2019-2020

LUCAS GALÍPOLO URIARTE
JULEN FERNÁNDEZ

SI2

[CHALLENGE 4: SECURE

COMMUNI ON SERV ES

INDEX

1. Contextualization

Once we have all the basic services installed in our network, we should ensure that the network is secure and that the clients and servers can communicate each other. For this purpose, we must avoid all the traffic through the firewall, except for those communications that are absolutely necessary for a good system performance. In the router we are going to add new rules. To ensure all the users in our servers are known hosts, we are going to add an Active Directory to the dns server machine, and all the logins from the domain must authenticate against it. As coruscant.capital is the main network and the Jedi Masters work there, we must ask them to sign a certificate for us in order to maintain our data protected during all the communications. Further, for the communications, we are going to have a mail server and an instant messaging tool. By last, as we have obtained the layouts of the Death Star, we are going to have two printing servers so that we try to print their layouts and find weak points.

All the configurations have been done with root user, except the ones that are necessary with local users or specific users such as inspircd with the irc user. All the services must be restarted and checked after making any kind of change in the configuration file.

2. OpenLDAP

2.1. Introduction

In this challenge we are asked to create an Active Directory from scratch on a Debian10 Linux machine. For this task, we are going to use **OpenLDAP** as our main AD. Using the domain, *hoth.ally*, all the machines at DMZ network will login against this AD. Also, Mail Server and Instant messaging server will take advantage of this AD, so this services' users must authenticate via the OpenLDAP.

2.2. Installation

The DNS machine will be the responsible for managing the OpenLDAP. We will use the network configuration already put in our machine, with IP: *192.168.50.2*

To begin with, we are going to install some packages related to OpenLDAP on the server side and also, some other on the clients.

```
apt install slapd ldap-utils
```

Here we are asked to put the domain. In our case: *hoth.ally*

Then we put the admin password, our domain component (DC) and also our manager account, cn=admin,dc=hoth,dc=ally

After installing the necessary packages, we will start making our main tree. For this, we are using **.ldif** files. The first one will be:

```
nano base.ldif
```

```
dn: ou=people,dc=hoth,dc=ally
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=hoth,dc=ally
objectClass: organizationalUnit
ou: groups
```

Here we are creating *people* and *groups* Organizational Units, where the users and groups will be in. To "run" this ldif, we need to execute the following command:

```
ldapadd -x -D cn=admin,dc=hoth,dc=ally -W -f base.ldif
```

2.3. Configuration

Now we will configure the domain by creating the groups. In this ldif, only the Common Name and the GID number must be change compulsory:

Common Name	GID number
Jedi Masters	5001
Generals	5002
Captains	5003
Pilots	5004

The file to create this groups is the following.

```
nano add_group.ldif
```

```
dn: cn=Pilots,ou=groups,dc=hoth,dc=ally
objectClass: posixGroup
objectClass: top
cn: Pilots
gidNumber: 5004
description: Pilots Group
```

We run this command to execute the ldif.

```
ldapadd -x -D cn=admin,dc=hoth,dc=ally -W -f add_group.ldif
```

At this point, all groups are created, so only we need the users. Before going into the user creation, we will generate a hashed password, in order to secure our password.

```
slappasswd -h {SHA}
```

enter password

This command will return us the given password but encrypted. In our case, the password was **M@ythe4th** so the result is this:

{SHA}fHR+jrbh05loU6s+tNx42ldD+ts=

The following table will show the attributes and its value for each user.

UID CN	**Given Name**	**SN**	**Mail x@hoth.ally**	**UID Number**	**GID Number**	**Home /home/nfs/x**
yoda	Yoda		yoda	2001	5001	yoda
windu	Mace	Windu	windu	2002	5001	windu
luke	Skywalker	Luke	luke	2003	5002	luke
simms	Merrick	Simms	simms	2004	5003	simms
naytaan	Nozzo	Naytaan	naytaan	2005	5004	naytaan
porkins	Jek	Porkins	porkins	2006	5004	porkins
rue	Elyhek	Rue	rue	2007	5004	rue
narra	Arhul	Narra	narra	2008	5004	narra

The ldif file to create a user is the following.

```
nano add_user.ldif
```

```
dn: uid=narra,ou=people,dc=hoth,dc=ally
uid: narra
cn: narra
givenName: Arhul
sn: Narra
mail: narra@hoth.ally
objectClass: inetOrgPerson
```

```
objectClass: posixAccount
objectClass: top
loginShell: /bin/bash
uidNumber: 2008
gidNumber: 5004
homeDirectory: /home/nfs/narra
userPassword: {SHA}fHR+jrbh05loU6s+tNx42ldD+ts=
```

```
ldapadd -x -D cn=admin,dc=hoth,dc=ally -W -f add_user.ldif
```

With the next ldif, we add some users to a specific group.

```
nano add_user_group.ldif
```

```
dn: cn=Pilots,ou=groups,dc=hoth,dc=ally
changetype: modify
add: memberUid
memberUid: naytaan
memberUid: porkins
memberUid: rue
memberUid: narra
```

```
ldapadd -x -D cn=admin,dc=hoth,dc=ally -W -f add_user_group.ldif
```

If we want to see all the domain, we can just run **slapcat**, and it will show us all the Active Directory tree. Also another resource to see our domain is with *LAM* (LDAP Account Manager) which runs on an Apache server.

2.4. Services

Start OpenLDAP service

```
systemctl start slapd
```

Stop the LDAP

```
systemctl stop slapd

systemctl restart slapd

systemctl status slapd
```

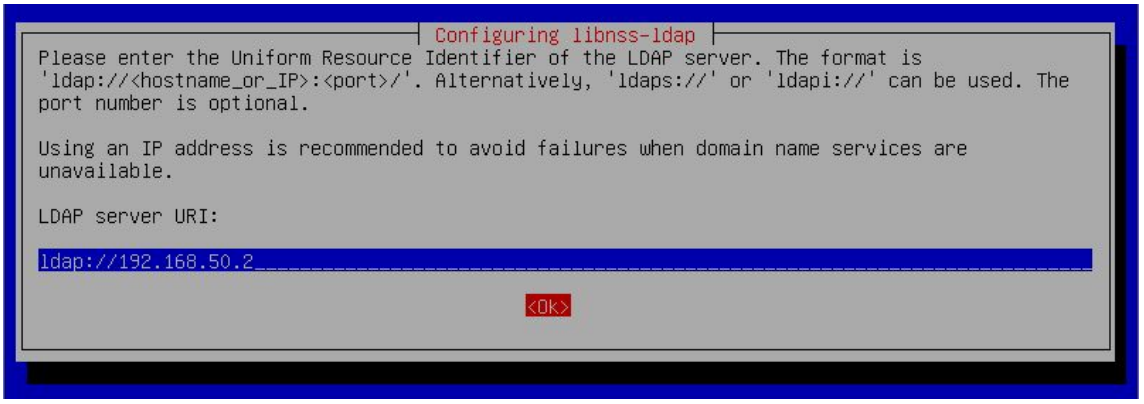
See the ldap status, if everything is ok, the status must be green, if not, red.

2.5. Client side

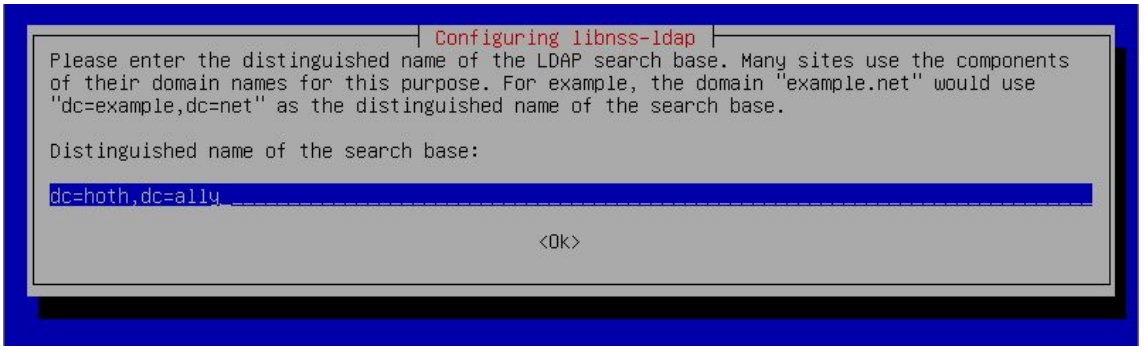
We have already installed the OpenLDAP server on the DNS, so we will configure a Debian10 machine in order to login to that LDAP. First of all, our machine's DNS must the LDAP's IP, 192.168.50.2. We install some packages.

```
apt install libnss-ldap libpam-ldap ldap-utils
```

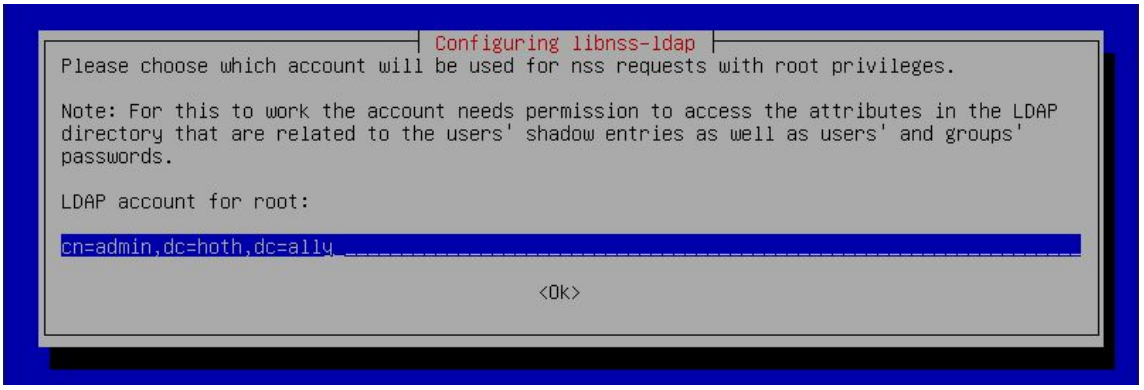
A blue terminal will show up, follow the images.



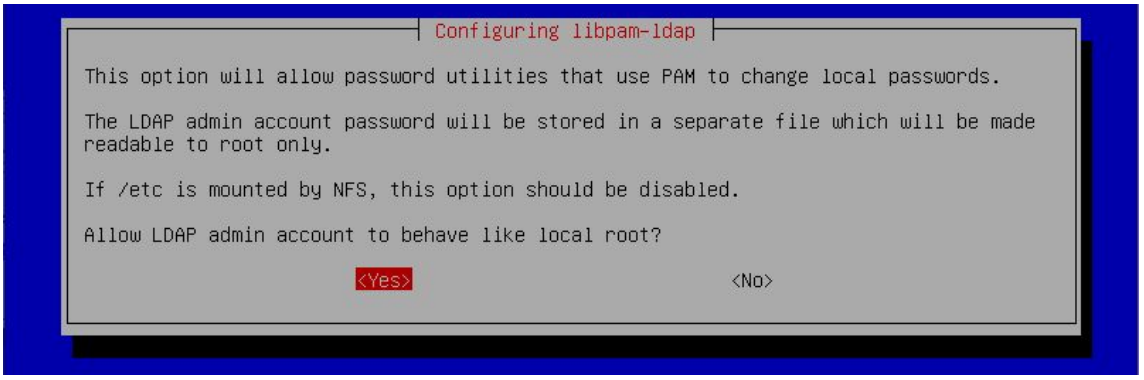
We put ours LDAP's IP address. The prefix must be ***ldap://***



We put our Distinguished Name.



The manager account. LDAP administrator.



When it's finished, we will configure some files.

nano /etc/nsswitch.conf

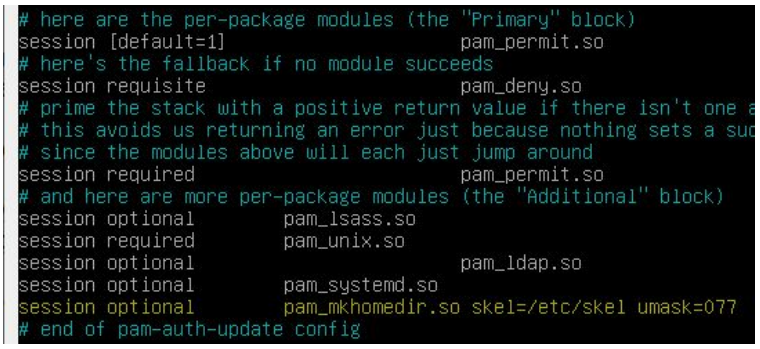
```
passwd:         compat ldap files systemd
group:          compat ldap files systemd
shadow:         compat files
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

nano /etc/pam.d/common-password

```
# here are the per-package modules (the "Primary" block)
password        [success=3 default=ignore]      pam_lsass.so
password        [success=2 default=ignore]      pam_unix.so obscure try_first_pass sha512
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so use_authtok try_first_p$
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
```

Delete the highlighted word ***use_authtok***

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



Add the highlighted line to that file

To restart the libnss-ldap service:

```
systemctl restart nscd
```

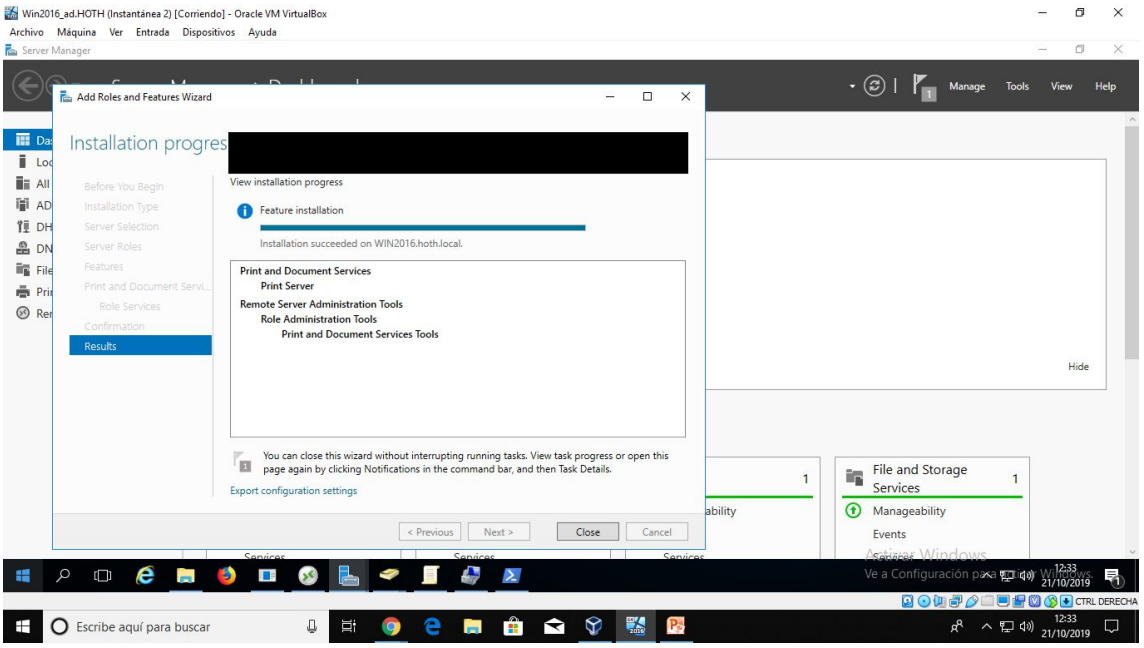
3. Printer Management

3.1. Introduction

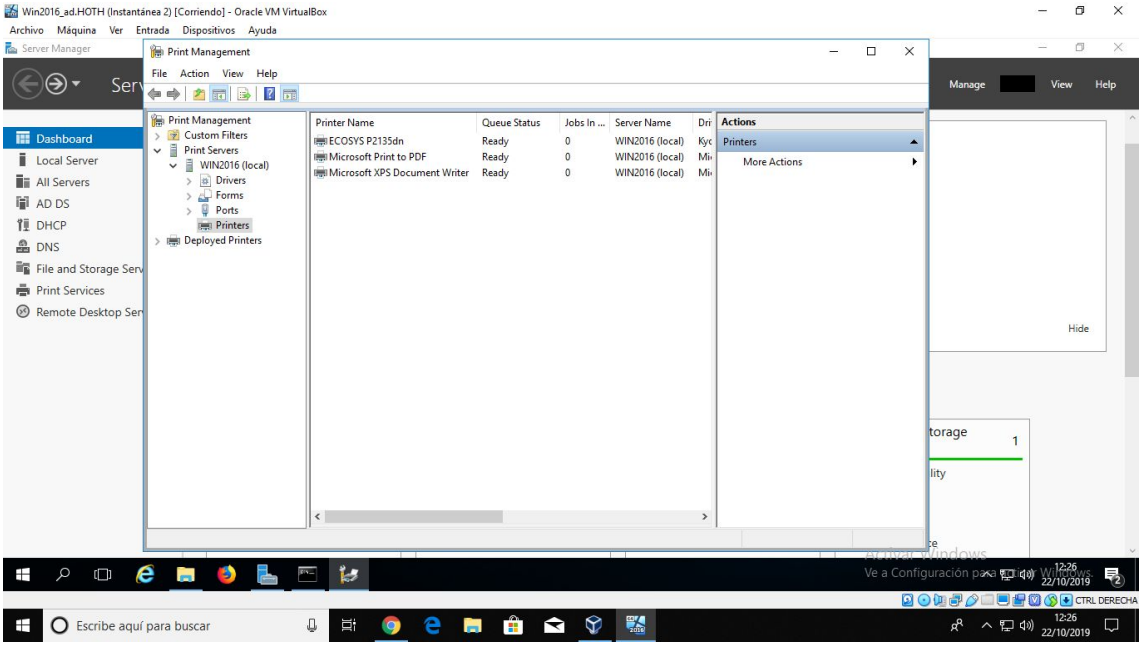
As we have obtained the layouts of the Death Star, we are going to have two printing servers so that we try to print their layouts and find weak points.
For this purpose we are going to use two network printers with their correspondent printing server.

3.2. Network Printer (WServer2016)

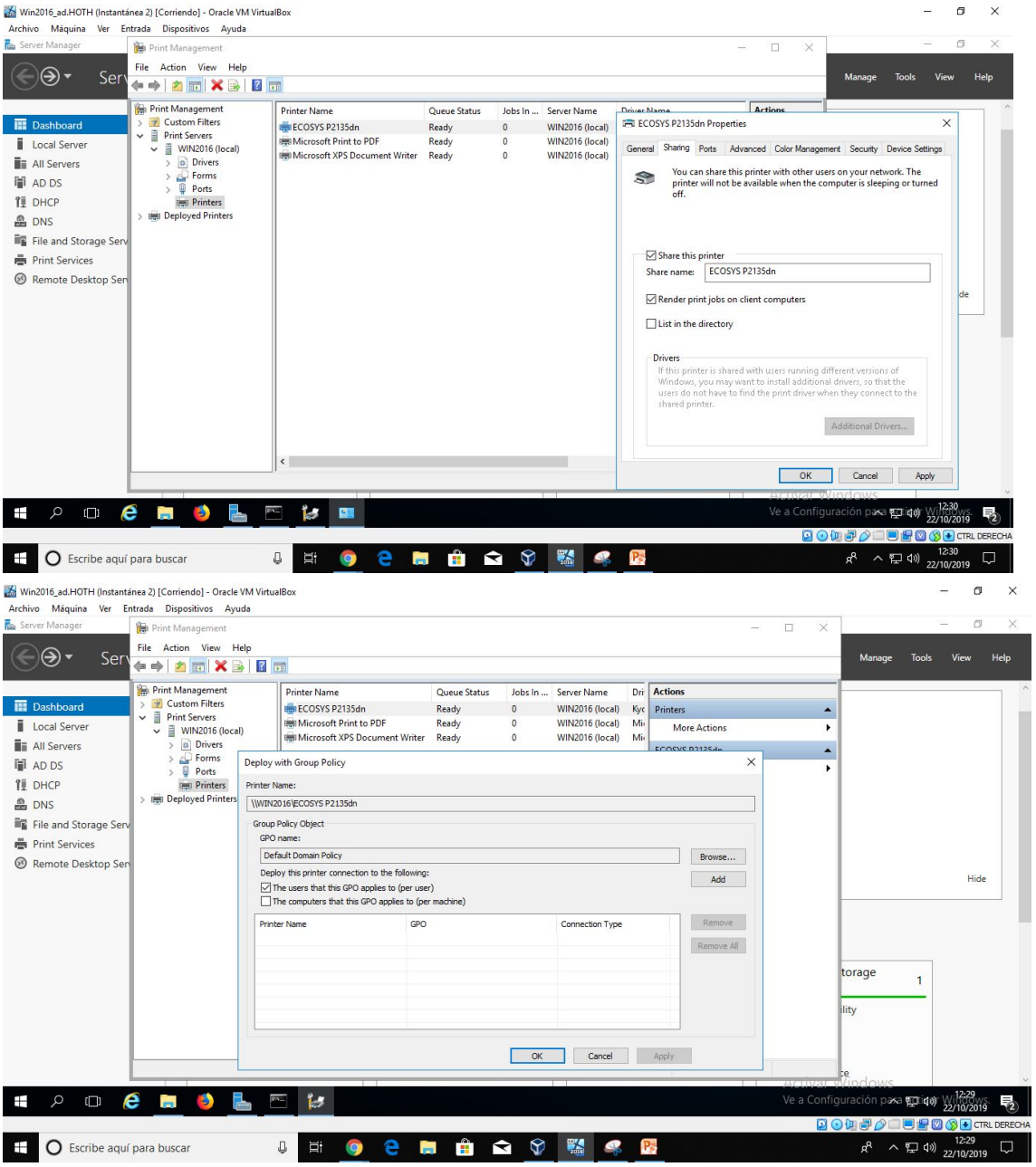
The first one is a network printer directly connected to the network. It is going to be connected to our .local switch. I
After that, we are going to install in our Windows Server 16 machine the Print Server role.



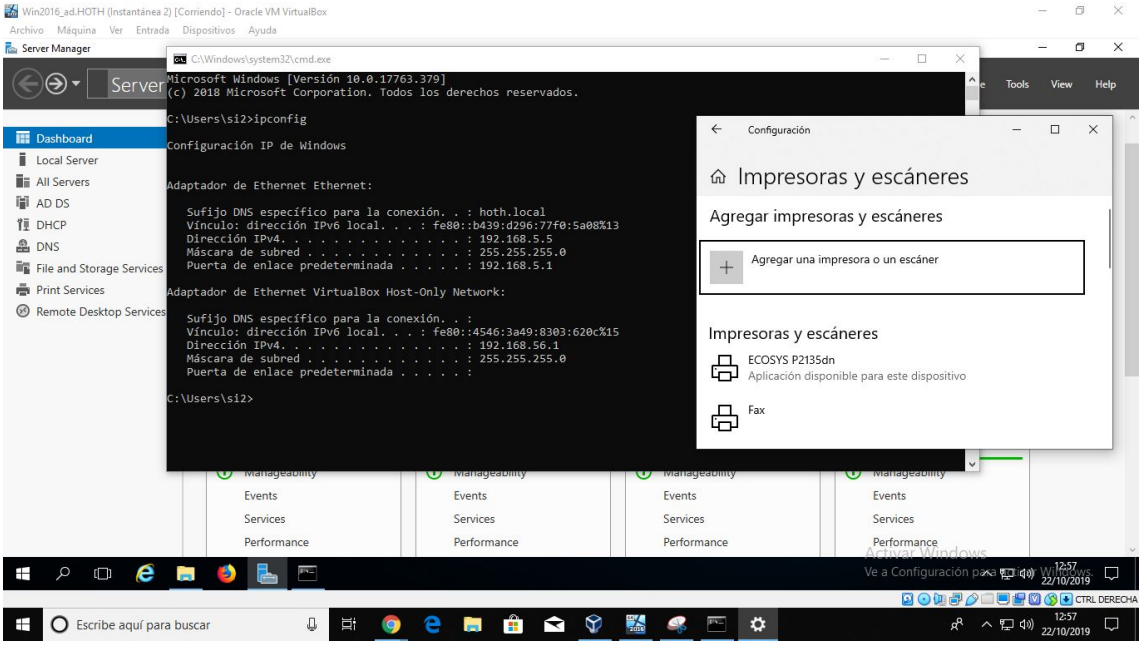
With this tool we can check all the printers that our computer detects.



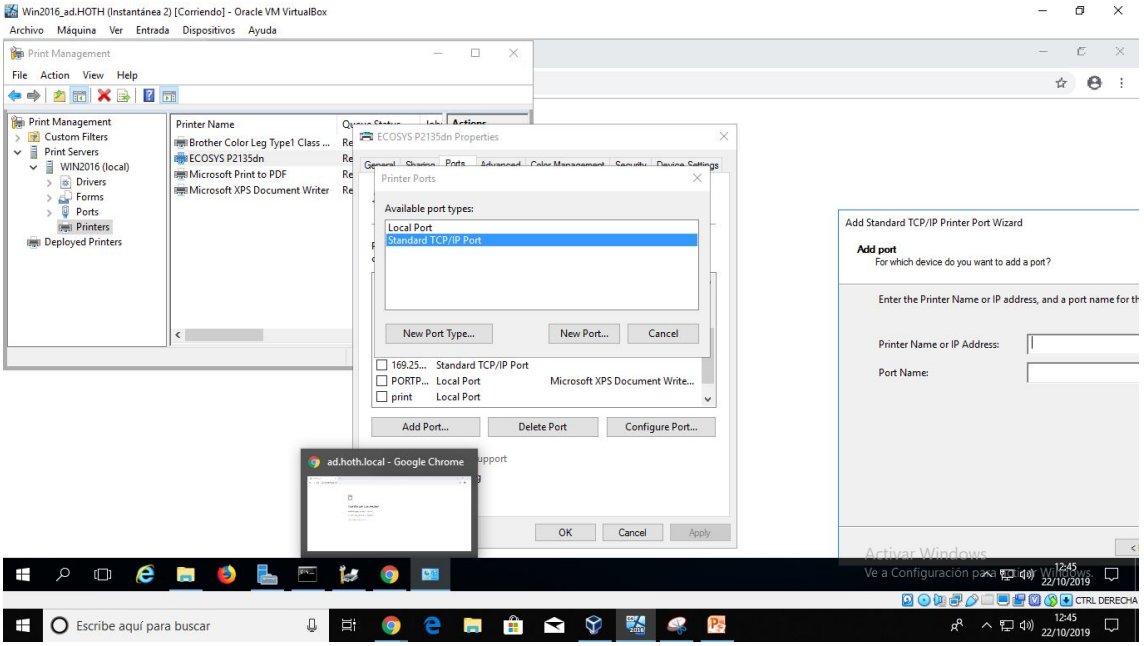
ECOSYS P2135dn is the name of the network printer. We must share it and works pretty well adding this GPO to the Default Domain Policy.



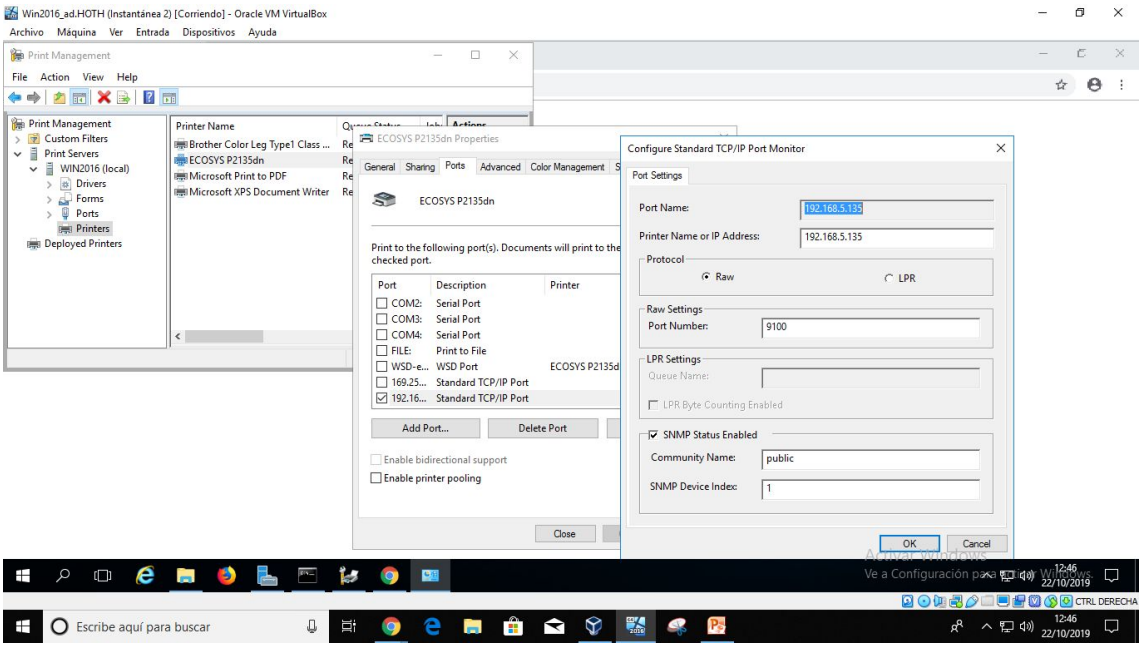
Another client in the network is able to detect this printer.



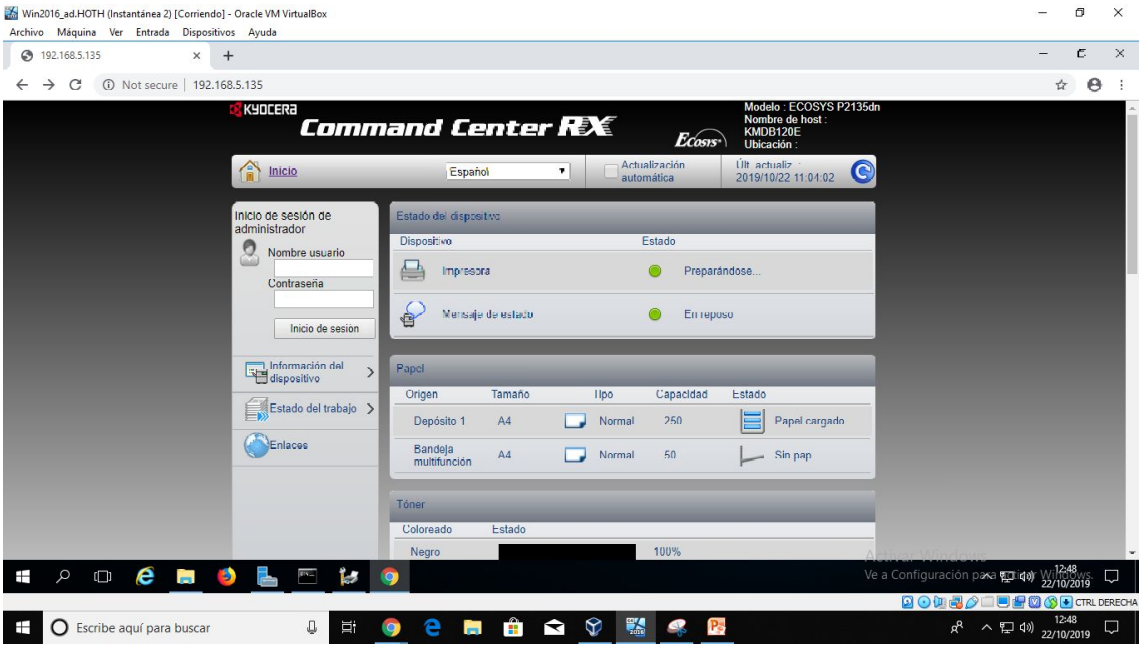
Using the IPP (Internet Printer Protocol) we are going to be able to connect to the printer server via its IP.



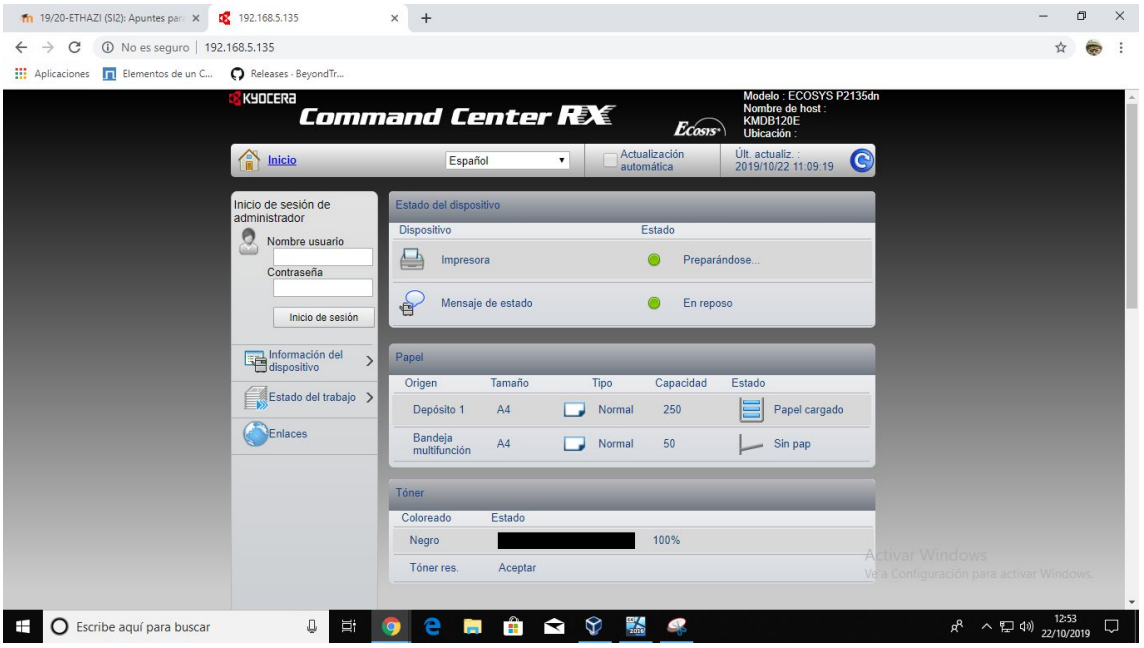
In our case, the printer is registered in our DHCP server and must have a reserved IP, 192.168.5.135 in our network.



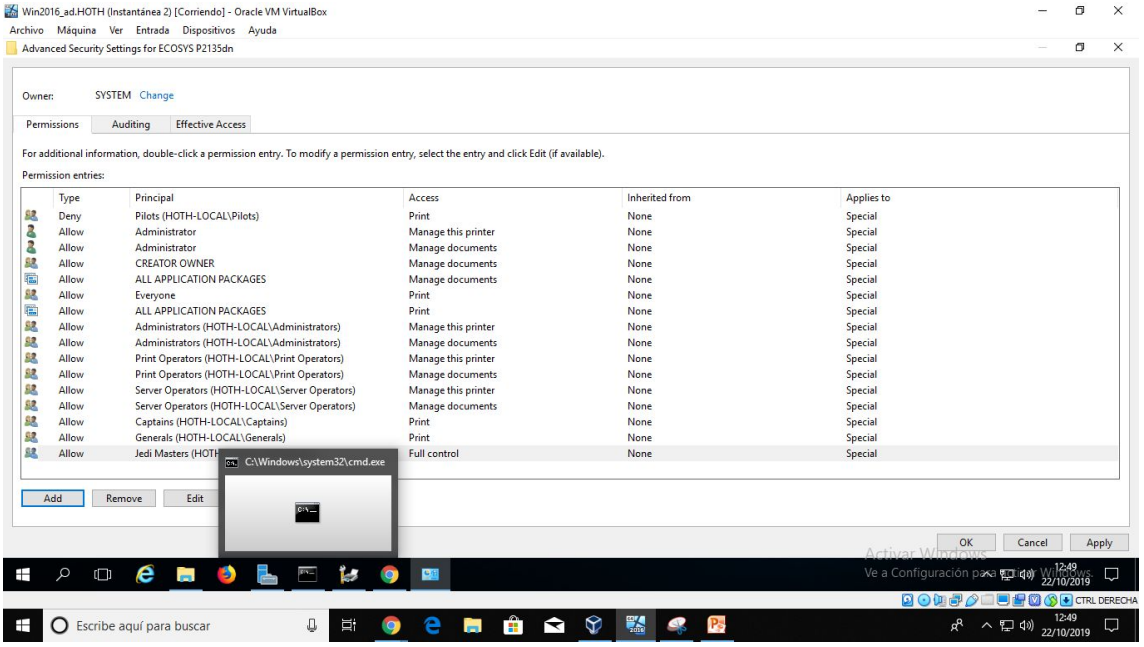
After opening the port, we can connect to the printer server navigating to that IP.



The client is also able to connect to the printer server.



As we don't want all the users to be capable of printing documents or managing the printer, we have configured logical permissions for the groups of the domain.



3.3. Network Printer (Linux)

The other network printer is going to be configured in our Raspberry Pi. Cups(Common Unix Printing System) is the service we are going to use.

```
sudo apt-get install cups
```

We will need CUPS accessible across whole network, at this moment it will block any non-localhost traffic.

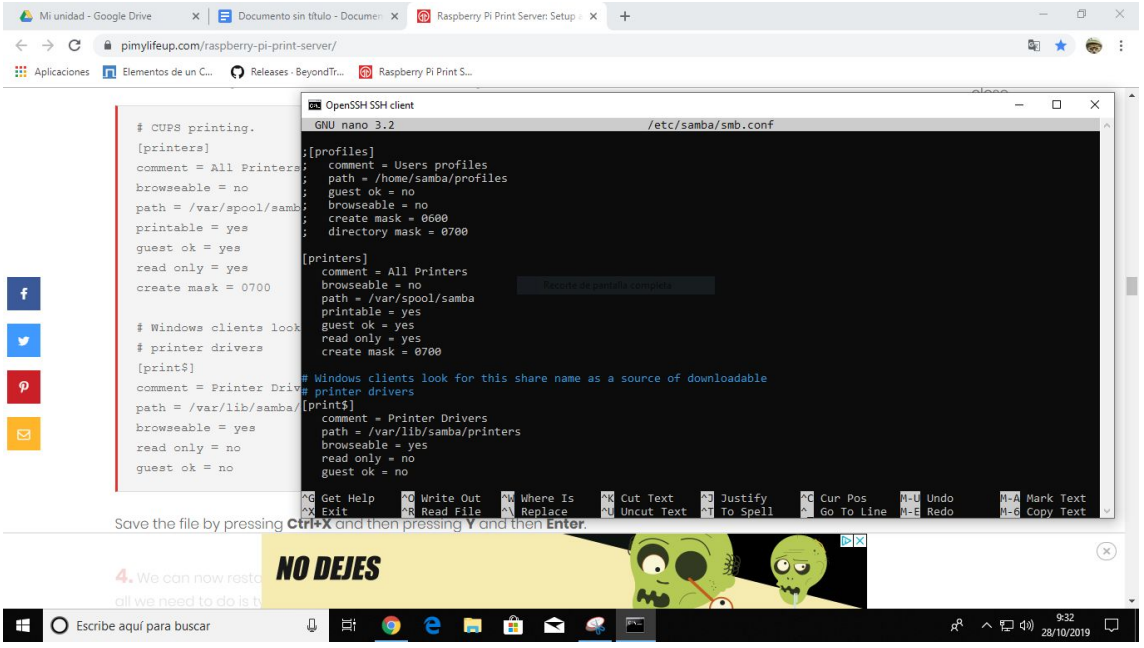
```
sudo cupsctl --remote-any
```

```
sudo /etc/init.d/cups restart
```

As we want to use our print server with Windows, then setting up SAMBA correctly is necessary.

```
sudo apt-get install samba

sudo nano /etc/samba/smb.conf
```

We have to change some values in this file and must match with the ones this file.

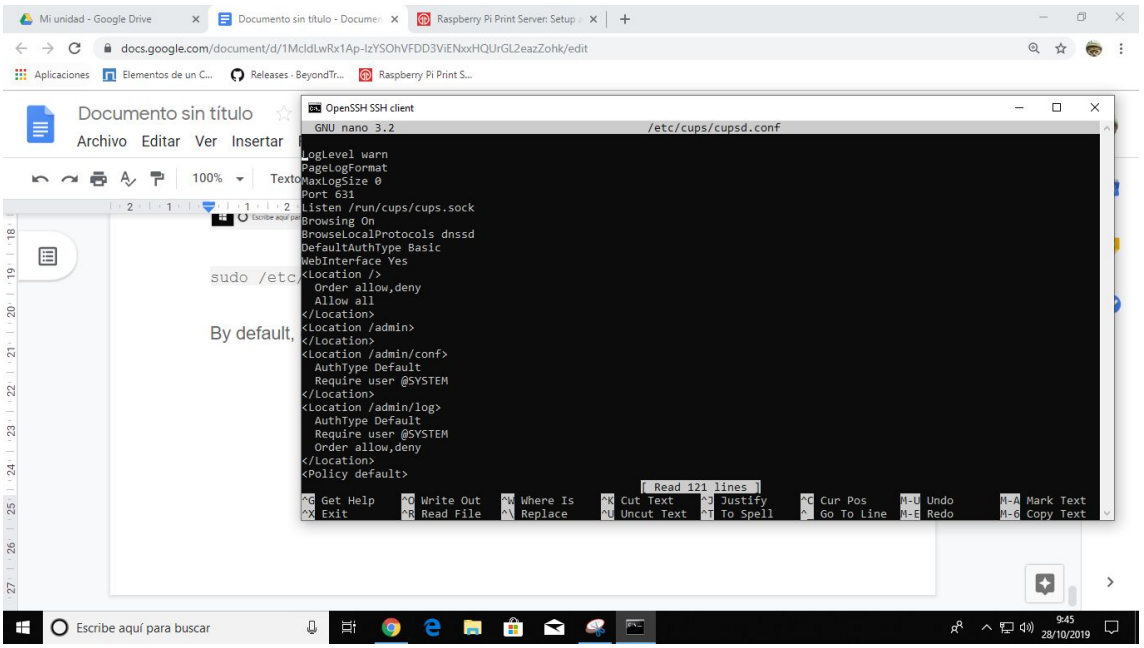


We restart the service and check that everything works properly,

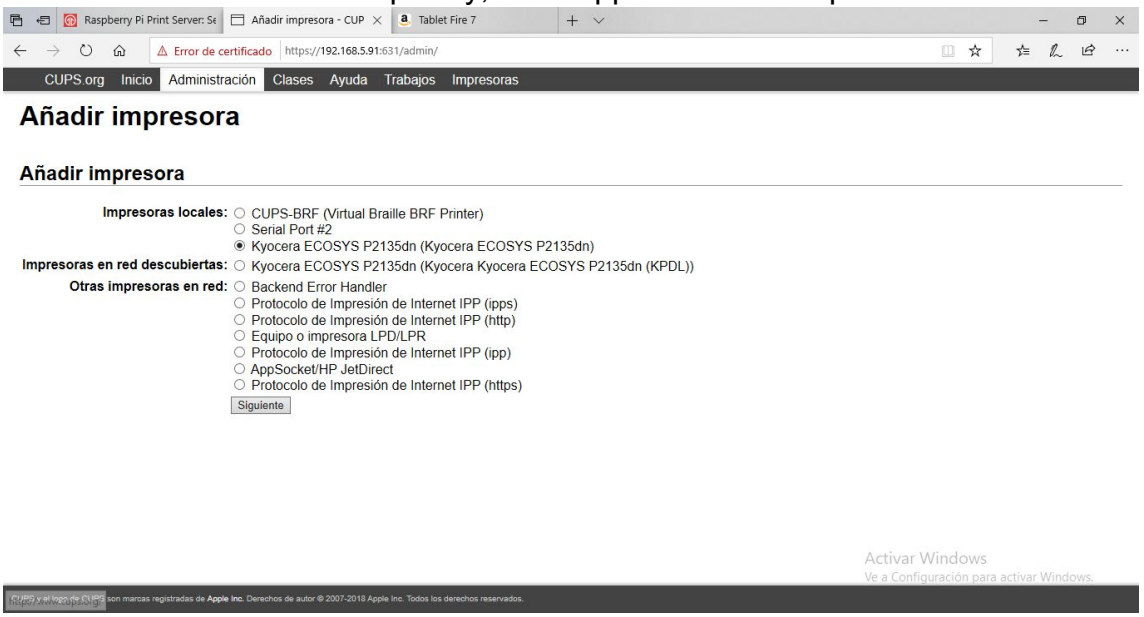
```
service smbd restart

service smbd status
```

By default, cups uses the port 631 as it is configured in this file:

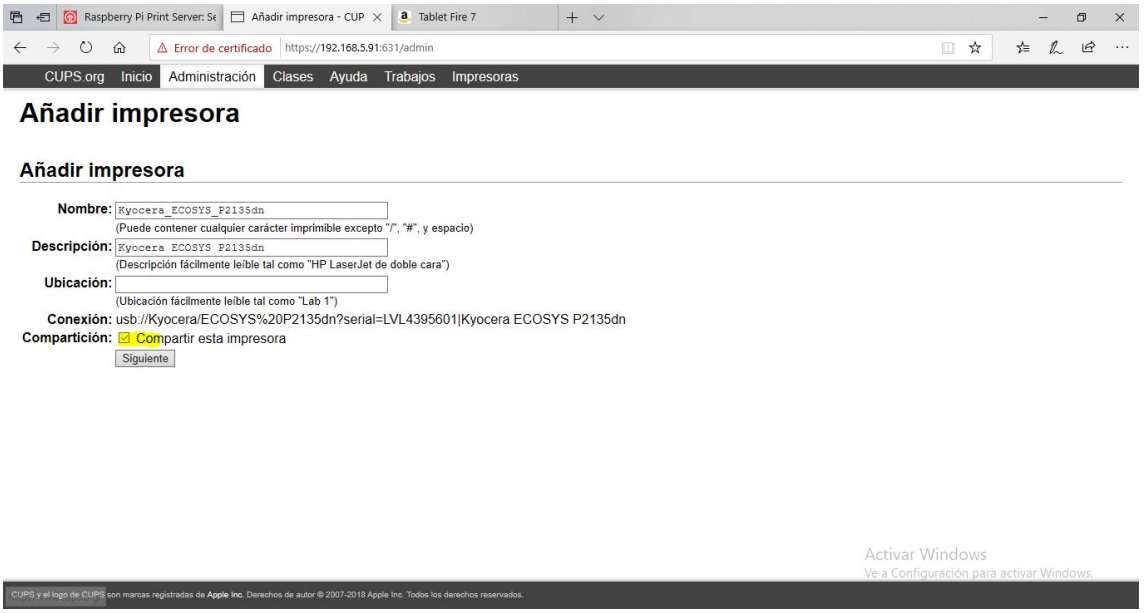
nano /etc/cups/cupsd.conf

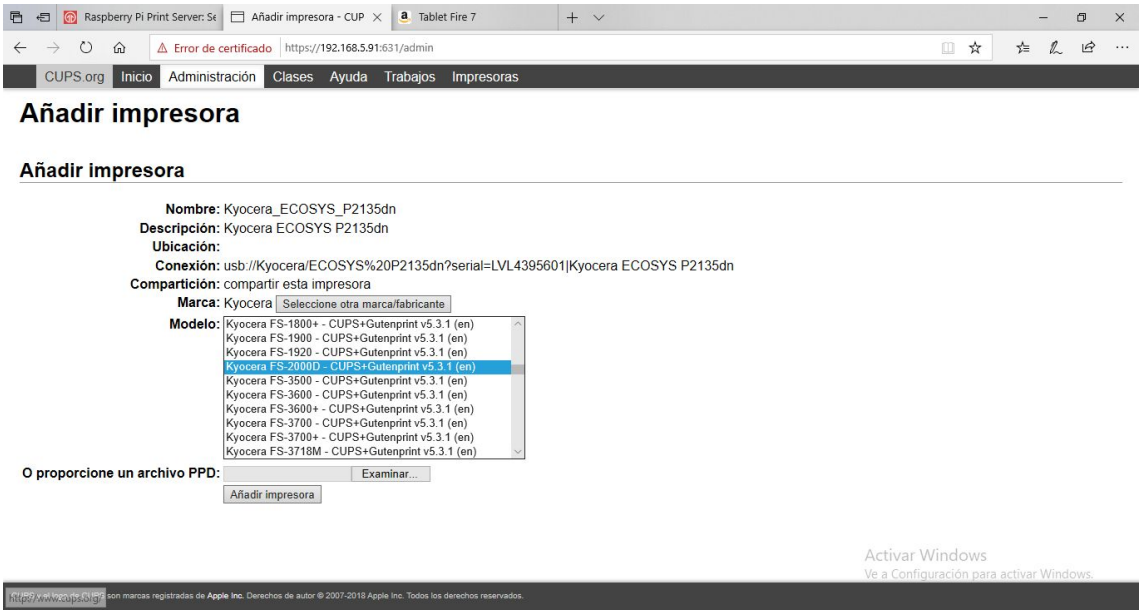


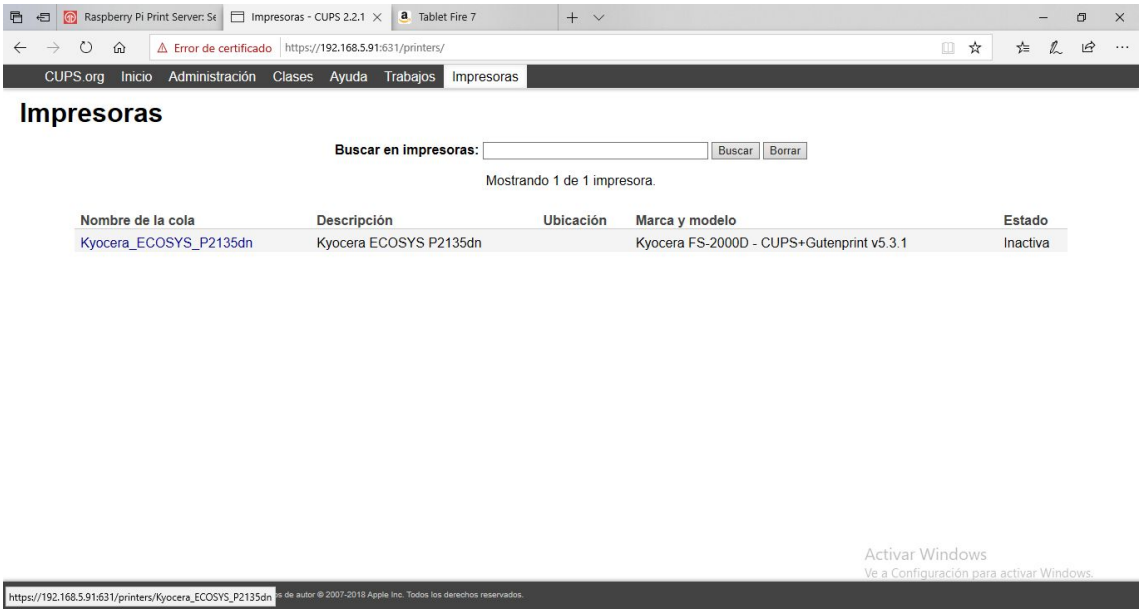
So now we are going to connect to the printer server and configure our printer. As its connected to the Raspberry, it will appear as a local printer.

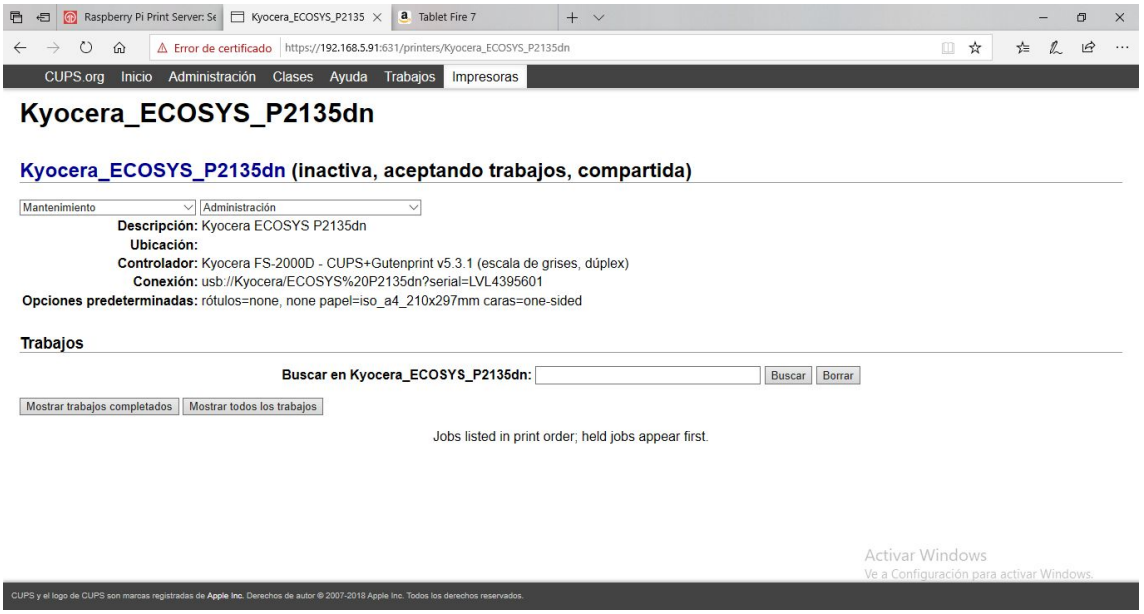


We must share it.

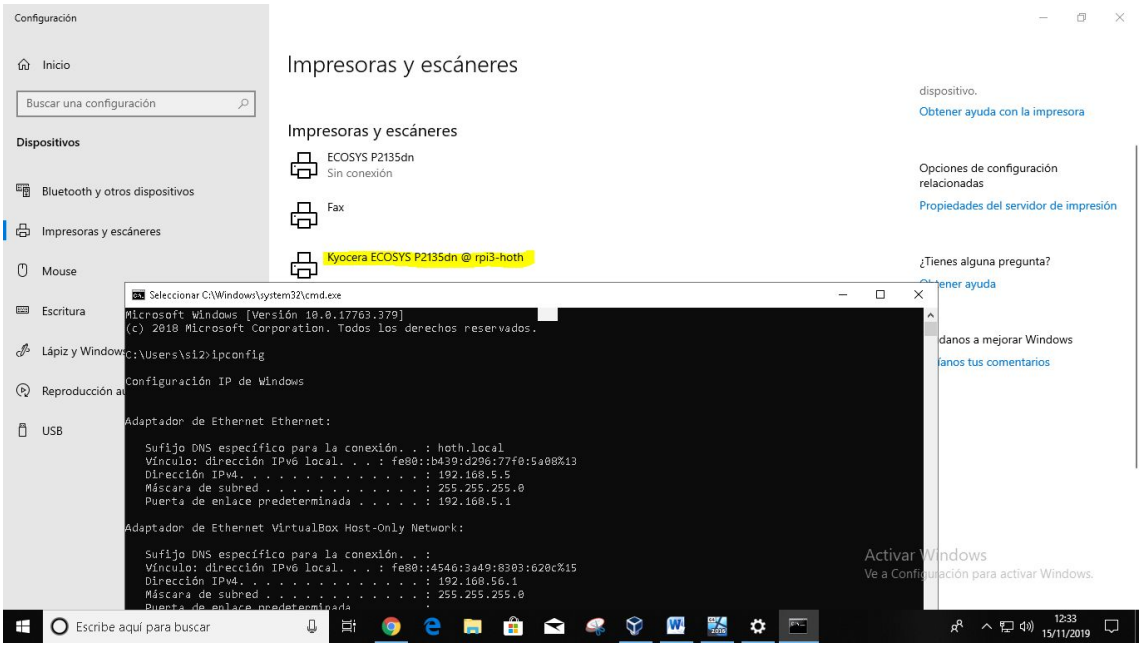

Raspberry Pi Print Server: Se
Añadir impresora - CUP
Tablet Fire 7
Error de certificado
https://192.168.5.91:631/admin
CUPS.org Inicio Administración Clases Ayuda Trabajos Impresoras
Añadir impresora
Añadir impresora
Nombre: Kyocera_ECOSYS_P2135dn
(Puede contener cualquier carácter imprimible excepto "/", "#", y espacio)
Descripción: Kyocera ECOSYS P2135dn
(Descripción fácilmente leíble tal como "HP LaserJet de doble cara")
Ubicación:
(Ubicación fácilmente leíble tal como "Lab 1")
Conexión: usb://Kyocera/ECOSYS%20P2135dn?serial=LVL4395601|Kyocera ECOSYS P2135dn
Compartición: Compartir esta impresora
Siguiente
Activar Windows
Ve a Configuración para activar Windows.
CUPS y el logo de CUPS son marcas registradas de Apple Inc. Derechos de autor © 2007-2018 Apple Inc. Todos los derechos reservados.


Raspberry Pi Print Server: Se
Añadir impresora - CUP
Tablet Fire 7
Error de certificado
https://192.168.5.91:631/admin
CUPS.org Inicio Administración Clases Ayuda Trabajos Impresoras
Añadir impresora
Añadir impresora
Nombre: Kyocera_ECOSYS_P2135dn
Descripción: Kyocera ECOSYS P2135dn
Ubicación:
Conexión: usb://Kyocera/ECOSYS%20P2135dn?serial=LVL4395601|Kyocera ECOSYS P2135dn
Compartición: compartir esta impresora
Marca: Kyocera Seleccione otra marca/fabricante
Modelo:
Kyocera FS-1800+ - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-1900 - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-1920 - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-2000D - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3500 - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3600 - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3600+ - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3700 - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3700+ - CUPS+Gutenprint v5.3.1 (en)
Kyocera FS-3718M - CUPS+Gutenprint v5.3.1 (en)
O proporcione un archivo PPD: Examinar...
Añadir impresora
Activar Windows
Ve a Configuración para activar Windows.
son marcas registradas de Apple Inc. Derechos de autor © 2007-2018 Apple Inc. Todos los derechos reservados.





Now we know that the printer is shared, we are going to check that another client from our .local domain can print with this printer.



4. Firewall

4.1. Introduction

In order to prevent unauthorized people entering our router or private area, we are going to restrict many of the firewall rules. The router must be strictive enough to have connection from .local to outside but from outside to .local no, from .ally to outside but from outside to .ally, the connection will be limited, only some ports will be shown.

4.2. Script

```
nano /etc/init.d/firewall_rules.sh
```

```
#!/bin/bash

### BEGIN INIT INFO
# Provides:          fw.sh
# Required-Start:    $all
# Required-Stop:     $all
# Default-Start:     2 3 4 5
# Default-Stop:              0 1 6
# Short-Description: Firewall
# Description:               Establece el firewall en este router
### END INIT INFO

# Activar enrutamiento
```

```
        echo 1 > /proc/sys/net/ipv4/ip_forward

        # Variables
        RED_LOCAL=192.168.5.0/24
        RED_DMZ=192.168.50.0/24
        RED_CLASE=172.20.202.0/24
        IFACE_OUT=enp2s5
        IP_MAIL=192.168.50.4
        IP_CHAT=$IP_MAIL
        IP_DNS=192.168.50.2
        IP_AD=$IP_DNS
        IP_WEB=192.168.50.3
        IP_DHCP=192.168.5.91
        IP_ROUTER=172.20.202.35

        ## Borrar todas las reglas
        iptables -F
        iptables -t nat -F

        ## Politicas por defecto
        iptables -P INPUT DROP
        iptables -P OUTPUT DROP
        iptables -P FORWARD DROP

        ## Logs a todos los intentos de conexión
        iptables -A FORWARD -s $RED_CLASE -j LOG --log-prefix
'IPTABLES-CORUSCANT-FORWARD# '
        iptables -A INPUT -s $RED_CLASE -j LOG --log-prefix
'IPTABLES-CORUSCANT-INPUT# '

        ## Aceptar todos los paquetes que hayan establecido conexión
        iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
        iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
        iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT

        ## Aceptar puertos en router
        # Poder meterse por SSH
        iptables -A INPUT -p tcp --dport 22 -j ACCEPT
        # Necesarios para acceder a la red desde el router
        iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT  # Salida HTTP
        iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT  # Salida HTTPS
        iptables -A OUTPUT -p tcp --dport 21 -j ACCEPT  # Salida FTP
        iptables -A OUTPUT -p udp --dport 53 -j ACCEPT # Salida DNS
        # Poder hacer Ping
        iptables -A OUTPUT -p icmp -j ACCEPT # Salida de ping
```

```
        # Solo los de la DMZ pueden hacerle ping
        iptables -A INPUT -s $RED_DMZ -p icmp -j ACCEPT
        # Aceptar pasar los ping que pasa por el router hacia afuera y no al
reves
        iptables -A FORWARD -s $RED_DMZ -p icmp -j ACCEPT
        iptables -A FORWARD -s $RED_LOCAL -p icmp -j ACCEPT



        ## Puertos de los distintos servicios
        # Router
        iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
        # Servidor Web 192.168.50.3
        iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
        iptables -A FORWARD -p tcp --dport 443 -j ACCEPT
        # Servidor DNS 192.168.50.2
        iptables -A FORWARD -p udp --dport 53 -j ACCEPT
        # Servidor Mail 192.168.50.4
        iptables -A FORWARD -p tcp --dport 25 -j ACCEPT
        iptables -A FORWARD -p tcp --dport 587 -j ACCEPT
        iptables -A FORWARD -p tcp --dport 143 -j ACCEPT
        iptables -A FORWARD -p tcp --dport 993 -j ACCEPT
        iptables -A FORWARD -p tcp --dport 6667 -j ACCEPT
        # Servidor DHCP 192.168.5.91
        iptables -A FORWARD -p tcp --dport 631 -j ACCEPT

        ## Redirecciones
        # Servidor DNS 192.168.50.2
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 22502 -j
DNAT --to $IP_DNS:22502
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p udp --dport 53 -j
DNAT --to $IP_DNS:53
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 8001 -j
DNAT --to $IP_AD:80
        # Servidor Web 192.168.50.3
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 22503 -j
DNAT --to $IP_WEB:22
        # Servidor Mail 192.168.50.4
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 22504 -j
DNAT --to $IP_MAIL:22
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 25 -j
DNAT --to $IP_MAIL:25
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 587 -j
DNAT --to $IP_MAIL:587
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 143 -j
DNAT --to $IP_MAIL:143
```

```
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 993 -j
DNAT --to $IP_MAIL:993
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 8002 -j
DNAT --to $IP_MAIL:80
        iptables -t nat -A PREROUTING -i $IFACE_OUT -p tcp --dport 6667 -j
DNAT --to $IP_CHAT:6667

        ## Acceso desde redes internas a internet
        # Red 192.168.5.0/24
        iptables -A FORWARD -s $RED_LOCAL -p tcp --dport 21 -j ACCEPT
        # Red 192.168.50.0/24
        iptables -A FORWARD -s $RED_DMZ -p tcp --dport 21 -j ACCEPT

        #Activar enrutamiento
        iptables -t nat -A POSTROUTING -o enp2s5 -j MASQUERADE
```

5. Digital certificates

5.1. Introduction

A digital signature is an encrypted file that travels with the electronic document that needs to be signed and returns with it after the transaction has been completed. The file contains and captures data about where the electronic document traveled, which accounts opened it and the IP address of the devices that signed it as most important information.
We are going to have a Mail server and is recommendable to sign all the documents we are going to send. All of this data protects the validity of the signature and that's why we are going to use a digital certificate in our domain, one that is going to be signed by coruscant.capital.

5.2. Configuration

The tool selected for this purpose is openssl. First of all we install it with this command:

```
apt install openssl ca-certificates
```

First we are going to generate a private key and a *certificate signing request. The command for the generation of the private key is:*

```
openssl genrsa -des3 -out server.key 2048
```

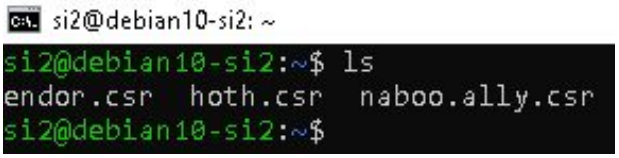
For the generation of the signing request we are going to generate a .csr file using the private key generated before.

```
openssl req -new -key server.key -out server.csr –subj
‘/C=RC/ST=Hoth/O=Hoth/OU=Hoth/CN=mail.hoth.ally’
```

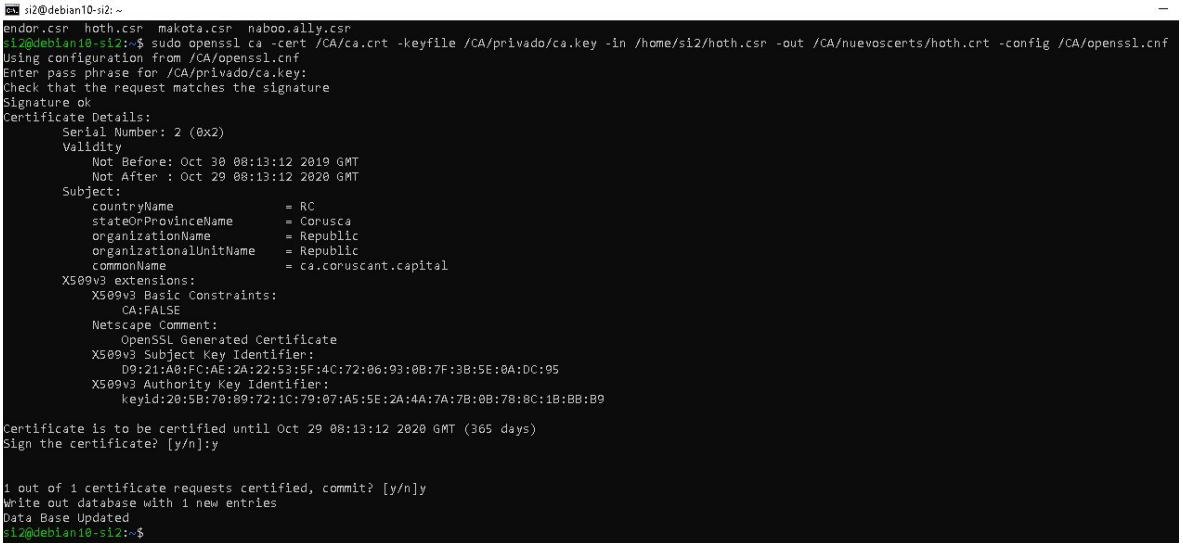
Then we are going to copy this file in the computer of the company which we are going to ask to sign the certificate. For this we are going to use scp command as both computers can connect via ssh.

```
scp hoth.csr si2@172.20.202.252:/home/si2
```

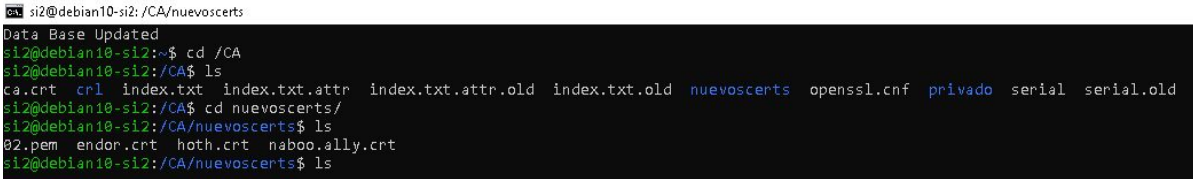
We check that the file has been copied.
For this purpose we must connect via ssh to the company’s server.



Then, we are going to generate our own certificate using the company's private key, their certificate and configuration and our certificate request. For this purpose we must connect via ssh to the company’s server.



Here we check that has been created correctly.



This certificate can also have the .pem format which is used in mail services.

6. Electronic Mail Server

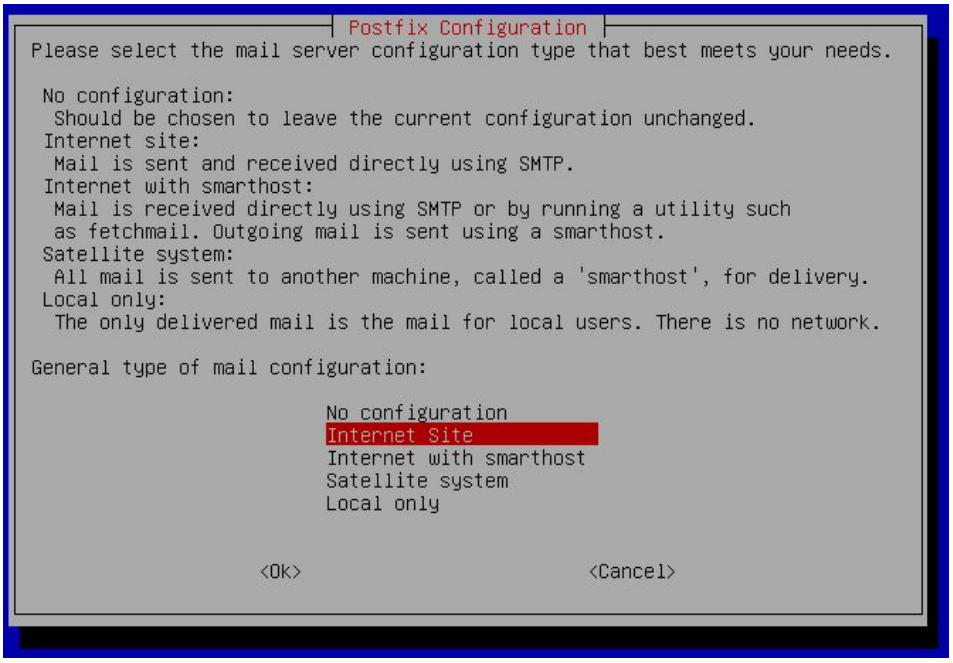
6.1. Introduction

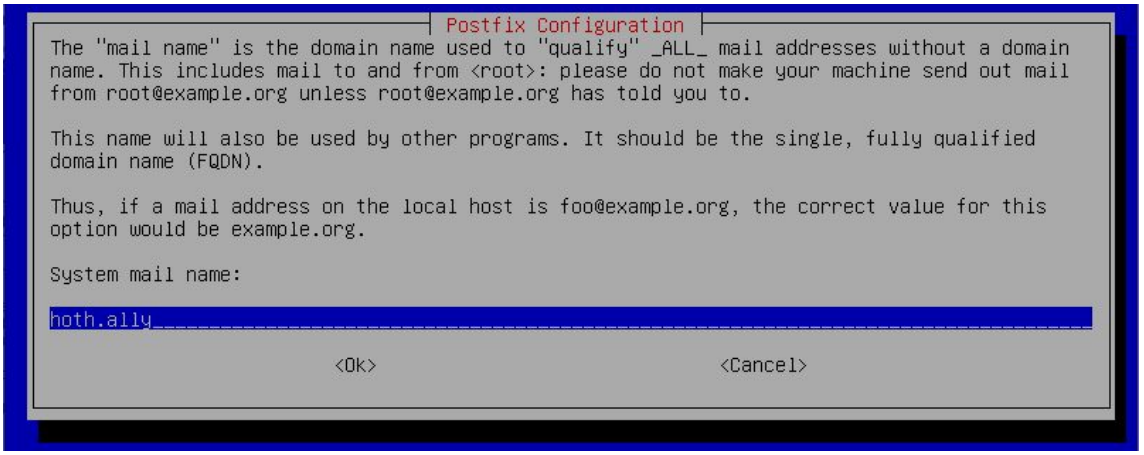
We have to create an email server inside the DMZ, exactly on 192.168.50.4 machine. The DNS is already configured with a Mail Exchanger. A mail server works with SMTP, IMAP and POP3 protocols. The SMTP is for data transferring between servers and from client to server, whereas IMAP and POP only works from server to client. In this occasion, we will use *Postfix* for SMTP and *Dovecot* for IMAP and POP3.

6.2. Installation

We will install Postfix

```
apt install postfix
```



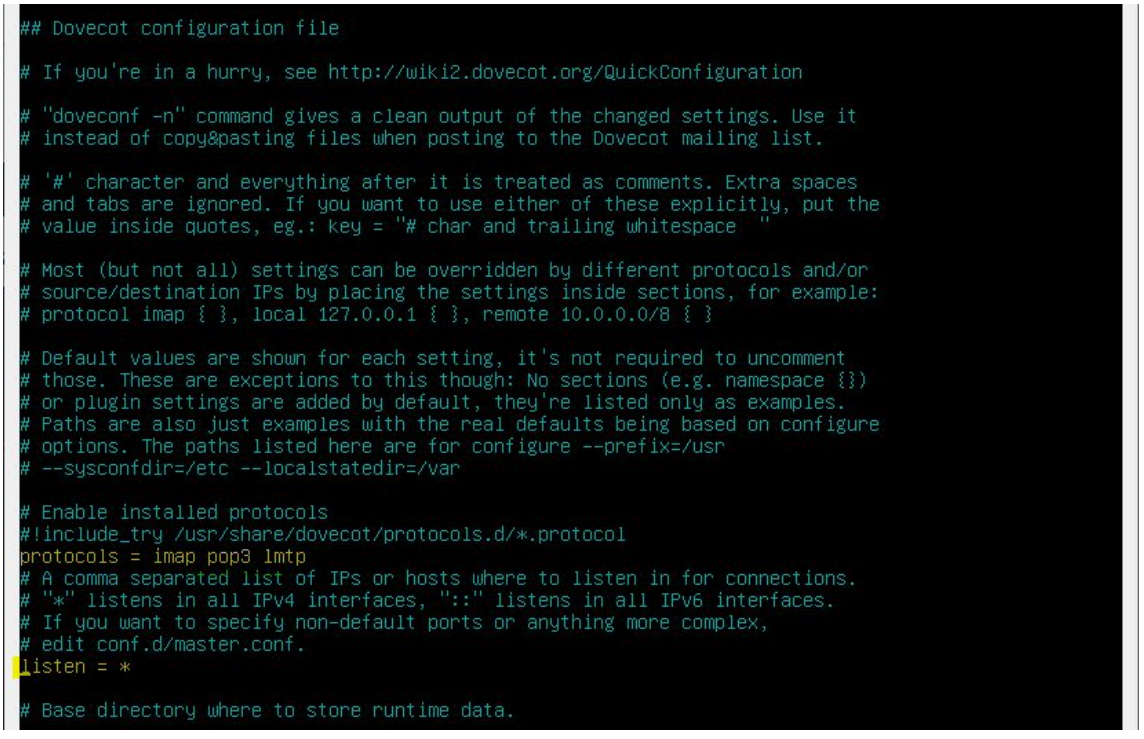


Now we install dovecot

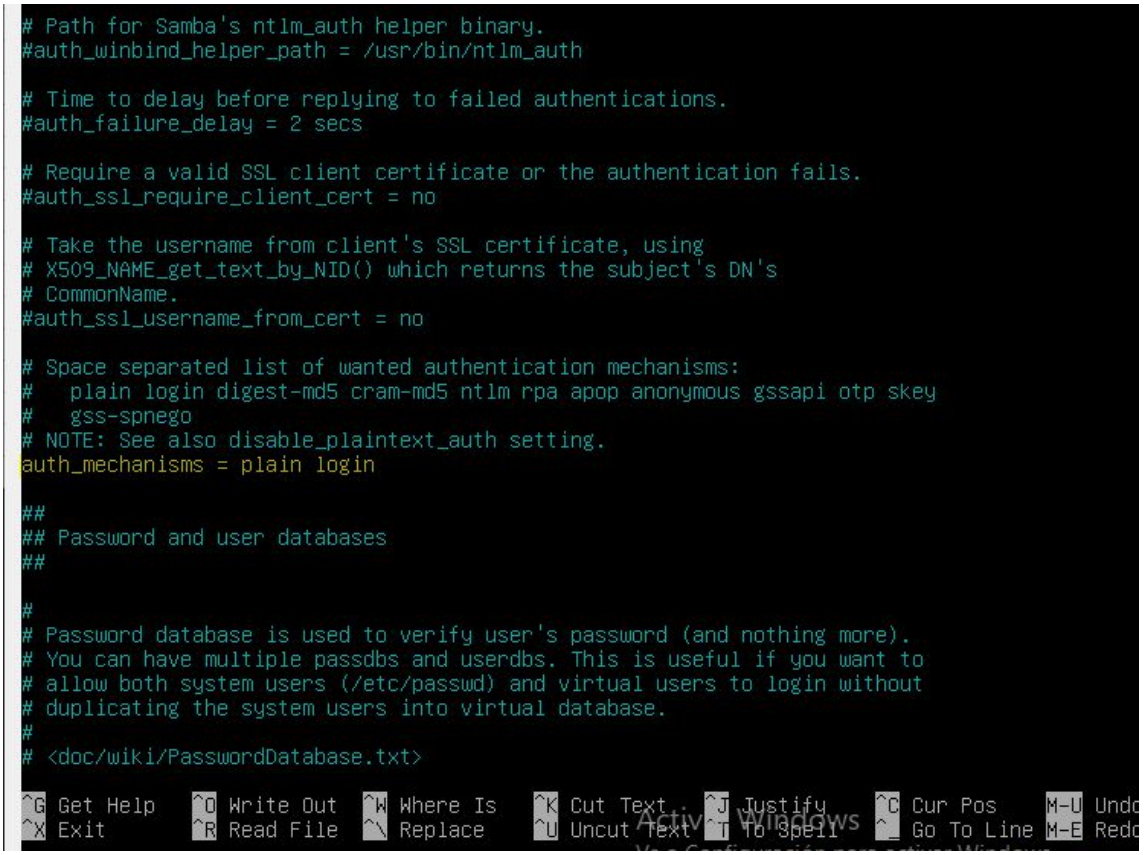
```
apt install dovecot-core dovecot-imapd
```

We need to configure dovecot. We add the following lines.

```
nano /etc/dovecot/dovecot.conf
```




```
nano /etc/dovecot/conf.d/10-auth.conf
```


Path for Samba's ntlm_auth helper binary.
#auth_winbind_helper_path = /usr/bin/ntlm_auth
Time to delay before replying to failed authentications.
#auth_failure_delay = 2 secs
Require a valid SSL client certificate or the authentication fails.
#auth_ssl_require_client_cert = no
Take the username from client's SSL certificate, using
X509_NAME_get_text_by_NID() which returns the subject's DN's
CommonName.
#auth_ssl_username_from_cert = no
# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login
##
Password and user databases
##
#
Password database is used to verify user's password (and nothing more).
You can have multiple passdbs and userdbs. This is useful if you want to
allow both system users (/etc/passwd) and virtual users to login without
duplicating the system users into virtual database.
#
<doc/wiki/PasswordDatabase.txt>
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo

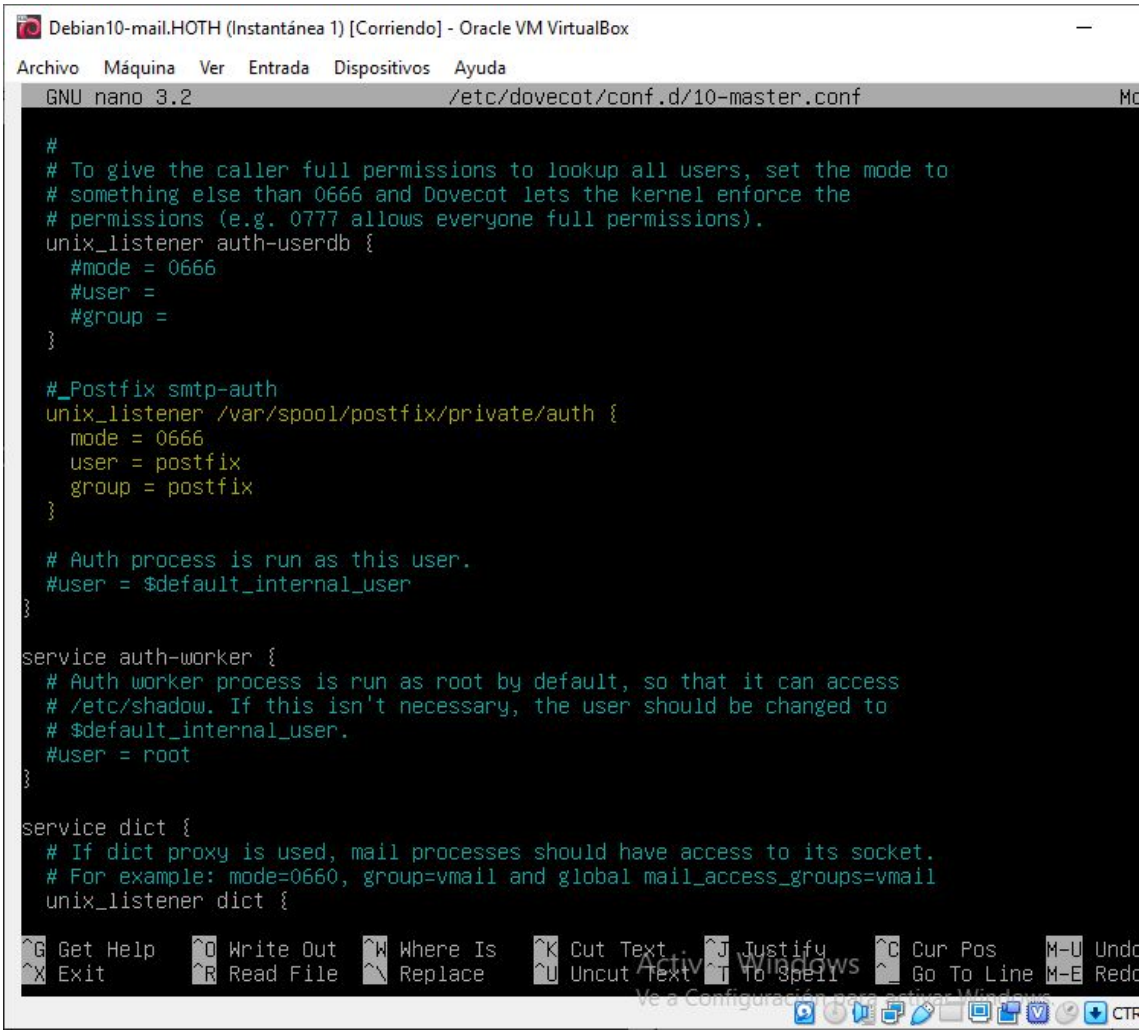
```
##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = no

# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth, PAM and vpopmail require cache_key to be set for caching to be used.
#auth_cache_size = 0
# Time to live for cached data. After TTL expires the cached record is no
# longer used, *except* if the main database lookup returns internal failure.
# We also try to handle password changes automatically: If user's previous
# authentication was successful, but this one wasn't, the cache isn't used.
# For now this works only with plaintext authentication.
#auth_cache_ttl = 1 hour
# TTL for negative hits (user not found, password mismatch).
# 0 disables caching them completely.
#auth_cache_negative_ttl = 1 hour

# Space separated list of realms for SASL authentication mechanisms that need
# them. You can leave it empty if you don't want to support multiple realms.
# Many clients simply use the first one listed here, so keep the default realm
# first.
#auth_realms =

# Default realm/domain to use if none was specified. This is used for both
# SASL realms and appending @domain to username in plaintext logins.
```

```
##
## Mailbox locations and namespaces
##

# Location for users' mailboxes. The default is empty, which means that Dovecot
# tries to find the mailboxes automatically. This won't work if the user
# doesn't yet have any mail, so you should explicitly tell Dovecot the full
# location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
#
#   %u - username
#   %n - user part in user@domain, same as %u if there's no domain
#   %d - domain part in user@domain, empty if there's no domain
#   %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
   _mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = mbox:~/mail:INBOX=/var/mail/%u

# If you need to set multiple mailbox locations or want to change default

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo
```

mail_location = mbox:~/mail:INBOX=/var/mail%u

Here the default mail location for each user will be: **/var/mail/%user%**

nano /etc/dovecot/conf.d/10-master.conf



nano /etc/dovecot/conf.d/10-ssl.conf

This file is for enabling SSL on dovecot

ssl=yes

ssl_cert = </etc/ssl/certs/hoth.pem

ssl_key = </etc/ssl/private/key.pem

Now we will link dovecot with the LDAP.

```
apt install dovecot-ldap
```

Enter the **/etc/dovecot/dovecot-ldap.conf.ext** and edit some parameters.

```
nano /etc/dovecot/dovecot-ldap.conf.ext
```

hosts = ad.hoth.ally

dn = cn=admin,dc=hoth,dc=ally

tls=no

auth_bind=yes

auth_bin_userdn= cn=%u,ou=people,dc=hoth,dc=ally

ldap_version 3

base = ou=people,dc=hoth,dc=ally

scope=subtree

user_attrs=homeDirectory=home,uidNumber=uid,gidNumber=gid

user_filter=(&(objectClass=posixAccount)(uid=%u))

pass_attrs= uid=user,userPassword=password

pass_filter =(&(objectClass=posixAccount)(uid=%u))

Now that we have installed and configured our mail server, its time to make a mail web server that will use this mail server. The web server that we are going to use, will be **SquirrelMail**. This is run into an Apache server with PHP, so for that we will install some dependencies.

```
apt install apache2 php7
```

Now we will install the SquirrelMail zip file.

```
wget https://sourceforge.net/projects/squirrelmail/files/stable/1.4.22/squirrelmail-webmail-1.4.22.zip
```

We unzip it, so it lefts a folder with some files.

```
unzip squirrelmail-webmail-1.4.22.zip
```

We move SquirrelMail folder to the Apache default folder for hosting webpages.

```
mv squirrelmail-webmail-1.4.22 /var/www/html/
```

We give some privileges on the folder to the apache user.

```
chown -R www-data:www-data /var/www/html/squirrelmail-webmail-1.4.22/

chmod 755 -R /var/www/html/squirrelmail-webmail-1.4.22/

mv /var/www/html/squirrelmail-webmail-1.4.22/ /var/www/html/
```

SquirrelMail uses a very known language called *perl*, which is used for configuring the squirrelmail.

```
perl /var/www/html/config/conf.pl
```

Here a minimalist terminal will show up.

2 -> 1. Domain name: hoth.ally

D -> Select *Dovecot*

Now we need to create the user to be logged in. But we are using an LDAP, so once you login from the SquirrelMail, automatically will create the user on the home directory.

7. Instant messaging server

7.1. Introduction

For the local communication with an instant messaging service, we have decided to use inspircd which is compatible with ldap and ssl certificates. This tool is going to be installed in our mail server, the one with 192.168.50.4 IP.

7.2. Installation

We have to install this tool in the server.

```
apt-get install inspircd
```

The configurartion file must be changed to match with the necessary values.

```
nano /etc/inspircd/inspircd.conf
```

#server tag. This tag is where you enter the details of your server. We must #change the name, chat.hoth.ally in our case.

```
        <server name="chat.hoth.ally"
                description="Hoth IRC Server"
                network="hoth.ally"
                id="47T">
```

#admin tag. These settings are the administrative details of your server. Yoda #is going to be the admin in our server.

```
        <admin name="yoda"
               nick="yoda"
               email="yoda@hoth.ally">
```

#bind tag. This tag is used for opening the service. You can define the server #and the clients endpoint to listen for connections on.

```
        ## START SSL MODULE CONFIGURATION
        <bind address="" port="6667" type="clients" ssl="gnutls">


        <module name="m_ssl_gnutls.so">

        <gnutls advertisedports="192.168.50.4:6667"
                cafile="/etc/inspircd/ca.pem"
                certfile="/etc/inspircd/cert.pem"
                ciphers="DEFAULT"
                cipherserverpref="yes"
                compression="no"
                hash="sha1"
                keyfile="/etc/inspircd/key.pem"
                renegotiation="yes"
                showports="yes"
                sslv3="no"
                tlsv1="no">
        ## END SSL MODULE CONFIGURATION
```

#power . This tag defines two passwords.

```
        <power diepass="M@ythe4th" restartpass="M@ythe4th" pause="2">

        <connect allow="*"
                timeout="60"
                flood="20"
```

```
                threshold="1"
                limit="10"
                pingfreq="120"
                sendq="262144"
                recvq="8192"
                localmax="3"
                globalmax="10">

        <connect
                deny="172.20.202.*"
                reason="Forbide">

        <connect
                deny="172.20.14.*"
                reason="Forbide">

        <connect deny="192.168.50.*"
                reason="Forbide">

        <module name="m_ldapauth.so">
        <ldapauth baserdn="ou=people,dc=hoth,dc=ally"
                attribute="uid"
                server="ldap://192.168.50.2"
                killreason="LDAP auth failed"
                searchscope="subtree"
                binddn="cn=admin,dc=hoth,dc=ally"
                bindauth="M@ythe4th"
                verbose="yes"
                userfield="no"
                dbid="ldap-users">

        <class name="Shutdown"
                commands="DIE RESTART REHASH LOADMODULE
UNLOADMODULE RELOAD">
        <class name="ServerLink"
                commands="CONNECT SQUIT RCONNECT MKPASSWD
MKSHA256">
        <class name="BanControl"
                commands="KILL GLINE KLINE ZLINE QLINE ELINE">
        <class name="OperChat"
                commands="WALLOPS GLOBOPS SETIDLE SPYLIST
SPYNAMES">
        <class name="HostCloak"
                commands="SETHOST SETIDENT SETNAME CHGHOST
CHGIDENT">

        <type name="NetAdmin"
```

```
            classes="OperChat BanControl HostCloak Shutdown ServerLink"
            host="netadmin.omega.org.za">
        <type name="GlobalOp"
            classes="OperChat BanControl HostCloak ServerLink"
            host="ircop.omega.org.za">
        <type name="Helper"
            classes="HostCloak"
            host="helper.omega.org.za">

#oper tag. These define the operator logins. In our system the opers are going
#to be the Jedi Masters and Generals.


        <oper name="windu"
            password="M@ythe4th"
            host="*@192.168.50.* *@192.168.5.*"
            type="NetAdmin">

        <oper name="yoda"
            password="M@ythe4th"
            host="*@192.168.50.* *@192.168.5.*"
            type="NetAdmin">

        <oper name="luke"
            password="M@ythe4th"
            host="*@192.168.50.* *@192.168.5.*"
            type="NetAdmin">

        <files motd="/etc/inspircd/inspircd.motd"
              rules="/etc/inspircd/inspircd.rules">

        <channels users="10"
                 opers="60">

#dns tag: Here you have to add the IP of the dns server.

        <dns server="192.168.50.2" timeout="5">

        <pid file="/var/run/inspircd.pid">

        <options prefixquit="Quit: "
                noservices="no"
                qaprefixes="no"
                deprotectself="no"
                deprotectothers="no"
                flatlinks="no"
                hideulines="no"
```

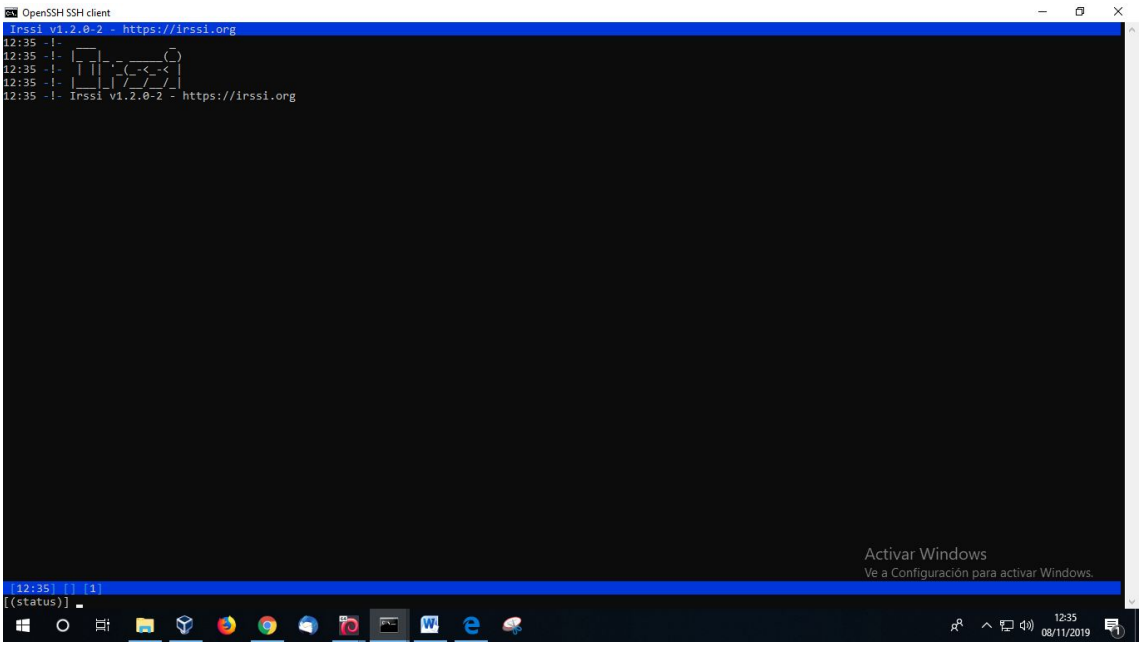
```
        syntaxhints="no"
        cyclehosts="yes"
        ircumsgprefix="no"
        announcets="yes"
        disablehmac="no"
        hostintopic="yes"
        quietbursts="yes"
        pingwarning="15"
        allowhalfop="yes"
        exemptchanops="">

<security hidewhois=""
        userstats="Pu"
        customversion=""
        hidesplits="no"
        hidebans="no"
        operspywhois="no"
        hidemodes="eI"
        maxtargets="20">

<performance nouserdns="no"
          maxwho="128"
          softlimit="1024"
          somaxconn="128"
          netbuffersize="10240">

<whowas groupsize="10"
      maxgroups="100000"
      maxkeep="3d">

<timesync enable="no" master="no">

<badnick nick="ChanServ" reason="Reserved For Services">
<badnick nick="NickServ" reason="Reserved For Services">
<badnick nick="OperServ" reason="Reserved For Services">
<badnick nick="MemoServ" reason="Reserved For Services">
<badnick nick="Vader" reason="Banned User">
<badnick nick="DarthVader" reason="Banned User">
```

Install the irssi application through the repositories for using an IRC client:

```
apt-get install irssi
```

To open it:

```
irssi
```



7.3. LDAP Configuration

To synchronize ldap and inspircd we have to add this module in the inspircd configuration file.
We have to load the ldapauth module and point it to our ldap server,

```
<module name="m_ldapauth.so">
<ldapauth baserdn="ou=people,dc=hoth,dc=ally"
        attribute="uid"
        server="ldap://192.168.50.2"
        killreason="LDAP auth failed"
        searchscope="subtree"
        binddn="cn=admin,dc=hoth,dc=ally"
        bindauth="M@ythe4th"
        verbose="yes"
        userfield="no"
        dbid="ldap-users">
```

7.4. Configuration

As we want to ensure that our data is protected, SSL service is compatible with inspircd and we can use our certificates for secure communication.

We have to attach this module in the inspircd configuration file.

We must include three files: the coruscant.capital.pem file (first we have to convert it from .crt format and it can be done with cp command, only changing the extension), our certificate (cert.pem) and our private key(private.key).

```
<server name="chat.hoth.ally"
        description="Hoth IRC Server"
        network="hoth.ally"
        id="47T">

<admin name="yoda"
       nick="yoda"
       email="yoda@hoth.ally">

<module name="m_ssl_gnutls.so">

<bind address="" port="6667" type="clients" ssl="gnutls">
<gnutls cafile="/etc/ssl/certs/ca.pem"
        certfile="/etc/ssl/certs/hoth.pem"
        keyfile="/etc/ssl/private/hoth.key"
        priority="SECURE192"
        advertisedports="192.168.50.4:6667"
        dhbits="2048"
        hash="sha1"
        showports="yes"
        starttls="yes">


<power diepass="M@ythe4th" restartpass="M@ythe4th" pause="2">

<connect allow="*"
         timeout="60"
         flood="20"
         threshold="1"
         pingfreq="120"
         sendq="262144"
         recvq="8192"
         localmax="3"
         globalmax="10">
```

Then we restart and assure that the config is correct.

```
service inspircd restart

service inspircd status
```

```
rue@mail: /root
root@mail:~# service inspircd statusc
Usage: /etc/init.d/inspircd {start|stop|status|restart|reload|force-reload|cron}
root@mail:~# service inspircd status
● inspircd.service - IRC server
   Loaded: loaded (/lib/systemd/system/inspircd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-11-11 12:35:09 CET; 1min 45s ago
     Docs: man:inspircd(1)
 Main PID: 4884 (inspircd)
    Tasks: 1 (limit: 2348)
   Memory: 3.0M
   CGroup: /system.slice/inspircd.service
           └─4884 /usr/sbin/inspircd --logfile /var/log/inspircd.log --config /etc/inspircd/inspircd.conf --nofork

Nov 11 12:35:09 mail inspircd[4884]: (C) InspIRCd Development Team.
Nov 11 12:35:09 mail inspircd[4884]: Developers:
Nov 11 12:35:09 mail inspircd[4884]:         Brain, FrostyCoolSlug, w00t, Om, Special, peavey
Nov 11 12:35:09 mail inspircd[4884]:         aquanight, psychon, dz, danieldg, jackmcbarn
Nov 11 12:35:09 mail inspircd[4884]:         Attila
Nov 11 12:35:09 mail inspircd[4884]: Others:                      See /INFO Output
Nov 11 12:35:09 mail inspircd[4884]: Loading core commands.....................................................
Nov 11 12:35:09 mail inspircd[4884]: [*] Loading module:        m_ssl_gnutls.so
Nov 11 12:35:09 mail inspircd[4884]: [*] Loading module:        m_ldapauth.so
Nov 11 12:35:09 mail inspircd[4884]: InspIRCd is now running as 'chat.hoth.ally'[47T] with 1024 max open sockets
```

7.5. Rules

Some of the rules we are going to have in our servers:

Yedi Masters and Generals will be able to connect from .ally and .local. Rest of the users only from .local.

```
        connect deny="192.168.50.*"
              reason="Forbide">
```

```
        <oper name="windu"
            password="M@ythe4th"
            host="*@192.168.50.* *@192.168.5.*"
```

```
        type="NetAdmin">

    <oper name="yoda"
        password="M@ythe4th"
        host="*@192.168.50.* *@192.168.5.*"
        type="NetAdmin">

    <oper name="luke"
        password="M@ythe4th"
        host="*@192.168.50.* *@192.168.5.*"
        type="NetAdmin">
```

Connections from 172.20.202.0/24 or 172.20.14.0/24 will not be allowed.

```
    <connect
        deny="172.20.202.*"
        reason="Forbide">

    <connect
        deny="172.20.14.*"
        reason="Forbide">
```

There cannot be more than 10 users connected at the same time and these nicknames will be forbidden: Vader and DarthVader.

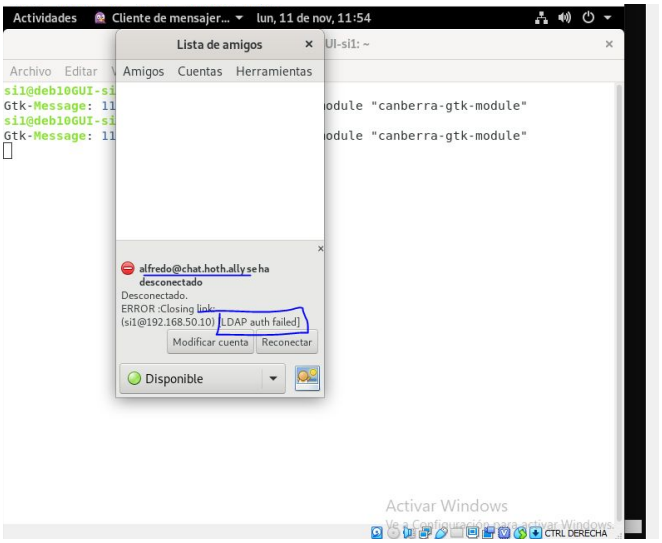
```
    <connect allow="*"
        timeout="60"
        flood="20"
        threshold="1"
        limit="10"
        pingfreq="120"
        sendq="262144"
        recvq="8192"
        localmax="3"
        globalmax="10">
```

```
    <badnick nick="Vader" reason="Banned User">
    <badnick nick="DarthVader" reason="Banned User">
```

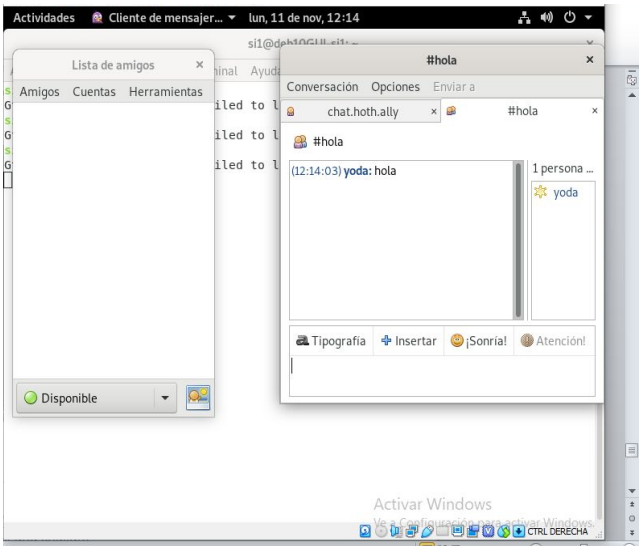
7.6. Checkings (Pidgin IRC)

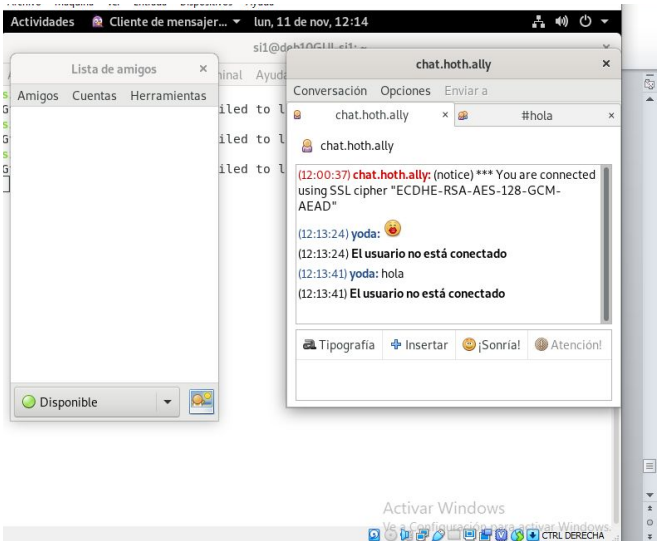
We are going to verify that all this configuration is working installing Pidgin IRC in a client.

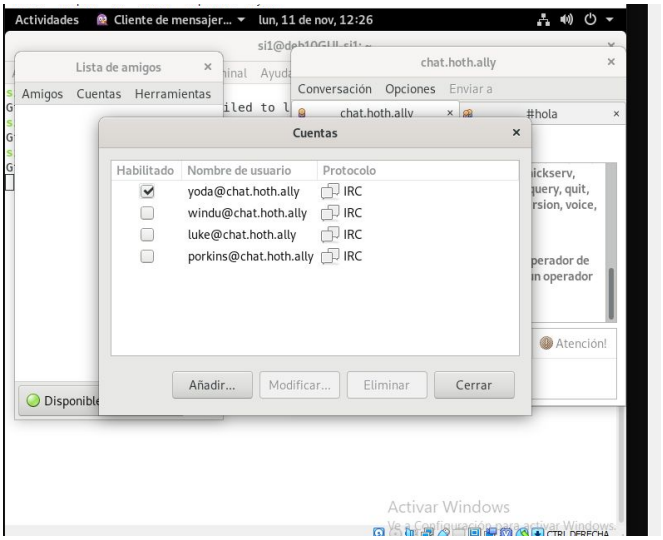
First of all, we are trying to access our chat called “chat.hoth.ally” with a username out of our Active Directory. It must show an error and tell that the LDAP auth failed.



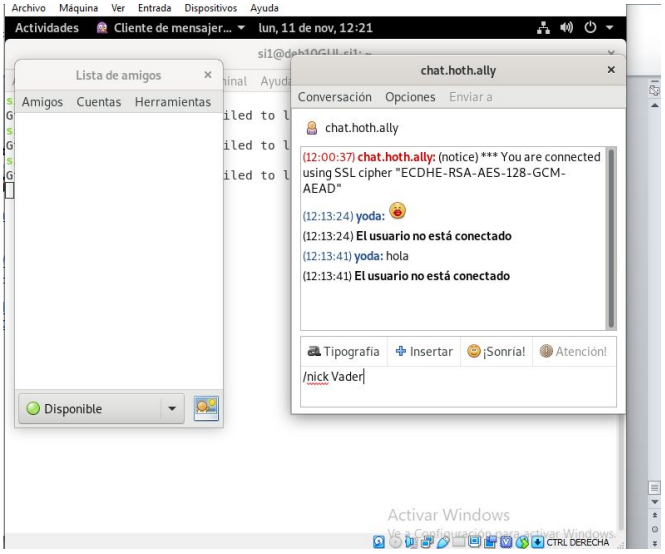
If we try to connect with yoda user, we can join the server and write in any channel we create. As we can see in the second screenshot, the SSL verification works fine.

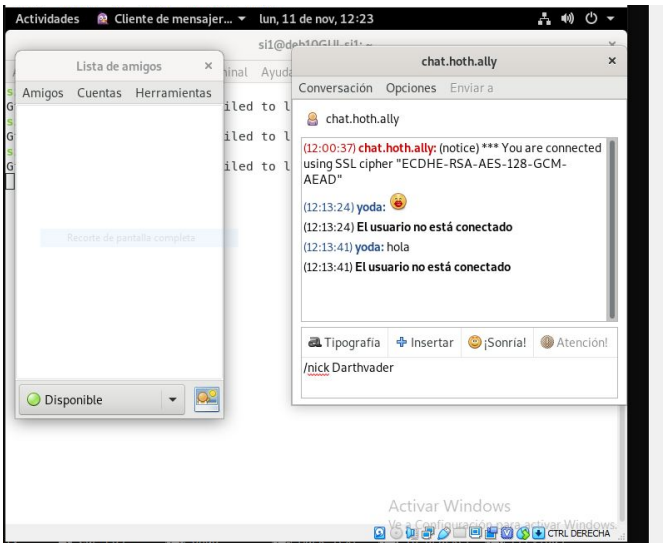


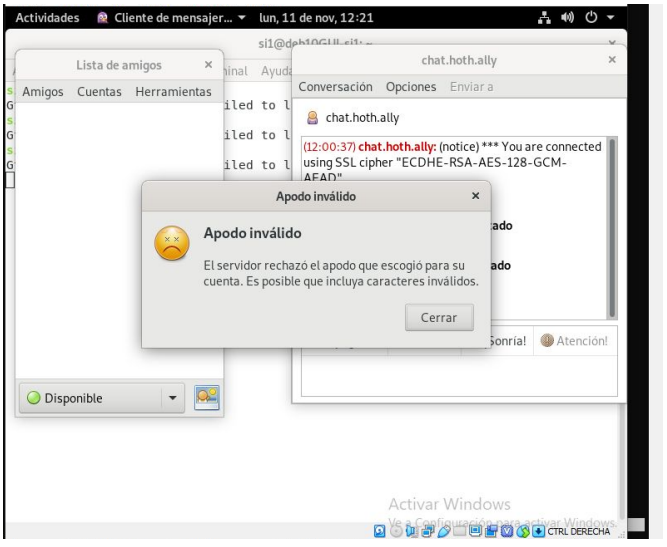




Vader and Darthvader nicks are going to be forbidden.

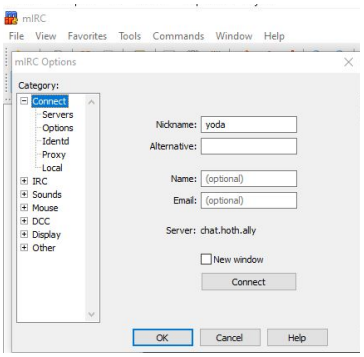

Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades
Cliente de mensajer...
lun, 11 de nov, 12:21
Lista de amigos
Amigos Cuentas Herramientas
Disponible
chat.hoth.ally
Conversación Opciones Enviar a
chat.hoth.ally
(12:00:37) chat.hoth.ally: (notice) *** You are connected using SSL cipher "ECDHE-RSA-AES-128-GCM-AEAD"
(12:13:24) yoda:
(12:13:24) El usuario no está conectado
(12:13:41) yoda: hola
(12:13:41) El usuario no está conectado
Tipografía Insertar ¡Sonría! Atención!
/nick Vader
Activar Windows
CTRL DERECHA


Actividades
Cliente de mensajer...
lun, 11 de nov, 12:23
Lista de amigos
Amigos Cuentas Herramientas
Disponible
chat.hoth.ally
Conversación Opciones Enviar a
chat.hoth.ally
(12:00:37) chat.hoth.ally: (notice) *** You are connected using SSL cipher "ECDHE-RSA-AES-128-GCM-AEAD"
(12:13:24) yoda:
(12:13:24) El usuario no está conectado
(12:13:41) yoda: hola
(12:13:41) El usuario no está conectado
Tipografía Insertar ¡Sonría! Atención!
/nick Darthvader
Activar Windows
CTRL DERECHA

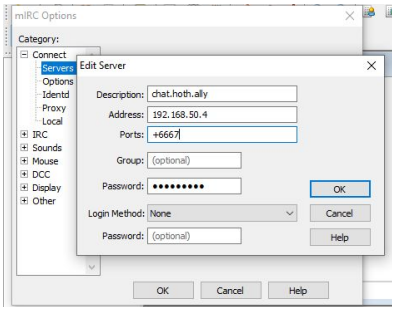

Actividades
Cliente de mensajer...
lun, 11 de nov, 12:21
Lista de amigos
Amigos Cuentas Herramientas
Disponible
chat.hoth.ally
Conversación Opciones Enviar a
chat.hoth.ally
(12:00:37) chat.hoth.ally: (notice) *** You are connected using SSL cipher "ECDHE-RSA-AES-128-GCM-AEAD"
Apodo inválido
Apodo inválido
El servidor rechazó el apodo que escogió para su cuenta. Es posible que incluya caracteres inválidos.
Cerrar
Activar Windows
CTRL DERECHA

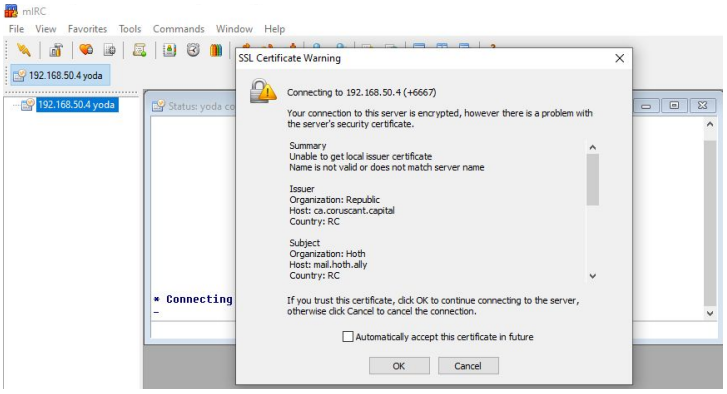
7.7. Checkings(MIRC)

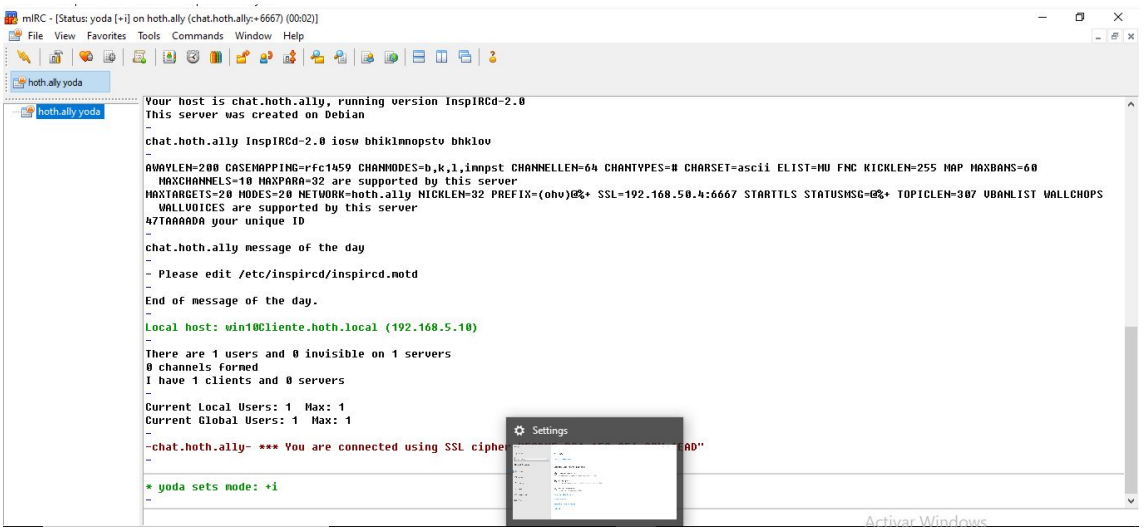
From our W10 client which is in hoth.local domain, we are going to access to the chat server.



We have to créate the server and add here the IP of the server, the password for LDAP authentication and a + before the port so that ssl certificate can do its checking.







8. Webgraphy

OpenLDAP

- https://www.youtube.com/watch?v=2yjhxGNbDjo&t=781s

Printer Management

- https://pimylifeup.com/raspberry-pi-print-server/
- https://www.solvetic.com/tutoriales/article/3349-crear-configurar-servidor-de-impresion-windows-server-2016/

Firewall

- http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf

Digital certificates

- https://www.digitalocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs

Mail

- https://www.tecmint.com/setup-postfix-mail-server-in-ubuntu-debian/
- https://www.tecmint.com/install-postfix-mail-server-with-webmail-in-debian/
- https://www.youtube.com/watch?v=KNLgJm-2F2o
- https://help.ubuntu.com/community/DovecotLDAP

Chat

- https://docs.inspircd.org/2/configuration/
- https://www.digitalocean.com/community/tutorials/how-to-set-up-an-irc-server-on-ubuntu-14-04-with-inspircd-2-0-and-shalture