

Patricia Suárez Díaz

Índice

Introducción	3
VPN	4
Comparativa de protocolos VPN	5
OpenVPN	7
Ventajas y desventajas	8
Tipos de funcionamiento	10
Seguridad	11
Instalación	11
Creación de claves y certificados	13
Configuración de parámetros	16
Direcciones IP	17
Configuración del servidor OpenVPN	18
Inicio del servicio OpenVPN	20
Asignación de IP fija en el servidor	21
Apertura de puertos en router y DDNS	22
Configuración del cliente	23
Conexión con el servidor	27
Gestor de base de datos	28
Comparativa de SQL Server y MySQL	29
SQL Server	30
Diseño de la base de datos	31
Instalación	32
Código de creación	38
Creación de un dispositivo de copias	40
Copia de seguridad completa	41
Creación de un plan de mantenimiento	42
LDAP	48

Comparativa de OpenLDAP y Active Directory	49
OpenLDAP	50
Esquema del directorio	51
Instalación	52
RADIUS	60
FreeRADIUS	61
Instalación	62
TLS	68
Instalación	69
Conclusión	74

Introducción

Una empresa necesita la creación de varios servidores (VPN, base de datos y radius)

El servidor VPN es para que los trabajadores se puedan conectar a la red de la empresa desde sus casas. Dispone de un servidor Windows server 2019 desde donde se puede crear la VPN y los equipo de trabajo desde donde se quieren conectar los empleados son Windows 10

Para solucionar esta petición se decidió utilizar OpenVPN para la creación y conexión a la VPN

También se necesita crear una base de datos para almacenar los datos de los dispositivos del cau

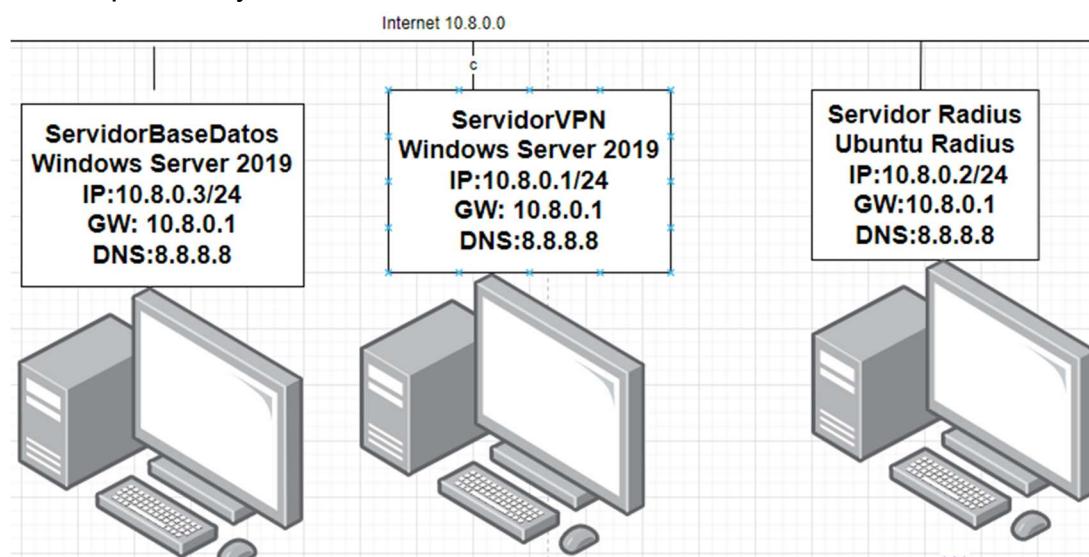
Las características de red del servidor son:

- IP 10.8.0.1
- Mascara de red 255.255.255.0
- Puerta de enlace 10.8.0.1
- DNS 8.8.8.8

A los clientes los datos de red se los proporcionará la VPN en el rango del 10.8.0.2 hasta la 10.8.0.254. Con una máscara de red de clase C (255.255.255.255)

El servidor de base de datos se utilizará para que el departamento del cau lleve un registro de los dispositivos. Se utilizará Microsoft Server SQL instalado en un Windows Server 2019 y tendrá la IP 10.8.3

El servidor de Radius se utilizara para el control de acceso y implementando el protocolo TLS para una mayor seguridad Se optó por freeradius en un equipo Ubuntu Desktop 20.04 y tendrá la IP 10.8.2



VPN

Una VPN (Virtual Private Network) es una red privada virtual que garantiza la privacidad en el intercambio de información. Permite crear una conexión segura entre

las 2 redes porque permite una comunicación sobre redes públicas como si fueran privadas. Se aplica a la funcionalidad, seguridad y políticas de gestión como las de una red privada. La conexión puede ser mediante conexiones dedicadas, cifrado o ambas.

Algunas ventajas de su uso son:

- Anonimato
- Seguridad
- Libertad

Los usos más frecuentes son:

- Acceder a los recursos con acceso restringido de la empresa
- Acceder a la red del trabajo desde fuera de la oficina
- Ocultar los datos de navegación
- Saltarse los bloqueos por geolocalización
- Administrar la red de forma remota
- Descargar de forma anónima

Funcionamiento

1. El software VPN del cliente cifra el tráfico de datos y los envía al servidor VPN por una conexión segura
2. El servidor VPN descifra los datos
3. El servidor VPN envía los datos a Internet
4. El servidor VPN cifra los datos de nuevo y los envía al cliente
5. El software VPN del cliente descifra los datos y ya se pueden usar



Comparativa de protocolos VPN

	PPTP	L2TP/IPsec	OpenVPN ™	Chameleon ™
--	------	------------	-----------	-------------

Encriptación	128 bits	128 bits	160 bits 256 bits	256 bits
Compatible con las apps de VyprVPN	Windows Mac Android	Windows Mac Android iOS	Windows Mac Android	Windows Mac Android
Compatible con configuración manual	Windows Mac OS X Linux iOS Android DD-WRT	Windows Mac OS X Linux iOS Android	Windows Mac OS X Linux Android	Windows Mac OS X Android
Seguridad	Encriptación básica	Comprobación de integridad de los datos y doble encapsulación	Autenticación de los datos utilizando certificados digitales.	Autenticación de los datos utilizando certificados digitales.
Velocidad	Rápido	Necesita más proceso de la CPU para la encapsulación	Velocidades elevadas	El protocolo que ofrece mejor rendimiento. Frustración de la inspección Velocidades elevadas
Estabilidad	Muy estable.	Compatible con dispositivos NAT.	La más fiable y estable..	Oculta el tráfico de VPN
Compatibilidad	Nativo en la mayoría de los sistemas operativos.	Nativo en la mayoría de los sistemas operativos	Compatible con la mayoría de los sistemas operativos	Compatible con la mayoría de los sistemas operativos



Es una aplicación de código abierto y licencia de software libre que permite realizar conexiones VPN.

Está basada en enlaces de tipo SSL y TLS

Utiliza claves de cifrado SSL/TLS +RSA

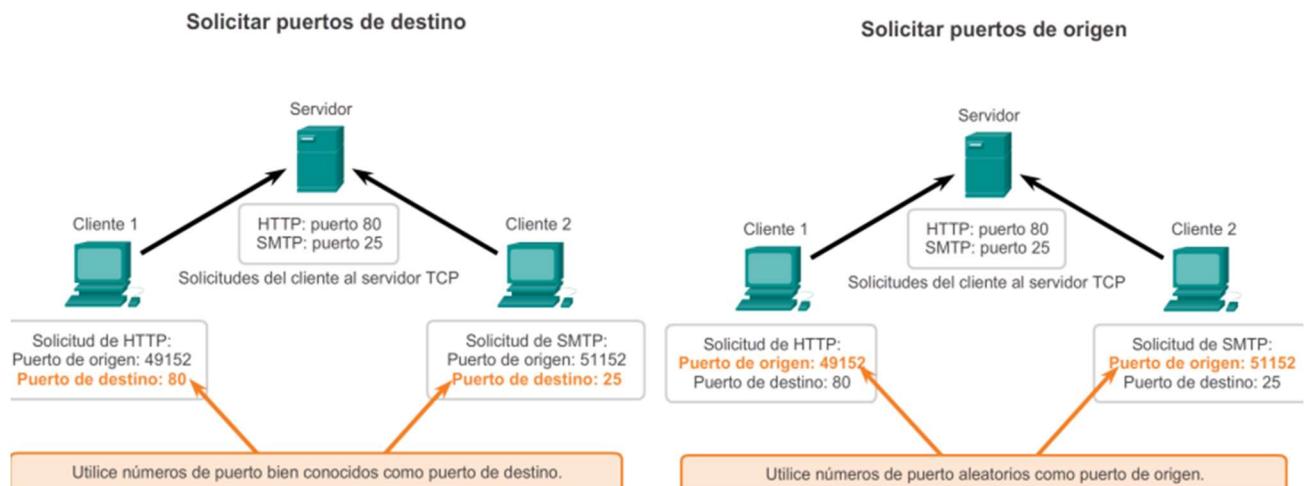
Características

- Protocolo multiplataforma.
- Modo multi-cliente.
- Portable.
- Modo multi-acceso.
- Control de acceso el cual permite o deniega a usuarios o grupos el acceso granular a la red.
- Implementación dinámica de aplicaciones
- Soporta diversos métodos de autenticación como PAM, LDAP, RADIUS, y Local DB.
- Altos niveles de escalabilidad la cual permite tener de 1000 a 100.000 VPN concurrentes por sesiones y conexiones.
- Alta disponibilidad.
- Generar diversos reportes de estadística.
- Flexible con la configuración DMZ.
- Múltiples niveles de seguridad.

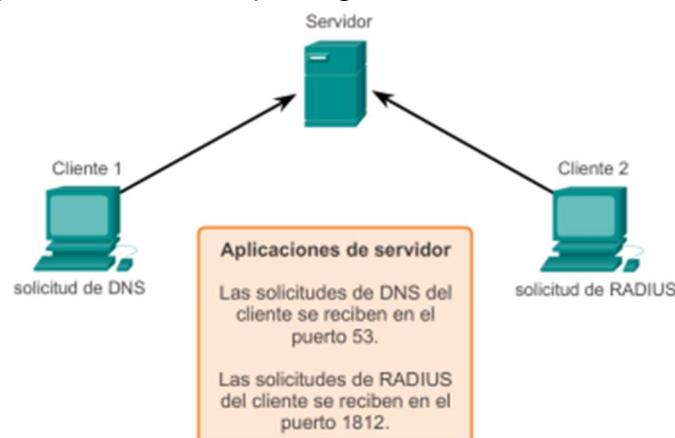
Ventajas y desventajas

Ventajas

- Soporta claves de cifrado de 256 bits y códigos de alta gama.
- Soporta el protocolo HTTPS
- Se puede usar tanto TCP como UDP
 - TCP es un protocolo orientado a la conexión, por lo que se debe abrir la comunicación antes de enviar, asegurando que los datos van a llegar por tener corrección de errores pero es más lento



- UDP es un protocolo que no está orientado a la conexión lo que supone que el cliente y el servidor no necesitan aceptar la comunicación para realizarla por lo que es más rápida pero no asegura que los datos lleguen al destino o que lleguen en orden.



- Es de código abierto
- Se puede usar en diferentes plataformas
- Gran capacidad de actualización

- Es uno de los más seguros de la actualidad
- Utiliza certificados para la identificación y el cifrado
- Permite la conexión a través de cualquier firewall
- Está entre las capas del modelo OSI
 - Enlace: construye las tramas de bits con la información para controlar que la transmisión se realice correctamente. Se realiza el primer encapsulado de datos para transportarlo
 - Red: identifica el enruteamiento entre las redes conectadas. Se crean los túneles para transportar los datos y se encripta la información de enruteamiento, como es la dirección IP de origen y destino.
 - Aplicación: permite a los usuarios ejecutar acciones y comandos. El túnel también se puede hacer en esta capa a través de protocolos SSL y TLS. Otro protocolo utilizado es el HTTPS. Con los mecanismos de cifrado OpenVPN se salta los firewall

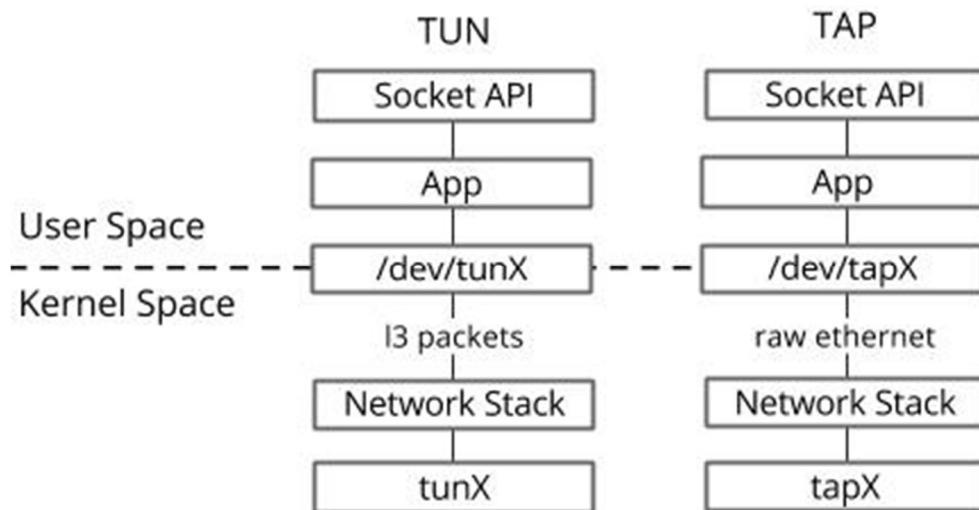


Desventajas

- Dificultad de configuración a través de comandos
- Deterioro del ancho de banda y latencia

Tipos de funcionamiento

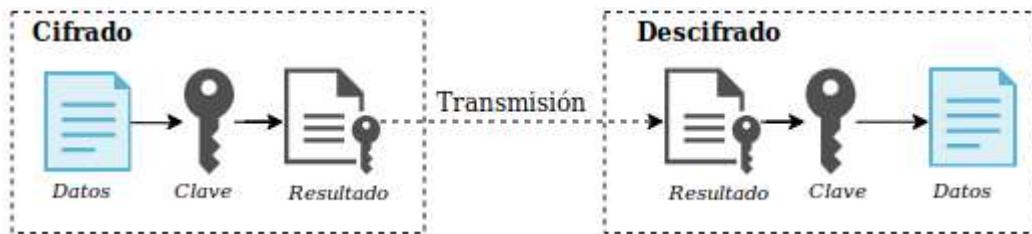
- TUN imita a un dispositivo punto a punto, se utiliza para crear túneles virtuales con el protocolo IP. Se encapsulan los paquetes que se transporta como segmentos TCP o datagramas UDP por los que los dispositivos seran de distintas subredes
- TAP permite empaquetar entramados diferentes al IP por lo que los dispositivos pueden operar como parte de la misma subred



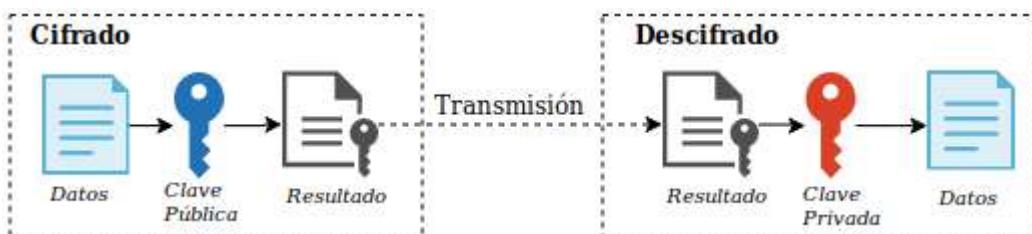
Seguridad

Utiliza dos métodos que son las claves pre-compartidas y los certificados SSL/TLS + RSA.

En la claves precompartidas (también llamado sistema de cifrado simétrico) se instala primero una clave en todos los clientes para acceder al servidor VPN y los nodos que tengan la clave podrán descifrar el tráfico de la red. Se considera inseguro porque si se obtiene la clave se puede ver todo el contenido de la red.



En los certificados SSL/TLS + RSA cada servidor y cada cliente utilizan dos claves públicas y dos privadas basadas en OpenSSL (por lo que es más seguro). La clave pública sirve para cifrar los datos,(se envía a todos los clientes que deseen conectarse) y la clave privada es la que los descifra. El RSA es un algoritmo que se utiliza tanto para la creación del certificado como para la firma.



Instalación

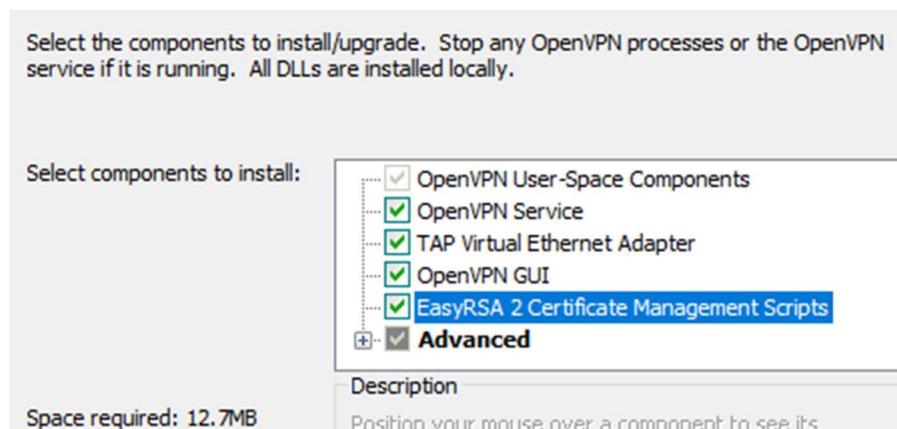
La instalación la debe de realizar un usuario con privilegios de administrador aunque después la puede usar cualquier usuario.

Ejecutamos el instalador que descargamos de la página oficial de OpenVPN:
<https://openvpn.net/community-downloads/>

La primera ventana es de bienvenida por lo que pulsamos en next

Después aceptaremos la licencias

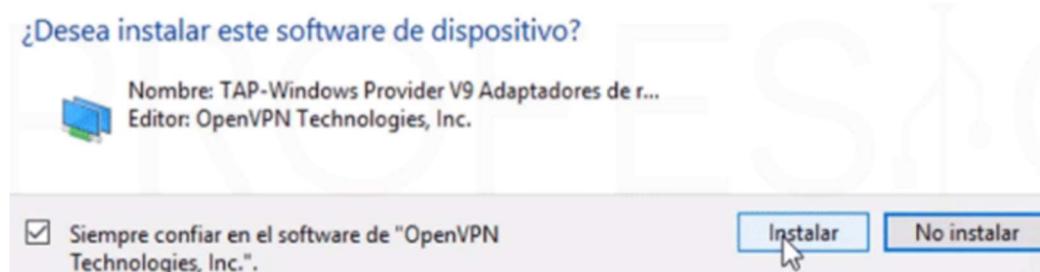
Seleccionamos los componentes además de los que vienen por defecto, marcamos la opción de EasyRSA 2 Certificate Management Scripts.



Esta opción permite generar los certificados para el servidor y cliente y así poder hacer la conexión cifrada

Otra opción importante es la OpenVPN Service que permite realizar la comunicación y un adaptador virtual de red TAP para efectuar la configuración de la IP para la red VPN y la comunicación

Puede saltar el siguiente aviso para aceptar la instalación del adaptador TAP que pulsaremos a instalar



Finalmente elegimos la carpeta de la instalación que por defecto es C:\Program Files\OpenVPN y ya estaría instalado

Abrimos cmd como administrador y nos dirigimos a la carpeta donde está instalado OpenVPN con cd "C:\Program Files\OpenVPN\easy-rsa".

Para iniciar la configuración escribimos init-config que no debe de mostrar ninguna salida

A continuación abrimos con el bloc de notas el archivo vars.bat

Es el que suministrará la información necesaria para los certificados

```
Microsoft Windows [Versión 10.0.17763.379]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
    1 archivo(s) copiado(s).

C:\Program Files\OpenVPN\easy-rsa>Notepad vars.bat

C:\Program Files\OpenVPN\easy-rsa>
```

Editamos los campos de country, province, city, org, email añadiendo nuestro datos y lo guardamos (se encuentra al final del documento)

```
set KEY_COUNTRY=SP
set KEY_PROVINCE=GA
set KEY_CITY=Coruña
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@admin.server2019|
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Volvemos al cmd como administrador y ejecutamos los comandos vars y seguidamente clean-all no debes cerrar el terminal porque lo vamos a seguir utilizando

```
C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
    1 archivo(s) copiado(s).
    1 archivo(s) copiado(s).
```

Creación de claves y certificados

El siguiente paso es crear los certificados del servidor que vamos a necesitar para la conexión. Al final de este paso tendremos 4 ficheros

El primer paso es ejecutar el comando build-ca.bat

Sirve para la generación de la entidad certificadora que se encarga de generar los certificados. Aparecer las líneas que anteriormente hemos modificado con el bloc de notas

Podemos pulsar intro hasta el apartado Common name (eg, your name or your server's hostname) que pondremos el nombre de nuestro servidor VPN (no tiene porque ser el nombre del equipo pero lo tendremos que recordar porque lo vamos a utilizar más adelante) por defecto es OpenVPN-CA

Los que aparecen entre corchetes no hacen falta cubrirlos porque ya los hemos cubierto anteriormente al editar el vars.bat

```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
Generating a RSA private key
-----
...+++++
writing new private key to 'keys\ca.key'

-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]:
State or Province Name (full name) [GA]:
Locality Name (eg, city) [Coruña]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:server2019
Name [changeme]:server2019
Email Address [mail@admin.server2019]:
```

Ahora creamos las claves del servidor

A continuación ejecutamos el comando build-key-server y el nombre introducido en common name que en este caso es server2019

El proceso es similar al anterior por lo que podemos pulsar intro hasta el apartado Common name que le introduciremos el mismo nombre

Sirve para generar el certificado del servidor

Si lo deseamos podemos introducir una contraseña para el inicio en el apartado Challenge password

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server server2019
Generating a RSA private key
.....
.+++++
.....
writing new private key to 'keys\server2019.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]:
State or Province Name (full name) [GA]:
Locality Name (eg, city) [Coruña]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:server2019
Name [changeme]:server
Email Address [mail@admin.server2019]:
```

Podemos pulsar intro hasta Sign the certificate? [y/n]: donde escribimos y
Esto sirve para firmar el certificado y que sea de nuestra confianza
En la siguiente pregunta también escribimos y. Para terminar de firmar el certificado

```
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'SP'
stateOrProvinceName :PRINTABLE:'GA'
localityName         :T61STRING:'Coru\0xFFFFFB1a'
organizationName    :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'server2019'
name                 :PRINTABLE:'server'
emailAddress         :IA5STRING:'mail@admin.server2019'
Certificate is to be certified until Dec 20 07:51:25 2031 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Solo nos faltaría encriptar los archivos para que la conexión sea segura. Esto lo hacemos con el comando build-dh. Este comando puede tardar desde unos segundos hasta unos minutos dependiendo del hardware.

```
C:\Program Files\OpenVPN\easy-rsa> build-dh
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+..
.....+..
.....+..
.....+..+*++*++*++*
C:\Program Files\OpenVPN\easy-rsa>
```

Configuración de parámetros

La configuración del VPN en el servidor se realiza a través de un archivo de configuración.

Primero abrimos OpenVPN Sample Configuration Files que es donde se encuentran los archivos de configuración de ejemplo.

 client	31/10/2019 18:56	OpenVPN Config ...	4 KB
 sample	31/10/2019 18:56	OpenVPN Config ...	3 KB
 server	31/10/2019 18:56	OpenVPN Config ...	11 KB

Y copiamos el server.ovpn a la ruta C:\Program Files\OpenVPN\config

 README	18/12/2021 13:21	Documento de tex...	1 KB
 server	31/10/2019 18:56	OpenVPN Config ...	11 KB

Lo editamos (preferiblemente en un programa como WordPad porque el bloc de notas puede descolocar el contenido).cambiamos las líneas:

```
ca ca.crt → ca C:\\Users\\user\\OpenVPN\\config\\ca.crt
cert server.crt → cert C:\\Users\\user\\OpenVPN\\config\\server.crt
key server.key → key C:\\Users\\user\\OpenVPN\\config\\server.key
```

Server es el nombre que se introduce en el Common Name por lo que en nuestro caso será:

```
ca C:\\Users\\user\\OpenVPN\\config\\ca.crt
cert C:\\Users\\user\\OpenVPN\\config\\server2019.crt
key C:\\Users\\user\\OpenVPN\\config\\server2019.key
```

```
dh dh2040.pem
dh C:\\Users\\user\\OpenVPN\\config\\server2019.key\\dh2048.pem
Debemos comprobar que en la ruta C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ existe el archivo dh2048.pem o por lo contrario es dh4096.pem si este es el caso el cambio sería: dh dh2040.pem por
dh C:\\Users\\user\\OpenVPN\\config\\server2019.keydh2096.pem
  ca C:\\Users\\user\\OpenVPN\\config\\ca.crt
  cert C:\\Users\\user\\OpenVPN\\config\\server2019.crt
  key C:\\Users\\user\\OpenVPN\\config\\server2019.key
  # This file should be kept secret
  #   openssl dhparam -out dh2048.pem 2048
  dh C:\\Users\\user\\OpenVPN\\config\\dh2048.pem
```

Estos cambios son para indicar al servidor donde se encuentran los certificados y las claves para establecer la conexión

Direcciones IP

Podemos modificar el archivo server.ovpn en la asignación de la dirección IP de la red al servidor

Este paso es opcional, por defecto el servidor VPN adoptará la dirección IP 10.8.0.1 en su adaptador TAP y continuará teniendo la IP real de nuestra LAN interna. Así

mismo la asignación de IP a los clientes conectados irá desde la 10.8.0.2 hasta la 10.8.0.254 y mascara de red 255.255.255.0

```
# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0
```

Es importante tener en cuenta que, si nuestro router por ejemplo tiene la dirección IP 192.168.0.1, no debemos utilizar en el fichero de configuración la red 192.168.0.0, ya que la IP del router entraría en conflicto con la del TAP, y la conexión no se podría efectuar

Por último comprobamos que la línea tls-auth ta.key tenga el valor 0

```
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
```

El valor 0 se deja para el servidor y el 1 para el cliente

Guardamos el archivo

El tls-auth agrega una firma HMAC adicional a todos los paquetes de protocolo de enlace SSL / TLS para verificar la integridad. Para proteger:

- Ataques Dos se genera una cantidad masiva de peticiones al servidor desde el mismo dispositivo o IP para consumir los recursos del servicio hasta el punto de que se produzca una denegación de servicio
- Escaneo de puertos
- Vulnerabilidades en la implantación de SSL / TLS
- Inicio de protocolo de enlace SSL / TLS en dispositivos no autorizados

Configuración del servidor OpenVPN

Para terminar realizaremos la generación de ta.key, modificación del path y copia de certificados y claves a config

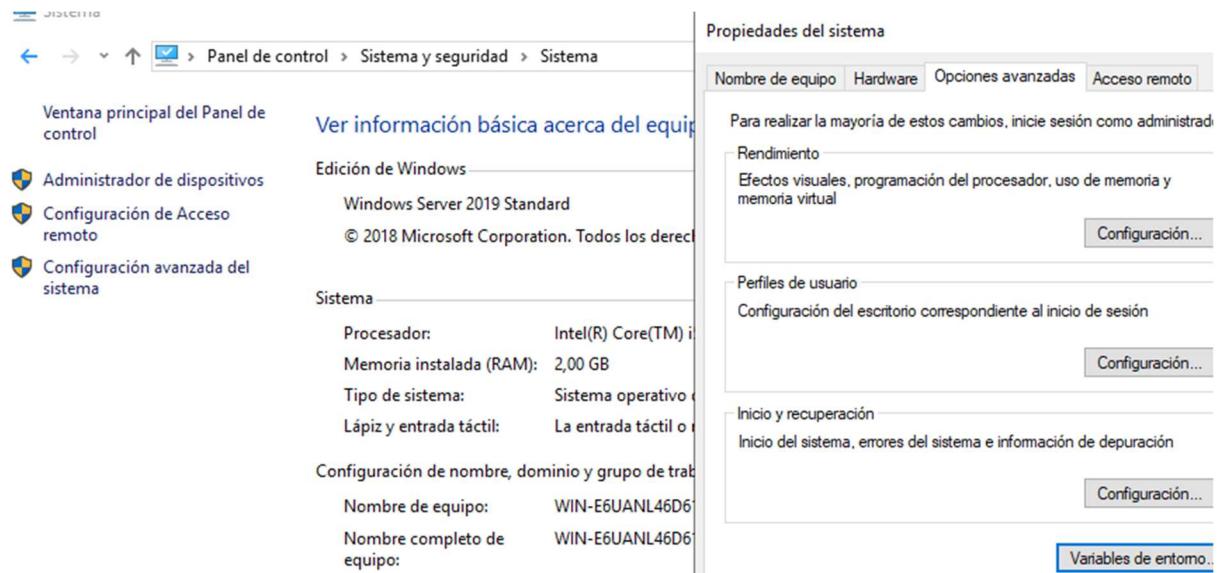
Empezamos por la modificación del path

El path es donde el sistema busca los comandos que se ejecutan en el terminal

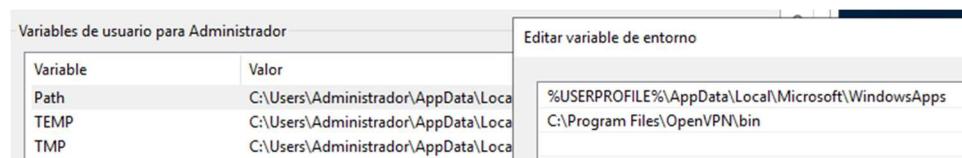
Iremos a utilizar el openvpn

Tenemos dos opciones: modificar el path o ejecutar el comando openvpn directamente

Vamos al panel de control → sistema y seguridad → sistema → configuración avanzada del sistema → variables del entorno.



Editamos el Path y añadimos la ruta C:\Program Files\OpenVPN\bin



Para crear la última clave para el servidor con el comando:

Abrimos el cmd: cd C:\Program Files\OpenVPN\bin

y ejecutamos el comando openvpn --genkey --secret ta.key para crear la última clave para el servidor que requiere el uso de tls-auth

```
C:\Program Files\OpenVPN\bin>openvpn --genkey --secret ta.key
C:\Program Files\OpenVPN\bin>
```

El comando genera una clave OpenVPN y la escribirá en el archivo ta.key que se debe de copiar a través de un medio seguro a todos

Ya solo nos falta copiar todos los archivos creados a la misma carpeta del archivo de configuración del servidor.

Por último vamos cogemos los cuatro ficheros generados que deberán de estar en: C:\Program Files\OpenVPN\easy-rsa\keys

01.pem	22/12/2021 8:52	Archivo PEM	9 KB
ca	22/12/2021 8:50	Certificado de seg...	3 KB
ca.key	22/12/2021 8:49	Archivo KEY	4 KB
dh2048.pem	22/12/2021 8:57	Archivo PEM	1 KB
index	22/12/2021 8:52	Documento de tex...	1 KB
index.txt.attr	22/12/2021 8:52	Archivo ATTR	1 KB
serial	22/12/2021 8:52	Archivo	1 KB
server2019	22/12/2021 8:52	Certificado de seg...	9 KB
server2019.csr	22/12/2021 8:51	Archivo CSR	2 KB
server2019.key	22/12/2021 8:50	Archivo KEY	4 KB

Y en \easy-rsa copiamos el archivo ta.key

libcrypto-1_1-x64.dll	31/10/2019 19:09	Extensión de la apl...	2.971 KB
liblzo2-2.dll	31/10/2019 19:09	Extensión de la apl...	220 KB
libpkcs11-helper-1.dll	31/10/2019 19:09	Extensión de la apl...	124 KB
libssl-1_1-x64.dll	31/10/2019 19:09	Extensión de la apl...	618 KB
openssl	31/10/2019 19:09	Aplicación	925 KB
openvpn	31/10/2019 19:09	Aplicación	821 KB
openvpn-gui	31/10/2019 19:09	Aplicación	654 KB
openvpnserv	31/10/2019 19:09	Aplicación	65 KB
openvpnserv2	06/03/2018 9:58	Aplicación	24 KB
ta.key	22/12/2021 9:26	Archivo KEY	1 KB

Si hemos ejecutado el openvpn desde la carpeta bin el ta.key ya se encuentra en el directorio

Los archivos los pegamos a la ruta C:\Program Files\OpenVPN\config (en esta ruta tendremos que tener 7 archivos contando el readme)

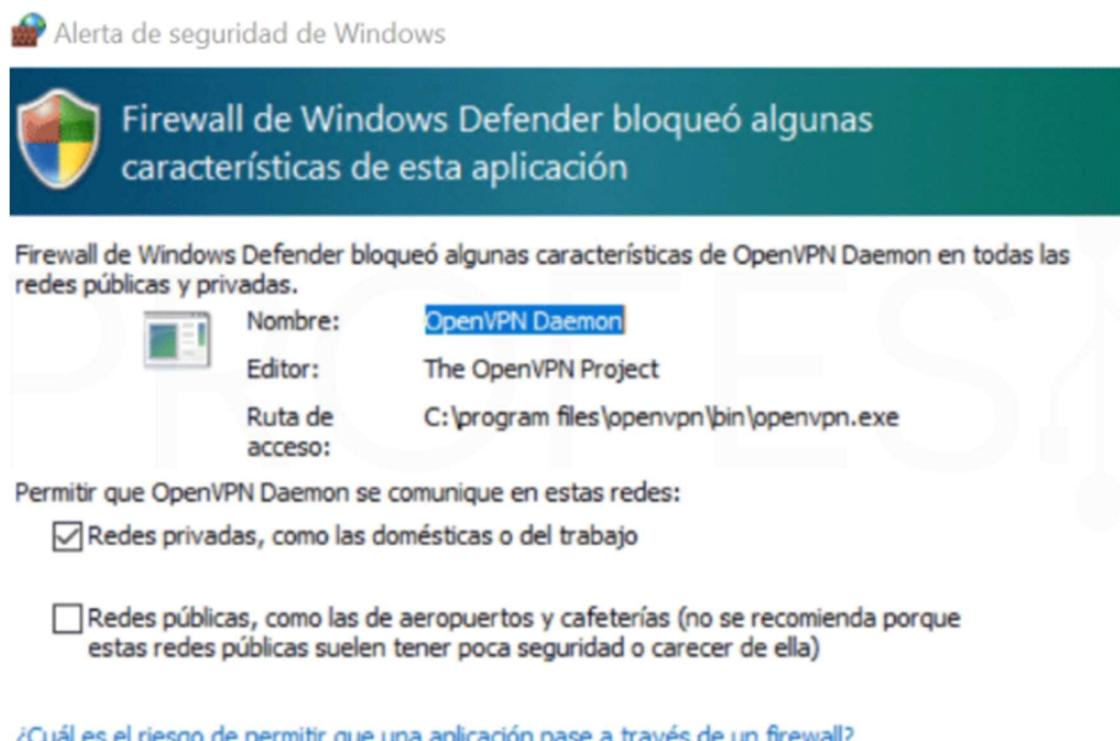
ca	22/12/2021 8:50	Certificado de seg...	3 KB
dh2048.pem	22/12/2021 8:57	Archivo PEM	1 KB
README	18/12/2021 13:21	Documento de tex...	1 KB
server	22/12/2021 9:20	OpenVPN Config ...	11 KB
server2019	22/12/2021 8:52	Certificado de seg...	9 KB
server2019.key	22/12/2021 8:50	Archivo KEY	4 KB
ta.key	22/12/2021 9:26	Archivo KEY	1 KB

Inicio del servicio OpenVPN

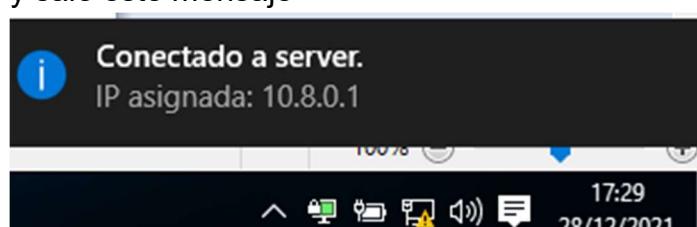
Tendremos que ejecutar el OpenVPN GUI y en la barra de tareas pulsamos con el botón derecho en la opción connect.

Puede ser que tengamos que permitir el acceso del servicio OpenVPN a las redes a través del firewall de Windows.

En el caso de utilizarlo con Wifi o de forma remota hay que activar las casillas de redes privadas y públicas.



Cuando el servicio inicia correctamente se ve un log y sale este mensaje



Asignación de IP fija en el servidor

Es muy importante que el servidor tenga una IP fija para que así el router pueda entregar los paquetes pidiendo la conexión desde el equipo clientes.

El siguiente paso es asignar una IP al servidor, para esto hay dos opciones: directamente desde el router asociado con la MAC de la tarjeta de red. o en la configuración de Windows

Explicaremos la segunda opción que es más rápida y sencilla

Vamos a Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador → Propiedades

Introducimos:

- Dirección IP
- Máscara de red
- Puerta de enlace predeterminada
- Servidor DNS preferido
- Servidor DNS alternativo

Apertura de puertos en router y DDNS

En el caso de usar conexiones remotas para poder conectarnos desde cualquier lugar del mundo debemos tener en cuenta los requisitos que son:

- Efectuar una apertura del puerto utilizado por OpenVPN
- Tener una IP fija o en su caso usar un DDNS,(DNS dinámico)

Lo primero es abrir el puerto 1194 UDP del router, en casi todos se puede hacer con la configuración de port forwarding.

Accedemos con la IP en el apartado de WAN.(en la pestaña Virtual Server / Port Forwarding)

Completamos los datos:

- Service name
- External Port: 1194
- Internal IP Address
- Protocol UDP

Basic Config				
Enable Port Forwarding		ON		
Port Forwarding List (Max Limit : 64)				
Service Name	External Port	Internal Port	Internal IP Address	Protocol

Ya tendríamos acceso a nuestro servidor VPN desde el exterior

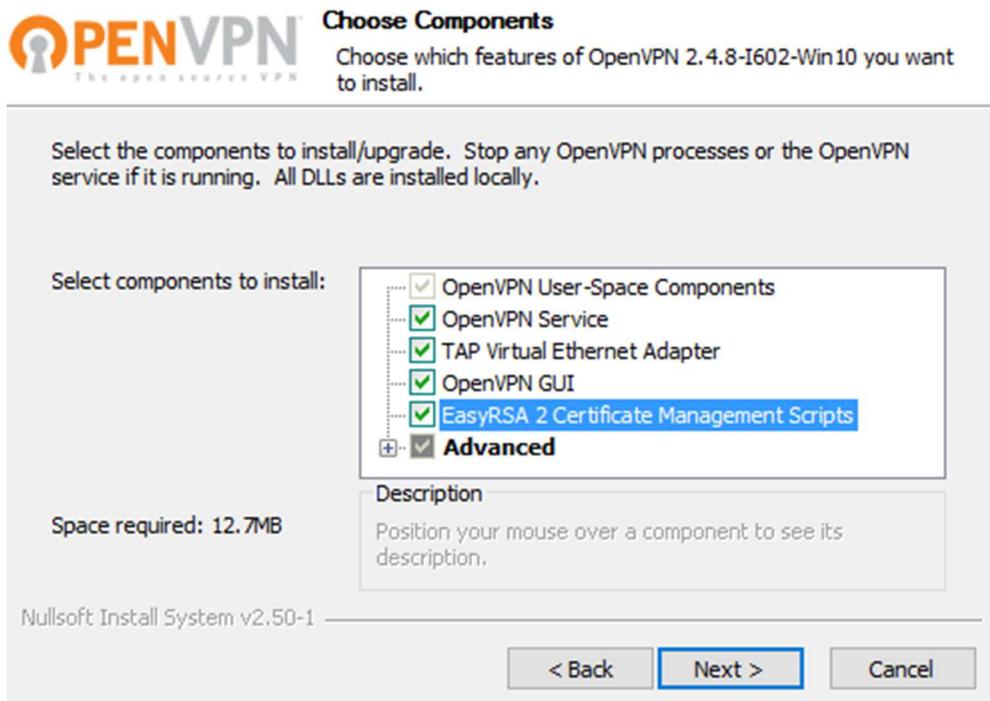
En el caso de que no tengamos una IP fija configuraremos la pestaña DDNS.

DDNS Service	
Desea habilitar el cliente DDNS	<input checked="" type="radio"/> Sí <input type="radio"/> No
DDNS status	Registro realizado correctamente.
Method to retrieve WAN IP	Internal ▾
Servidor	Www.DYNDNS.ORG ▾ Prueba gratuita
Nombre de host	[REDACTED]
Nombre de usuario o dirección de correo electrónico	[REDACTED]
Contraseña o clave de DDNS	[REDACTED]
Desea habilitar los comodines	<input checked="" type="radio"/> Sí <input type="radio"/> No
Forced update interval (in days)	21
Verificación de la dirección IP WAN y del nombre de host	<input checked="" type="radio"/> Sí <input type="radio"/> No

Configuración del cliente

En el cliente

Como ya tenemos la VPN creada en Windows configuraremos un cliente OpenVPN. Lo primero es instalar el programa con los mismos pasos que para el servidor. Seleccionamos los componentes además de los que vienen por defecto, marcamos la opción de EasyRSA 2 Certificate Management Scripts. Es posible que nos aparezca un mensaje al finalizar la instalación indicando que no hay ningún archivo de configuración, clic en Aceptar.



Copiamos los archivos que hemos generado en el servidor en la carpeta C:\Program Files\OpenVPN\config.

	ca	03/03/2022 16:10	Certificado de seg...	3 KB
	dh2048.pem	03/03/2022 16:10	Archivo PEM	1 KB
	ipp	03/03/2022 16:10	Documento de tex...	0 KB
	openvpn-status	03/03/2022 16:10	Documento de tex...	1 KB
	README	06/01/2022 17:37	Documento de tex...	1 KB
	server2019	03/03/2022 16:10	Certificado de seg...	9 KB
	server2019.key	03/03/2022 16:10	Archivo KEY	4 KB
	ta.key	03/03/2022 16:10	Archivo KEY	1 KB

El procedimiento en el archivo de configuración del cliente es similar al del servidor. En la ruta C:\Program Files\OpenVPN\sample-config cogemos el archivo client y lo ponemos en C:\Program Files\OpenVPN\config. Además necesitamos renombrarlo al nombre que pusimos en common name que era clientew10

 ca	03/03/2022 16:10	Certificado de seg...	3 KB
 clientew10	31/10/2019 18:56	OpenVPN Config ...	4 KB
 dh2048.pem	03/03/2022 16:10	Archivo PEM	1 KB
 ipp	03/03/2022 16:10	Documento de tex...	0 KB
 openvpn-status	03/03/2022 16:10	Documento de tex...	1 KB
 README	06/01/2022 17:37	Documento de tex...	1 KB
 server2019	03/03/2022 16:10	Certificado de seg...	9 KB
 server2019.key	03/03/2022 16:10	Archivo KEY	4 KB
 ta.key	03/03/2022 16:10	Archivo KEY	1 KB

Recuerda abrirlo con un programa como Word modificamos el archivo las líneas:
remote → remote (IP del servidor)

remote 10.8.0.1 1194

ca → "C:\\Program Files\\OpenVPN\\config\\ca.crt"

cert → "C:\\Program Files\\OpenVPN\\config\\clientew10.crt"

key → "C:\\Program Files\\OpenVPN\\config\\clientew10.key"

y guardamos el archivo

```
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\clientew10.crt"
key "C:\\Program Files\\OpenVPN\\config\\clientew10.key"
```

Con esto ya estaría todo perfectamente configurado para realizar la conexión entre cliente – servidor

En el servidor

Ejecutamos el comando vars que no debería devolver ninguna salida

```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>
```

A continuación ejecutamos build-key nombre del cliente en nuestro caso es build-key clientew10

Recuerda que no tiene porque ser el nombre del equipo ni el del usuario sino el que prefieras

Como en el servidor pulsa intro hasta llegar al common name donde pondremos el nombre del cliente que anteriormente hemos indicado

Podemos pulsar intro hasta Sign the certificate? [y/n]: donde escribimos y

En la siguiente pregunta también escribimos y.

```
C:\Program Files\OpenVPN\easy-rsa>build-key clientew10
Generating a RSA private key
-----
writing new private key to 'keys\clientew10.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [SP]: SP
State or Province Name (full name) [GA]: GA
Locality Name (eg, city) [Coru  a]: Coru  a
Organization Name (eg, company) [OpenVPN]: OpenVPN
Organizational Unit Name (eg, section) [changeme]: changeme
Common Name (eg, your name or your server's hostname) [changeme]:clientew10
Name [changeme]:
Email Address [mail@admin.server2019]: mail@admin.server2019

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123.
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'SP'
stateOrProvinceName :PRINTABLE:'GA'
localityName         :T61STRING:'Coru\0xFFFFFB1a'
organizationName    :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'changeme'
commonName          :PRINTABLE:'clientew10'
name                :PRINTABLE:'changeme'
emailAddress        :IA5STRING:'mail@admin.server2019'
Certificate is to be certified until Feb 29 15:26:04 2032 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Ahora copiamos los certificados y claves correspondientes para transportarlos hacia el equipo cliente, que serán:

ca.crt (creado ya en el servidor)

ta.key (creado ya en el servidor)

nombrecliente.crt (en nuestro caso clientew10.crt)

nombrecliente.key (en nuestro caso clientew10.key)

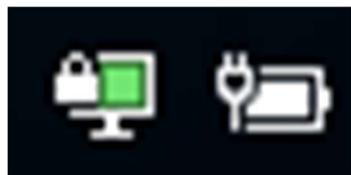
 ca.crt	03/03/2022 16:32	Certificado de seg...	3 KB
 clientew10.crt	03/03/2022 16:32	Certificado de seg...	9 KB
 clientew10.key	03/03/2022 16:32	Archivo KEY	4 KB
 ta.key	03/03/2022 16:37	Archivo KEY	1 KB

Conexión con el servidor

Solo nos falta iniciar OpenVPN GUI en el equipo cliente y conectar, para comprobar que la conexión es correcta y que nuestro cliente se ha conectado al servidor de OpenVPN.

Si todo es correcto, el ícono de la VPN en la barra de tareas deberá estar en verde.

Si está en amarillo significa que al conexión no se ha podido realizar.



Gestor de base de datos

Es un programa que permite almacenar, modificar y extraer datos de una base de datos. También tienen formas para la integridad, administración de acceso y recuperar los datos. La mayor parte contienen un generador de informes y un modo gráfico para obtener la información con gráficos o tablas. Se accede a la información utilizando lenguajes de consultas como SQL.

Tipos:

- Jerárquico es el modelo más antiguo en donde los datos se guardan de manera jerárquica formando un árbol al revés su objetivo principal es almacenar grandes cantidades de datos. Su estructura era un nodo raíz que podría tener nodos padres y estos nodos hijos así sucesivamente.
Ejemplos: Adabas, GT.M, IMS y Focus.
- En red es un modelo donde los datos están representados de una forma gráfica formando una red en el cual se muestra la estructura lógica con las limitaciones de acceso a estos datos. Ejemplos: IDMS.
- Relacional es un modelo en donde los datos se representan en una tabla en la cual las filas se denominan tuplas y las columnas variables.
Ejemplos: Microsoft SQL Server, Oracle, DB2, PostgreSQL, MariaDB y MySQL.
- Orientado a Objetos es un modelo en el cual los datos están representados como objetos para así poder unir las características de las bases de datos con las de los lenguajes de programación orientados a objetos como C++ o Java. En este modelo los datos se combinan en un objeto con todos sus atributos. Estos objetos se dividen en clases o subclases. A cada dato se le asigna un código de identificación que es único para facilitar la gestión. Ejemplos: Object Database ++, ObjectStore, GemStone/S, Wakanda y ObjectDB.
- Distributivo: es un modelo en el que los datos están en diferentes espacios físicos (los datos están almacenados en varios ordenadores que están conectados entre sí o también se pueden almacenar los datos en diferentes sitios de la red) formando un sistema de comunicación.
Ejemplos: Microsoft SQL Server 2008, Oracle 11g, Apache Cassandra, Apache HBase, MySQL Cluster MongoDB.

Comparativa de SQL Server y MySQL

	MySQL	SQL Server
Plataformas	FreeBSD Linux OS X Solaris Windows	Linux Windows
Lenguajes	Ada C C# C++ D Delphi Eiffel Erlang Haskell Java JavaScript (Node.js) Objective-C OCaml Perl PHP Python Ruby Scheme Tcl	C# C++ Delphi Go Java JavaScript (Node.js) PHP Python R Ruby Visual Basic
Motor	MyISAM e InnoDB	Propio
ACID	Depende del motor	Si
Replicación	Master-Master Master-Slave	Si
Transacciones	Si	Si
Reportes	No	Si
Vistas	Si	Si
Procedimientos Almacenados	Si	Si
Triggers	Si	Si
Límite de Memoria	No	No



Es un sistema de gestión de base de datos relacional producido por Microsoft. Su principal lenguaje de consulta es Transact-SQL, una aplicación de las normas ANSI / ISO estándar Structured Query Language (SQL) utilizado por ambas Microsoft y Sybase.

Características:

- Soportar transacciones.
- Escalabilidad, estabilidad y seguridad.
- Soportar procedimientos almacenados.
- Potente entorno gráfico de administración, que permite el uso de comandos DDL y DML gráficamente.
- Trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y las terminales o clientes de la red sólo acceden a la información.
- Administrar información de otros servidores de datos

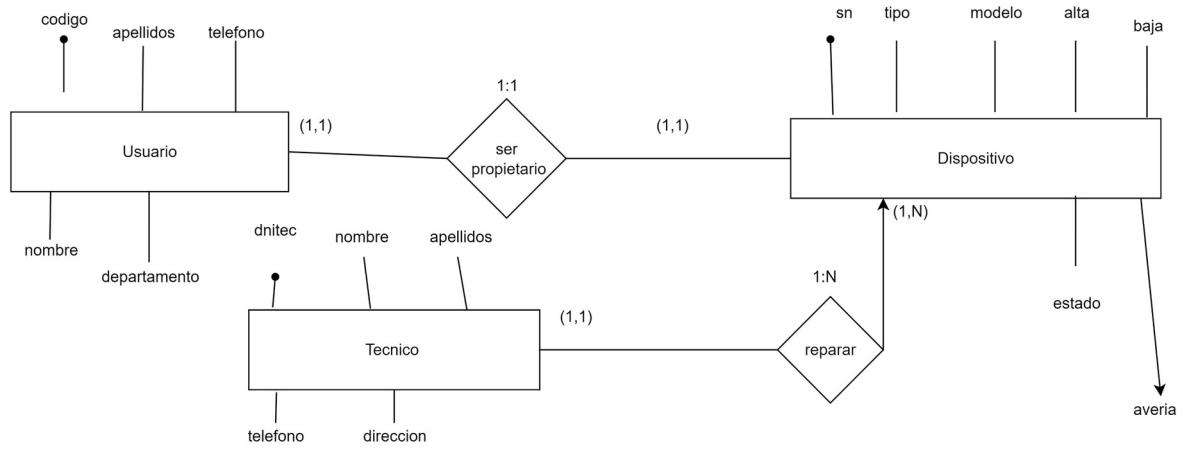
Ventajas:

- Seguridad de los datos
- Facilidad de configuración
- Almacenamiento de datos optimizado
- Soporte de recuperación de datos

Desventajas:

- Enorme cantidad de RAM
- Es de pago
- Compatibilidad restringida

Diseño de la base de datos



Tecnico (dnitec, nombre, apellido, telefono, direccion)

Usuario (cod, nombre, apellido, telefono, departamento)

Dispositivos (sn, tipo, modelo, alta, baja, estado, cod,dnitec)

Averia (sn, averia)

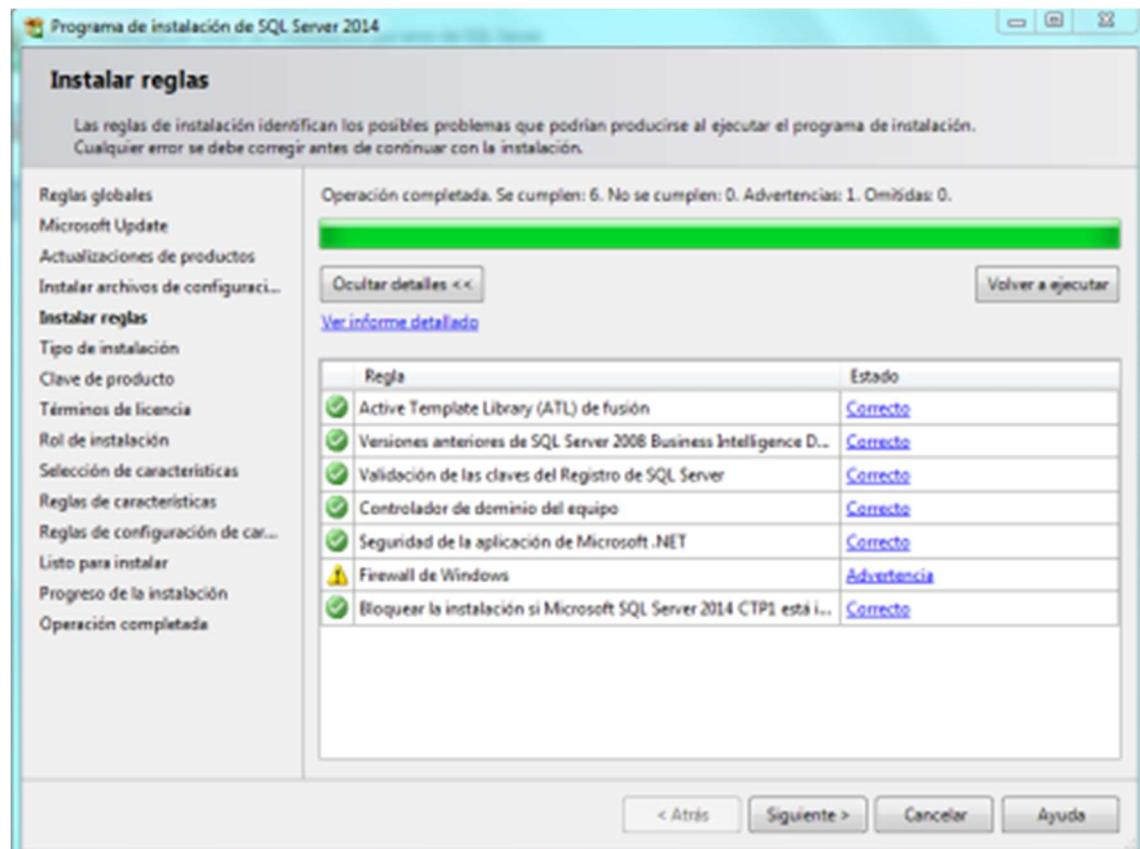
Instalación

El primer paso es abrir el centro de instalación de SQL Server. En donde pulsamos a instalación una vez leídos los requisitos de hardware y software

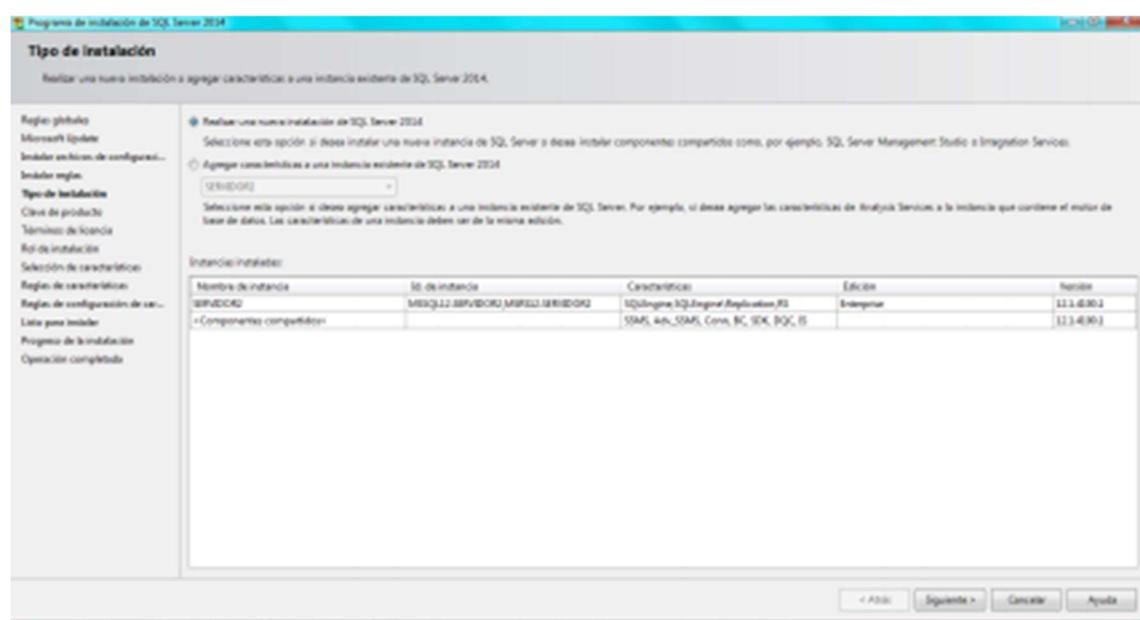
Pulsamos a Nueva instalación independiente de SQL Server o agregar características a una instalación existente



Sale un aviso en el firewall debido a que utiliza el puerto 1433 que por defecto Microsoft lo tiene cerrado. Este puerto lo usa para poder conectarse con otros equipos

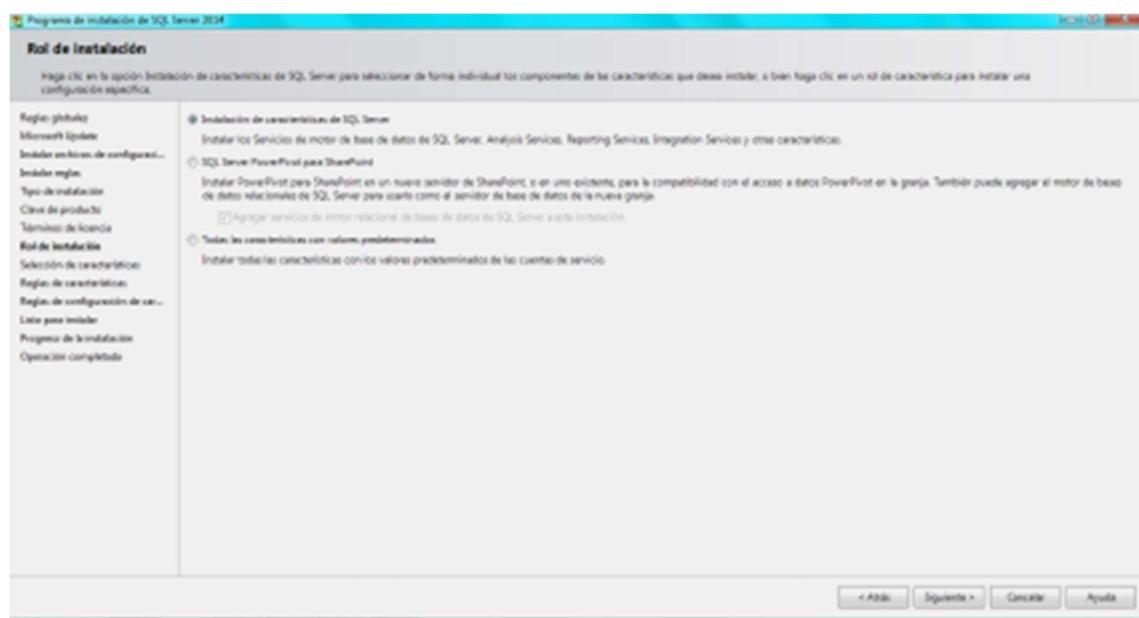


Como vamos a crear una nueva instancia de SQL Server marcamos la opción de realizar nueva instancia SQL Server



A continuación insertaremos los roles de la base de datos para eso marcamos

la opción instalación de características de SQL Server



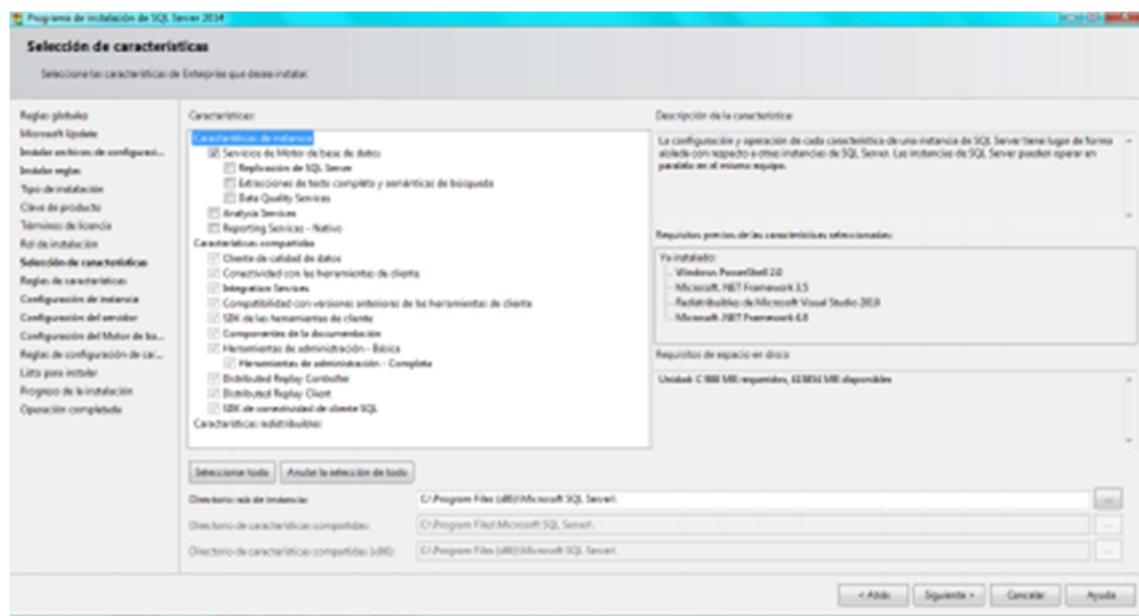
Ahora seleccionamos las características deseadas. En nuestro caso marcaremos solamente Servicios de Motor de Base de datos. Las características compartidas están marcadas porque ya se crearon con la instalación de otra instancia.

Servicios de bases de datos es el servidor de la base de datos

Replicación de SQL Server se usa para publicar la base de datos

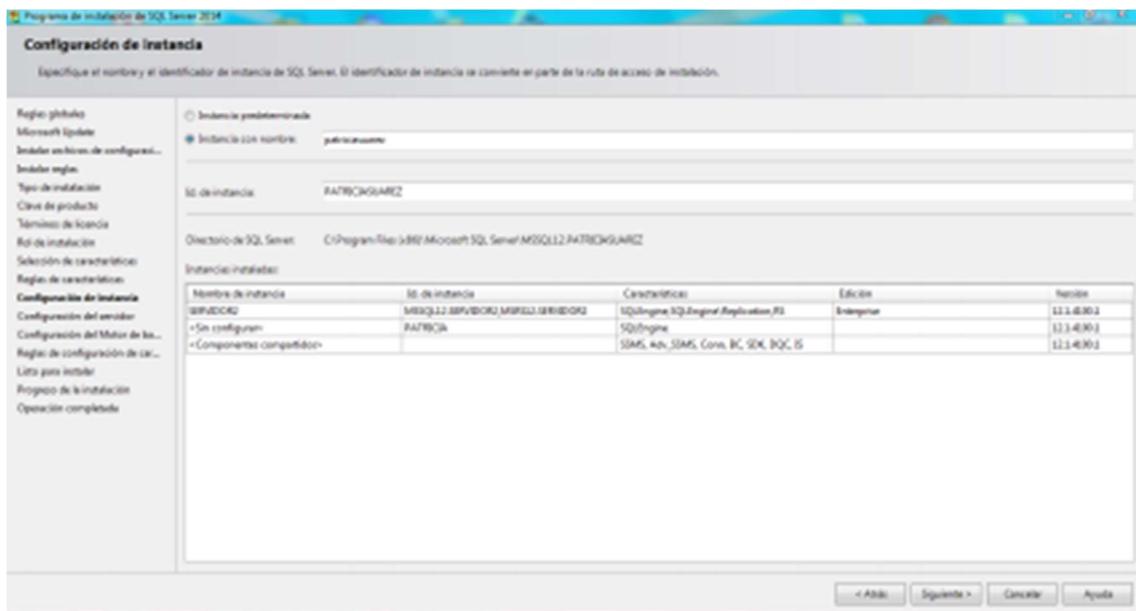
Analysis Services se utiliza para saber como evoluciona la base de datos

Reporting Services es un generador de informes



Marcamos la opción Instancia con nombre y le ponemos patriciasuarez.

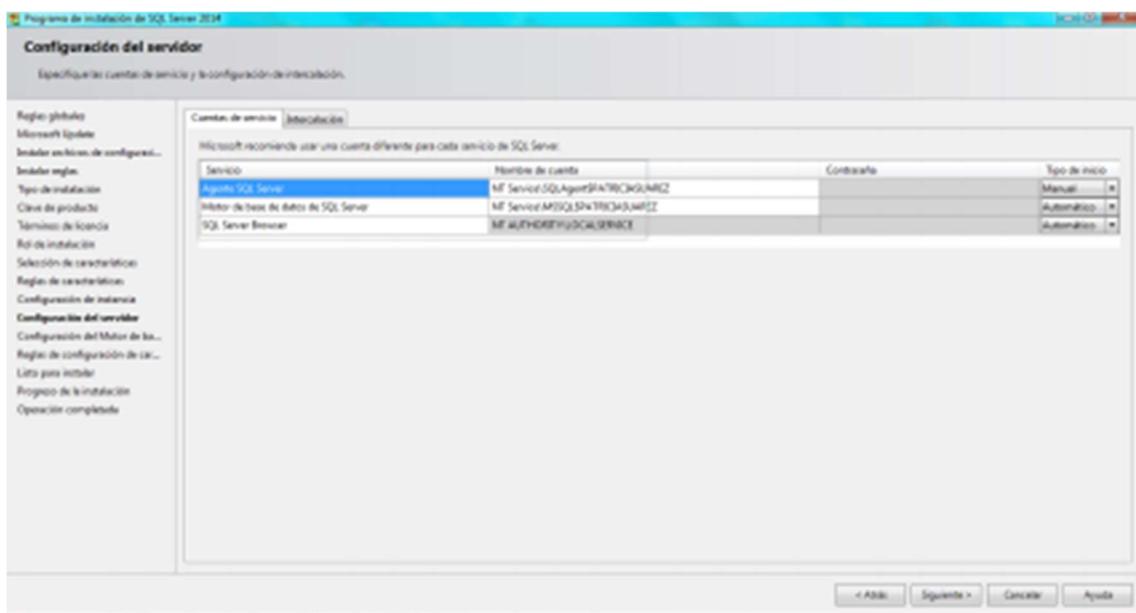
La opción de instancia predeterminada utiliza el nombre del equipo pero como es la segunda instancia que se instala no deja elegir esta opción



Aunque solo marcamos el servicios de motor de bases de datos también se instala el Agente de base de datos y el SQL Server Browser porque son obligatorios

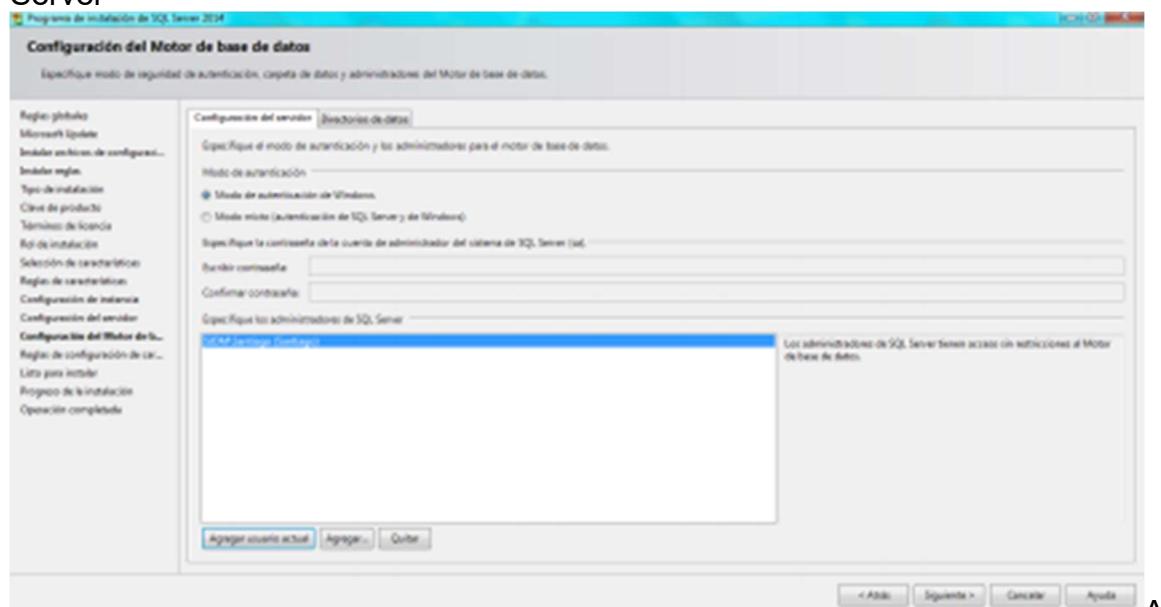
Agente SQL Server se usa para las tareas programadas

SQL Server Browser se usa como explorador de SQL Server que esta a la escucha de las peticiones de los clientes para conectarse

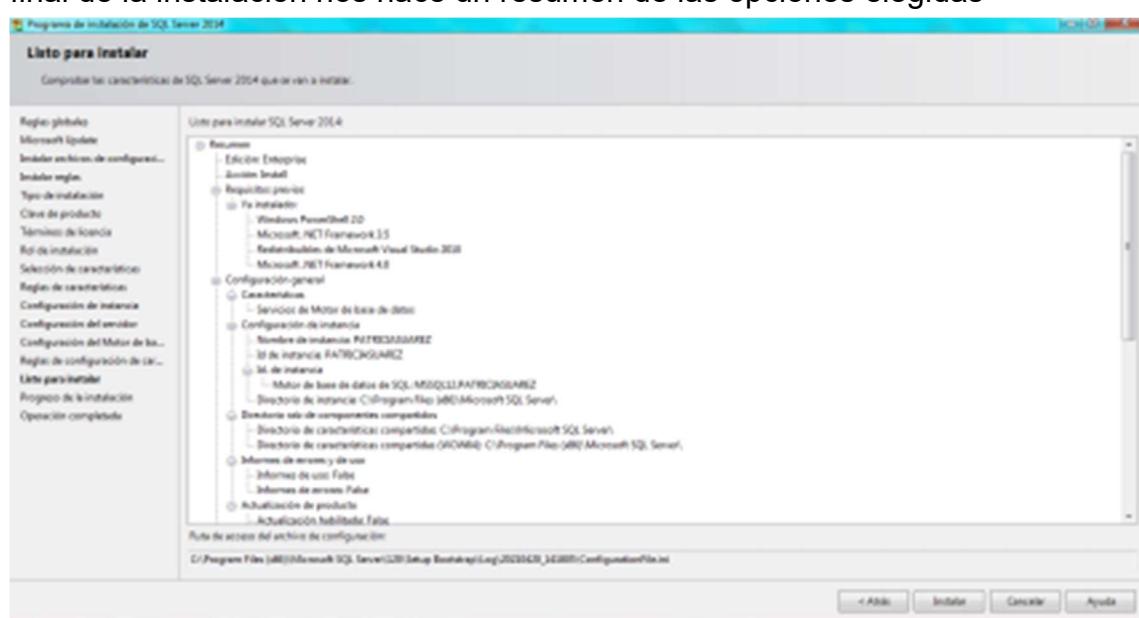


Elegimos el modo de autenticación de Windows y agregamos el usuario actual En el modo de autenticación Windows el usuario utiliza la cuenta de Windows del sistema En el modo de autenticación mixto el usuario tiene un usuario y contraseña para SQL

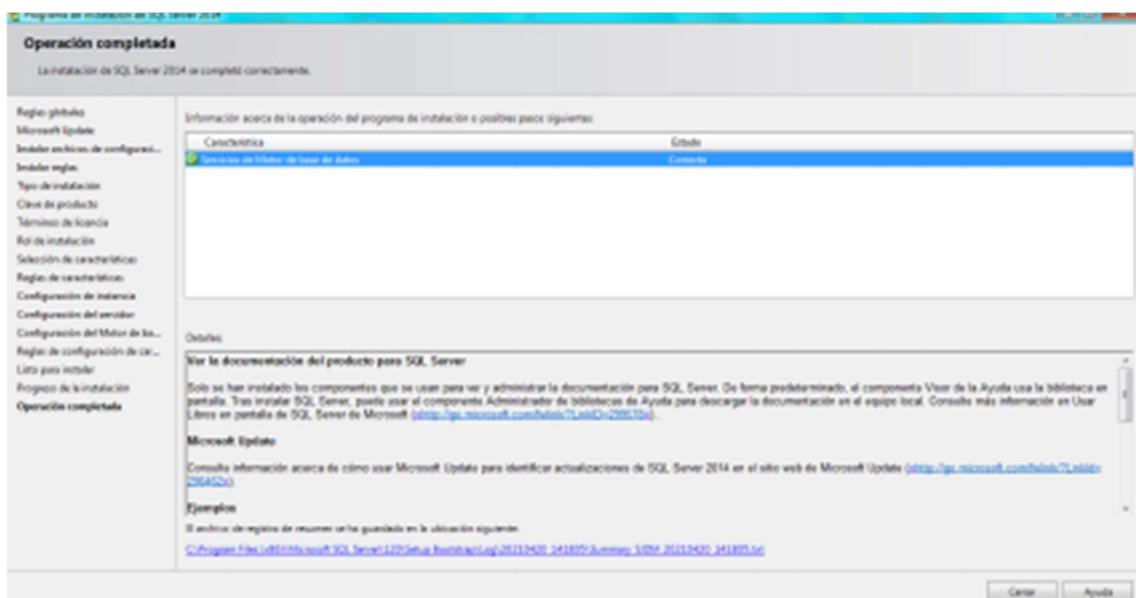
Server



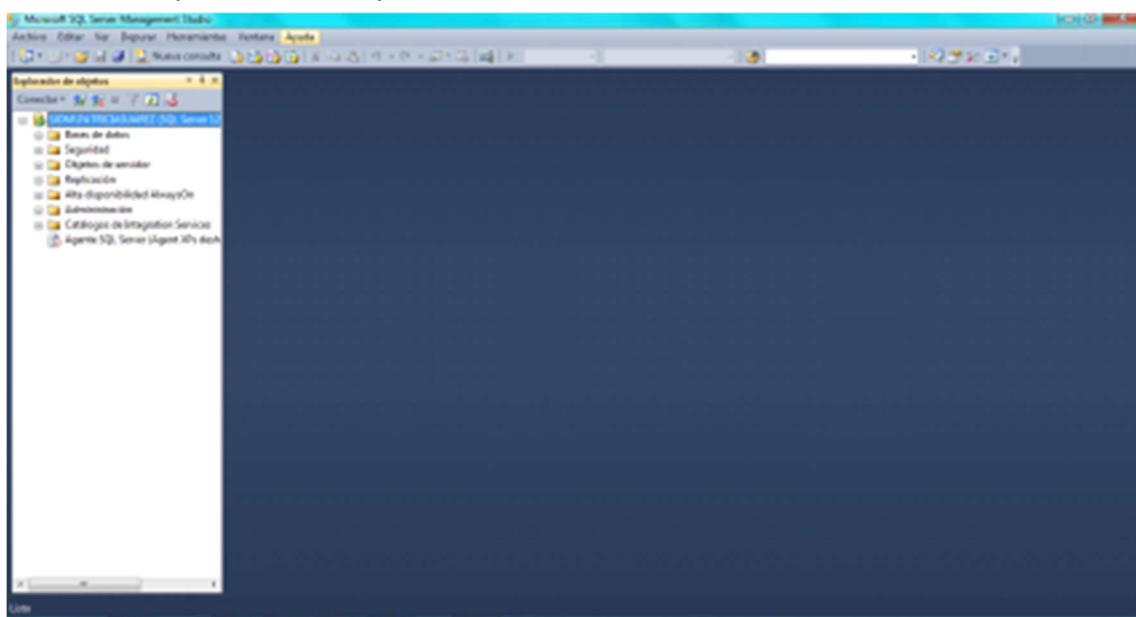
final de la instalación nos hace un resumen de las opciones elegidas



Y ya estaría instalado



También lo podemos comprobar al entrar el SQL Server



Código de creación

```
USE master;
GO
IF DB_ID ('N'Centro') IS NOT NULL
DROP DATABASE Centro;
GO

CREATE DATABASE Centro
ON
(NAME = Centro_dat,
 FILENAME = 'C:\Program Files (x86)\Microsoft SQL
Server\MSSQL12.PATRICIASUAREZ\MSSQL\DATA\Centrodat.mdf',
 SIZE =10,
 MAXSIZE = unlimited,
 FILEGROWTH = 5 )
LOG ON
( NAME = Centro_log,
 FILENAME = 'C:\Program Files (x86)\Microsoft SQL
Server\MSSQL12.PATRICIASUAREZ\MSSQL\DATA\Centrolog.ldf',
 SIZE = 5MB,
 MAXSIZE = unlimited,
 FILEGROWTH = 5MB );

GO
use Centro
go
Create Table tecnico
(dniTecnico char(9) primary key,
nombre varchar(50) not null,
apellidos varchar(50) not null,
direccion varchar(50),
telefono char(9) not null,);

GO
Create Table usuario
(cod char(9) primary key,
nombre varchar(50) not null,
apellidos varchar(50) not null,
departamento varchar(50),
telefono char(9) not null,);

GO

Create Table dispositivo
(sn char (9) primary key,
modelo varchar(50) not null,
tipo varchar (50),
alta char(8) not null,
```

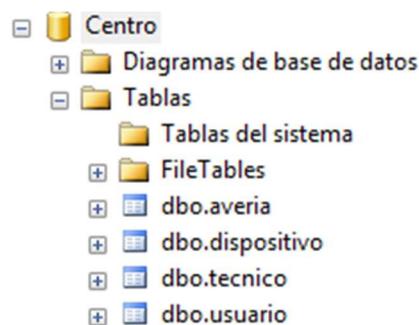
```
baja char(8),  
estado varchar(50),  
telefono char(9) not null,  
dniTecnico char(9),  
cod char(9) ,  
Foreign key (cod) references usuario (cod) on update cascade,  
Foreign key (dniTecnico) references tecnico (dniTecnico) on update cascade,);
```

Create Table averia

```
(sn char (9),  
averia varchar (50),
```

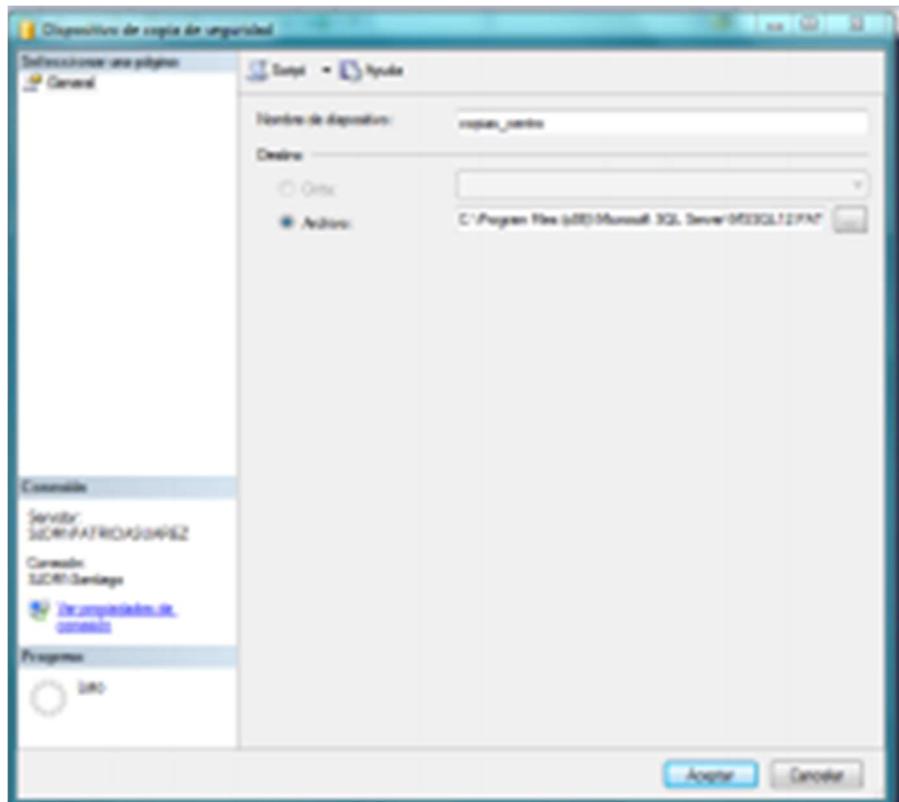
Primary key (sn, averia),

```
Foreign key (sn) references dispositivo (sn) on update cascade,);
```



Creación de un dispositivo de copias

Para crearlo expandimos bases de datos y objetos del servidor. Hacemos clic derecho sobre dispositivos de copias y nuevo dispositivo de copia

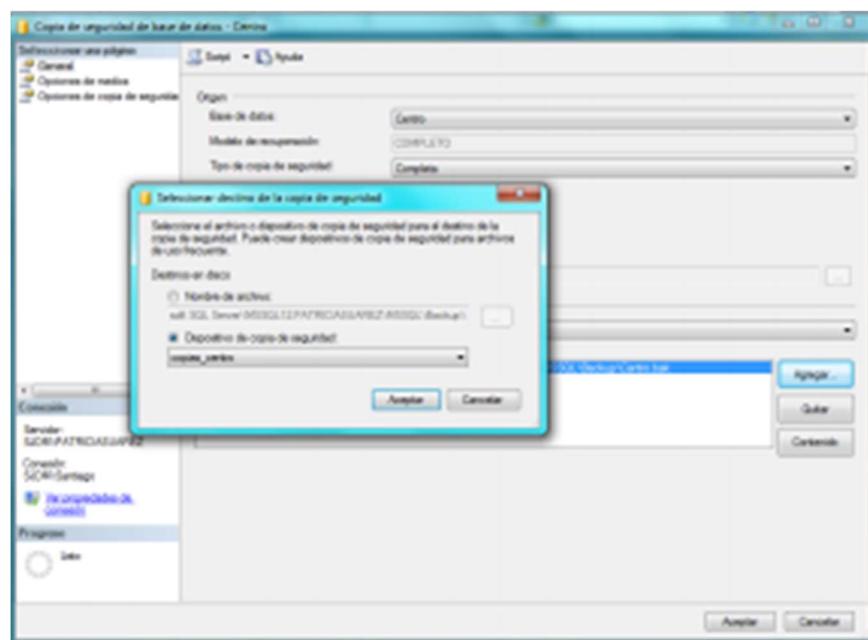


Aceptamos y ya esta creado

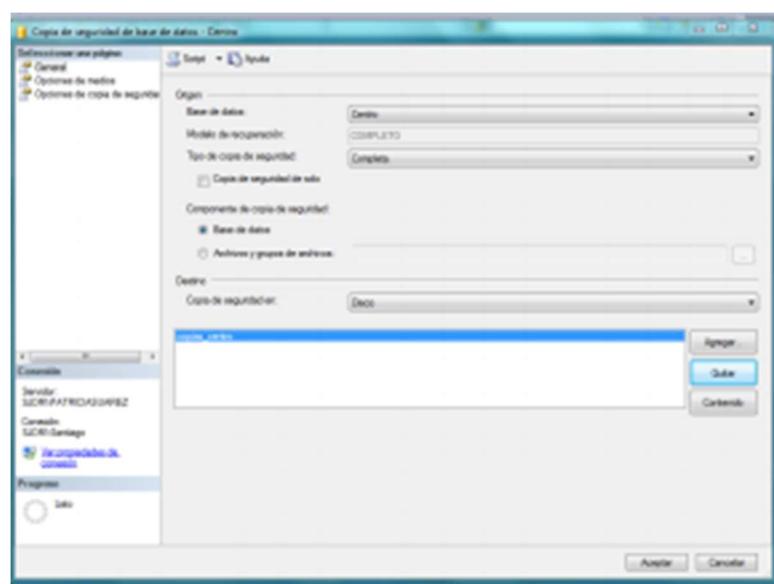
Copia de seguridad completa

Como es la primera copia de seguridad tiene que ser completa. Para hacerla expandimos la carpeta Bases de datos y clic derecho sobre nuestra base de datos. Elegimos tareas y copias de seguridad

Para que se guarde en el dispositivo en destino pulsamos a agregar y seleccionamos dispositivo de copia



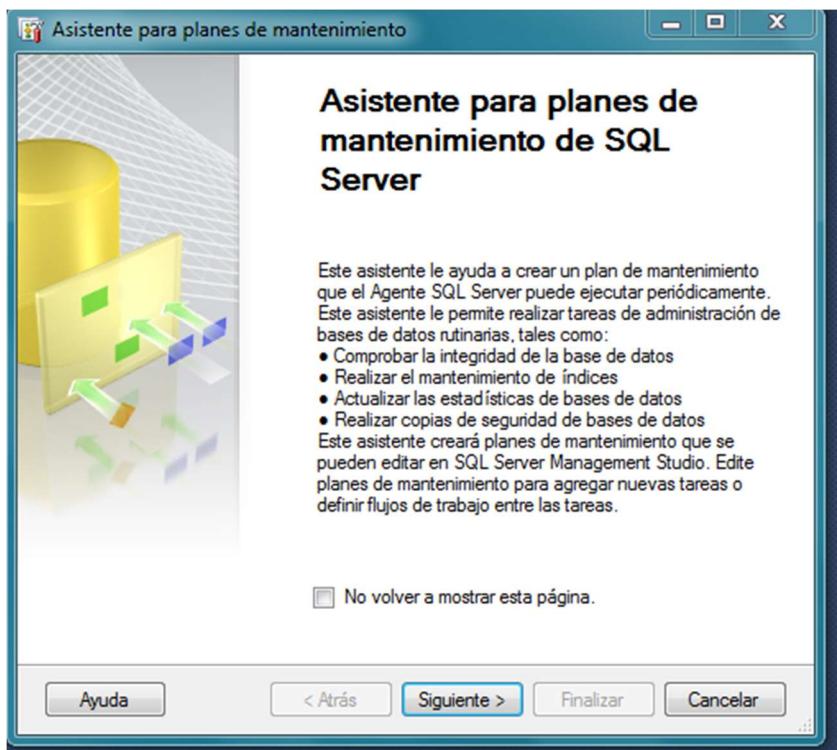
Le ponemos un nombre



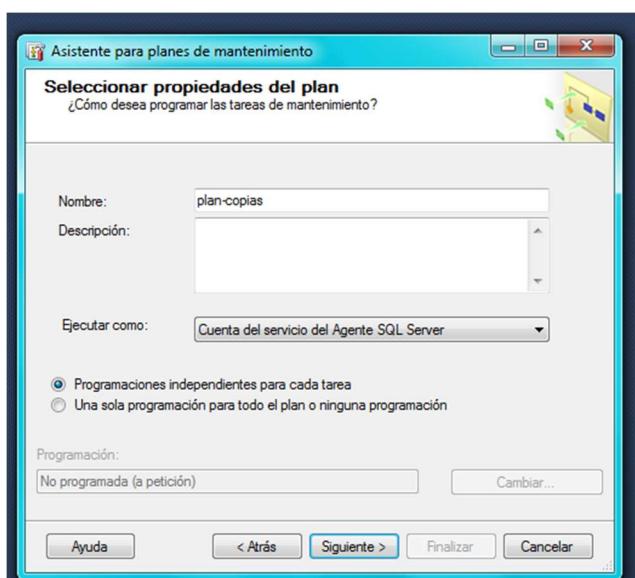
Y al pulsar a aceptar comprobamos que no se produjo ningún error

Creación de un plan de mantenimiento

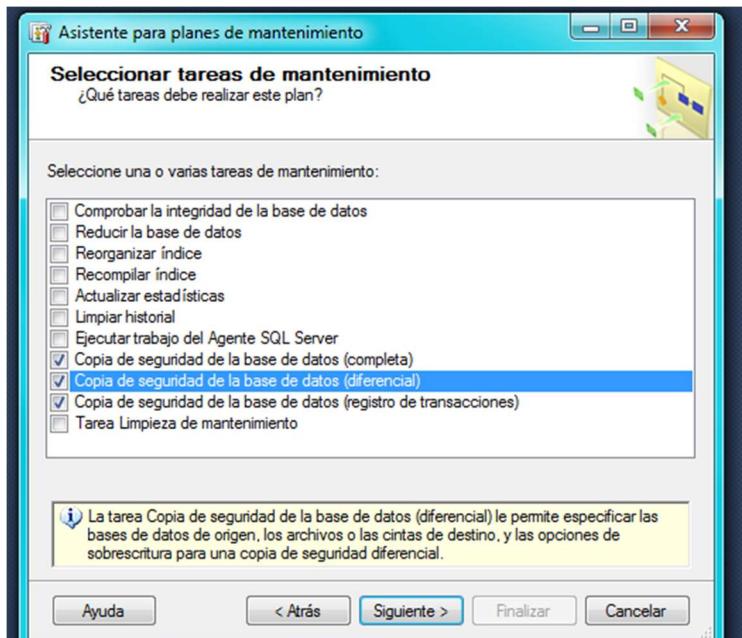
El primer paso para crear un plan de mantenimiento es expandir la carpeta de administración, clic derecho sobre plan de mantenimiento y elegimos el asistente



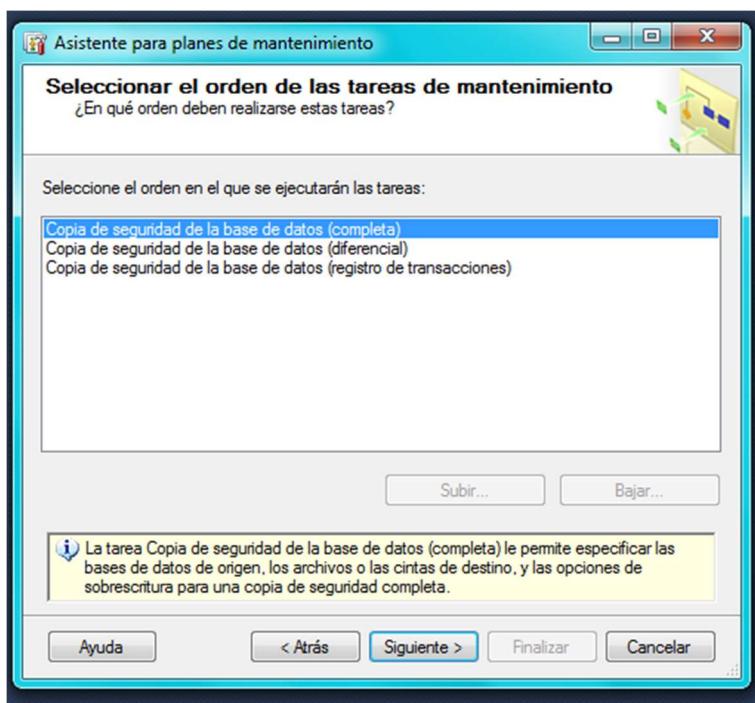
Le escribimos un nombre y marcamos la casilla de programación independiente porque cada copia de seguridad tendrá su propia programación



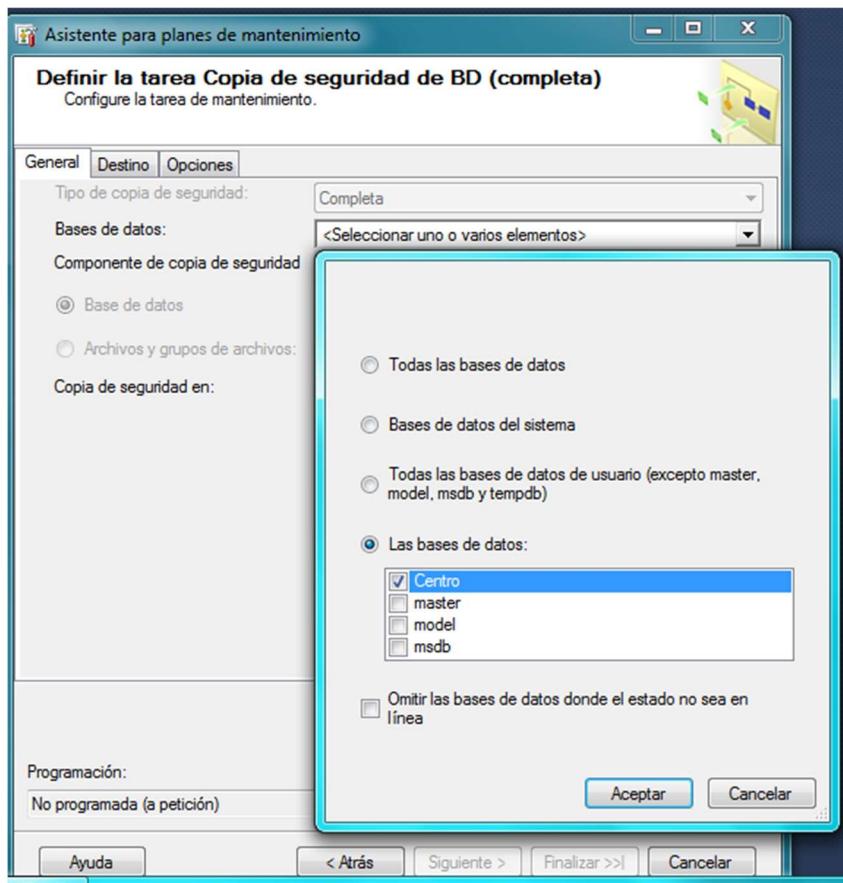
Lo siguiente es elegir qué operaciones debe de realizar en nuestro caso es realizar las copias de seguridad completa, diferencial y del registro de transacciones



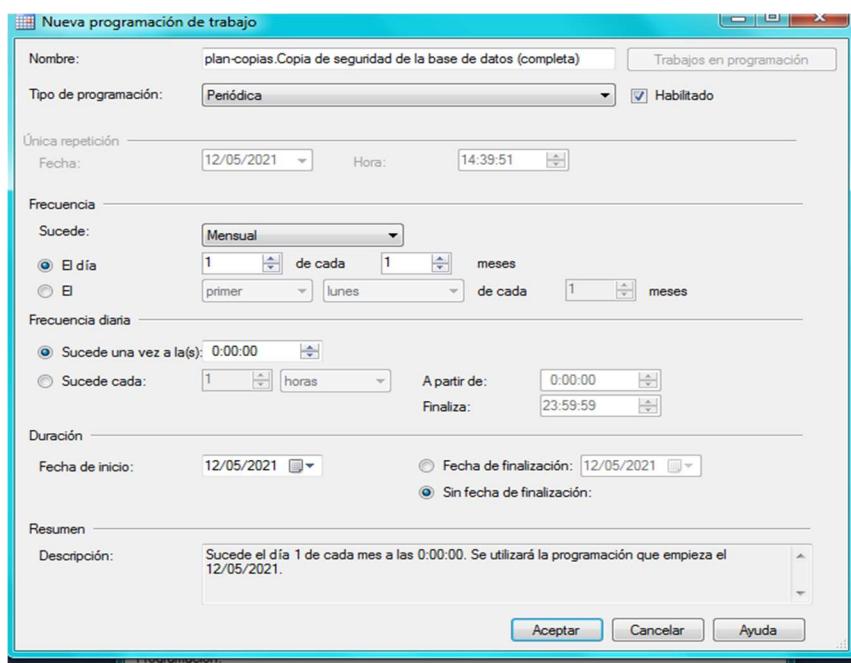
Podemos ponerle un orden a las tareas pero lo dejamos por defecto



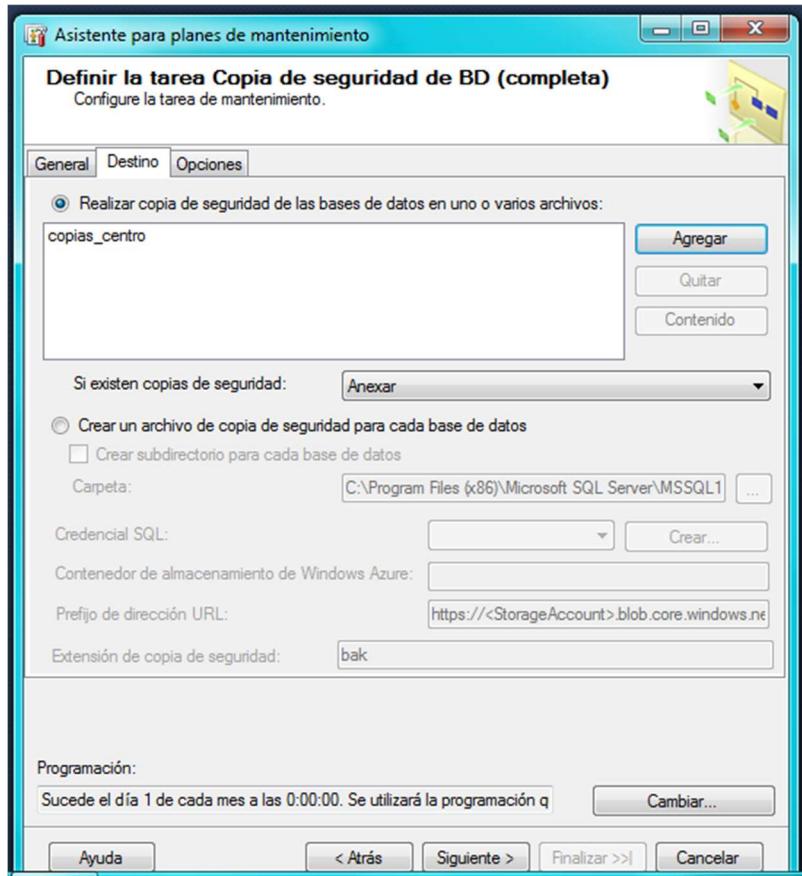
A continuación ponemos las características de las tareas. Primero será la copia completa, le marcamos nuestra base de datos



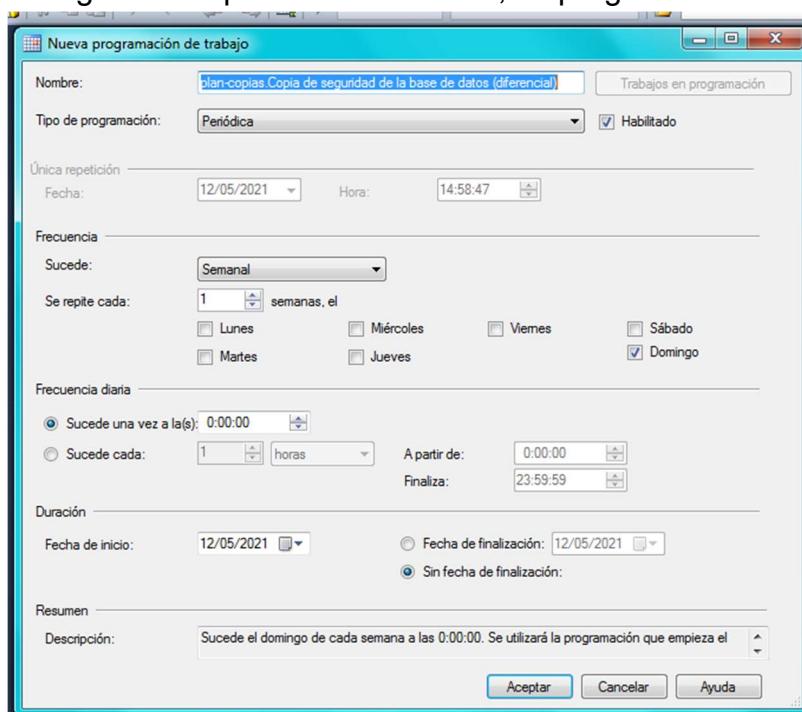
Y le introducimos la programación que definimos en la política de copias de seguridad que es una copia mensual



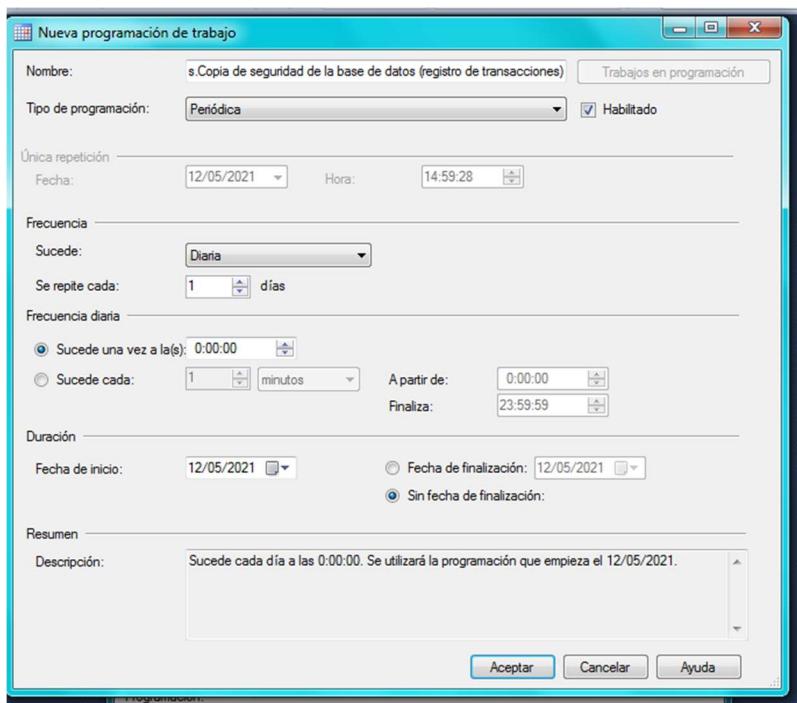
Vamos a la pestaña de destino y agregamos el dispositivo creado para las copias de seguridad



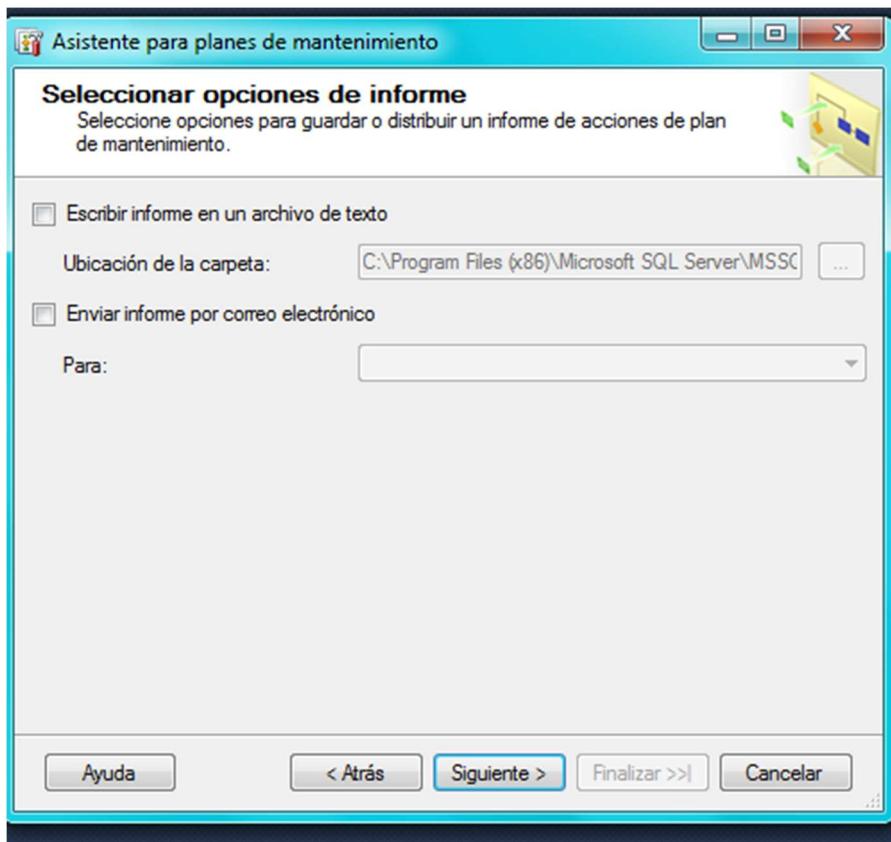
La siguiente copia es la diferencial, su programación será una copia semanal



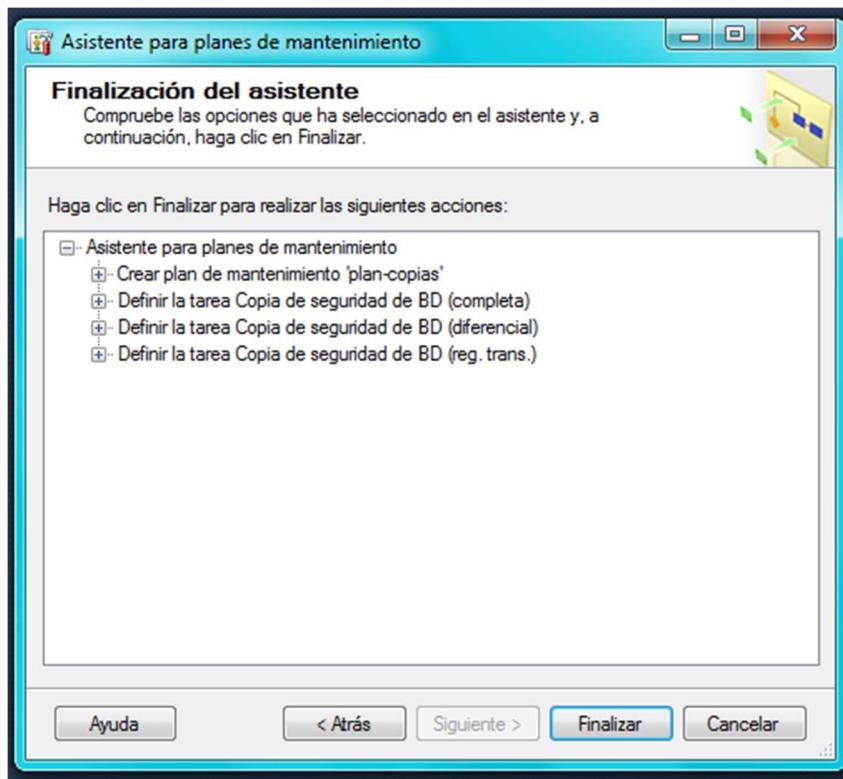
Y finalmente la copia del registro de transacciones que será diaria



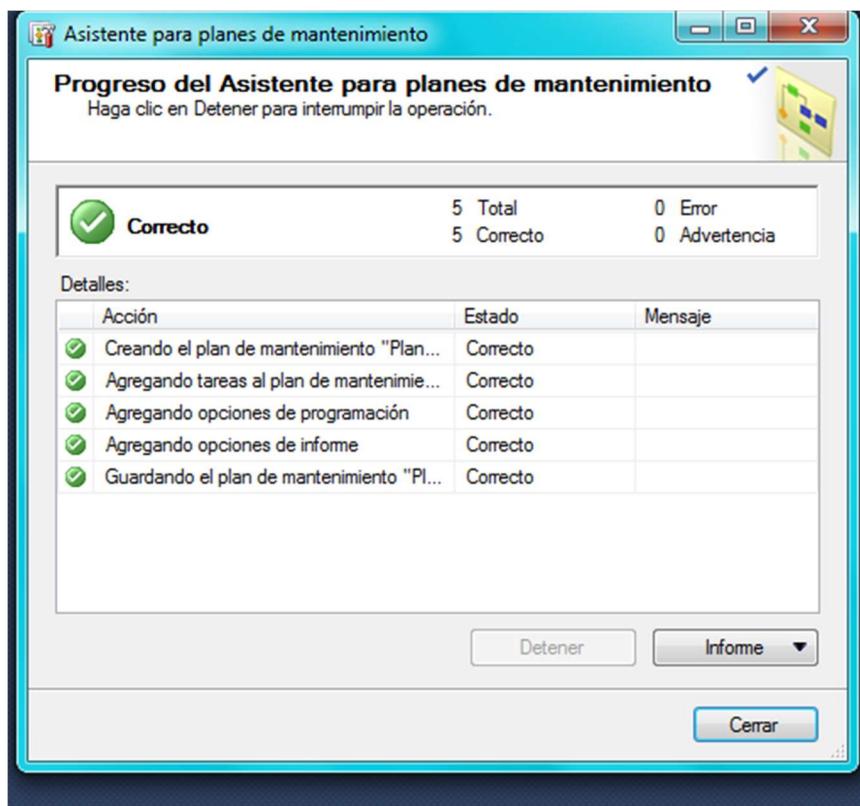
Podemos desmarcar la opción de escribir error



Este es el resumen de la creación del plan de mantenimiento



Como se puede comprobar se creó correctamente



LDAP

Sus siglas significan protocolo ligero de acceso a directorios.

Es un protocolo de licencia libre del nivel de aplicaciones que permite el acceso a la información de los directorios ordenados en una red. Utiliza el protocolo X.500 (es un directorio que contiene información de forma jerárquica)

Funcionamiento

- Es un sistema cliente/servidor
- El servidor utiliza la base de datos para guardar el directorio.
- Cliente puede consultar o modificar un directorio



Ventajas

- Toda la información está en un repositorio central
- Soporta un gran número de bases de datos
- Permite el acceso a la cuenta desde cualquier cliente LDAP

Desventajas

- Se debe habilitar un cliente

Usos

- Tener a los usuarios y otros objetos de red en una base de datos central.
- Almacena información como información de texto sin formato, imágenes, datos binarios, certificados de clave pública en la base de datos central.
- Proporciona servicios de autenticación y autorización como la gestión de inicio de sesión.
- Almacenar registros DNS en la base de datos.

Comparativa de OpenLDAP y Active Directory

	OpenLDAP	Active Directory
Definición	Programa para modificar y consultar elementos en proveedores de servicios de directorio	Sistema de base de datos de Microsoft que proporciona servicios de directorio, autenticación, políticas, DNS y
Estándar	Código abierto	Propiedad de Microsoft y requiere un controlador de dominio de Microsoft
Plataformas compatibles	Windows y Linux	Windows
Flexibilidad	Muy flexible	Poco flexible
Gestión de dispositivos	No tiene	Administra dispositivos Windows a través de objetos de política de grupo (GPO).

OpenLDAP

Es una implementación de libre y de código abierto del protocolo LDAP. Su licencia es OpenLDAP Public License

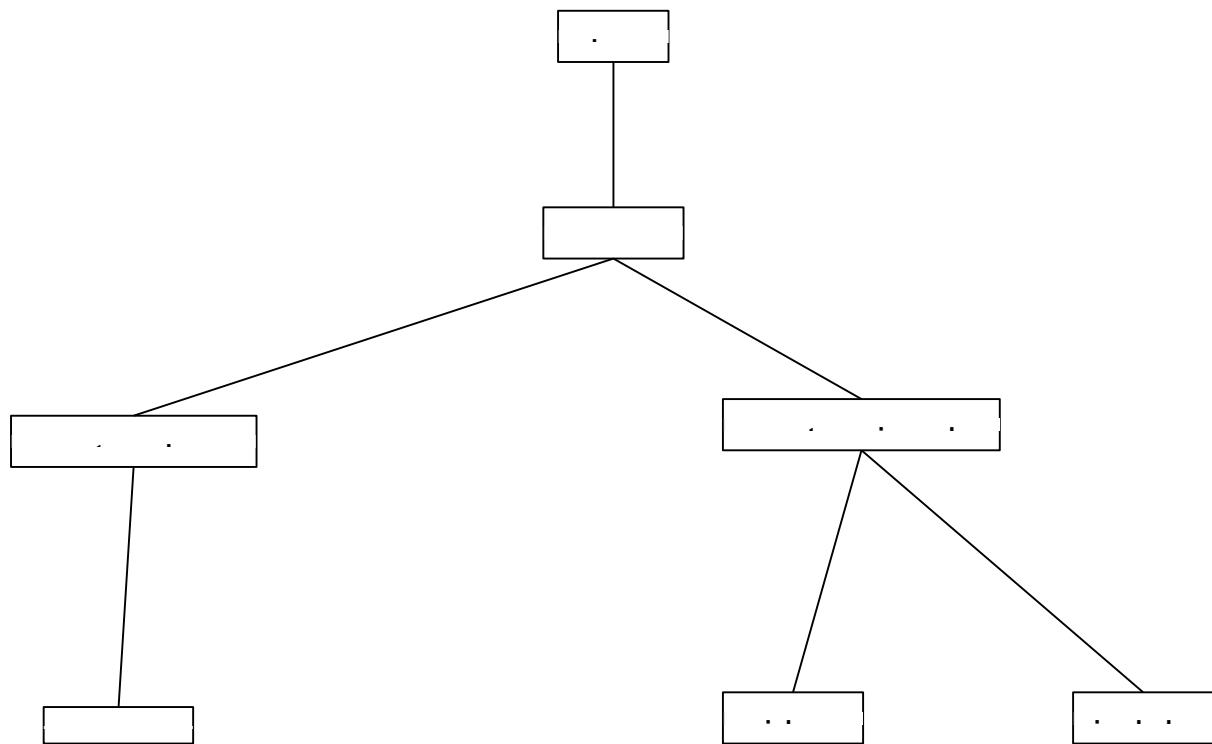
Características

- Soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL)
- Soporta IPv6
- Permite la comunicación dentro de un sistema usando comunicación interproceso (IPC), por lo que se mejora la seguridad al eliminar la necesidad de comunicarse a través de la red.
- API de C actualizada
- Soporte LDIFv1 que hace que sea compatible con el formato de intercambio de datos, Data Interchange Format (LDIF) versión 1.

Componentes principales:

- slapd – demonio LDAP autónomo.
- slurpd – demonio de replicación de actualizaciones LDAP autónomo.
- Rutinas de biblioteca de soporte del protocolo LDAP
- Utilidades, herramientas y clientes.

Esquema del directorio



dc es el componente de dominio

ou es la unidad organizativa

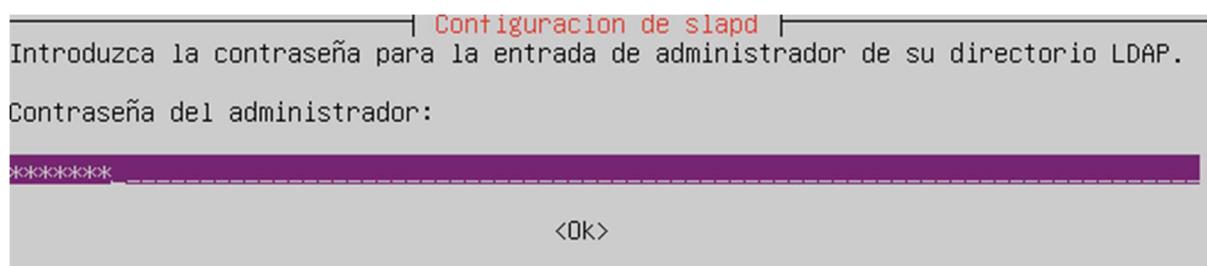
uid es el identificador del usuario

Instalación

Comenzaremos con la instalación de los paquetes necesarios utilizando el comando
sudo apt-get install slapd ldap-utils

```
usuario@equipo:~/Escritorio$ sudo apt-get install slapd ldap-utils
[sudo] contraseña para usuario:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  golang-golang-x-net-dev golang-golang-x-sys-dev golang-golang-x-text-dev
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libodbc1
Paquetes sugeridos:
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal libmyodbc
  odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
  ldap-utils libodbc1 slapd
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 96 no actualizados.
Se necesita descargar 1.708 kB de archivos.
Se utilizarán 17,7 MB de espacio de disco adicional después de esta operación.
Desea continuar? [S/n] s
```

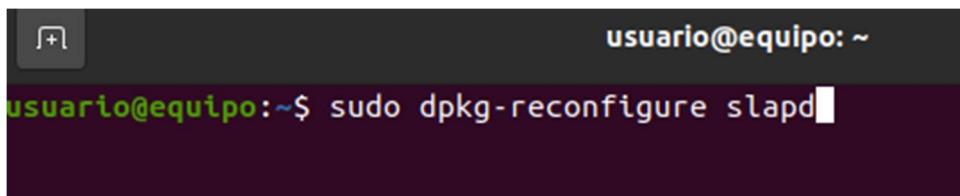
A continuación nos pide que se le introduzca una contraseña para el administrador



Volvemos a configurar slap con el comando sudo dpkg-reconfigure slapd

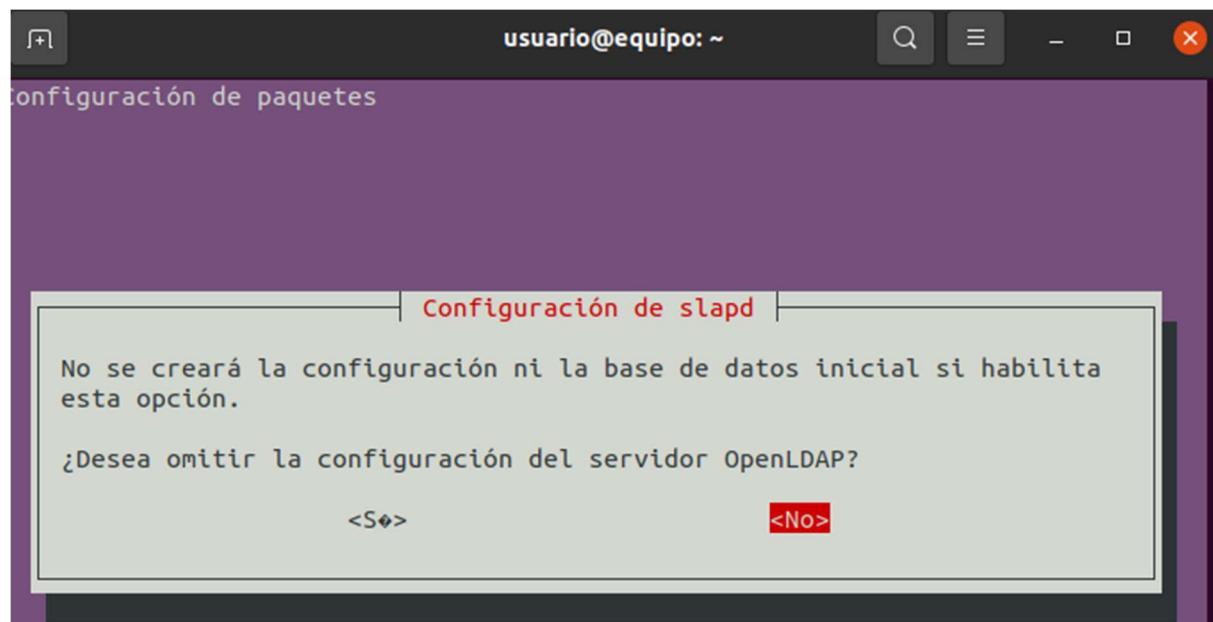
para introducir:

- El nombre del dominio que será cau
- La organización tecnicosCAU
- La contraseña del administrador
- La base de datos que será MariaDB

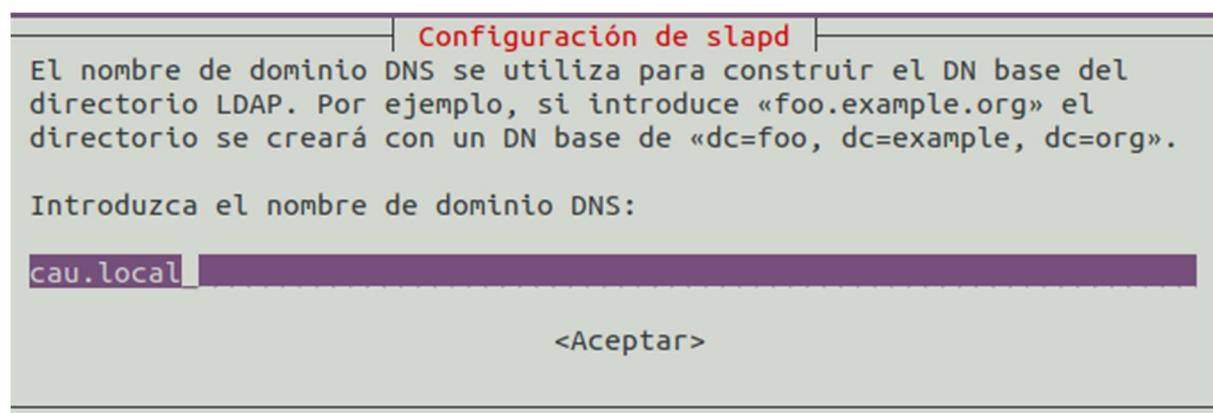


A terminal window titled "usuario@equipo: ~". The command "sudo dpkg-reconfigure slapd" is being typed into the terminal.

Primero salta la siguiente ventana



Pedirá el nombre del dominio



Introducimos el nombre de la organización

Configuración de slapd

Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

tecnicosCAU

<Aceptar>

Ponemos la contraseña del administrador

Configuración de slapd

Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

<Aceptar>

Preguntara qué hacer con la base de datos en el caso de purgar slap

Configuración de slapd

¿Desea que se borre la base de datos cuando se purge el paquete slapd?

<S+>

<No>

También preguntará cómo proceder con los datos de una base de datos antigua antes de crear la nueva

Existen ficheros en «/var/lib/ldap» que probablemente interrumpan el proceso de configuración. Si activa esta opción, se moverán los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.

¿Desea mover la base de datos antigua?

<S+>

<No>

Ya estará instalado

```
usuario@equipo:~$ sudo dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.49+dfsg-2ubuntu1.8... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
usuario@equipo:~$
```

Se puede comprobar que ldap está escuchando, para esto necesitaremos instalar primero el paquete net-tools

```
usuario@equipo:~$ sudo apt-get install net-tools
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

Ahora ya podemos utilizar el comando netstat -ta |more. Y efectivamente esta ldap a la escucha

```
usuario@equipo:~$ netstat -ta |more
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Enviad Dirección local           Dirección remota      Estado
tcp      0      0 localhost:domain          0.0.0.0:*
tcp      0      0 localhost:ipp            0.0.0.0:*
tcp      0      0 0.0.0.0:ldap            0.0.0.0:*
tcp      0      0 AG1SS24_55V.xunta:50170 banjo.canonical.co:http TIME_WAIT
tcp6     0      0 ip6-localhost:ipp        [::]:*
tcp6     0      0 [::]:ldap              [::]:*
```

Reiniciamos el servicio con el comando sudo /etc/init.d/slapd restart

```
usuario@equipo:~$ sudo /etc/init.d/slapd restart
[sudo] contraseña para usuario:
Restarting slapd (via systemctl): slapd.service.
usuario@equipo:~$
```

Para ver la configuración y la base de datos ejecutamos el comando ldapsearch -x -b "cd=cau,dc=local"

```
usuario@equipo:~$ ldapsearch -x -b "dc=cau,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=cau,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# cau.local
dn: dc=cau,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: tecnicosCAU
dc: cau

# admin, cau.local
dn: cn=admin,dc=cau,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

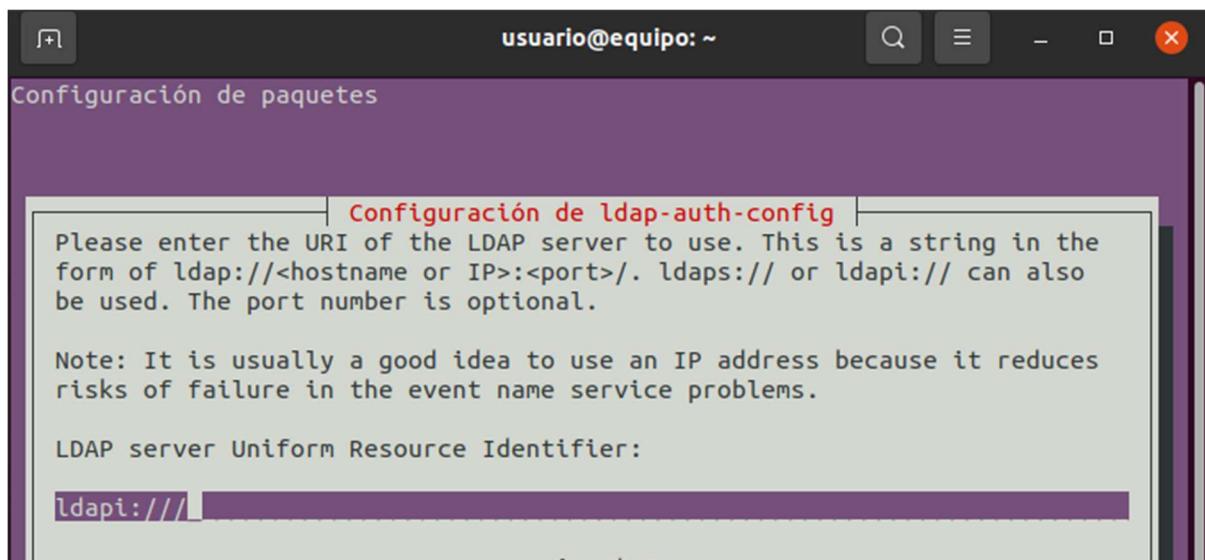
# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
usuario@equipo:~$
```

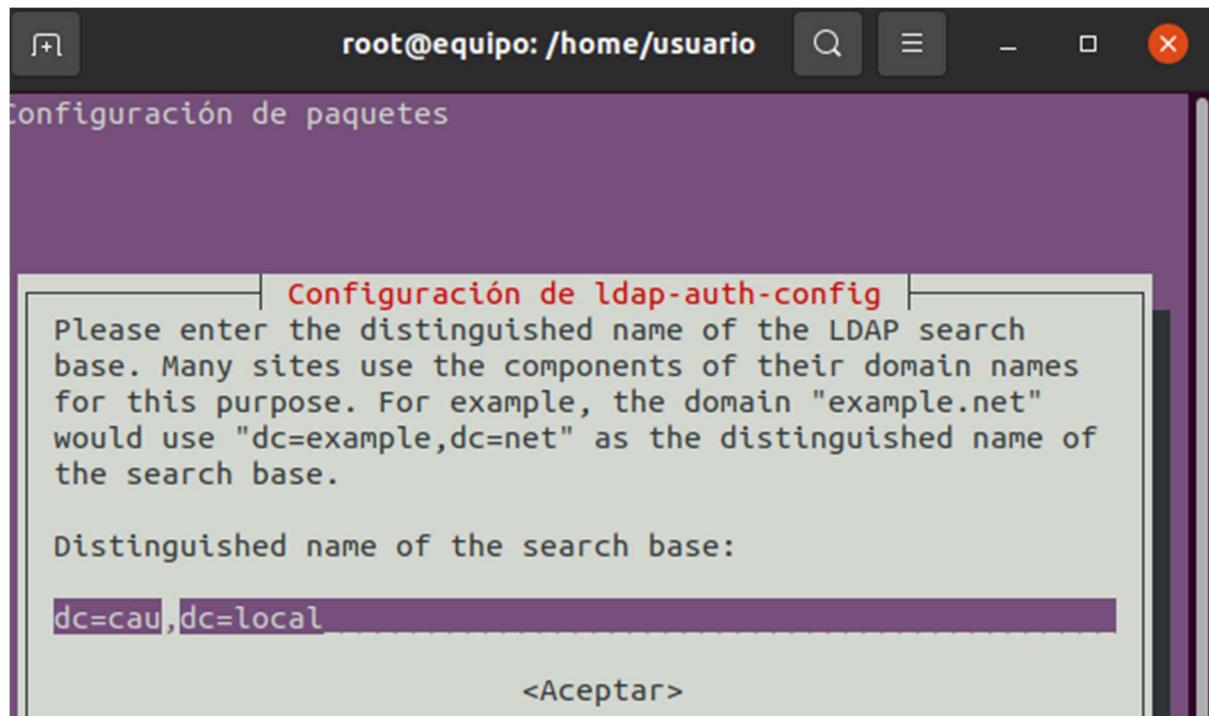
Ya está instalado, ahora nos falta instalar los paquetes necesarios para que los usuarios de la base de datos se puedan autenticar. Para eso utilizamos el comando sudo apt--get install libnss--ldap libpam--ldap

```
usuario@equipo:~$ sudo apt-get install libnss-ldap libpam-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  golang-golang-x-net-dev golang-golang-x-sys-dev golang-golang-x-text-dev
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  ldap-auth-client ldap-auth-config
Paquetes sugeridos:
  nscd
Se instalarán los siguientes paquetes NUEVOS:
  ldap-auth-client ldap-auth-config libnss-ldap libpam-ldap
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 125 no actualizados.
Se necesita descargar 109 kB de archivos.
Se utilizarán 353 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

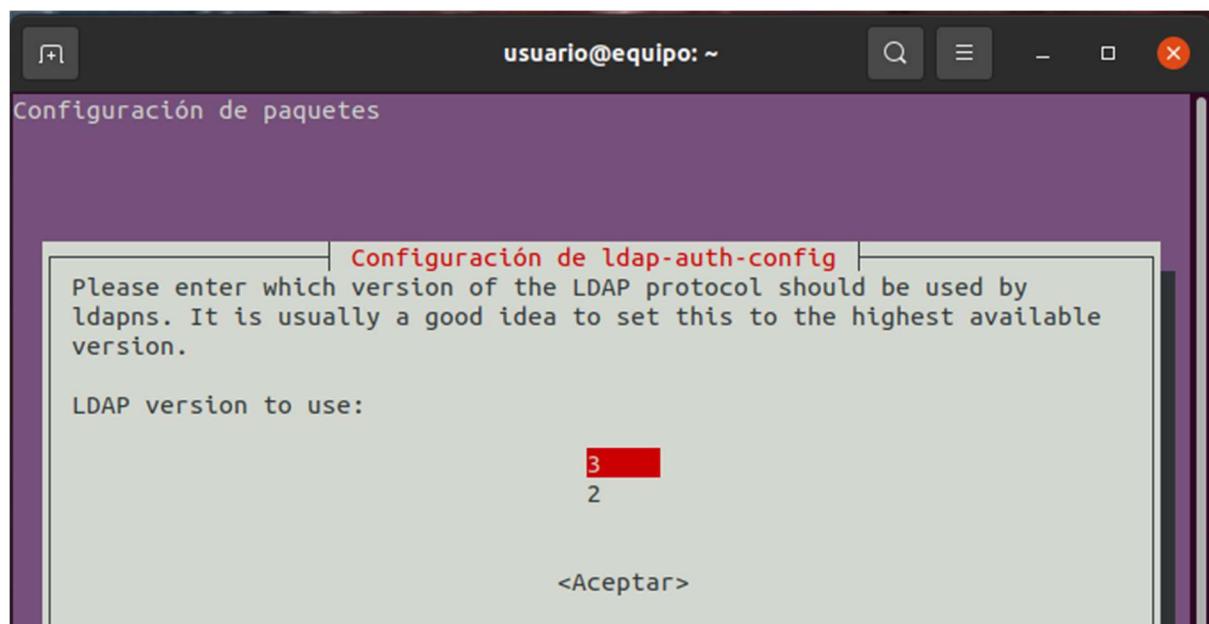
Se abre un asistente que el primer parámetro que nos pide introducir es donde esta instalado el servidor LDAP, como lo tenemos en localhost lo dejamos en ldapi:///.



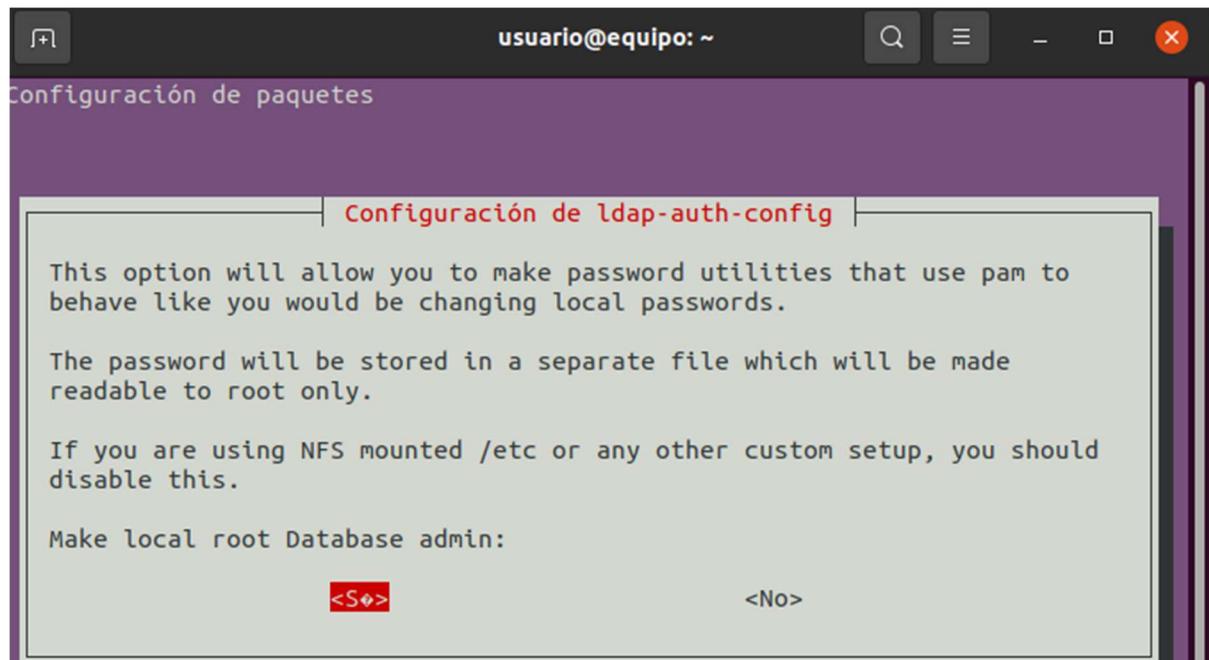
A continuación introducimos el nombre de la base de datos que en este caso es dc=cau, dc=local



Los siguiente es introducir la versión que deseamos de LDAP, que podemos dejar en 3 salvo que dispongamos de clientes antiguos en la red



La siguiente pantalla nos pregunta si las utilidades de PAM deberían comportarse del mismo modo que cuando cambiamos contraseñas locales. Esto hará que las contraseñas se guarden en un archivo independiente que sólo podrá ser leído por el superusuario



Por último nos pregunta si es necesario identificarse para realizar consultas en la base de datos



Solo nos quedaría configurar la autenticación de los usuarios en el sistema para eso utilizamos auth-client-config --t nss --p lac_ldap

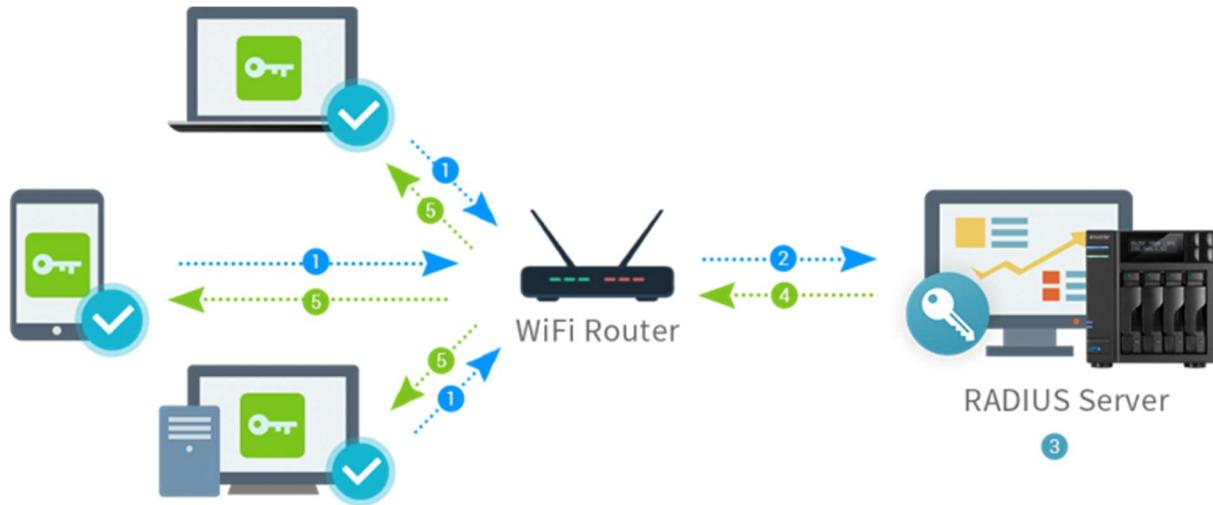
- --t nss: indica que los ficheros que se modifican son los de NSS
- -p lac_ldap: indica que los datos para la configuración son los del fichero lac_ldap, que se generó en la instalación.

```
root@equipo:/home/usuario# : sudo auth-client-config -t -nss -p lac_ldap
root@equipo:/home/usuario#
```

RADIUS

Es un protocolo que ofrece un mecanismo de seguridad , flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red. Utiliza un esquema de cliente-servidor. Hace uso del protocolo de

transporte UDP en el puerto 1812 para establecer las conexiones entre los equipos para la autenticación aunque se puede configurar para que use el TCP



Características:

- Manejar las sesiones, notificar cuándo comienza y termina una conexión
- Determinar el consumo
- El modelo de seguridad es punto-a-punto

Ventajas

- Seguridad de la red.
- Seguimiento de los accesos a la red por los nombres de los usuarios.
- Aplicar restricciones a un usuario concreto.
- Los accesos a la red individuales están encriptados.
- Es posible desconectar a un único usuario o dispositivo sin afectar al resto.
- No tiene requisitos previos

Desventajas

- Si los usuarios se conectan a la red inalámbrica con dispositivos personales, 802.1X/RADIUS puede ser más difícil o complejo de configurar

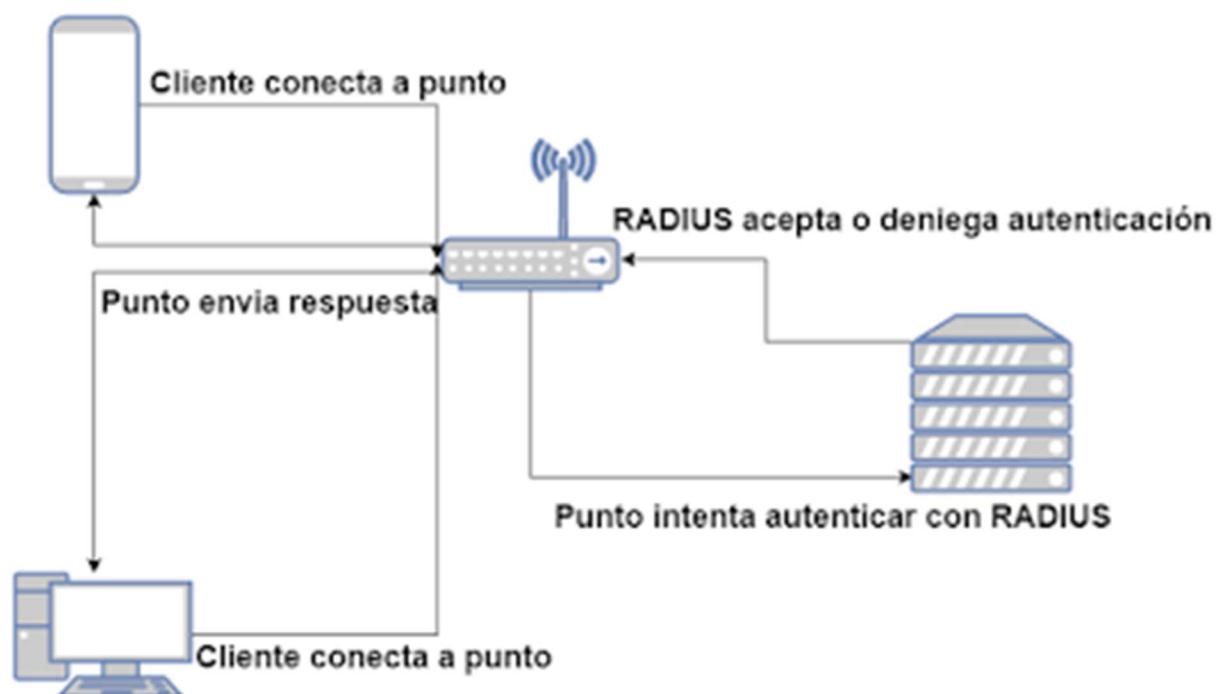


Es un servidor de políticas multiprotocolo altamente configurable y de alto rendimiento, compatible con RADIUS, DHCPv4, DHCPv6, TACACS + y VMPS. Permite centralizar la autenticación y autorización de una red y minimiza la cantidad de cambios que deben realizarse al agregar o eliminar nuevos usuarios a una red.

También puede autenticar usuarios en sistemas como 802.1x (WiFi), acceso telefónico, PPPoE, VPN, VoIP.. Es compatible con bases de datos back-end como son MySQL, PostgreSQL, Oracle, Microsoft Active Directory, Apache Cassandra, Redis, OpenLDAP.

Funcionamiento

1. El usuario inicia la autenticación PPP a la NAS.
2. La NAS incita para el nombre de usuario y contraseña (si protocolo password authentication [PAP]) o el desafío (sí Challenge Handshake Authentication Protocol [CHAP]).
3. Contestaciones del usuario.
4. El cliente RADIUS envía el username y la contraseña cifrada al servidor de RADIUS.
5. El servidor de RADIUS responde con valida, rechaza, o desafía.
6. Los actos del cliente RADIUS sobre los servicios y los parámetros de los servicios ligados con validan o rechazan.



Instalación

Se instala con el comando `sudo apt-get install freeradius`

```
root@equipo:/home/usuario# sudo apt-get install freeradius
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  golang-golang-x-net-dev golang-golang-x-sys-dev
  golang-golang-x-text-dev linux-headers-5.11.0-27-generic
  linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic
  linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  freeradius-common freeradius-config freeradius-utils
  freetds-common libct4 libdbi-perl libfreeradius3
Paquetes sugeridos:
  freeradius-ldap freeradius-postgresql freeradius-mysql
  freeradius-krb5 snmp freeradius-python3 libclone-perl
  libmldb perl libnet-daemon-perl libsql-statement-perl
Se instalarán los siguientes paquetes NUEVOS:
  freeradius freeradius-common freeradius-config
  freeradius-utils freetds-common libct4 libdbi-perl
  libfreeradius3
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 125 no actualizados.
Se necesita descargar 2.066 kB de archivos.
Se utilizarán 8.063 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

A continuación se instala el paquete para que RADIUS se pueda conectar con OpenLDAP: sudo apt--get install freeradius--ldap

```

usuario@equipo:~$ sudo apt-get install freeradius-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  golang-golang-x-net-dev golang-golang-x-sys-dev golang-golang-x-text-dev
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  freeradius-ldap
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 125 no actualizados.
Se necesita descargar 35,1 kB de archivos.
Se utilizarán 139 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 freeradius-ldap a
md64 3.0.20+dfsg-3build1 [35,1 kB]
Descargados 35,1 kB en 0s (82,0 kB/s)
Seleccionando el paquete freeradius-ldap previamente no seleccionado.
(Leyendo la base de datos ... 237209 ficheros o directorios instalados actualmen
te.)

```

Después editamos el archivo de configuración que se encuentra en la ruta:
 /etc/freeradius/modules/ldap
 Para indicarle donde se encuentra el servidor LDAP y que se pueda conectar con el

GNU nano 4.8	ldap	Modificado
-*- text -*-		
\$Id: 1741d7e6ed472617f190f90a545272be980a6ff1 \$		
 Lightweight Directory Access Protocol (LDAP)		
dap {	# Note that this needs to match the name(s) in the LDAP >	
	# certificate, if you're using ldaps. See OpenLDAP docu>	
	# for the behavioral semantics of specifying more than o>	
	#	
	# Depending on the libldap in use, server may be an LDAP>	
	# In the case of OpenLDAP this allows additional the fol>	
	# additional schemes:	
	# - ldaps:// (LDAP over SSL)	
	# - ldapi:// (LDAP over Unix socket)	
	# - ldapc:// (Connectionless LDAP)	
	server = "equipo"	
	identity= "cn=tecnicosCAU,dc=cau,dc=local"	
	password=abc123.	

Otro documento que modificaremos es /etc/freeradius/radiusd.conf. Para activar los mensajes de login y desactivar el proxy

```
GNU nano 4.8          radiusd.conf      Modificado
#   allowed values: {no, yes}
#
auth = yes

# Log Access-Accept results to the log file.
#
# This is only used if "auth = no"
#
# allowed values: {no, yes}
#
# auth_accept = no

# Log Access-Reject results to the log file.
#
# This is only used if "auth = no"
#
# allowed values: {no, yes}
#
# auth_reject = no

# Log passwords with the authentication requests.
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
#
# allowed values: {no, yes}
#
# auth_badpass = yes
# auth_goodpass = yes
```

```
# proxy_requests = no
$INCLUDE proxy.conf
```

El último archivo que se modifica es /etc/freeradius/clients.conf. Este contiene los parámetros para que los clientes puedan comunicarse con el servidor RADIUS

```
GNU nano 4.8          clients.conf          Modificado
#####
#
# Per-socket client lists. The configuration entries are exactly
# the same as above, but they are nested inside of a section.
#
# You can have as many per-socket client lists as you have "list>
# sections, or you can re-use a list among multiple "listen" sec>
#
# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combinat>
# will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#    client socket_client {
#        ipaddr = 192.0.2.4
#        secret = testing123
#    }
#}
client ldap {
ipaddr = 10.0.2.15
secret = Periheli0/
nastype = other
}
```

Podemos crear en apache un servidor virtual para la conexión con LDAP para eso copiamos /etc/freeradius/sites-available/default y lo renombramos a ldap

```
root@equipo:/etc/freeradius/3.0# ls -l sites-enabled/
total 0
lrwxrwxrwx 1 freerad freerad 26 feb  1 19:13 default -> ../../sites-available/default
lrwxrwxrwx 1 freerad freerad 31 feb  1 19:13 inner-tunnel -> ../../sites-available/inner-tunnel
root@equipo:/etc/freeradius/3.0#
```

```
root@equipo:/etc/freeradius/3.0# ln -s sites-available/ldap sites-enabled/
```

```
intivo ya existe
root@equipo:/etc/freeradius/3.0# ls -l sites-enabled/
total 0
lrwxrwxrwx 1 freerad freerad 26 feb 1 19:13 default -> ../sites-available/default
lrwxrwxrwx 1 freerad freerad 31 feb 1 19:13 inner-tunnel -> ../sites-available/inner-tunnel
lrwxrwxrwx 1 root      root     20 feb 1 19:31 ldap -> sites-available/ldap
root@equipo:/etc/freeradius/3.0#
```

Lo último es editar el fichero /etc/freeradius/sites-available/ldap para que el servidor RADIUS sólo establezca conexiones a través del protocolo ldap. Esto se consigue borrando las referencias a otros métodos de autenticación (dejando únicamente ldap)

```
authorize {
    preprocess
    ldap
    expiration
    logintime

authenticate {
    Auth-Type LDAP(
        ldap|
```

TLS

Es un protocolo criptográfico que proporciona una comunicación segura en la red.

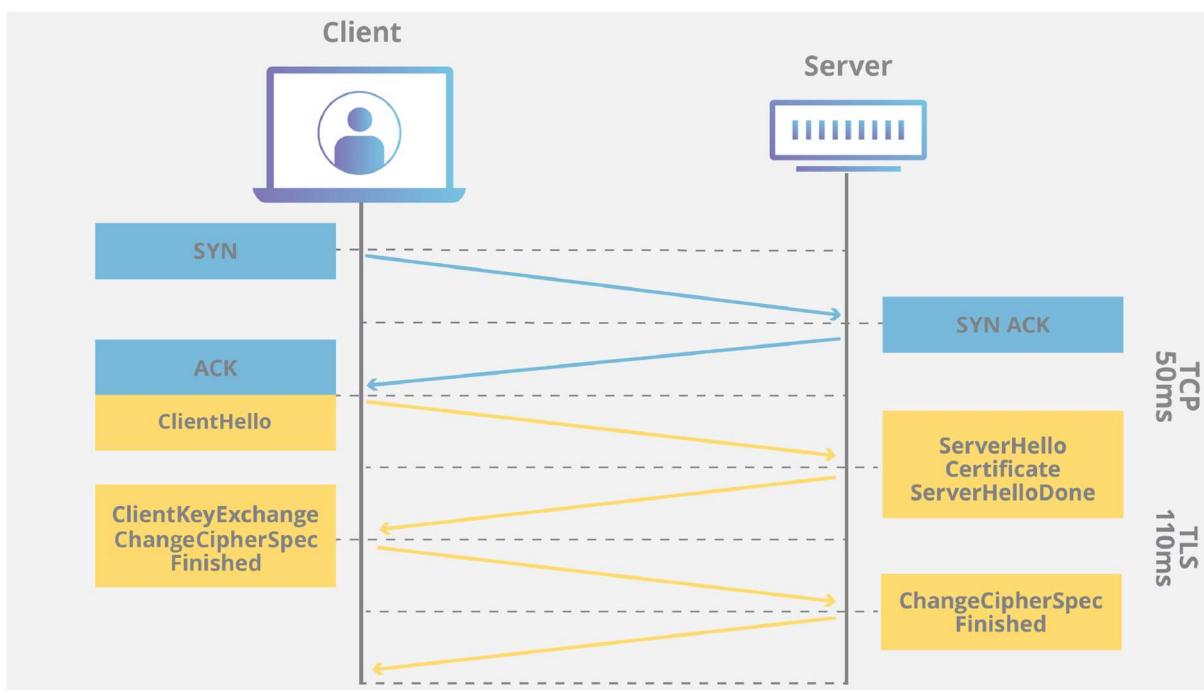
Usa certificados X.509

Características:

- Cifrado. Los datos que se intercambian son cifrados por lo que se impide que un tercero pueda acceder a su contenido.
- Integridad de los datos. En la transferencia, los datos no pueden ni modificarse, ni dañarse, sin que este proceso sea detectado.
- Autenticación. Permite acreditar a los usuarios la identidad del servidor web

Funcionamiento

1. Cuando el cliente contacta con el servidor web, este le envía primero su certificado. Este certificado SSL prueba que el servidor es auténtico y no está simulando una identidad falsa.
2. El cliente comprueba la validez del certificado y envía al servidor un número aleatorio cifrado con la clave pública del servidor.
3. A partir de ese número aleatorio, el servidor genera la clave de sesión con la que debe encriptar la comunicación.
4. El servidor remite la clave de sesión al cliente de forma cifrada.
5. Ahora, ambas partes pueden enviar sus datos de forma segura con la clave de sesión.



Instalación

Para el método de autenticación EAP-TTLS necesitamos tener un certificado de servidor. Las opciones para tener este certificado son:

1. Usar el certificado que se crea automáticamente al instalar freeradius.
2. Crear un certificado autofirmado.
3. Crear nuestra propia autoridad de certificación, con la que generamos dicho certificado.

En este documento se explica la segunda opción aunque la primera es la más fácil de realizar

Para usar TLS en nuestro servidor LDAP, necesitaremos:

- Certificado público
- Llave privada
- Autoridad certificadora que es la encargada de firmar el certificado

Utilizaremos la herramienta gnutlsbin que se instala con el comando sudo apt-get install gnutls-bin

```
usuario@equipo:~$ sudo apt-get install gnutls-bin
[sudo] contraseña para usuario:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  golang-golang-x-net-dev golang-golang-x-sys-dev golang-golang-x-text-dev
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27
  linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libgnutls-dane0 libopts25 libunbound8
Se instalarán los siguientes paquetes NUEVOS:
  gnutls-bin libgnutls-dane0 libopts25 libunbound8
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 129 no actualizados.
Se necesita descargar 713 kB de archivos.
Se utilizarán 2.761 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Al terminar la instalación creamos la clave privada con la instrucción `sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"`

```
usuario@equipo:~$ sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
Generating a 3072 bit RSA private key...
usuario@equipo:~$
```

Podemos crear una plantilla para guardar los datos de la Autoridad certificadora con el comando

`sudo nano /etc/ssl/ca.info` y le añadimos las líneas que se ven en la imagen

```
GNU nano 4.8          /etc/ssl/ca.info
cn = equipo
ca
cert_signing_key
```

Cambiamos de usuario al root para poder generar el certificado autofirmado con la plantilla que acabamos de crear con el comando (en tres partes)

1. sudo certtool --generate-self-signed --load-privkey /etc/ssl/private/cakey.pem \
2. --template /etc/ssl/ca.info \
3. --outfile /etc/ssl/certs/cacert.pem

```
root@equipo:/home/usuario# sudo certtool --generate-self-signed --load-privkey
/etc/ssl/private/cakey.pem \
> --template /etc/ssl/ca.info \
> --outfile /etc/ssl/certs/cacert.pem
Generating a self signed certificate...
X.509 Certificate Information:
  Version: 3
  Serial Number (hex): 32bdc5ac0d7155b07eb42e8a5dbdd57338389076
  Validity:
    Not Before: Wed Feb 02 17:16:58 UTC 2022
    Not After: Thu Feb 02 17:16:58 UTC 2023
  Subject: CN=equipo
  Subject Public Key Algorithm: RSA
  Algorithm Security Level: High (3072 bits)
    Modulus (bits 3072):
      00:a9:5c:64:b8:b0:ca:4a:6d:0d:ac:17:3b:e4:75:80
      3b:5f:7b:41:ca:a4:5d:1f:82:a1:ad:d7:7b:04:cd:30
      74:b3:59:95:6f:c1:95:b9:80:06:83:e3:9a:7a:17:a6
      c7:65:6b:14:84:40:a3:fc:8d:28:82:ad:1c:7a:70:69
      7f:4e:61:a9:a2:b3:6f:db:99:15:47:40:9e:7d:35:d2
      38:68:23:a2:00:2a:07:81:31:df:c6:16:b0:0a:f7:ff
      30:d9:f4:8c:4c:7e:4c:3e:2a:14:3c:37:f1:34:fa:0c
      3b
    Exponent (bits 24):
      01:00:01
  Extensions:
    Basic Constraints (critical):
      Certificate Authority (CA): TRUE
    Key Usage (critical):
      Certificate signing.
    Subject Key Identifier (not critical):
      8e1631fb87d6774489535b6f558e74876df82bb4
Other Information:
  Public Key ID:
    sha1:8e1631fb87d6774489535b6f558e74876df82bb4
    sha256:3cb480488fc40049da01f7c19559c3ab21e9a218141317cb75c4d8d
37426170a
  Public Key PIN:
    pin-sha256:PLSASI/EAEnaAffBlVnDqyHpohgUExfLdcTY03QmFwo=
```

Signing certificate...

```
root@equipo:/home/usuario#
```

Continuamos con la creación de la llave privada con el comando (en tres partes)

1. sudo certtool --generate-privkey /etc/ssl/private/radius_slapd_key.pem \
2. --bits 2048 \
3. --outfile

```
root@equipo:/# sudo certtool --generate-privkey \
> --bits 2048 \
> --outfile /etc/ssl/private/radius_slapd_key.pem
** Note: You may use '--sec-param Medium' instead of '--bits 2048'
Generating a 2048 bit RSA private key...
root@equipo:/#
```

Creamos una plantilla para crear y firmar el certificado con el comando sudo nano /etc/ssl/radius.info y añadimos las lineas que se ven en la imagen

GNU nano 4.8	/etc/ssl/radius.info
organization = equipo	
cn= cua	
tls_www_server	
encryption_key	
signing_key	
expitation_days = 3650	

Después generamos y firmamos el certificado con el comando (en seis partes)

1. sudo certtool --generate-certificate \

2. --load-privkey /etc/ssl/private/radius_slapd_key.pem \
3. --load-ca-certificate /etc/ssl/certs/cacert.pem \
4. --load-ca-privkey /etc/ssl/private/cakey.pem \
5. --template /etc/ssl/radius.info \
6. --outfile /etc/ssl/certs/radius_slapd_cert.pem

```
root@equipo:/home# sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/radius_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/radius.info \
--outfile /etc/ssl/certs/radius_slapd_cert.pem
Warning: skipping unknown option 'expitation_days'
Generating a signed certificate...

Expiration time: Thu Feb  2 18:53:13 2023
CA expiration time: Thu Feb  2 18:16:58 2023
Warning: The time set exceeds the CA's expiration time
X.509 Certificate Information:
  Version: 3
  Serial Number (hex): 46e44434256781c82222aa2ddf79397267b3576
  Validity:
    Not Before: Wed Feb 02 17:53:13 UTC 2022
    Not After: Thu Feb  2 17:53:13 UTC 2023
  Subject: O=equipo,CN=cua
  Subject Public Key Algorithm: RSA
  Algorithm Security Level: Medium (2048 bits)
    Modulus (bits 2048):
      00:d2:c7:06:a9:b2:f1:4d:65:ae:80:9a:f0:3b:a3:74
```

```
  1b
  Exponent (bits 24):
    01:00:01
  Extensions:
    Basic Constraints (critical):
      Certificate Authority (CA): FALSE
    Key Purpose (not critical):
      TLS WWW Server.
    Key Usage (critical):
      Digital signature.
      Key encipherment.
    Subject Key Identifier (not critical):
      f52a9c44f3b44dd707fb9db1843e9684487b18ca
    Authority Key Identifier (not critical):
      8e1631fb87d6774489535b6f558e74876df82bb4
  Other Information:
    Public Key ID:
      sha1:f52a9c44f3b44dd707fb9db1843e9684487b18ca
      sha256:b0014267b2ba5923a3e6be0e928a303e26482e092cc0060989f7f47
      94eee9da3
    Public Key PIN:
      pin-sha256:sAFCZ7K6WS0j5r40koowPiZILgkswAYJiff0eU7unaM=
```

Signing certificate...
root@equipo:/home#

Activar Windows
Vea la Configuración para activar Windows.

Conclusión

Se creó un red específica que se puede acceder a internet a través del servidor VPN, en esta red se podría utilizar únicamente para la empresa ya que solo sería accesible a través del servidor VPN por lo que se da seguridad. También se implementó un sistema de autenticación en otro servidor que es el Radius y un tercer servidor que tendrá una base de datos con la información de los dispositivos a cargo del departamento del CAU así como información de sus usuarios.

Este proyecto se podría mejorar con la unión de los servidores Radius y VPN para que los usuarios antes de conectarse a la red de la empresa se tuvieran que autenticar en el servidor Radius y así aumentar la seguridad de la red