muy parecido a lo anterior solo con pequeñas diferencias ya que para esta es necesario utilizar la herramienta wizard llamada "NRPE", tal y como se muestra a continuación:



The screenshot shows the Nagios XI web interface for the "Wizard de configuracion: NRPE - paso 1". The "Informacion del Sistema" section contains a "Direccion IP:" field set to "192.168.16.117" and a "Centro de Operaciones:" dropdown menu set to "Linux - Ubuntu". Navigation buttons "Atras" and "Proximo" are at the bottom.

Desarrollo

Realizado todo lo anterior poder ver satisfactoriamente el estado de la monitorización, terminando así con el desarrollo de este proyecto y obteniendo lo esperado.

Mostrando 1-15 de 21 total de registros

Página 1 of 2 15 Por página

Buscar...

Host	Servicio	Estatus	Duración	Intento	Ultimo Chequeo	Información de Estatus
NRPE	Alive	Ok	1d 8h 26m 0s	1/5	2021-08-13 22:26:24	OK - load average: 0.11, 0.11, 0.14
	Current Users	Ok	1d 8h 26m 0s	1/5	2021-08-13 22:26:56	USERS OK - 1 users currently logged in
	Ping	Ok	1d 8h 26m 0s	1/5	2021-08-12 17:19:07	OK - 192.168.16.117 rta 1.219ms lost 0%
	Total Processes	Desconocido	1d 8h 22m 27s	5/5	2021-08-12 17:19:18	NRPE: Command 'check_procs' not defined
SNMP	/ Disk Usage	Critico	1d 8h 25m 59s	5/5	2021-08-12 17:17:37	ERROR: Description/Type table : No response from remote host "192.168.16.117".
	CPU Usage	Desconocido	1d 8h 25m 59s	5/5	2021-08-12 17:19:31	No answer from host
	Memory Usage	Critico	1d 8h 25m 4s	5/5	2021-08-12 17:17:50	ERROR: Description/Type table : No response from remote host "192.168.16.117".
	Ping	Ok	5d 14h 20m 38s	1/5	2021-08-13 22:26:35	OK - 192.168.16.117 rta 1.023ms lost 0%
localhost	Swap Usage	Critico	1d 8h 23m 49s	5/5	2021-08-13 22:27:07	ERROR: Description/Type table : No response from remote host "192.168.16.117".
	Current Load	Ok	64d 7h 13m 25s	1/4	2021-08-12 17:16:11	OK - load average: 0.44, 0.22, 0.20
	Current Users	Ok	64d 7h 13m 0s	1/4	2021-08-12 17:17:01	USERS OK - 0 users currently logged in
	HTTP	Ok	64d 7h 12m 35s	1/4	2021-08-12 17:17:24	HTTP OK: HTTP/1.1 200 OK - 3470 bytes in 0.007 second response time
	Memory Usage	Ok	64d 7h 12m 10s	1/4	2021-08-12 17:18:01	OK - 1342 / 1828 MB (73%) Free Memory, Used: 456 MB, Shared: 9 MB, Buffers + Cached: 267 MB
	PING	Ok	64d 7h 11m 45s	1/4	2021-08-12 17:18:26	PING OK - Packet loss = 0%, RTA = 0.10 ms
	Root Partition	Ok	5d 19h 54m 52s	1/4	2021-08-13 22:26:46	DISK OK - free space: / 32107 MB (91.09% inode=96%):

Conclusiones

Como se pudo observar a lo largo del documento fue un proyecto un tanto laborioso y con algunos problemas ya que en principio se intentó instalar una máquina virtual solamente de FreePBX (Asterisk) sin necesidad de que se montara en otra máquina virtual, lo cual no se pudo lograr.

Es por eso que se optó por la alternativa que se mostró en este escrito, montar todo el servicio de Asterisk en una máquina virtual de Ubuntu y así evitar más problemas de compatibilidad e instalación de plugins.

Este trabajo nos deja distintos aprendizajes tanto en el ámbito de seguridad como en el de planeación y por su puesto en el manejo de distintos entornos a los cuales nos tuvimos que familiarizar para poder lograr todo lo descrito con anterioridad.

Cabe destacar que se logró lo planteado al inicio del proyecto, que era crear un canal seguro para la comunicación entre dos extensiones. Así se pudo observar la importancia de distintos protocolos de seguridad y políticas que se deben de tomar en cuenta.

Todo esto para poder mantener a salvo la información y la comunicación por medio de distintas configuraciones como creación de contraseñas, implementación de protocolos y la monitorización para así detectar y erradicar en su mayoría las anomalías que llegarán a presentarse.

Referencias

- <https://www.vix.com/es/btg/tech/13022/que-es-ubuntu>
- <https://quarea.com/es/que-es-asterisk-centralita-telefonica-ip/>
- <https://www.north-networks.com/que-es-nagios/>
- <https://www.linuxadictos.com/zoiper-una-aplicacion-multiplataforma-gratuita-para-voip.html>
- <https://taskroom.sp.saskatchewan.ca/Documents/Communications-and-Network-Security-Policy.pdf>
- <https://www.cellnextelecom.com/politica-seguridad-la-informacion/>
- <https://www.exabeam.com/information-security/information-security-policy/>
- <https://securityscorecard.com/blog/what-is-an-information-security-policy-and-what-should-it-include#:~:text=An%20information%20security%20policy%20>