

# Laboratorio completo

Plataforma: VirtualBox Versión 6.0.24 r139119 (Qt5.6.2)

Red NAT: Red Virtual Personal - 10.128.0.0/24 - No DHCP

Máquinas:

- Servers
  - Ubuntu 20.04 Samba Server (10.128.0.10)
    - RAM: 1024 MB
    - Procesadores: 1
    - HDD: 10 GB
  - Ubuntu 20.04 Keycloak Server (10.128.0.20)
    - RAM: 1024 MB
    - Procesadores: 1
    - HDD: 20 GB
  - Ubuntu 20.04 JS.Console Server (10.128.0.30)
    - RAM: 1024 MB
    - Procesadores: 1
    - HDD: 50 GB
  - Ubuntu 20.04 Zammad Server (10.128.0.40)
    - RAM: 4096 MB
    - Procesadores: 2
    - HDD: 50 GB
- Clients
  - Windows 10 Desktop Client (10.128.0.60)
    - RAM: 2048 MB
    - Procesadores: 2
    - HDD: 50 GB
  - Ubuntu 18.04 Desktop Client (10.128.0.70)
    - RAM: 2048 MB
    - Procesadores: 2
    - HDD: 25 GB

## Servidor de SAMBA Active Directory

1. Configurar el hostname del servidor, en este caso es "samba":

```
$ sudo hostnamectl set-hostname samba
```

2. Agregar al archivos de hosts la ip de la máquina del servidor, el hostname y el FQDN:

```
$ 10.128.0.10 samba samba.diinf.lan
```

Reiniciar el servidor.

3. Instalar los paquetes necesarios:

```
$ sudo apt install -y samba smbclient winbind  
libpam-winbind libnss-winbind krb5-kdc libpam-krb5
```

Durante la instalación se consultará sobre el realm de kerberos, ingresar en este caso en el siguiente orden: **DIINF.LAN**, **diinf.lan**, **diinf.lan** (tomar en cuenta las mayúsculas).

4. Para configurar el servidor es necesario eliminar algunas de las configuraciones que vienen por defecto utilizando los siguientes comandos

```
$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.bak  
$ sudo mv /etc/krb5.conf /etc/krb5.conf.bak
```

5. Comenzar la configuración de SAMBA mediante la función interactiva:

```
$ sudo samba-tool domain provision --use-rfc2307  
--interactive
```

Ingresar los siguientes valores (utilizar una password con mínimo una mayúscula, un número y un símbolo):

```
Realm: DIINF.LAN  
Domain [DIINF]:  
Server Role [dc]:  
DNS backend [SAMBA_INTERNAL]:  
DNS forwarder IP address [8.8.8.8]:  
Administrator password:  
Retype password:
```

6. Copiar la configuración de kerberos:

```
$ sudo cp /var/lib/samba/private/krb5.conf /etc
```

7. Para configurar que SAMBA Active Directory funcione al hacer boot utilizar los siguientes comandos:

```
$ sudo systemctl mask smbd nmbd winbind
$ sudo systemctl disable smbd nmbd winbind
$ sudo systemctl stop smbd nmbd winbind
$ sudo systemctl unmask samba-ad-dc
$ sudo systemctl start samba-ad-dc
$ sudo systemctl enable samba-ad-dc
```

Reiniciar el servidor.

8. Para configurar a SAMBA como DNS para otros servidores/clientes:

```
$ sudo systemctl stop systemd-resolved
$ sudo systemctl disable systemd-resolved
```

Desconectar resolv.conf:

```
$ sudo unlink /etc/resolv.conf
```

Modificar el contenido de resolv.conf:

```
$ sudo nano /etc/resolv.conf
```

```
nameserver 10.128.0.10
search DIINF.LAN
```

Reiniciar el servidor.

9. Pruebas:

```
$ host -t SRV _ldap._tcp.diinf.lan
Resp: _ldap._tcp.diinf.lan has SRV record 0 100 389
samba.diinf.lan.
```

```
$ kinit Administrator
Resp: Your password will expire in 41 days ...
```

## Servidor de Keycloak

1. Apuntar al servidor de SAMBA como DNS:

```
$ sudo nano /etc/netplan/00-installer-config.yaml
```

```
nameservers:
  addresses: [10.128.0.10]
```

```
GNU nano 4.8
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
        - 10.128.0.20/24
      gateway4: 10.128.0.1
      nameservers:
        addresses: [10.128.0.10]
        search: []
  version: 2
```

```
$ sudo netplan apply
```

2. Copiar el certificado de SAMBA:

```
$ openssl s_client -connect samba.diinf.lan:636
</dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END
CERTIFICATE-/p' > sambaCert.pem
```

3. Levantar el contenedor de Keycloak y la base de datos postgres mediante docker-compose

```
$ sudo docker-compose up -d
```

El contenido del docker-compose.yml está en la siguiente página.

## docker-compose.yml

```
version: '3'

volumes:
  postgres_data:
    driver: local

services:
  postgres:
    image: postgres:13.3
    container_name: postgres_db
    hostname: postgres
    restart: unless-stopped
    volumes:
      - postgres_data:/var/lib/postgresql/data
    environment:
      POSTGRES_DB: keycloak
      POSTGRES_USER: keycloak
      POSTGRES_PASSWORD: keycloakPassword
    ports:
      - 5432:5432
  keycloak:
    image: quay.io/keycloak/keycloak:14.0.0
    container_name: keycloak_app
    hostname: keycloak
    restart: unless-stopped
    volumes:
      - /$PWD/sambaCert.pem:/opt/jboss/keycloak/sambaCert.pem
    environment:
      DB_VENDOR: POSTGRES
      DB_ADDR: postgres
      DB_DATABASE: keycloak
      DB_USER: keycloak
      DB_SCHEMA: public
      DB_PASSWORD: keycloakPassword
      KEYCLOAK_USER: admin
      KEYCLOAK_PASSWORD: Diinf1*
      # Uncomment the line below if you want to specify JDBC parameters.
      # The parameter below is just an example, and it shouldn't be used in
      # production without knowledge. It is highly recommended that you read the
      # PostgreSQL JDBC driver documentation in order to use it.
      #JDBC_PARAMS: "ssl=true"
    ports:
      - 443:8443
    extra_hosts:
      - "samba.diinf.lan:10.128.0.10"
    depends_on:
      - postgres
```

4. Ingresar al contenedor y agregar el certificado de SAMBA al archivo **cacerts** global de JAVA:

```
$ sudo docker exec -u 0 keycloak_app keytool -import
-trustcacerts -file /opt/jboss/keycloak/sambaCert.pem
-alias samba.diinf.lan -keystore
/usr/lib/jvm/java-11-openjdk-11.0.11.0.9-2.el8_4.x86_64/
lib/security/cacerts -storepass changeit -noprompt
```

5. Ingresar a la interfaz web por https (en este caso <https://keycloak.diinf.tk/auth>), presionar en “Administration Console” e ingresar con las credenciales configuradas en el docker-compose.yml. Una vez dentro crear un nuevo Realm:

### Add realm



Import

Name \*

Enabled ☒

6. Una vez dentro del nuevo Realm, ir a “User Federation” y agregar un **Idap provider**:

### Add user federation provider

#### Required Settings



Enabled ? ☒

Console Display Name ?

Priority ?

Import Users ? ☒

Edit Mode ?

Sync Registrations ? ☒

* Vendor ?	Active Directory
* Username LDAP attribute ?	sAMAccountName
* RDN LDAP attribute ?	cn
* UUID LDAP attribute ?	objectGUID
* User Object Classes ?	person, organizationalPerson, user
* Connection URL ?	ldaps://samba.dlinf.lan
* Users DN ?	OU=DIINF,DC=dlinf,DC=lan
Custom User LDAP Filter ?	LDAP Filter
Search Scope ?	One Level
* Bind Type ?	simple
* Bind DN ?	CN=Administrator,CN=Users,DC=dlinf,DC=lan
* Bind Credential ?	Dlinf1*

Si los botones de “**Test connection**” y “**Test authentication**” dan resultados positivos, guardar la configuración y posteriormente presionar en “**Synchronize all users**”.

7. Configurar a Google USACH como un Identity Provider. Ir a “Identity Providers” y agregar un **Google Social provider**:

### Add identity provider

Redirect URI ?	https://keycloak.dlinf.tk/auth/realms/DIINF/broker/google/endpoint
* Client ID ?	1085152384203-d9uvsqtvbl9j5t5tgotp7hjfsqet6lrf.apps.googleusercontent.com
* Client Secret ?	.....
Hosted Domain ?	
Use userIp Param ?	<input type="checkbox"/> OFF
Request refresh token ?	<input type="checkbox"/> OFF
Default Scopes ?	
Store Tokens ?	<input type="checkbox"/> OFF
Stored Tokens Readable ?	<input type="checkbox"/> OFF
Enabled ?	<input checked="" type="checkbox"/> ON

Accepts prompt=none forward from client ?	<input type="checkbox"/> OFF
Disable User Info ?	<input type="checkbox"/> OFF
Trust Email ?	<input checked="" type="checkbox"/> ON
Account Linking Only ?	<input type="checkbox"/> OFF
Hide on Login Page ?	<input type="checkbox"/> OFF
GUI order ?	<input type="text"/>
First Login Flow ?	<input type="text" value="first broker login"/>
Post Login Flow ?	<input type="text"/>
Sync Mode ?	<input type="text" value="import"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Las credenciales se obtienen de la consola de Google Cloud, lo que requiere configuración previa fuera de Keycloak.



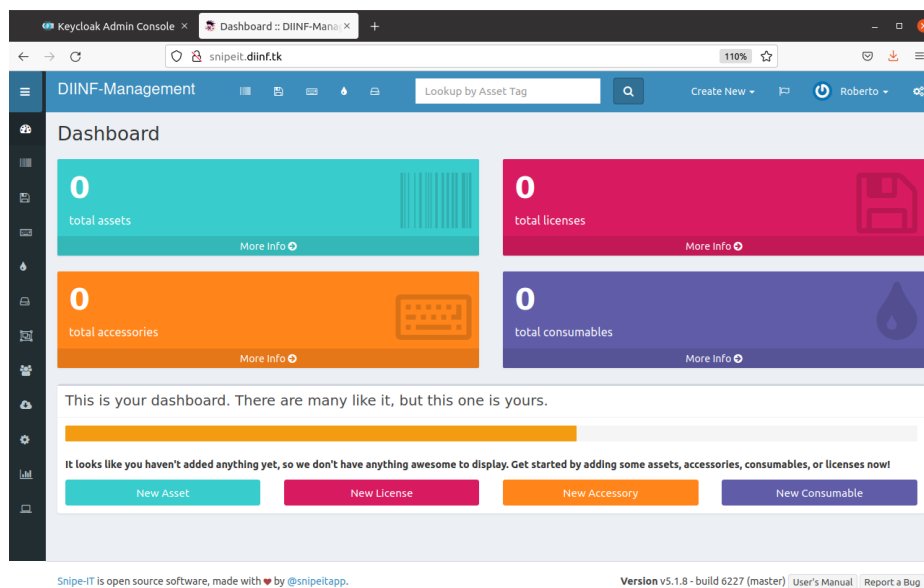
# Aplicaciones / Servidores de prueba

## Snipe-IT

1. Tutorial completo seguido paso a paso:

<https://www.hostnextra.com/kb/install-snipe-it-on-ubuntu-20-04/>

<https://stackoverflow.com/questions/42609445/sqlstatehy000-1045-access-denied-for-user-homesteadlocalhost-using-pas>



2. Ir a Configuración > SAML, Activar SAML Integration y guardar.

Update SAML Settings

**SAML**

**SAML Integration** ☒ SAML enabled

**Entity ID**

**Assertion Consumer Service (ACS) URL**

**Single Logout Service (SLS) URL**

**Public Certificate**  

```
-----BEGIN CERTIFICATE-----
MIIDbDCCAISgAwIBAgIBADANBgkqhkiG9w0BAQsFADBPMSwC
MAoGA1UECAwDTi9BMQwwCgYDVQQHDANOL0ExETAPBgNVB.
DwYDVQQDDAhtbmlwZS1JVDAAeFw0yMTA3MTgyMzQ0MjBhFwI
ME8xCzAJBgNVBAYTAiVMTQwwCgYDVQQIDANOL0ExDDAKBgI
A1UECgwIU25pcGUTSVQxETAPBgNVBAMMCFNuaXBLLUluMII
Bij/AQEFAAQCAQ8AMIIBGgKCAQEAQxmyL/M7GovwNT1feSmpaM6l
wV4adZSlyKyQGPgVWHm5WCzCk8RL4vzkluDP3rsk/+sD/OLch
TWgNKEoa1F3WSNan+7M5Pm4Pfyruzc47hu192QH8XSUoCjk2l
sdRcyprxng+29ZV3xRNTs6LdnKe8ST9VyyhMo3kRmu5PJGE6azu
-----
```

**Metadata URL**

[Download Metadata](#)

3. Presionar en el botón “Download Metadata” para descargar el XML con la información del servidor. Posteriormente, en la consola de Keycloak ir a Clients > Create > Import (Select file) y seleccionar el XML descargado.

[Clients](#) > Add Client

## Add Client

Import

View details

Clear import

Client ID \* ?

http://snipeit.dlinf.tk

Client Protocol ?

saml



Client SAML  
Endpoint ?

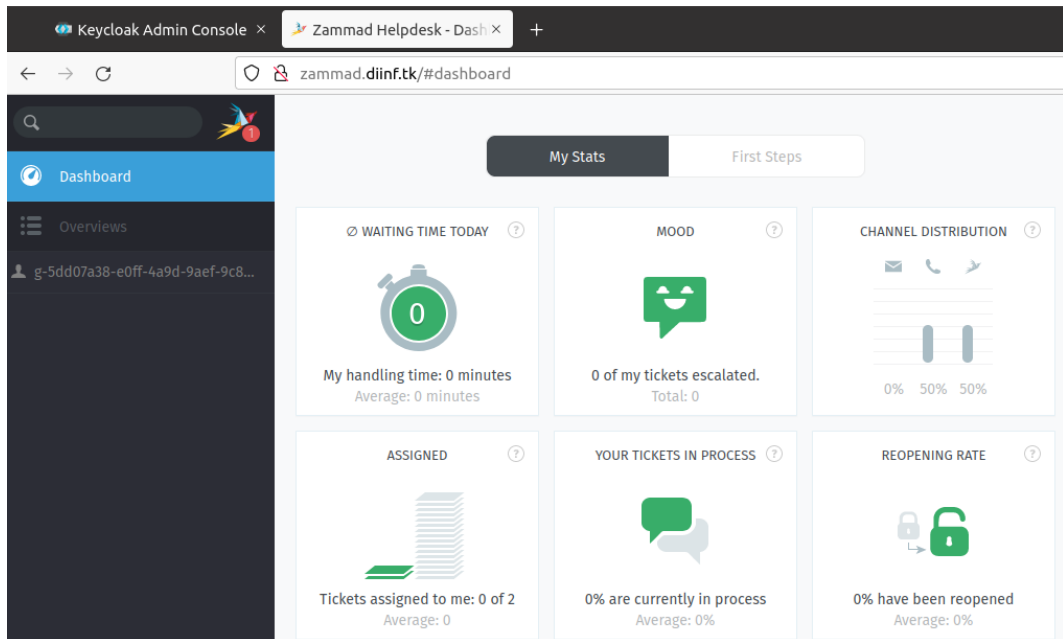
Save

Cancel

## Zammad

1. Tutorial seguido paso a paso

<https://computingforgeeks.com/install-zammad-helpdesk-system-on-ubuntu/>  
<https://admin-docs.zammad.org/en/latest/settings/security/third-party/saml.html>



2. Ir a <https://zammad.diinf.tk/auth/saml/metadata> y descarga el XML. Posteriormente, en la consola de Keycloak ir a Clients > Create > Import (Select file) y seleccionar el XML descargado.

[Clients](#) > Add Client

### Add Client

Import

[View details](#)

[Clear import](#)

Client ID \* ?

Client Protocol ?

saml

Client SAML  
Endpoint ?








[Save](#)

[Cancel](#)

3. Al interior de las configuraciones desactivar “Client Signature Required”.
4. Ir a la pestaña “Mappers” y crear un nuevo mapper con las siguientes configuraciones

[Clients](#) > <http://zammad.diinf.tk/auth/saml/metadata> > [Mappers](#) > EmailAddress-Email

### EmailAddress-Email

Protocol 	<input type="text" value="saml"/>
ID	<input type="text" value="c6083d3c-184f-46c2-b5fc-bdcc678db347"/>
Name 	<input type="text" value="EmailAddress-Email"/>
Mapper Type 	<input type="text" value="User Property"/>
Property 	<input type="text" value="emailAddress"/>
Friendly Name 	<input type="text"/>
SAML Attribute Name 	<input type="text" value="email"/>
SAML Attribute NameFormat 	<input type="text" value="Basic"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

5. Ir a la pestaña de Config > Security > Third-party Applications de Zammad y buscar la sección Authentication via SAML. Configurar de acuerdo a lo siguiente:

☒ Authentication via SAML

Enables user authentication via SAML.

IDP SSO TARGET URL

IDP CERTIFICATE


IDP CERTIFICATE FINGERPRINT

NAME IDENTIFIER FORMAT

- IDP SSO TARGET URL: url del servidor de keycloak encargado del protocolo SAML.
  - IDP CERTIFICATE: certificado del servidor de Keycloak, es posible encontrarlo en Realm Settings > Keys > RSA > Botón Certificate.
  - NAME IDENTIFIER FORMAT: se puede encontrar en el XML de Keycloak al que se puede acceder desde Realm Settings > SAML 2.0 Identity Provider Metadata, buscando el tag “<md:NameIDFormat>”.
6. Presionar en Submit e intentar hacer login mediante un usuario de Keycloak (En este caso un usuario USACH).

Si el usuario ya estaba logueado en la consola de Keycloak, otra aplicación o en el correo USACH se aplicará automáticamente el SSO.

Login with zammad.diinf.tk



USERNAME / EMAIL

PASSWORD

☐ Remember me

[Forgot password?](#)

Sign in

OR SIGN IN USING

SAML

You're already logged in with your email address if you're

DIINF

## Sign in to your account

Username or email

admin

Password


••••••

Sign In

Or sign in with



Google

 Acceder con Google

## Elegir una cuenta

para ir a [Keycloak Server](#)



**Roberto Lillo**

roberto.lillo@usach.cl

Saliste de tu cuenta



Usar otra cuenta

Para continuar, Google compartirá tu nombre, dirección de correo electrónico, preferencia de idioma y foto de perfil con Keycloak Server. Antes de usar Keycloak Server, revisa su [política de privacidad](#) y [condiciones del servicio](#).

Español (Latinoamérica) ▾

[Ayuda](#)

[Privacidad](#)

[Condiciones](#)

## Acceso correo corporativo USACH

Estimad@ Usuari@:  
Recuerde que la contraseña de su correo debe ser renovada al menos cada 180 días.

[Recuperación de contraseña](#) | [Cambiar informaciones recuperación contraseña](#)  
[Guía para cambio de contraseña](#)



UNIVERSIDAD  
DE SANTIAGO  
DE CHILE

Keycloak Admin Console x Zammad Helpdesk - My Tickets

zammad.diinf.tk/#ticket/view/my\_tickets

### My Tickets

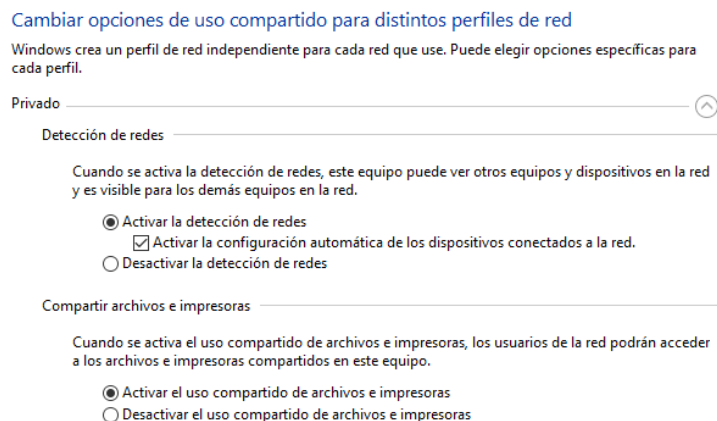
#	TITLE	STATE	CREATED AT
12002	Ticket de Prueba	new	33 minutes ago

Overview Ticket de Prueba

## Cliente de Windows 10

1. Ir a Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración de uso compartido avanzado:

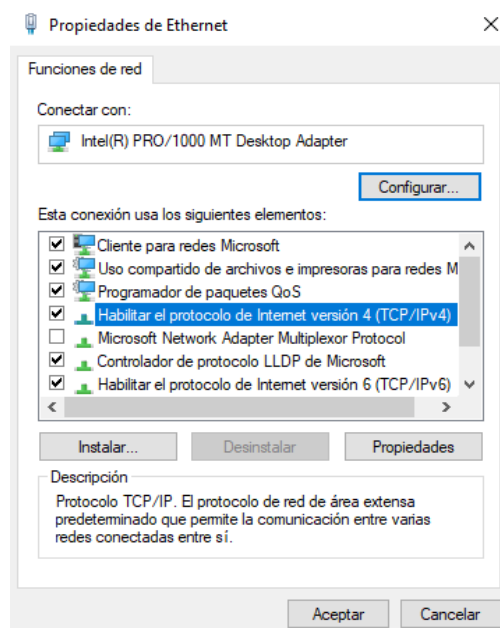
En la pestaña “**Privado**” activar la detección de redes y el uso compartido de archivos e impresoras.



Hacer lo mismo con la pestaña “**Invitado o público**”.

2. Ir a Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador:

En el adaptador de red Click derecho > Propiedades y en la ventana que se despliega buscar Habilitar el protocolo de Internet versión 4 (TCP/IPv4) > Propiedades.





Configurar manualmente la dirección IP y el servidor DNS.

Propiedades de Habilitar el protocolo de Internet versión 4 (TCP/IP... X

General

Puede hacer que la configuración IP se asigne automáticamente si la red admite esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

☐ Obtener una dirección IP automáticamente

☒ Usar la siguiente dirección IP:

Dirección IP: 10 . 128 . 0 . 60

Máscara de subred: 255 . 255 . 255 . 0

Puerta de enlace predeterminada: 10 . 128 . 0 . 1

☐ Obtener la dirección del servidor DNS automáticamente

☒ Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 10 . 128 . 0 . 10

Servidor DNS alternativo: . . .

☐ Validar configuración al salir

Opciones avanzadas...

Aceptar Cancelar

La IP del servidor DNS corresponde a la del servidor de SAMBA Active Directory.

3. Ir a Panel de control > Reloj y región > Fecha y hora > Hora de internet > Cambiar la configuración:

- Activar la sincronización con un servidor de internet
- Añadir **samba.diinf.lan** como servidor
- Presionar en “Actualizar ahora” (puede tomar más de una vez)

Configuración de hora de Internet X

Configure la hora de Internet:

☒ Sincronizar con un servidor horario de Internet

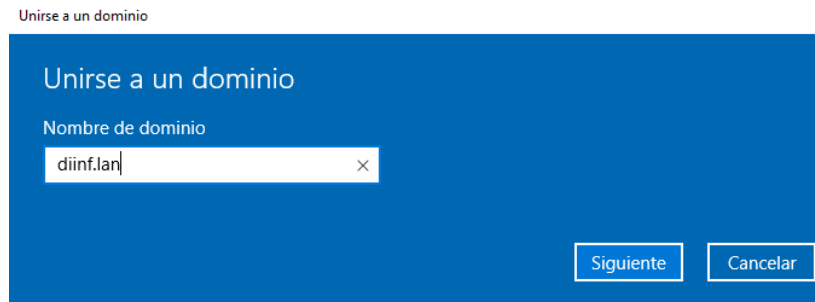
Servidor: samba.diinf.lan Actualizar ahora

Este equipo está configurado para sincronizarse automáticamente de forma programada.

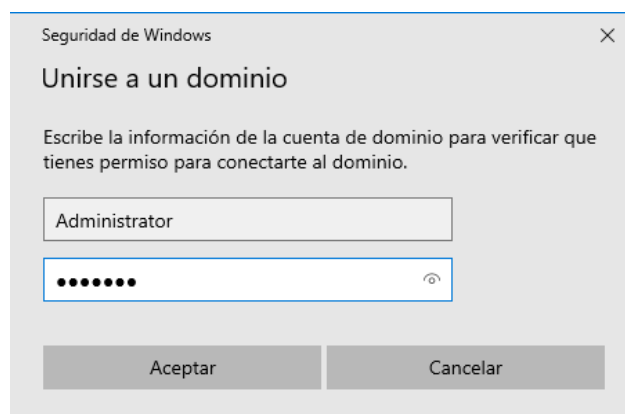
Aceptar Cancelar

4. Para añadir al cliente como parte del dominio dirigirse a Menú de Windows > Configuración > Cuentas > Acceder al trabajo o colegio > Conectar:

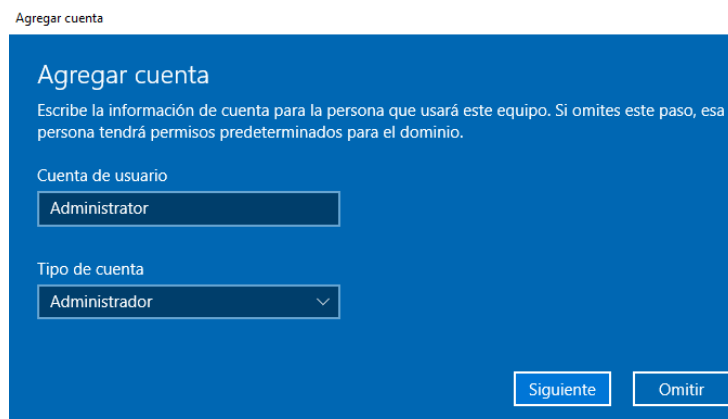
Al final de la ventana desplegada presionar en Unir este dispositivo a un dominio local de Active Directory, luego ingresar el dominio **diinf.lan**.



Al presionar el botón siguiente se solicitará el nombre de usuario y contraseña de algún administrador del dominio.



En el caso de que se quiera hacer uso de las herramientas RSAT, no olvidar colocar el tipo de cuenta como Administrador.



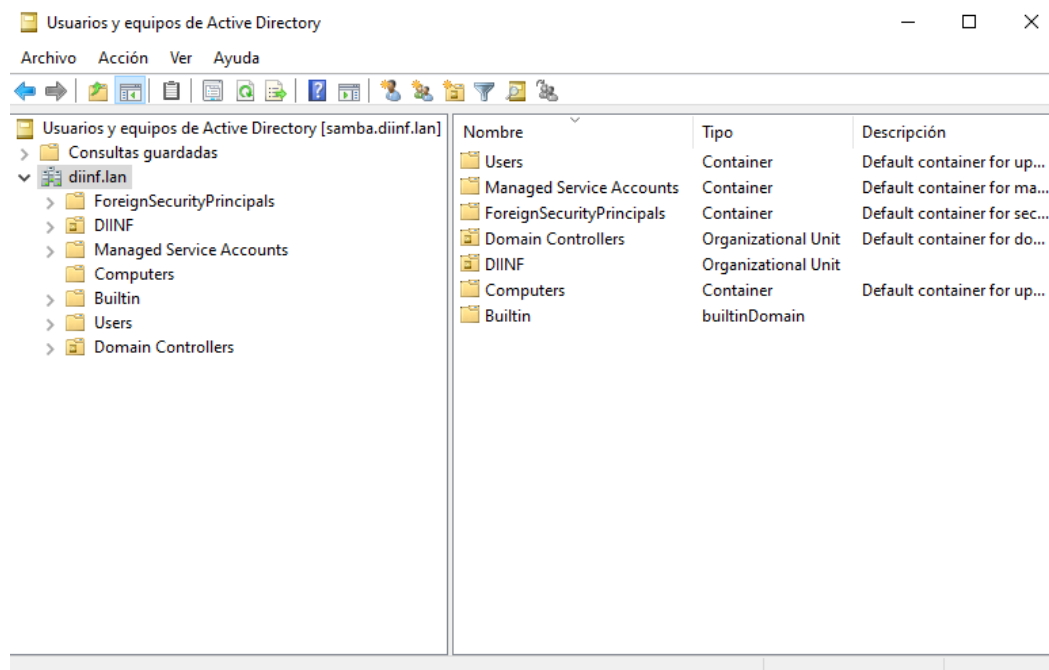
Reiniciar el computador.

5. **INSTALACIÓN HERRAMIENTAS RSAT.** Luego de iniciar sesión con la cuenta de administrador previamente configurada, ir a Menú de Windows > Configuración > Aplicaciones > Características Opcionales > Agregar una característica.

En el buscador ingresar “rsat” y buscar la aplicación “**RSAT: herramientas de Active Directory Domain Services y Lightweight Directory Services**”, seleccionar e instalar.

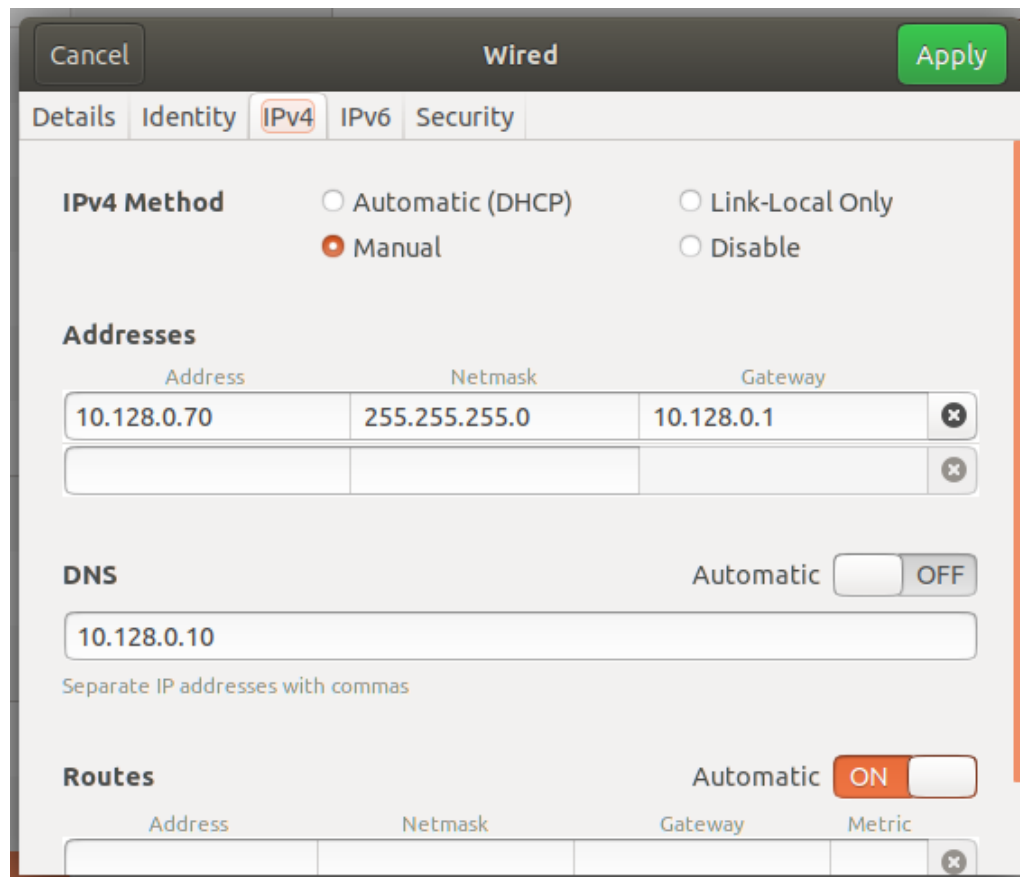


Una vez instalada es posible encontrar las herramientas en Menú de Windows > Herramientas administrativas de Windows > Usuarios y equipos de Active Directory.



## Cliente de Ubuntu 18.04 Desktop

1. Apuntar al servidor de SAMBA como DNS:



2. Actualizar e instalar los paquetes necesarios:

```
$ sudo apt update
$ sudo apt-get install -y realmd sssd sssd-tools
samba-common krb5-user packagekit samba-common-bin
samba-libs adcli ntp
```

Durante la instalación se consultará sobre el realm de kerberos, ingresar: **DIINF.LAN** (tomar en cuenta las mayúsculas).

3. Unir el computador al dominio:

```
$ sudo realm join diinf.lan -U 'Administrator@DIINF.LAN'
-v
```

Solicitará la contraseña de la cuenta utilizada para hacer el join.

#### 4. Configurar realmd:

```
$ sudo nano /etc/realmd.conf

[users]
default-home = /home/%D/%U
default-shell = /bin/bash

[active-directory]
default-client = sssd
os-name = Ubuntu Desktop Linux
os-version = 18.04

[service]
automatic-install = no

[diinf.lan]
fully-qualified-names = no
automatic-id-mapping = yes
user-principal = yes
manage-system = no
```

#### 5. Unir el computador a la red de kerberos en SAMBA Active Directory

```
$ sudo kinit Administrator@DIINF.LAN
```

Solicitará la contraseña de la cuenta utilizada para unirse.

#### 6. Configurar la creación automática de directorio local para los usuarios de AD:

```
$ sudo nano /etc/pam.d/common-session

session required pam_unix.so
session optional pam_winbind.so
session optional pam_sss.so
session optional pam_systemd.so
session required pam_mkhomedir.so skel=/etc/skel/
umask=0077
```

Reiniciar el computador.

#### 7. Hacer login con un usuario del directorio, utilizando uno de los formatos:

```
usuario@diinf.lan - diinf.lan\usuario
```