

## Cosa facciamo

- (1 lezione)
  - Un po' di teoria
  - Active directory
  - LDAP
  - Kerberos
  - Installazione server Linux Lubuntu
  - Vediamo l'infrastruttura virtuale che andremo a creare
  - Vediamo alcuni comandi
  - I servizi
- (2 lezione)
  - Cos'è un DNS?
  - Installiamo un DNS per gestire il dominio example.com
  - Installiamo BIND, il DNS linux
  - Configuriamo il dominio Active Directory example.local in ambiente linux
  - Installiamo SAMBA
  - Vediamo alcuni comandi
  - Creiamo un server SSH centralizzato
- (3 lezione)
  - Installiamo un PC windows
  - Mettiamo il PC nel dominio example.local
  - Amministriamo il dominio linux dal PC windows
  - Vediamo i Ruoli FSMO e come modificano
  - Gestiamo il client con le Policy
  - Installiamo LdapAdmin e facciamo delle query LDAP
- (4 lezione)
  - Crittografia asimmetrica e Certification Authority
  - RADIUS
  - Che cos'è Radius e dove si usa
  - Configuriamo freeradius

## Active Directory

Servizio che permette di centralizzare e gestire informazioni e risorse (utenti, computer, stampanti, ...)

### Active Directory vs Workgroup

Active directory è un servizio di Directory implementato da Microsoft con Windows 2000 Server.

Le risorse che tipicamente vengono memorizzate all'interno di Active Directory sono:

- Account utente
- Gruppi di utenti
- Account computer
- Cartelle condivise
- Stampanti
- Policy di sicurezza
- Schema

Active Directory è implementata tramite un insieme di servizi, ecco i principali:

- LDAP: è il protocollo per accedere al database in cui vengono memorizzate le informazioni (Lightweight\_Directory\_Access\_Protocol)
- Kerberos : è un protocollo di rete che permette l'autenticazione tramite crittografia. Realizza inoltre il Single Sign On (SSO) dell'utente. L'utente si autentica una sola volta all'accesso ad un computer di Active Directory e poi le sue credenziali vengono usate per l'accesso ai servizi senza la necessità di ri-autenticarsi.
- DNS: per la risoluzione dei nomi all'interno dell'Active Directory
- NTP: sincronizzazione del time

## La struttura logica di Active Directory

### Dominio

Un dominio è un gruppo di oggetti (computer, stampanti, gruppi, etc..) che condivide un unico database di servizio di directory. Un dominio Active Directory corrisponde al dominio DNS, ovvero può condividere la stessa struttura gerarchica dei nomi: è proprio sul DNS che Active Directory basa tutto il suo funzionamento, infatti per ogni nuovo dominio Active Directory dev'esserci almeno un server DNS.

amministrazione.example.local; ricerca.example.local; produzione.example.local

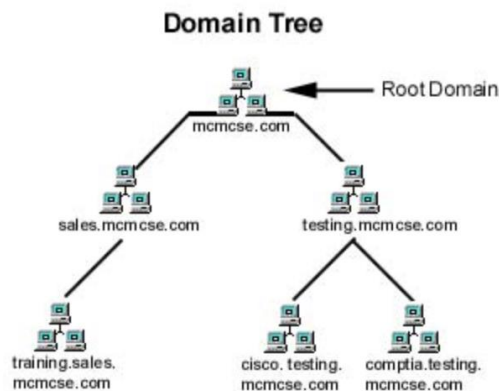
### Albero

Un albero è un insieme di domini nella foresta che condividono uno spazio dei nomi contiguo. Vi è una relazione di fiducia transitiva tra domini padre e figlio: quando si aggiunge un nuovo dominio ad un albero, il nuovo dominio viene chiamato dominio figlio. Per esempio: amministrazione.example.local e ricerca.example.local sono alberi con il nome DNS example.local in comune.

amministrazione = dominio figlio

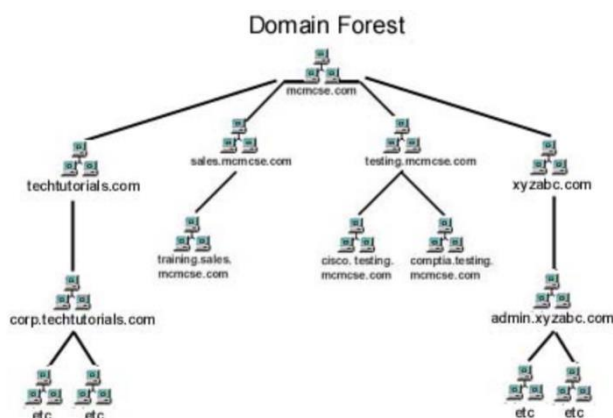
example.local = Root Domain o Top Level Domain

La combinazione dei nomi del dominio figlio insieme al dominio padre formano il nome DNS. Il top level domain è chiamato Root Domain.



## Foresta

Una foresta rappresenta uno più domini che condividono una configurazione, uno schema o un catalogo globale comuni. In pratica è un insieme di più alberi che non condividono lo stesso spazio dei nomi.



## Unità organizzativa (OU, organizational unit)

È un contenitore di oggetti utilizzato per organizzare gli oggetti stessi dentro un dominio. L'unità organizzativa può essere usata per organizzare oggetti come utenti, gruppi, computer, stampanti, e altre unità organizzative.

## Global Catalog (GC)

Contiene le informazioni relative agli oggetti presenti in Active directory, informazioni costituite da una replica completa di tutti gli oggetti di directory nel dominio host e una parziale di tutti gli oggetti di directory in tutti i domini della struttura. Il global catalog permette all'utente di autenticarsi ed accedere alla rete e al dominio. Poiché contiene informazioni sugli oggetti in tutto l'insieme di strutture, consente la ricerca di oggetti fornendo informazioni sulle ubicazioni in cui è possibile trovare l'oggetto.

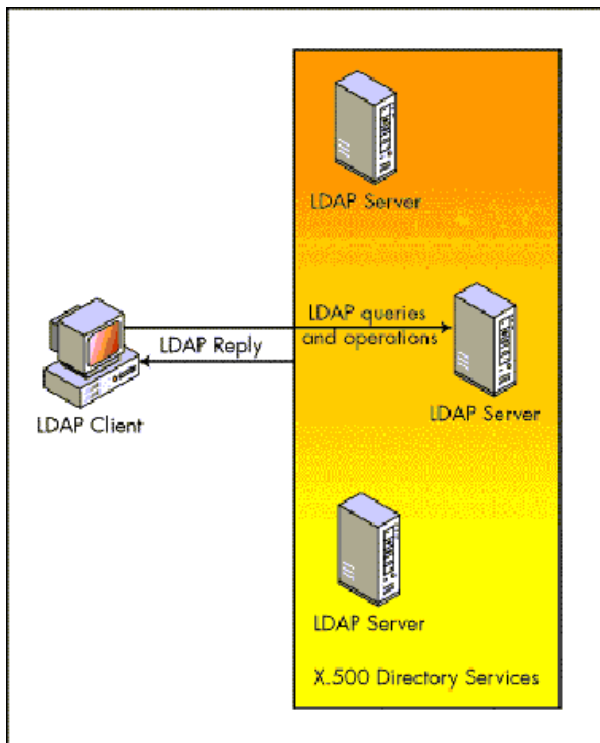
In ogni dominio è necessario avere almeno un GC e per impostazione predefinita al primo DC del dominio è assegnato automaticamente tale ruolo. E' possibile configurare un DC come GC e aggiungere altri GC ad un dominio per accelerare i tempi di risposta per le richieste di accesso e di ricerca.

## Siti

I siti sono un raggruppamento logico di PC o server in base al loro indirizzo IP e alla sottorete di appartenenza.

## LDAP

Protocollo per l'interrogazione e la modifica dei servizi di directory. Lo standard di riferimento è l'X500 ma è stato sviluppato uno standard più leggero chiamato LDAP (Light Directory Access Protocol)



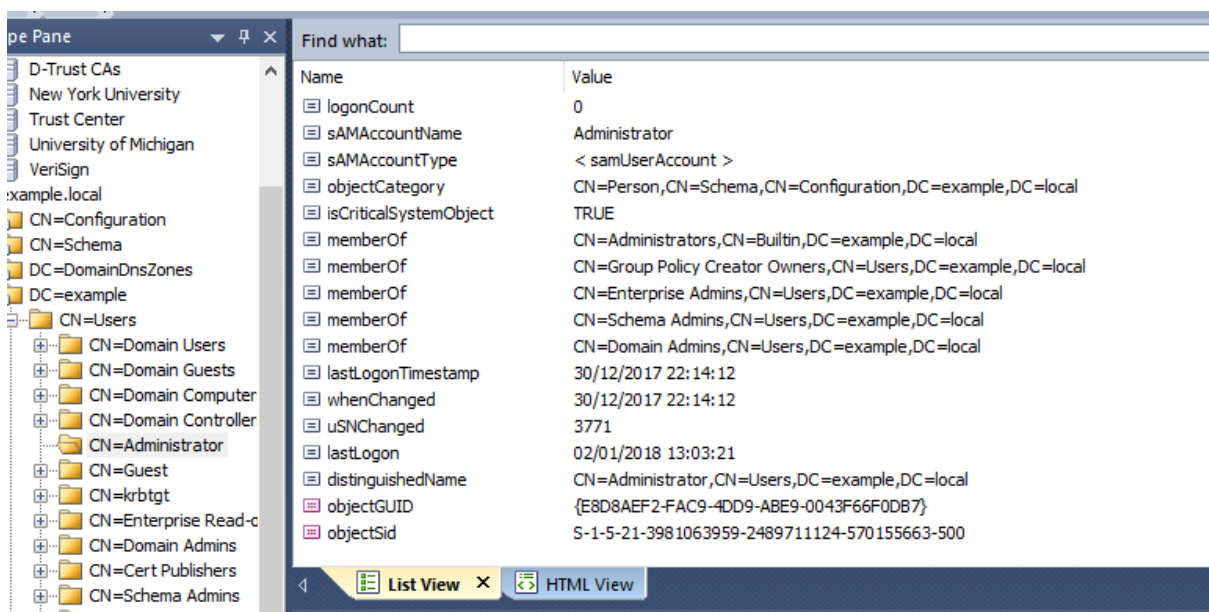
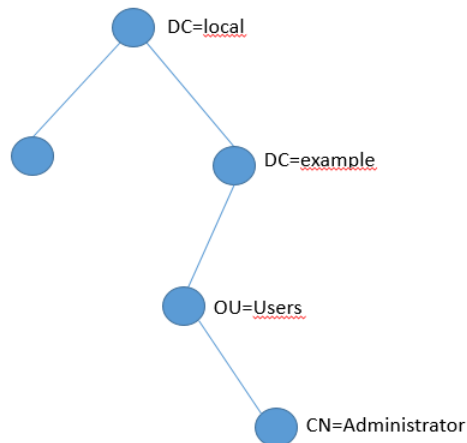
LDAP è il protocollo di accesso alla directory.

Il client può richiedere le seguenti operazioni:

- Bind — esegue l'autenticazione
- Search — esegue una ricerca
- Compare — esegue un test di confronto tra un valore e il valore assegnato ad un attributo
- Add - aggiunge un nuovo oggetto
- Delete - cancella un oggetto
- Modify - modifica gli attributi di un oggetto
- Modify Distinguished Name (DN) — sposta o rinomina un oggetto
- Abandon — annulla una richiesta inviata in precedenza
- Extended Operation — richiesta di operazioni estese (definite in altre RFC)
- Unbind — indica al server di chiudere la connessione (non è esattamente l'inverso della Bind)
- StartTLS — estensione per utilizzare Transport Layer Security (TLS) per eseguire la Bind

## Directory LDAP (informazioni organizzate ad Albero)

Directory organizzata in Entry.



Un entry è indicata con il suo distinguished name

*distinguished name (DN): "cn= Administrator,CN=Users,dc=example,dc=local"*

Un distinguished name o **DN** è una sequenza di distinguished names relative (RDN) collegati dalla virgola.

Un RDN è un attributo con un valore associato. Gli attributi possono essere i seguenti:

|               |                               |
|---------------|-------------------------------|
| <i>String</i> | <i>Attribute type</i>         |
| <i>DC</i>     | <i>domainComponent</i>        |
| <i>CN</i>     | <i>commonName</i>             |
| <i>OU</i>     | <i>organizationalUnitName</i> |
| <i>O</i>      | <i>organizationName</i>       |
| <i>STREET</i> | <i>streetAddress</i>          |
| <i>L</i>      | <i>localityName</i>           |
| <i>ST</i>     | <i>stateOrProvinceName</i>    |
| <i>C</i>      | <i>countryName</i>            |
| <i>UID</i>    | <i>Userid</i>                 |

Un entry contiene un insieme di informazioni.

Esempio di attributi di Active Directory

<http://www.kouti.com/tables/userattributes.htm>

Ogni oggetto ha un objectSID che è costituito da 2 parti

- Prefisso del dominio
- Numero incrementale (Relative Identifier) RID

Il Global Catalog ha le seguenti caratteristiche (molte letture, scritture dagli amministratori di sistema)

- ottimizzate in lettura
- Informazioni poco aggiornate
- comunicazione client/server (porte 389 e 636 crittografia LDAP v3)
- Replica delle directory
- Struttura gerarchica <> database relazionale
- Schema

## OpenLdap

Implementazione Open dell'LDAP (Lightweight Directory Access Protocol)

<https://help.ubuntu.com/lts/serverguide/kerberos-ldap.html>

## Kerberos

Kerberos è un protocollo di rete per l'autenticazione tramite crittografia modello client-server

Si basa sulla crittografia simmetrica in cui sia il client che il fornitore di servizio possono verificare l'identità dell'altro tramite una terza parte affidabile (il domain controller)

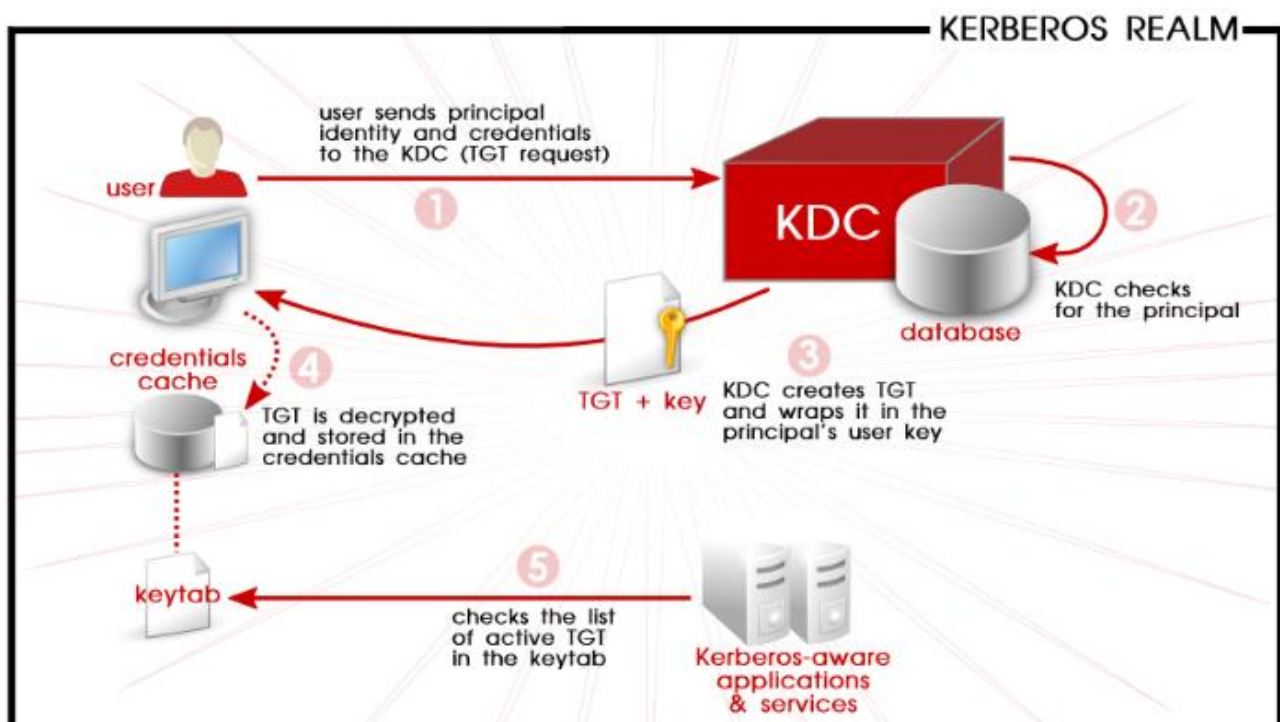
Kerberos si basa sul protocollo di Needham-Schroeder. Utilizza una terza parte affidabile per centralizzare la distribuzione delle chiavi detta Key Distribution Center (KDC), che consiste di due parti separate logicamente: l'Authentication Server (AS) e il Ticket Granting Server (TGS). Kerberos funziona utilizzando dei "biglietti" (detti ticket) che servono per provare l'identità degli utenti.

L'AS mantiene un database delle chiavi segrete; ogni entità sulla rete — che sia un client o un server — condivide la chiave segreta solo con l'AS. La conoscenza di questa chiave serve per provare l'identità di un'entità. Per comunicazioni tra due entità, Kerberos genera una chiave di sessione, che può essere utilizzata dai due terminali per comunicare.

Funzionamento

- **AS\_REQ** è la richiesta iniziale di autenticazione dell'utente (fatta con il kinit tanto per intenderci). Tale messaggio è diretto alla componente del KDC nota come Authentication Server (AS);

- **AS\_REP** è la risposta dell'Authentication Server alla richiesta precedente. Sostanzialmente contiene il TGT (criptato con la chiave segreta del TGS) e la chiave di sessione (criptata con la chiave segreta dell'utente richiedente);
- **TGS\_REQ** è la richiesta da parte del client rivolta al Ticket Granting Server (TGS) per un ticket di servizio. Dentro questo pacchetto viaggia il TGT ottenuto dal messaggio precedente e un autenticatore generato dal client e criptato con la session key;
- **TGS\_REP** è la risposta del Ticket Granting Server alla richiesta precedente. Ci si trova dentro il service ticket richiesto (criptato con la chiave segreta del servizio) e una chiave di sessione di servizio generata dal TGS e criptata con la precedente chiave di sessione generata dall'AS;
- **AP\_REQ** è la richiesta che il client manda ad un server applicativo per accedere ad un servizio. Le componenti sono il ticket di servizio ottenuto dal TGS con la risposta precedente e un autenticatore generato sempre dal client, ma questa volta criptato con la chiave di sessione del servizio (generata dal TGS);
- **AP\_REP** è la risposta che il server applicativo dà al client per provare di essere veramente il server che il client si aspetta. Questo pacchetto non è sempre richiesto. Il client lo richiede al server solo quando è necessaria la mutua autenticazione.



## Cos'è il realm in Kerberos?

Con il termine realm si indica un dominio amministrativo di autenticazione. Si intende cioè fissare i confini entro cui un server di autenticazione è autoritario nell'autenticare un utente, un host o un servizio.

Il nome di un realm è case sensitive, cioè fa differenza tra maiuscole e minuscole; tuttavia, per consuetudine, i realm sono sempre in maiuscolo.

## Kerberos e NTLM

Microsoft ha adottato Kerberos come protocollo di autenticazione preferito per Windows 2000 e per i domini Active Directory. Kerberos è usato solitamente quando un server appartiene ad un dominio Windows oppure se viene stabilito un trust con un dominio (come ad esempio accade nell'autenticazione tra Linux e Windows Active Directory).

NTLM (NT LAN Manager) è una suite di protocolli di sicurezza Microsoft che forniscono autenticazione, integrità e confidenzialità agli utenti

NTLM è utilizzato nelle seguenti situazioni:

- Il client si sta autenticando ad un server utilizzando un indirizzo IP
- Il client si sta autenticando ad un server che appartiene ad una foresta Active Directory differente che ha un legacy trust NTLM invece di un trust inter-foresta
- Il client si sta autenticando ad un server che non appartiene ad un dominio
- Non esiste un dominio Active Directory (ovvero quando esiste un workgroup oppure una rete peer-to-peer)

NTLM utilizza uno o entrambi i valori di password hashed, che sono entrambi memorizzati nel server (o nel domain controller) e che sono equivalenti alla password. Questo significa che se si riesce ad ottenere un hash password dal server, è possibile autenticarsi senza conoscere la password vera.

## Utilizzi

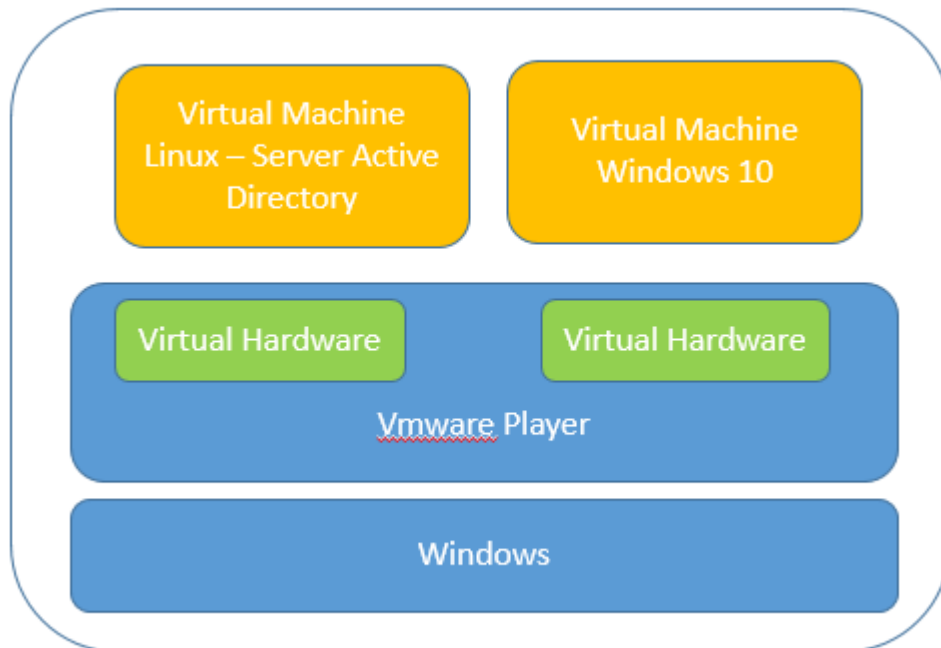
I seguenti software sono in grado di usare Kerberos per l'autenticazione:

- OpenSSH (con Kerberos 5 o successivo)
- NFS (a partire dalla versione NFSv4)
- PAM (con il modulo pam\_krb5)
- SOCKS (a partire da SOCKS5)

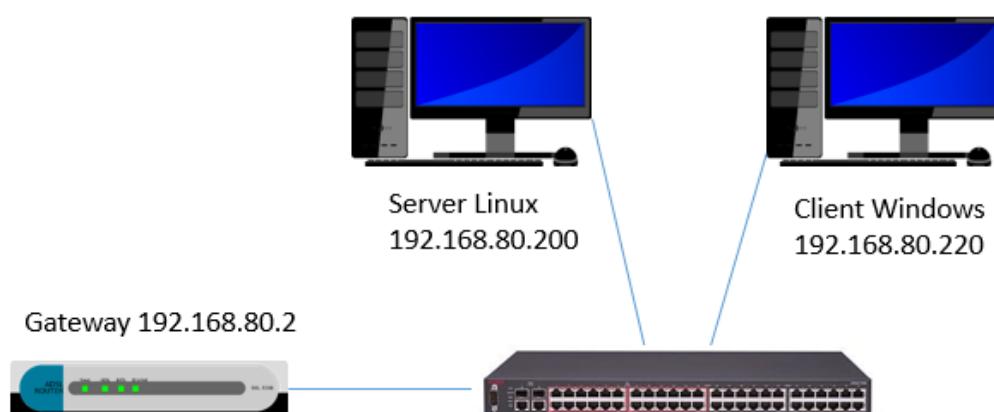


Cosa dobbiamo installare

## Le macchine virtuali

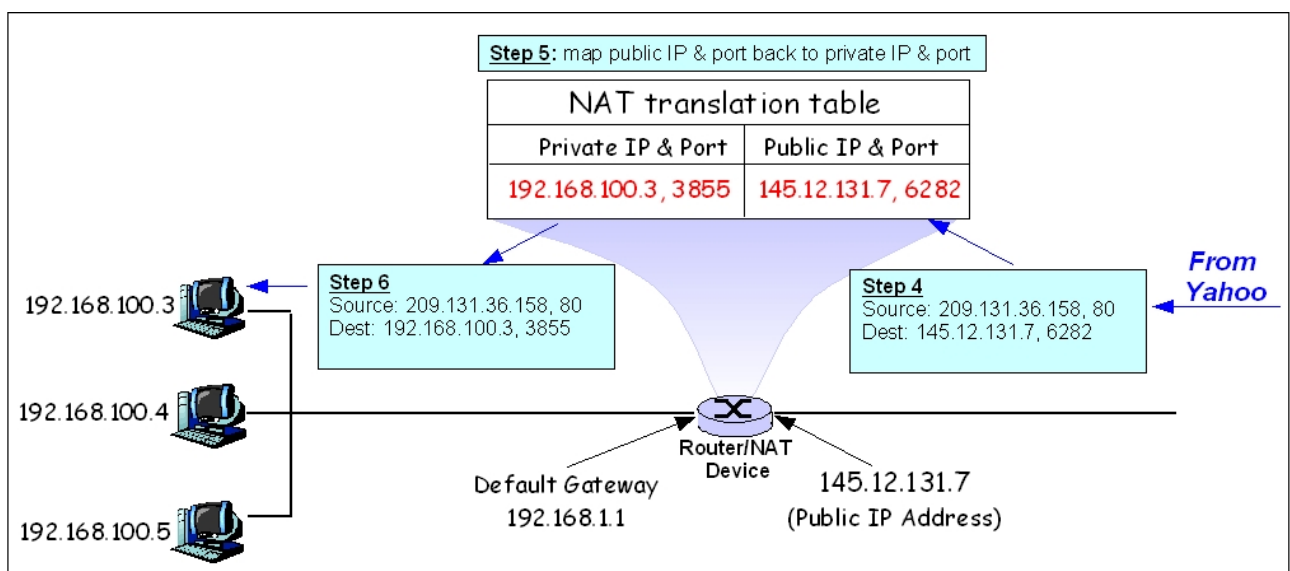
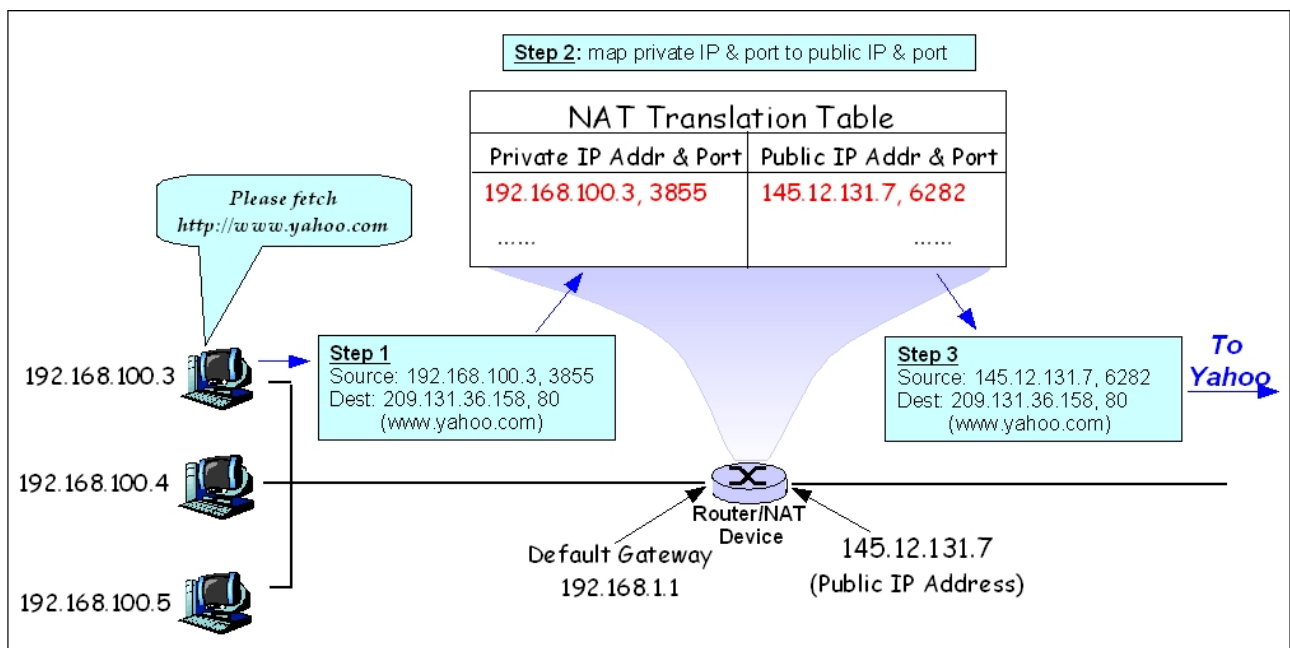


L'infrastruttura di rete che andremo a realizzare.



## NAT (Network Address Translation)

E' un meccanismo che permette di far collegare piu' computer ad una rete. I computer hanno IP privato ed escono con un solo indirizzo IP pubblico.



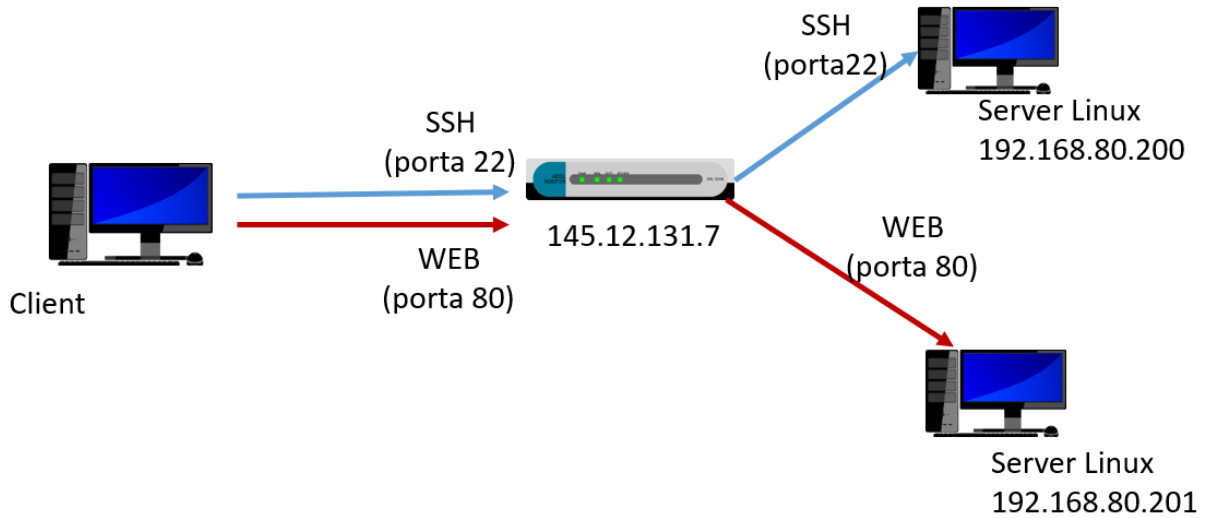
## MASQUERADING vs SNAT

Nel masquerading si definisce l'interfaccia in cui sono collegati i PC interni alla rete

Nel SNAT posso definire sia un pool di IP che le porte, L'SNAT ha senso quando il Router ha piu' indirizzi Pubblici.

## DNAT

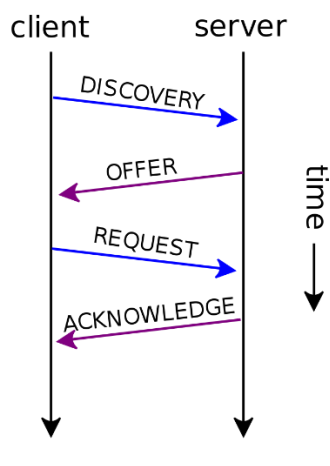
Il DNAT server per esporre dei servizi interni verso l'esterno.



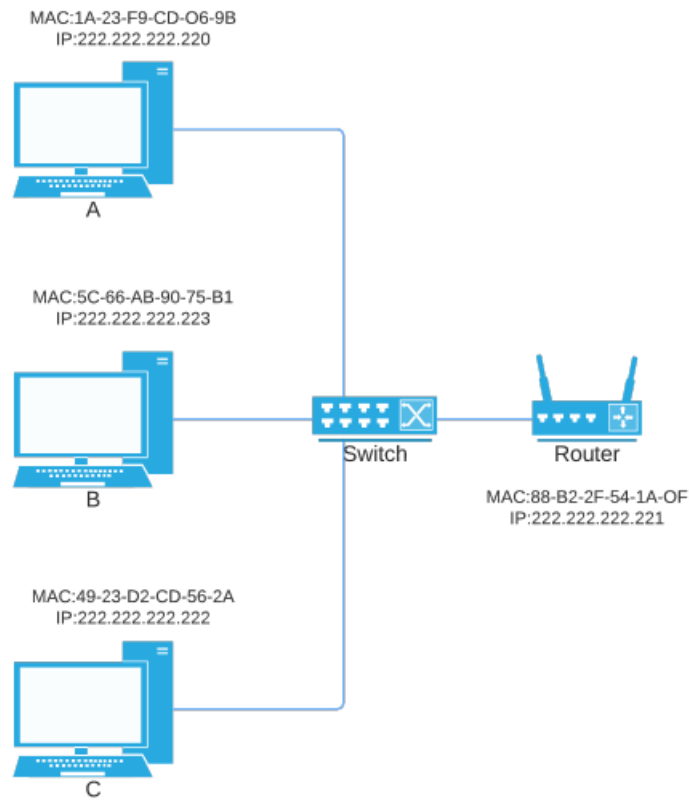
## Dynamic Host Configuration Protocol (DHCP)

(protocollo di configurazione IP dinamica) è un protocollo di rete di livello applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso a una rete IP.

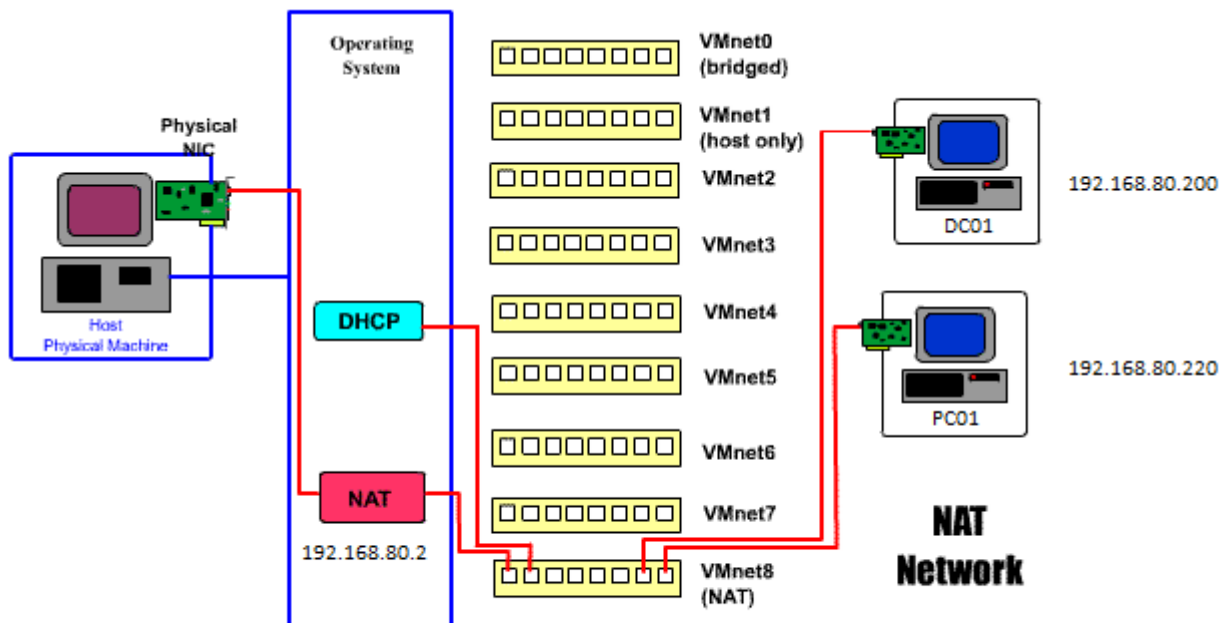
- Il client invia un pacchetto chiamato DHCPDISCOVER in broadcast, con indirizzo IP sorgente messo convenzionalmente a 0.0.0.0, e destinazione 255.255.255.255 (indirizzo di broadcast).
- Il server manda un pacchetto al Client con DCHPOffer, cioè l'IP proposto.
- Il client invia un pacchetto di DHCPREQUEST (o DHCPACCEPT) in broadcast
- Il server manda un pacchetto DHCPACK in broadcast all'indirizzo di livello datalink del client



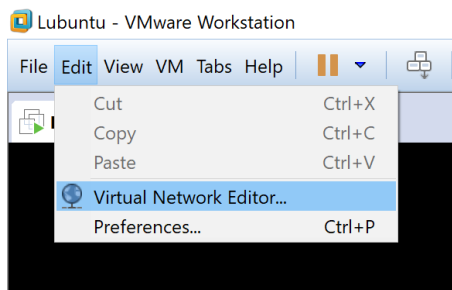
# ARP (Address Resolution Protocol)



## Vmware Configurazione NAT



Per realizzare tale infrastruttura dobbiamo modificare la configurazione della rete di VMware Workstation



Indichiamo a VMware Workstation che la rete natata deve avere IP 192.168.153.x

Virtual Network Editor

| Name   | Type      | External Connection | Host Connection | DHCP    | Subnet Address |
|--------|-----------|---------------------|-----------------|---------|----------------|
| VMnet0 | Bridged   | Auto-bridging       | -               | -       | -              |
| VMnet1 | Host-only | -                   | Connected       | Enabled | 192.168.46.0   |
| VMnet8 | NAT       | NAT                 | Connected       | Enabled | 192.168.80.0   |

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
 Bridged to: Automatic Automatic Settings...

☒ NAT (shared host's IP address with VMs) NAT Settings...

☐ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network  
 Host virtual adapter name: VMware Network Adapter VMnet8

☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 192 . 168 . 80 . 0 Subnet mask: 255 . 255 . 255 . 0

Restore Defaults OK Cancel Apply Help

Andiamo a cambiare l'indirizzo Ip del Gateway

NAT Settings

Network: vmnet8  
 Subnet IP: 192.168.80.0  
 Subnet mask: 255.255.255.0  
 Gateway IP: 192 . 168 . 80 . 2

Port Forwarding

| Host Port | Type | Virtual Machine IP Address | Description |
|-----------|------|----------------------------|-------------|
| 1812      | UDP  | 192.168.80.200:1812        | Radius      |

Add... Remove Properties

Advanced

☒ Allow active FTP  
☒ Allow any Organizationally Unique Identifier

UDP timeout (in seconds): 30

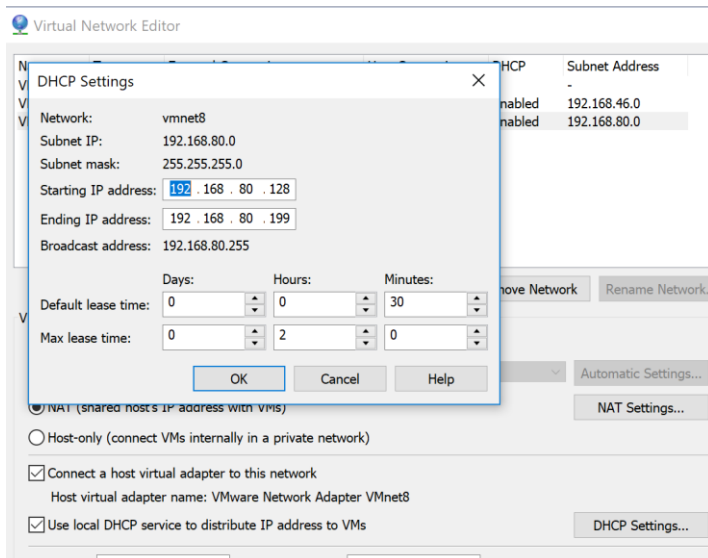
Config port: 0

☐ Enable IPv6  
 IPv6 prefix: fd15:4ba5:5a2b:1008::/64

DNS Settings... NetBIOS Settings...

OK Cancel Help

Configuriamo anche gli IP che devono essere rilasciati dal DHCP.



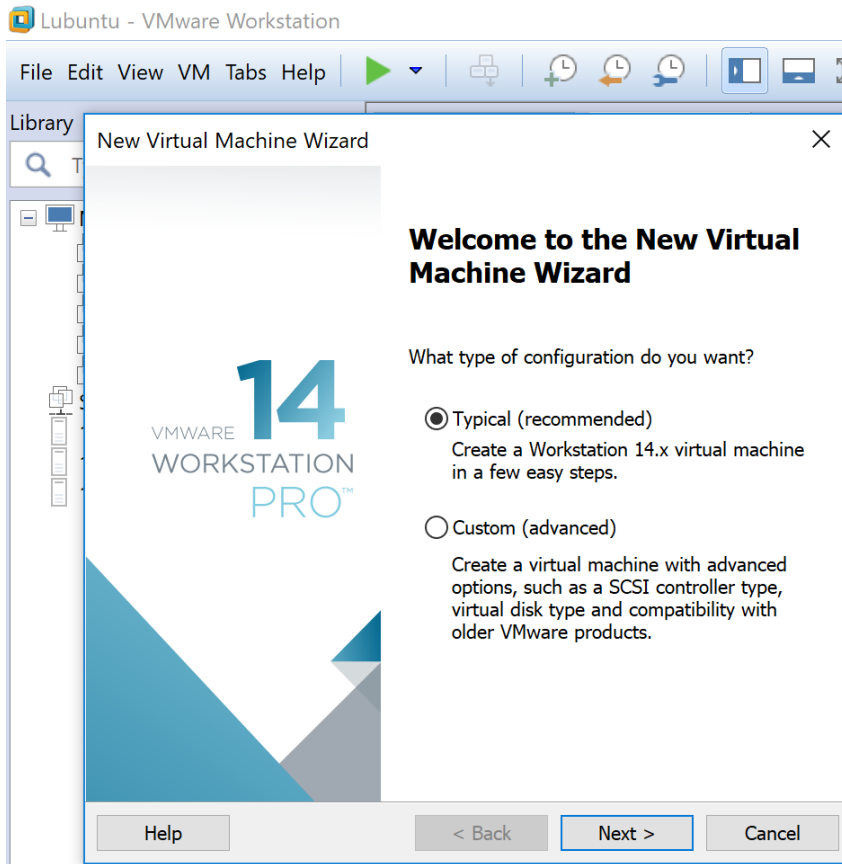
## **Quanta memoria assegnare alla singole macchina virtuale?**

4 GByte per la macchina Linux



## Installazione di Ubuntu 4GbRAM 2core

Creiamo una nuova macchina virtuale



Indichiamo il percorso dove si trova il file iso dell'installazione “\\isi-labso\SysInt\ISO\lubuntu-22.04.4-desktop-amd64.iso”

New Virtual Machine Wizard

**Guest Operating System Installation**  
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:  
No drives available

☒ Installer disc image file (iso):  
Select the installer disc image to continue.

☐ I will install the operating system later.  
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

Indichiamo il sistema operativo che stiamo installando

New Virtual Machine Wizard

**Select a Guest Operating System**  
Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows  
☒ Linux  
☐ Novell NetWare  
☐ Solaris  
☐ VMware ESX  
☐ Other

Version  
Ubuntu

Help < Back Next > Cancel

Indichiamo il nome della Macchina Virtuale (LDC01) e il percorso in cui mettere i file “\\isi-labso\SysInt\<nome gruppo>”

New Virtual Machine Wizard

×

**Name the Virtual Machine**  
What name would you like to use for this virtual machine?

Virtual machine name:

Location:  
  

Browse...

The default location can be changed at Edit > Preferences.

< Back

Next >

Cancel

Definiamo la grandezza del disco (20GB)

New Virtual Machine Wizard

×

**Specify Disk Capacity**  
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for Ubuntu: 20 GB

☐ Store virtual disk as a single file

☒ Split virtual disk into multiple files

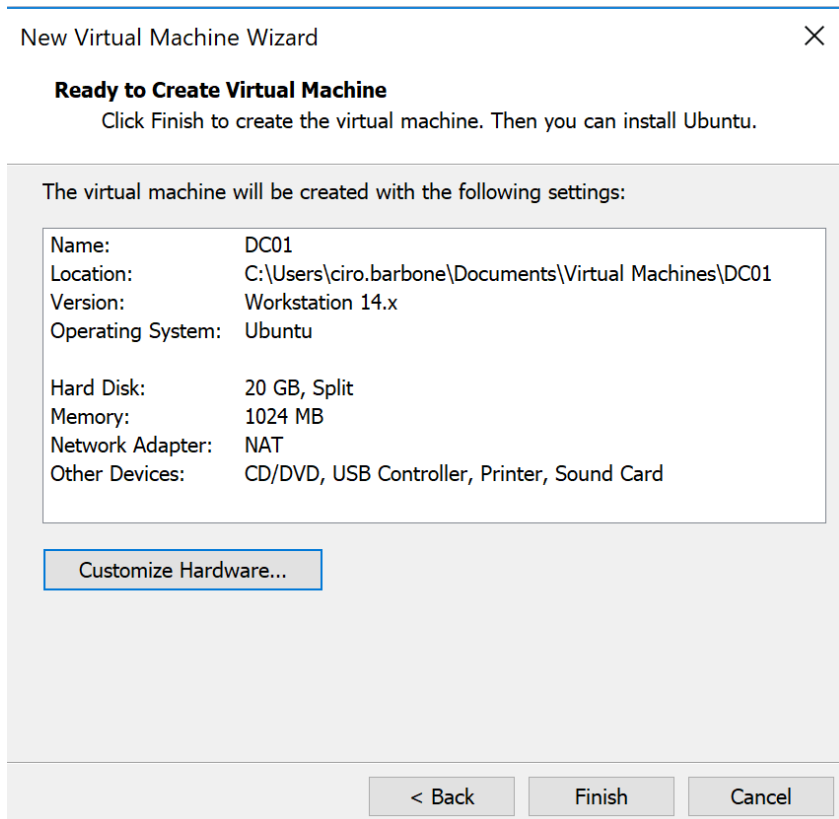
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help

< Back

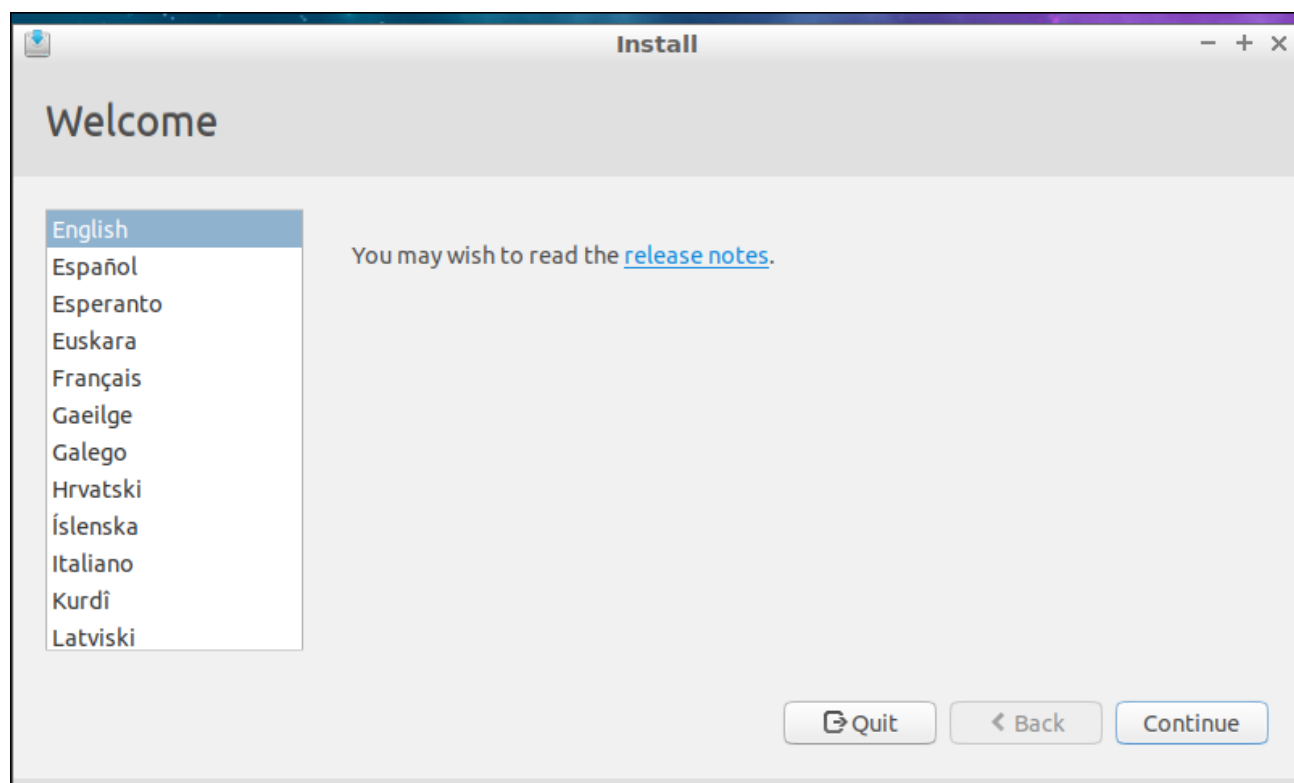
Next >

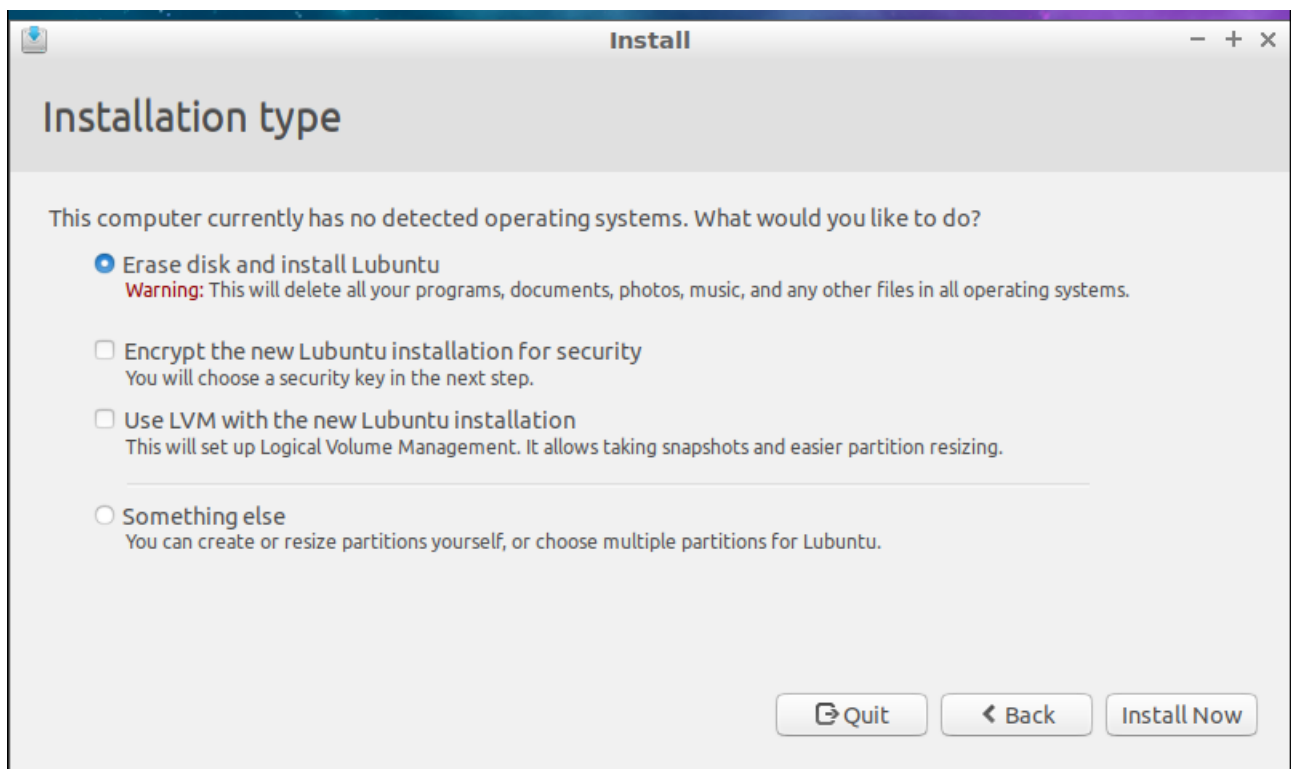
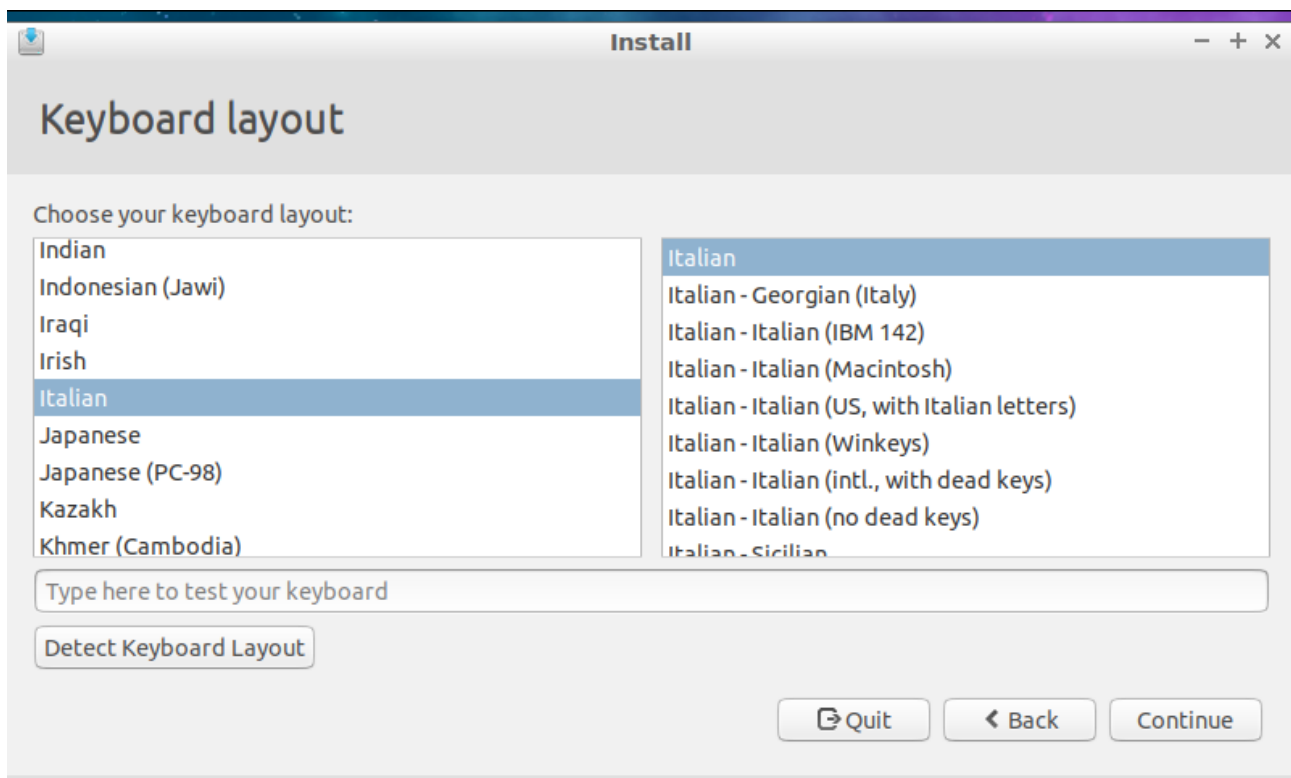
Cancel

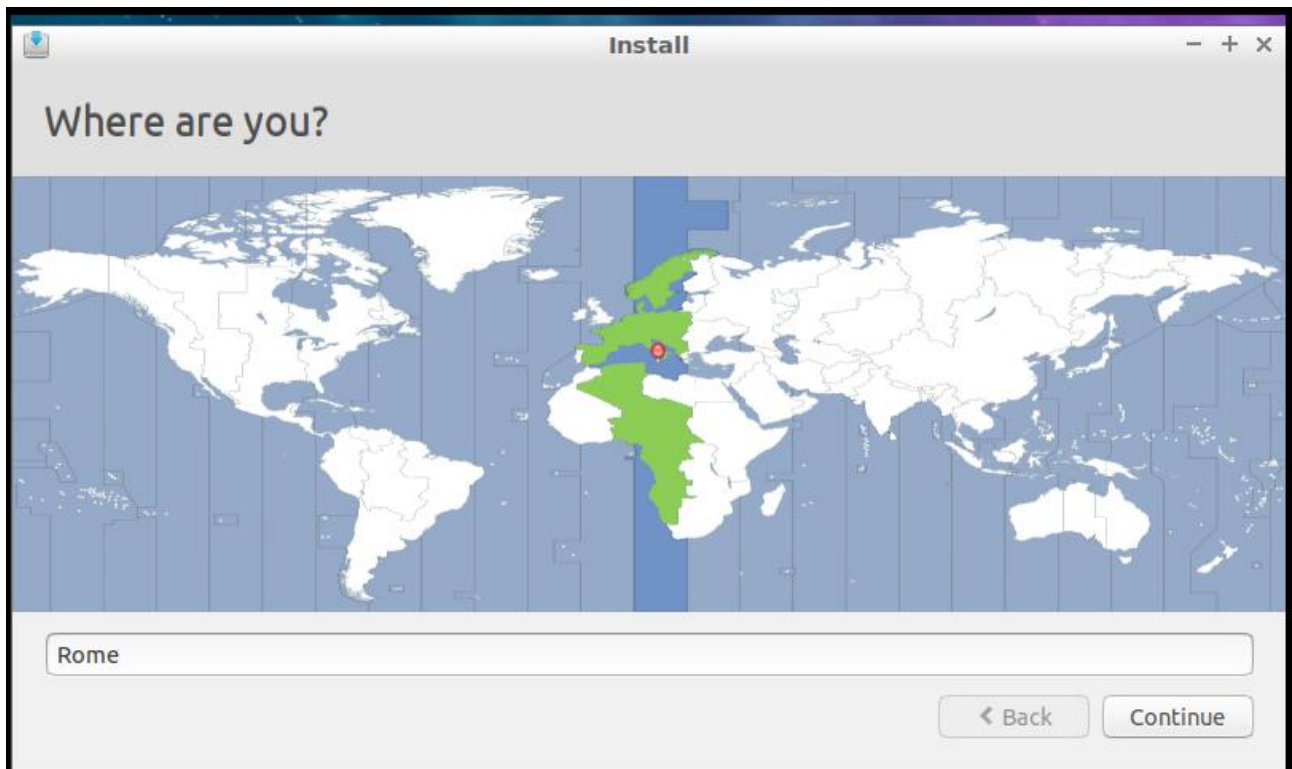
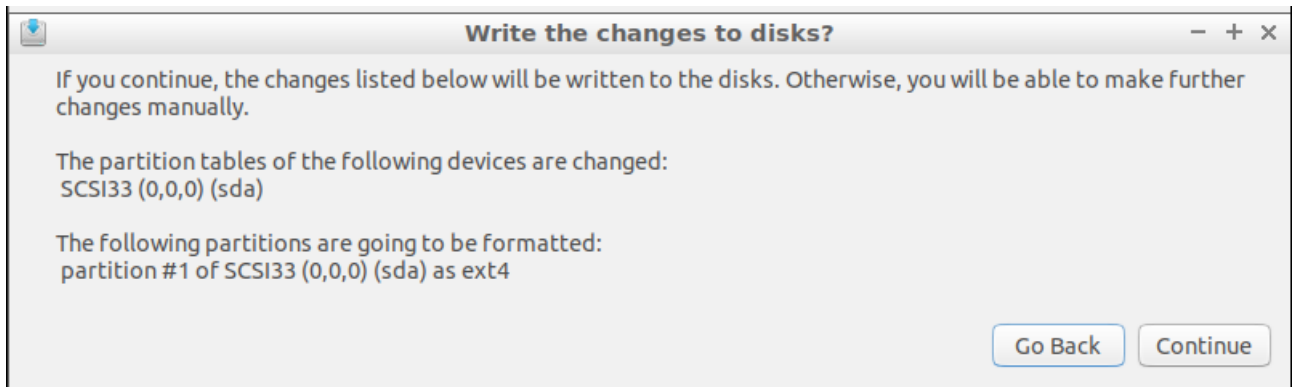


A questo punto possiamo avviare la macchina virtuale

La versione 22.04 parte come live CD. Nel desktop è presente l'icona per l'installazione.





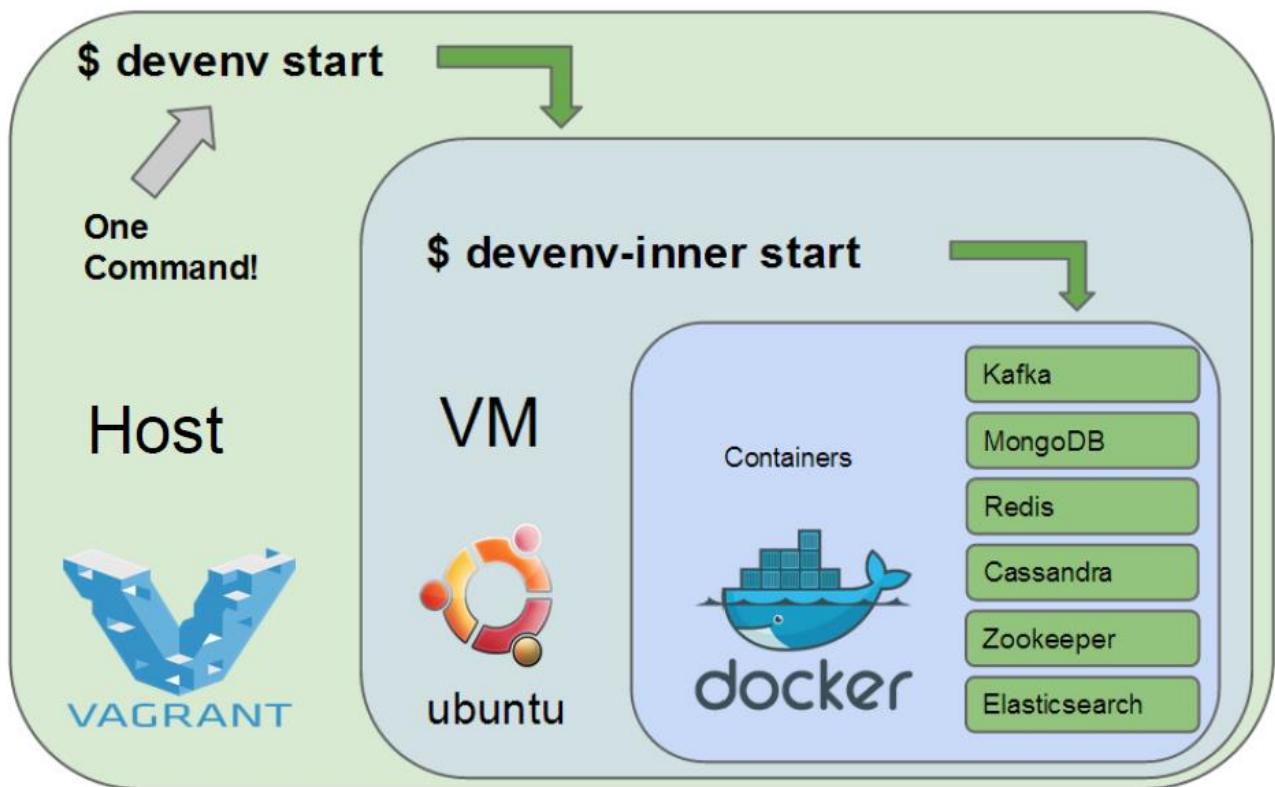


Utente: administrator

Password: Admin1234!

Nome computer: LDC01

## Vagrant e Docker



**Docker**

**Vagrant**

| Virtualization      | Linux container   | Virtual machine             |
|---------------------|-------------------|-----------------------------|
| Resource isolation  | Weak              | Strong                      |
| OS                  | Linux             | Linux, Windows, MacOS, .... |
| Starting time       | Seconds           | Minutes                     |
| Size                | 100M+             | 1G+                         |
| CM integration      | No                | Yes                         |
| Building image time | Short (mins)      | Long (10+ mins)             |
| Hosted number       | >50               | <10                         |
| Deployment tools    | CoreOS, Mesos,... | Terraform                   |
| Public images       | Yes (Docker Hub)  | Yes (Vagrant Cloud)         |



```

Vagrant.configure("2") do |config|
  config.vm.provider "virtualbox" do |v|
    v.memory = 4096
    v.cpus = 2
  end

  #config.vm.network "private_network", ip: "10.11.12.200"
  #config.vm.network "public_network", ip: "10.0.2.200"
  config.vm.hostname = "LDC01"

  config.vm.box = "chenhan/lubuntu-desktop-18.04"
  config.vm.synced_folder "shared/", "C:/Vagrant/shared"
  # config.vm.provision "shell", path: "setup.sh"
  config.vm.network :forwarded_port, guest: 22, host: 11022
  #config.vm.network :forwarded_port, guest: 443, host: 11443

  config.vm.provision "shell", inline: <<-SHELL

    apt update
    #apt -y upgrade
    #Copio tutti i file di configurazione nella cartella /home/vagrant
    cp -r /vagrant/shared/* /home/vagrant

  SHELL

end

```

## Ansible

Ansible è un sistema opensource che permette l'automazione e la gestione dell'infrastruttura IT.

L'obiettivo è il raggiungimento di uno stato B partendo da uno stato A.

E' di tipo agentless e si basa principalmente su ssh.

Utilizza

Inventory (file /etc/ansible)

```

[cez-aule]
cez-aula2-1.campusfc.unibo.it ansible_host=137.204.73.221
cez-aula2-10.campusfc.unibo.it ansible_host=137.204.73.230
cez-aula2-11.campusfc.unibo.it ansible_host=137.204.73.231
cez-aula2-12.campusfc.unibo.it ansible_host=137.204.73.232
cez-aula2-13.campusfc.unibo.it ansible_host=137.204.73.233
cez-aula2-14.campusfc.unibo.it ansible_host=137.204.73.201
cez-aula2-15.campusfc.unibo.it ansible_host=137.204.73.202
cez-aula2-16.campusfc.unibo.it ansible_host=137.204.73.203
cez-aula2-17.campusfc.unibo.it ansible_host=137.204.73.204
cez-aula2-3.campusfc.unibo.it ansible_host=137.204.73.223
cez-aula2-4.campusfc.unibo.it ansible_host=137.204.73.224
cez-aula2-5.campusfc.unibo.it ansible_host=137.204.73.225
cez-aula2-6.campusfc.unibo.it ansible_host=137.204.73.226
cez-aula2-7.campusfc.unibo.it ansible_host=137.204.73.227
cez-aula2-8.campusfc.unibo.it ansible_host=137.204.73.228

```

Playbook (Sono file yaml che definiscono cosa fare)

```
---
- name: Reboot the machine with all defaults
  hosts: psicelab2
  ansible.windows.win_reboot:
    reboot_timeout: 120
~
~
~
~
```

```
---
- name: Ansible script to automate a MAAS server install
  hosts: localhost
  connection: local
  vars_files:
    - "/ansible/maas/maas_install_ansible_var.yml"
  gather_facts: false

  tasks:
    - name: Waiting for system to become reachable
      wait_for_connection:

    - name: Gathering facts
      setup:

    - name: Updating system (apt update & upgrade)
      become: yes
      apt:
        # name: '*'
        # state: latest
        update_cache: yes
        when: ansible_distribution == 'Debian' or ansible_distribution == 'Ubuntu'

    - name: install snapd support
      become: yes
      apt:
        name: pip

    - name: install pip support
      become: yes
      apt:
        name: snapd

    - name: Installing Ansible prerequisites (Python)
      become: yes
      apt:
        name: python3, python3-pip
```

Prima di iniziare ad installare Active Directory lavoriamo un po' con Linux:

- Un po' di comandi
- Systemd: i servizi in ambiente linux
- Gli utenti locali e sudo
- Il server linux e il Network-manager
- Eliminazione del servizio Network-manager
- Configuriamo un indirizzo IP Statico
- Come ci colleghiamo al server? Installiamo un servizio sshd
- Cosa sono i vmware tool? Colleghiamoci in ssh ed installiamoli
- Un ottimo editor di testo. Installiamo vim
- E se sul server ci serve l'ambiente grafico? Installiamo xrdp e usiamo remote desktop

## Un po' di comandi

```
sudo su
```

Apt

```
apt update
```

```
apt install net-tools
```

Indirizzo IP

```
ifconfig
```

Routing

```
route
```

Porte di rete utilizzare

```
netstat
```

```
netstat -tulpn
```

Controllare i log

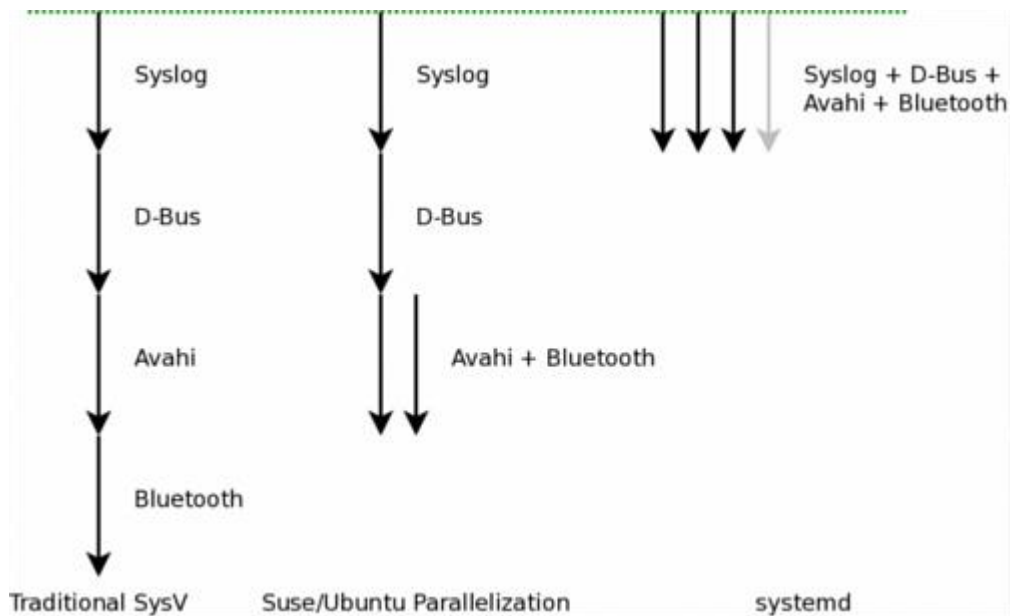
```
tail
```

Ricerche nei file

```
grep <stringa da cercare> file
```

## Systemd: i servizi in ambiente Linux

Responsabile della corretta procedura di avvio di tutti gli altri processi principali. Fino a qualche tempo fa era compito di init, adesso è systemd.



Il comando principale è

```
systemctl
# Avvio

systemctl start nomeservizio

# Arresto

systemctl stop nomeservizio

# Riavvio

systemctl restart nomeservizio
```

Oppure

```
# Avvio

service nomeservizio start

# Arresto

service nomeservizio stop

# Riavvio

service nomeservizio restart
```

service permette di gestire un sottoinsieme di comandi rispetto a systemctl.

Per vedere lo stato di un servizio possiamo usare

```
systemctl status nomeservizio
```

Per vedere lo stato di tutti i servizi possiamo usare

```
service --status-all
```

Per abilitare/disabilitare il servizio al boot

```
# Abilitare l'avvio del servizio in fase di boot
```

```
systemctl enable nomeservizio
```

```
# Disabilitare l'avvio del servizio in fase di boot
```

```
systemctl disable nomeservizio
```

Per vedere i log dei servizi in esecuzione

```
journalctl
```

oppure

```
journalctl /usr/bin/my_executable
```

oppure

```
journalctl _PID=123
```

## **I file di configurazione**

Il file di configurazione dei servizi sono presenti

```
/etc/systemd/system
```

Di seguito possiamo vedere com'è fatta la configurazione del servizio sshd

```
[Unit]
```

```
Description=OpenBSD Secure Shell server
```

```
After=network.target auditd.service
```

```
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run
```

```
[Service]
```

```
EnvironmentFile=/etc/default/ssh
```

```
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
```

```
ExecReload=/bin/kill -HUP $MAINPID
```

```
KillMode=process
```

```
Restart=on-failure
```

```
RestartPreventExitStatus=255
```

```
Type=notify
```

```
[Install]
```

```
WantedBy=multi-user.target
```

```
Alias=sshd.service
```

Maggiori informazioni possono essere trovate qui:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/system\\_administrators\\_guide/sect-managing\\_services\\_with\\_systemd-unit\\_files](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-managing_services_with_systemd-unit_files)

## Come ci colleghiamo al server? Installiamo un servizio sshd

```
sudo apt install ssh -y
```

Per verificare se un servizio è in esecuzione

```
service sshd status
```

## Cosa sono i vmware tool? Colleghiamoci in ssh ed installiamoli

I vmware tool sono degli strumenti che permettono alla macchina virtuale di vedere i dispositivi virtualizzati (interfacce di rete, ...) e permettono al virtualizzatore di eseguire operazioni sulla macchina virtuale (spegnimento della macchina virtuale)

```
# Per desktop:
```

```
apt install open-vm-tools open-vm-tools-desktop
```

```
# Per server
```

```
apt install open-vm-tools
```

## Gli utenti locali

Per aggiungere un utente locale

```
adduser test
```

oppure

```
adduser -p passwordtest test
```

per cambiare la password

```
passwd test
```

aggiungiamo un gruppo

```
groupadd testgroup
```

aggiungiamo l'utente test al gruppo testgroup

```
usermod -G testgroup test
```

## Il comando sudo

Entriamo con l'utente test.

Proviamo ad eseguire con l'utente test il comando

```
sudo apt update
```

Non funziona perché non può eseguire il sudo

Il sudo permette di eseguire un comando con privilegi superiori. Tutto ciò che viene eseguito viene registrato nei log.

Per abilitare l'utente ad effettuare il sudo aggiungere l'utente al gruppo sudo

```
gpasswd -a test sudo
```

Rieseguiamo il comando

```
sudo apt update
```

Eliminiamo l'utente test dal gruppo sudo

```
gpasswd -d test sudo
```

Con Sudo l'utente può eseguire tutti i comandi.

Il comando Sudo permette di controllare i comandi che un utente esegue. Ogni comando è registrato nel file di log /var/log/auth.log

Si può limitare le operazioni che un utente può fare con sudo andando a modificare la configurazione di sudo con il comando

```
visudo
```

- root ALL=(ALL:ALL) ALL  
Il primo campo è l'utente. Il Gruppo si indica con la @group
- root ALL=(ALL:ALL) ALL  
Il primo "ALL" indica che questa regola viene applicata a tutti gli host.
- root ALL=(ALL:ALL) ALL  
Indica l'utente con cui viene eseguito il comando.
- root ALL=(ALL:ALL) ALL  
Indica il gruppo con cui viene eseguito il comando.
- root ALL=(ALL:ALL) ALL  
Indica i comandi che possono essere eseguiti.

Provare a mettere dentro visudo

```
%testgroup ALL=(www-data:www-data) /usr/bin/vim
```

E poi eseguire il comando da un utente che appartiene al gruppo testgroup

```
sudo -u www-data vim /tmp/test
```

I comandi useradd groupadd hanno modificato i file

/etc/passwd

/etc/shadow

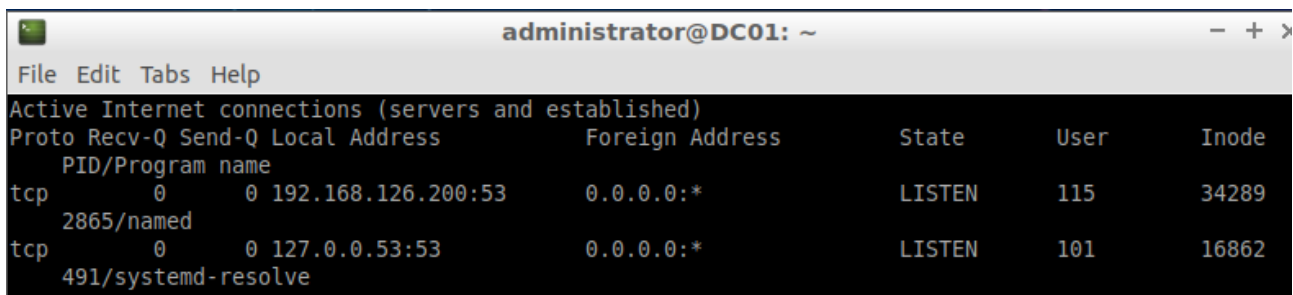
/etc/group

## Rimuoviamo Network-manager e systemd-resolve

Il network manager è un servizio che gestisce le interfacce di rete in ambiente grafico, mentre systemd-resolve ha la funzione di cache dns. Se l'obiettivo è installare un dominio Active Directory la risoluzione DNS dev'essere effettuata direttamente da BIND9.

Verifichiamo le porte usate.

```
sudo netstat -nape |more
```

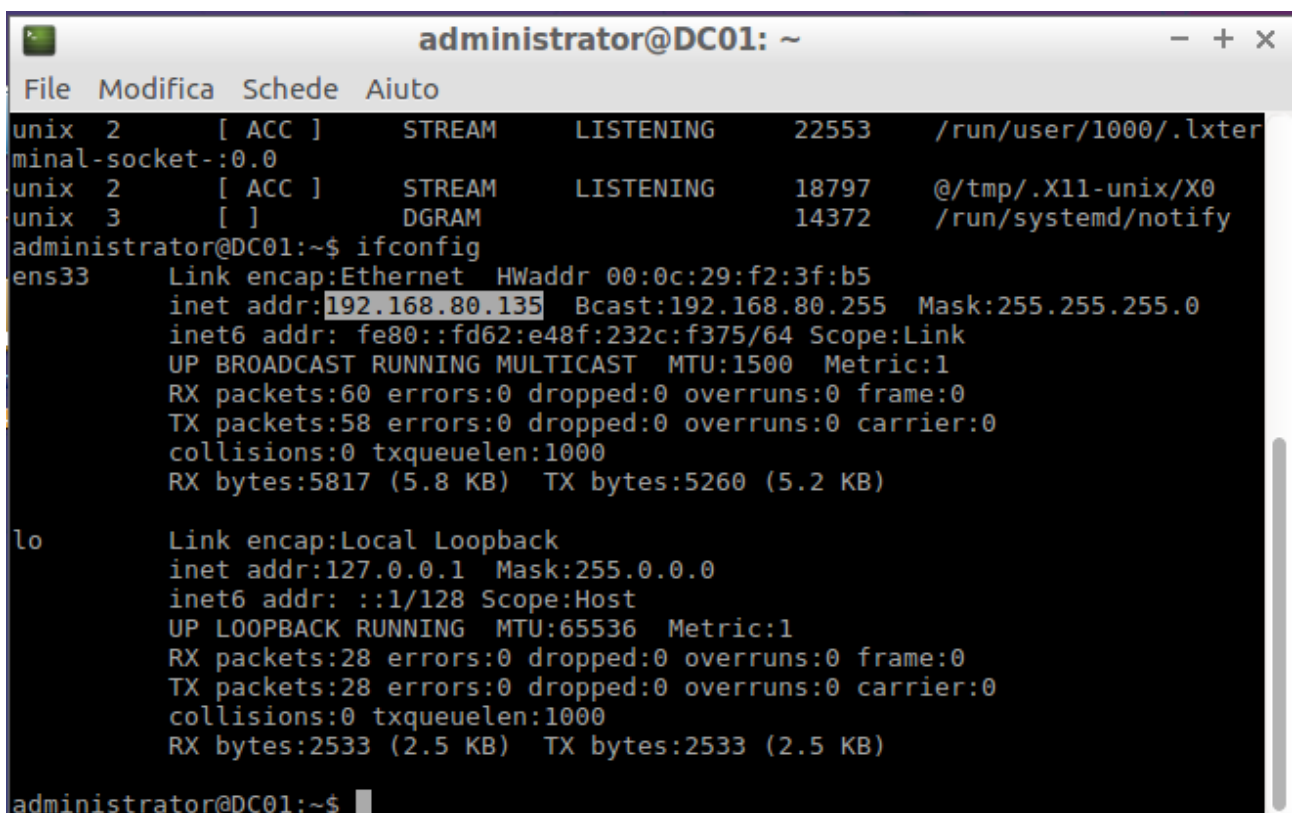


A terminal window titled 'administrator@DC01: ~' showing the output of 'sudo netstat -nape |more'. The output lists active Internet connections (servers and established) with columns for Proto, Recv-Q, Send-Q, Local Address, Foreign Address, State, User, and Inode. Two entries are visible: a TCP connection for 'named' (PID 2865) listening on 192.168.126.200:53, and a TCP connection for 'systemd-resolve' (PID 491) listening on 127.0.0.53:53.

| Proto               | Recv-Q | Send-Q | Local Address      | Foreign Address | State  | User | Inode |
|---------------------|--------|--------|--------------------|-----------------|--------|------|-------|
| tcp                 | 0      | 0      | 192.168.126.200:53 | 0.0.0.0:*       | LISTEN | 115  | 34289 |
| PID/Program name    |        |        |                    |                 |        |      |       |
| tcp                 | 0      | 0      | 127.0.0.53:53      | 0.0.0.0:*       | LISTEN | 101  | 16862 |
| 491/systemd-resolve |        |        |                    |                 |        |      |       |

systemd-resolve fornisce un servizio di cache DNS e di client DHCP.

Prima di disabilitare il Network-manager e systemd-resolve facciamo ifconfig e route per capire che classe di indirizzo è stata assegnata alla macchina virtuale.

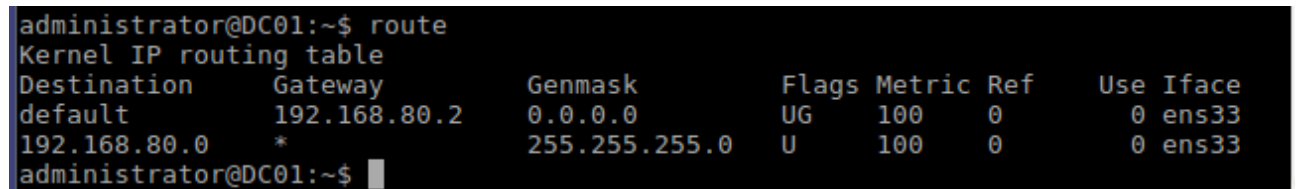


A terminal window titled 'administrator@DC01: ~' showing the output of 'ifconfig' and 'route' commands. The 'ifconfig' output shows details for 'ens33' (Ethernet) and 'lo' (Local Loopback). The 'route' output shows the kernel IP routing table.

| Protocol       | Recv-Q | Send-Q  | Local Address | Foreign Address | State | User                  | Inode |
|----------------|--------|---------|---------------|-----------------|-------|-----------------------|-------|
| unix           | 2      | [ ACC ] | STREAM        | LISTENING       | 22553 | /run/user/1000/.lxter |       |
| minial-socket- | 0.0    |         |               |                 |       |                       |       |
| unix           | 2      | [ ACC ] | STREAM        | LISTENING       | 18797 | @/tmp/.X11-unix/X0    |       |
| unix           | 3      | [ ]     | DGRAM         |                 | 14372 | /run/systemd/notify   |       |

| Destination  | Gateway      | Genmask       | Flags | Metric | Ref | Use | Iface |
|--------------|--------------|---------------|-------|--------|-----|-----|-------|
| default      | 192.168.80.2 | 0.0.0.0       | UG    | 100    | 0   | 0   | ens33 |
| 192.168.80.0 | *            | 255.255.255.0 | U     | 100    | 0   | 0   | ens33 |



A terminal window titled 'administrator@DC01: ~' showing the output of the 'route' command. The output displays the kernel IP routing table with columns for Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface.

| Destination  | Gateway      | Genmask       | Flags | Metric | Ref | Use | Iface |
|--------------|--------------|---------------|-------|--------|-----|-----|-------|
| default      | 192.168.80.2 | 0.0.0.0       | UG    | 100    | 0   | 0   | ens33 |
| 192.168.80.0 | *            | 255.255.255.0 | U     | 100    | 0   | 0   | ens33 |

Assegniamo un indirizzo statico **192.168.153.200** con gateway **192.168.153.2** mask **255.255.255.0** all'interfaccia ens33

Disabilitiamo il Network-manager con il comando systemctl

```
sudo systemctl stop NetworkManager
sudo systemctl disable NetworkManager
sudo systemctl mask NetworkManager
```

abilitiamo systemd-networkd.service



```
sudo systemctl unmask systemd-networkd.service
sudo systemctl enable systemd-networkd.service
sudo systemctl start systemd-networkd.service
```

Disabilitiamo system-resolved

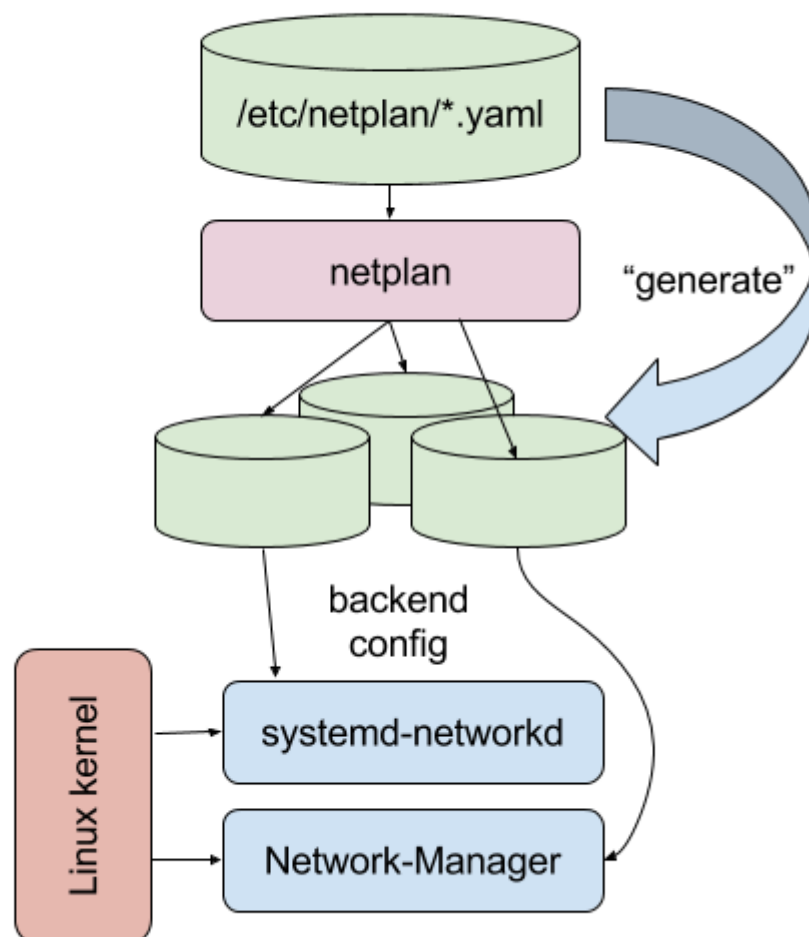
```
sudo systemctl disable systemd-resolved.service
sudo systemctl stop systemd-resolved.service
```

## Configuriamo un indirizzo IP Statico

Lubuntu e Ubuntu dalla versione 18.04 utilizzano un nuovo sistema per la configurazione della rete  
<https://netplan.io/examples>

In pratica si possono utilizzare gli stessi file di configurazione .yaml sia per Network-Manager che per systemd-networkd

### Design overview



```
sudo vim /etc/netplan/01-network-manager-all.yaml
```

```
network:
  version: 2
```

```
renderer: networkd
ethernets:
  ens33:
    addresses:
      - 192.168.153.200/24
    routes:
      - to: default
        via: 192.168.153.2

nameservers:
  search: [mydomain, otherdomain]
  addresses: [8.8.8.8]
```

Usiamo il comando netplan apply per applicare le modifiche

```
sudo netplan apply
```

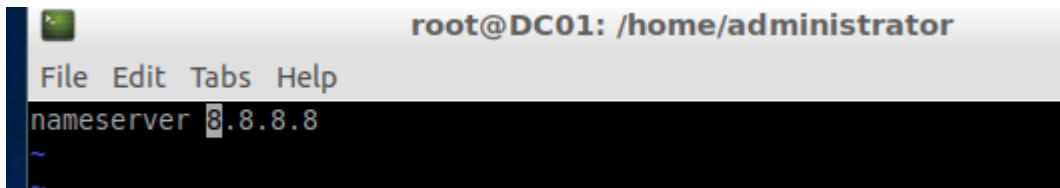
Proviamo a risolvere un dominio.

```
nslookup www.libero.it
```

Non funziona. Dobbiamo riavviare il PC, cancellare il link e rifare il file resolv.conf

Modifichiamo il file resolv.conf in modo da usare il DNS 8.8.8.8

```
sudo vim /etc/resolv.conf
```



## Cambiamo l'hostname

Per cambiare l'hostname bisogna modificare il file

/etc/hostname



oppure

```
sudo hostnamectl set-hostname LDC01
```

poi cambiamo il file /etc/hosts . Al posto di admin-vmwarevirtualplatform bisogna mettere ldc01 e ip 192.168.153.200

```
# Standard host addresses
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# This host address
192.168.153.200 ldc01
~
~
```

Per sicurezza a questo punto è meglio fare un reboot

## Un ottimo editor di testo. Installiamo vim

```
sudo apt install vim
```

## E se sul server ci serve l'ambiente grafico? Installiamo xrdp e usiamo remote desktop

```
sudo apt install xrdp
```

Per vedere se il servizio è partito

```
sudo service xrdp status
```

Aggiungere

```
sudo adduser xrdp ssl-cert
```

Modifichiamo la configurazione

```
sudo vim /etc/xrdp/startwm.sh
```

Aggiungiamo le seguenti righe prima di test -x ....

```
unset DBUS_SESSION_BUS_ADDRESS
unset XDG_RUNTIME_DIR
```

```
fi
unset DBUS_SESSION_BUS_ADDRESS
unset XDG_RUNTIME_DIR
#. $HOME/.profile
test -x /etc/X11/Xsession && exe
exec /bin/sh /etc/X11/Xsession
```

A questo punto riavviamo il servizio xrdp

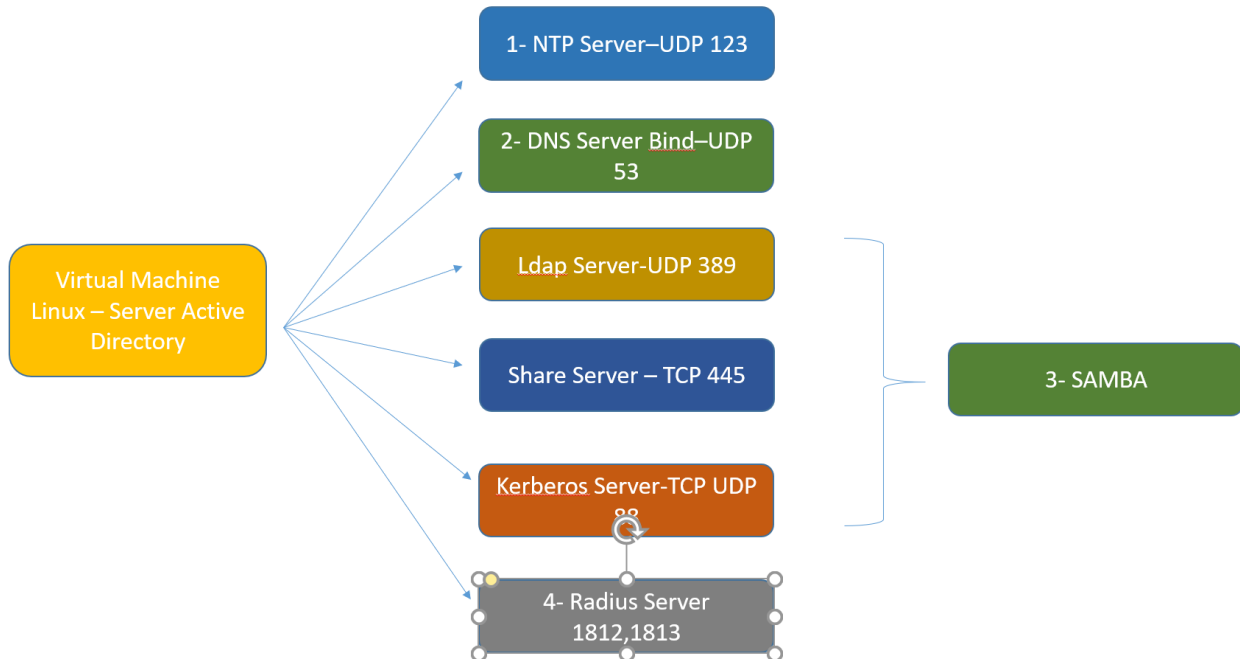
```
sudo service xrdp restart
```

Disabilitiamo il servizio all'avvio usando il comando

```
sudo systemctl disable xrdp
```

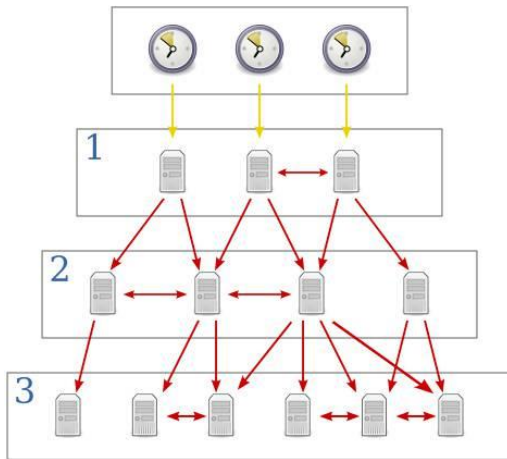
Riavviamo la macchina virtuale e vediamo cosa succede

## I servizi di rete che dobbiamo installare per Active Directory



## 1- Il servizio NTP

Il Network Time Protocol, in sigla NTP, è un protocollo per sincronizzare gli orologi dei computer all'interno di una rete a commutazione di pacchetto, quindi con tempi di latenza variabili ed inaffidabili. L'NTP è un protocollo client-server appartenente al livello applicativo ed è in ascolto sulla porta UDP 123.



Ogni livello della gerarchia è chiamato "strato", al quale è assegnato un numero progressivo partendo dallo zero: a questo strato appartengono le fonti temporali esterne – come orologi atomici, GPS oppure orologi radiocontrollati – che forniscono la marca temporale originaria (quella considerata più precisa e quindi presa come standard di riferimento). Un device sincronizzato con un altro dispositivo dello *strato*  $n$  apparterrà per definizione allo strato  $n+1$ .

In Active Directory il domain controller è anche un NTP server ed è fondamentale per l'autenticazione dei client. Kerberos si basa sui ticket che a loro volta usano il tempo come riferimento.

## Il servizio NTP in ambiente Linux

Per vedere lo stato dell'orologio del nostro PC

```
timedatectl status
```

Per modificare il timezone

```
sudo dpkg-reconfigure tzdata
```

Il comando `dpkg-reconfigure` viene utilizzato per eseguire il wizard di configurazione di alcuni servizi.

Oltre al comando `dpkg-reconfigure` è possibile modificare direttamente il file di configurazione

```
sudo cat /etc/timezone
```

Installiamo il servizio ntp con il comando

```
sudo apt install ntp
```

Per vedere lo stato del servizio ntp

```
service ntp status
```

## Abilitiamo la possibilità di usare il servizio NTP solo dai client della nostra rete.

Modifichiamo il file `/etc/ntp.conf` e scommentiamo la riga

```
restrict 192.168.153.0 mask 255.255.255.0 notrust
```

Assicurarsi di eliminare notrust

Riavviamo il servizio

```
sudo service ntp restart
```

## 2- Creiamo un nostro dominio DNS example.com. Il DNS.

Il servizio DNS in ambiente Linux è BIND.

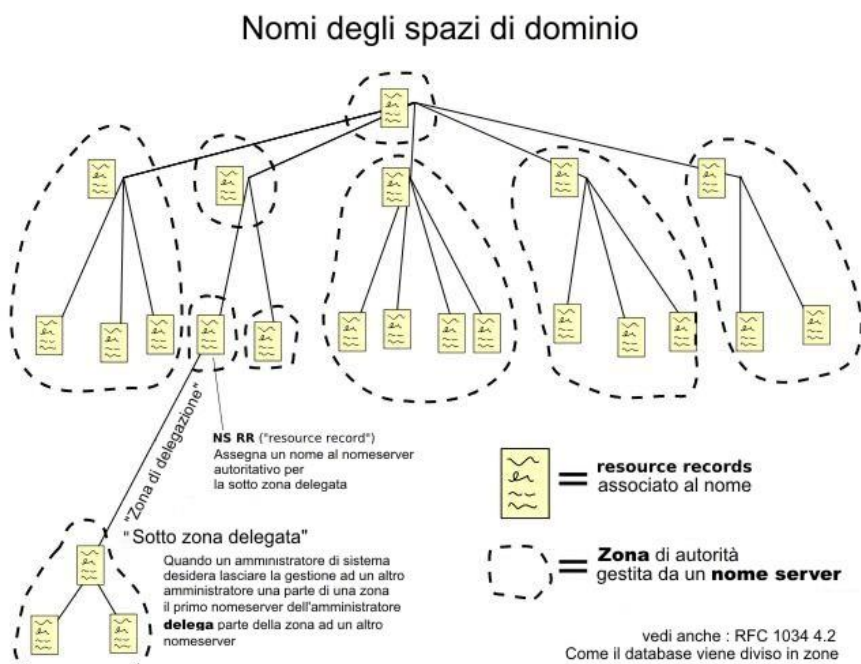
Il servizio DNS serve per risolvere i domini e può funzionare nelle seguenti modalità:

**Forwarding:** Tutte le richieste DNS vengono rigirate verso i DNS esterni tipo google. E' il compito che normalmente effettua il router di casa. Per esempio se noi cerchiamo di risolvere il dns `www.example.com` il server BIND prima cerca in cache e se non c'è la richiesta viene forwardata al DNS del provider (telecom, fastweb ...). Dnsmasq è un servizio DNS che usa forwarding

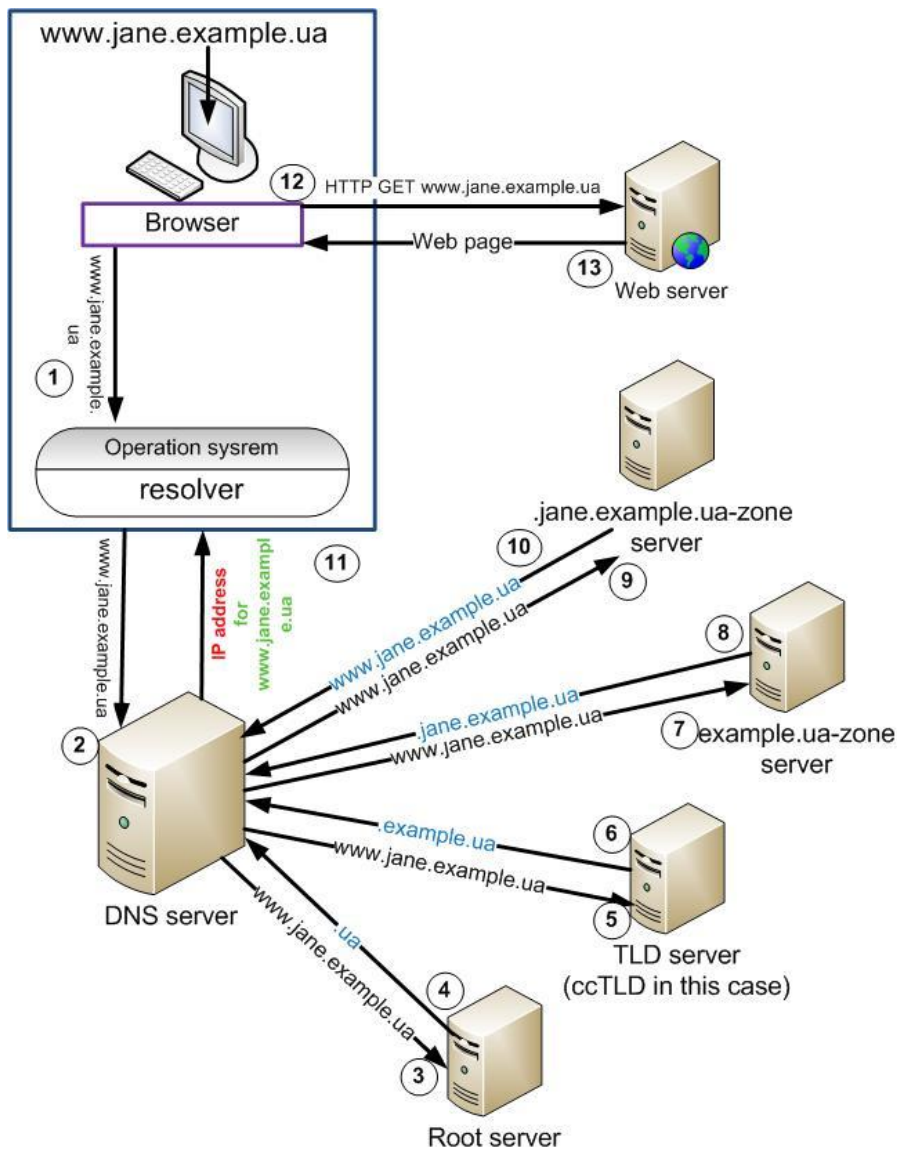
**Recursion:** Il server DNS risolve i domini andando ad effettuare delle query ricorsive. Per esempio per risolvere il dominio `foo.example.com` il server DNS prima effettua una query per sapere i server DNS che gestiscono il dominio `.com`. Poi recupera i server DNS che gestiscono il dominio `example.com` ed infine interroga i server DNS che gestiscono il dominio `example.com` per sapere l'indirizzo IP di `foo.example.com`

Per sicurezza il server DNS dovrebbe funzionare in modalità recursion solo per i client locali. (DNS Amplification Attack)

Ogni dominio possiede un server DNS autoritativo.



## Esempio di risoluzione di un dominio DNS



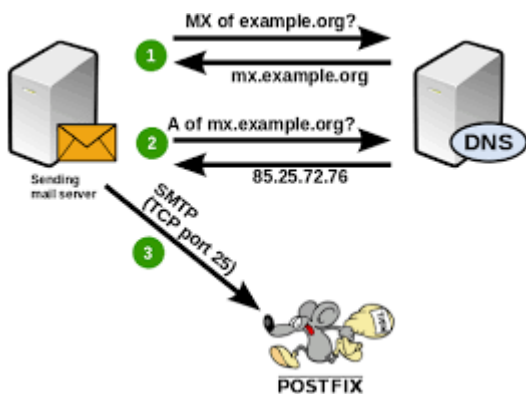
## Tipi di Record DNS

[https://it.wikipedia.org/wiki/Tipi\\_di\\_record\\_DNS](https://it.wikipedia.org/wiki/Tipi_di_record_DNS)

- CNAME: Alias
- A: Collego indirizzo IP ad un nome
- PTR: Puntatore ad un nome canonico utilizzato per la risoluzione DNS inversa.
- TXT: descrizione
- NS: name server DNS
- MX: Mail Server
- SRV: Service Record

Nell'esempio seguente si può vedere come recuperare il server di posta elettronica di un dominio





Si possono effettuare delle ricerche sui DNS andando a filtrare il tipo di record nel seguente modo:

```
root@DC1:~# nslookup
> set type=MX
> google.it
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
google.it    mail exchanger = 10 aspmx.l.google.com.
google.it    mail exchanger = 50 alt4.aspmx.l.google.com.
google.it    mail exchanger = 30 alt2.aspmx.l.google.com.
google.it    mail exchanger = 20 alt1.aspmx.l.google.com.
google.it    mail exchanger = 40 alt3.aspmx.l.google.com.

Authoritative answers can be found from:
>
```

Il record SRV permette di indicare i servizi

| # | _service._proto.name.  | TTL   | class | SRV | priority | weight | port | target.                |
|---|------------------------|-------|-------|-----|----------|--------|------|------------------------|
| 1 | _sip._tcp.example.com. | 86400 | IN    | SRV | 10       | 60     | 5060 | bigbox.example.com.    |
| 2 | _sip._tcp.example.com. | 86400 | IN    | SRV | 10       | 20     | 5060 | smallbox1.example.com. |
| 3 | _sip._tcp.example.com. | 86400 | IN    | SRV | 10       | 20     | 5060 | smallbox2.example.com. |
| 4 | _sip._tcp.example.com. | 86400 | IN    | SRV | 20       | 0      | 5060 | backupbox.example.com. |

## Installiamo il Sever DNS BIND

```
sudo apt install bind9 bind9utils bind9-doc
```

abilitiamo bind per rispondere su ipv4

```
sudo vim /etc/default/named
```

```
OPTIONS="-4 -u bind"
```

Riavviamo il servizio bind

```
service bind9 restart
```

e verifichiamo che sia in ascolto solo su ipv4

```
netstat -na |more
```

Vediamo i file di configurazione

```
/etc/bind/named.conf
```

questo comprende altri file di configurazione

## Abilitiamo gli utenti della nostra rete a fare richieste DNS sul nostro server

Per evitare eventuali problemi di sicurezza dobbiamo limitare le richieste DNS solo alla nostra sottorete. (<https://hacktips.it/tecniche-hacking-dns/>)

Apriamo il file /etc/bind/named.conf.options

```
acl trusted {  
    192.168.153.0/24;  
    127.0.0.1/32;  
};  
  
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    // forwarders {  
    //     0.0.0.0;  
    // };  
  
    //=====   
    // If BIND logs error messages about the root key being expired,  
    // you will need to update your keys. See https://www.isc.org/bind-keys  
    //=====   
    dnssec-validation auto;  
    recursion yes;           # enables recursive queries  
    allow-recursion { trusted; }; # allows recursive queries from "trusted" clients  
    listen-on { 192.168.153.200; 127.0.0.1; }; # ns1 private IP address - listen on private network only  
    allow-transfer { none; };   # disable zone transfers by default  
};
```

Aggiungiamo le ultime 4 righe nel file di configurazione:

Per verificare se la configurazione è giusta basta eseguire

```
sudo named-checkconf
```

Un test che si può effettuare è mettere nelle acl 192.168.153.200. Dopo aver riavviato bind9 possiamo verificare che le query DNS vengono risolte solo dal server non da altri PC con IP differenti dal 192.168.153.200.

## Verifichiamo il funzionamento del DNS

```
dig linuxfoundation.org  
nslookup www.google.it 192.168.153.200  
nslookup SERVER...
```

## Creiamo il dominio DNS example.com

Andiamo nella cartella /etc/bind e copiamo il file db.empty in db.example.com

```
sudo cp /etc/bind/db.empty /etc/bind/db.example.com
```

Apriamo il file db.example.com e vediamo la configurazione.

### File db.example.com

```
; BIND reverse data file for empty rfc1918 zone;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
$TTL 86400
@ IN SOA ldc01.example.com. root.example.com. (
    1      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    86400 ) ; Negative Cache TTL
;
@ IN NS ldc01.example.com.
LDC01.example.com. IN A 192.168.153.200
```

- 1. *Serial* : E' un numero senza segna a 32 bit che viene incrementato ad ogni aggiornamento del file. Questo permette ad un server secondario quando riaggiornare le informazioni. Per questo campo normalmente si usa il formato seguente: YYYYMMDDXX → 2018012701, 2018012702..
- 2. *Refresh* : tempo di refresh, entro il quale richiedere le info.
- 3. *Retry* : if an error occurs during the last refresh, it will be repeated at the end of time Retry.
- 4. *Expires*': the server is considered unavailable after the time expires.
- 5. *Negative cache TTL*': set the lifetime of a NXDOMAIN response from us.

Andiamo ad aggiungere il nuovo dominio nella configurazione di Bind in modo da far gestire al bind anche questo dominio.

Apriamo il file named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

```
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com"; # zone file path
    #allow-transfer { 10.128.20.12; };      # ns2 private IP address - secondary
};
```

Riavviamo il servizio bind9

```
service bind9 restart
```

e verifichiamo il funzionamento del dominio

```
nslookup ldc01.example.com
nslookup ldc01.example.com 192.168.153.200
```

Andiamo a cambiare il dns del nostro PC

```
sudo vim /etc/netplan/01-network-manager-all.yaml
```

```
# Let NetworkManager manage all devices on this system
```

```
network:
```

```
version: 2
```

```
renderer: networkd
```

```
ethernets:
```

```
ens33:
```

```
addresses:
```

```
- 192.168.153.200/24
```

```
routes:
```

```
- to: default
```

```
via: 192.168.153.2
```

```
nameservers:
```

```
search: [example.com]
```

```
addresses: [192.168.153.200]
```

poi

```
sudo netplan apply
```

Andiamo anche a modificare il file resolv.conf

```
nameserver 192.168.153.200
```

e verifichiamo il funzionamento del dominio

```
nslookup ldc01.example.com
```

## Cos'è il file “rovescio” nel DNS?

Di seguito un esempio del file rovescio che però non andremo a configurare perché questo lo faremo creare al dominio Active Directory.

### File db.153.168.192

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA LDC01.example.com. root.example.com. (
    1 ; Serial
    604800 ; Refresh
```

```

        86400      ; Retry
        2419200   ; Expire
        604800 )   ; Negative Cache TTL
;
IN NS LDC01.example.com.
200 IN PTR LDC01.example.com.
201 IN PTR test.example.com.
~

```

## Verifichiamo il file /etc/hosts

Bisogna ripulire i vecchi riferimenti al dns locale

```

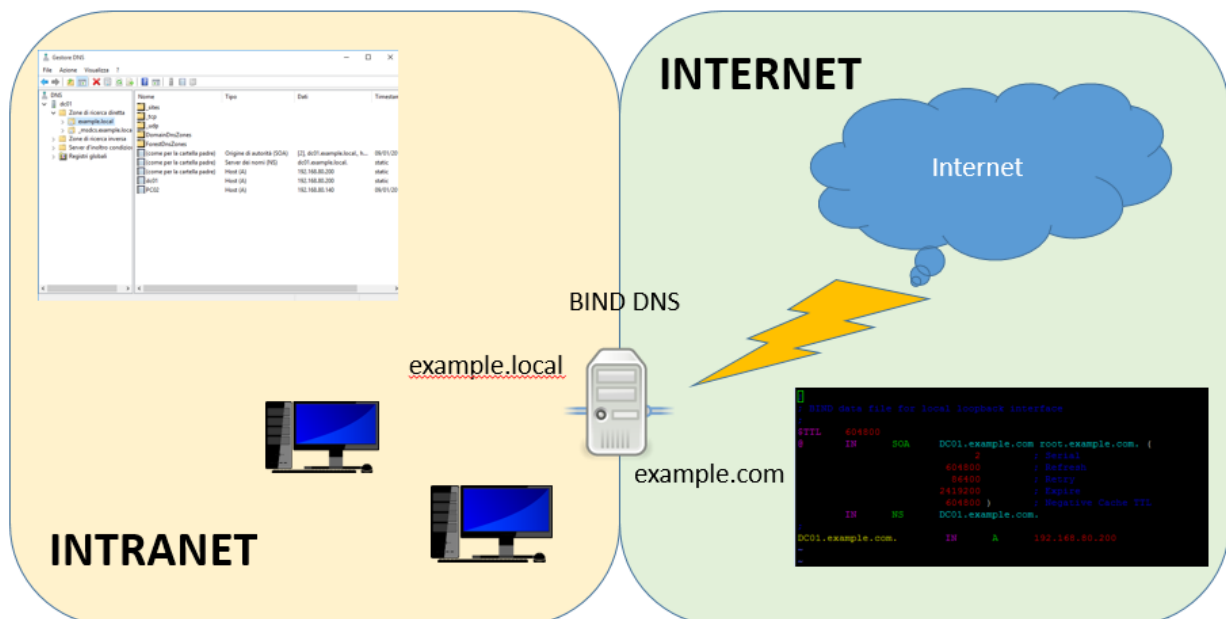
# Standard host addresses
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# This host address
192.168.153.200 ldc01
~
~
~

```

## Dominio DNS e dominio Active Directory Samba

Il dominio DNS è differente dal dominio Active Directory. Per sicurezza non è consigliabile esporre il dominio Active Directory “example.local”.

## Split DNS



Per evitare di dover replicare i servizi faremo un'installazione piu' complessa configurando BIND per gestire sia il dominio interno che quello esterno. Per ragioni di sicurezza non si espone mai il dominio Active Directory all'esterno della propria rete.

Con BIND è possibile dire quali IP possono vedere example.local e quali example.com.

Il dominio example.local è integrato all'interno di LDAP ed è gestito direttamente da SAMBA. Non è un file di testo come il dominio example.com.

```
// INTERNAL
view "internal-view" {
    match-clients { trusted; };
    include "/etc/named.internal.zones";
    include "/etc/named.common.zones";
};
// EXTERNAL
view "external-view" {
    match-clients { any; };
    include "/etc/named.external.zones";
    include "/etc/named.common.zones";
};
```

### 3- Samba

**Samba** è un progetto libero che fornisce servizi di condivisione di file e stampanti ai client usando il protocollo SMB/CIFS

Permette di interagire con server Microsoft Windows come se fosse un file server e un print server

Dalla release 4, Samba è in grado di svolgere le funzioni di un domain controller (DC), integrandosi anche con Active Directory (AD) di Windows Server. Inoltre, può comportarsi come un Primary Domain Controller (PDC). Comunque Samba rimane sostanzialmente uno strumento di interconnessione di un dominio Microsoft con tecnologie non Microsoft offrendo servizi di condivisione di risorse di rete: pur potendo svolgere alcuni semplici compiti di tipo AD (esempio l'autenticazione di un client e la sua registrazione su dominio al login) è da chiarire che non è attualmente in grado di implementare interamente la complessità funzionale dell'architettura AD di Microsoft.

L'SMB è un protocollo di condivisione di file in rete. CIFS è una parte del protocollo SMB.

Il protocollo SMB contiene le seguenti funzionalità:

- Ricerca dei server in rete Browsing
- Stampa su rete
- Autenticazione e accesso a share di rete, file e cartelle
- File lock
- Supporto unicode

SMB è spesso usato come livello Applicativo e come livello di trasporto viene usato NetBIOS.

SMB può essere usato anche senza NBT

- Senza NBT over TCP viene usata la porta 445
- Via NetBIOS AP può usare diverse porte
  - o UDP 137, 138 TCP 137, 139 (NetBIOS over TCP/IP)

SMB usa IPC "Inter Process Communication" come meccanismo di comunicazione per servizi tra computer. L'IPC viene usato da alcuni servizi quali DCP/RPC over SMB

NetBIOS è un protocollo di livello sessione, sviluppato da IBM e Sytec per la cosiddetta PC-Network all'inizio degli anni ottanta. Nonostante sia stato pubblicato solo in un manuale della IBM, le API del protocollo divennero di fatto standard.

NetBIOS su TokenRing o Ethernet è ora chiamato NetBEUI (NetBIOS Extended User Interface). Era ancora molto usato finché fu messo in commercio il sistema operativo Microsoft Windows 98.

NetBIOS su TCP/IP è chiamato NBT ed è stato standardizzato dalle RFC 1001 e 1002. NBT offre un'emulazione di PC-Network LAN basata su NetBIOS su una rete basata su IP. Questo protocollo è stato introdotto con Microsoft Windows 2000 ed è il trasporto preferito su NetBIOS.

NetBIOS offre sempre tre servizi:

- Name service: registrazione e risoluzione del nome (la ricerca del nome è parte dell'SMB, un livello superiore)
- Session service: comunicazione affidabile orientata alla connessione
- Datagram distribution service: comunicazione non fidata senza connessione

NetBIOS e NetBEUI sono destinati solo all'uso sulle reti locali. Per questo motivo, non hanno il supporto per il routing e possono gestire un massimo di 72 nodi. L'uso delle trasmissioni è intenso, specialmente per le operazioni collegate al name service.

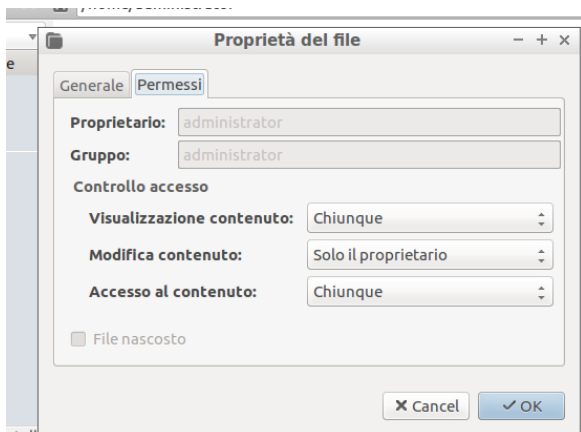
NBT (NetBIOS su TCP/IP) usa uno o più NBNS (NetBIOS Name Server) per coprire il servizio dei nomi su subnet multiple (mentre la trasmissione - broadcast - è limitata ad un unico subnet). Un NBNS è una specie di DNS dinamico. L'implementazione Microsoft di NBNS è chiamata WINS. Inoltre, per estendere le reti virtuali NetBIOS attraverso sotto-reti a IP multipli, lo standard ha introdotto l'uso di uno o più server NBDD (NetBIOS Datagram Distribution).

Winbind è un ambiente integrato all'interno di Samba e viene utilizzato come provider di autenticazione su Linux è disponibile al sistema come Modulo PAM (Pluggable Authentication Module) e quindi può essere usato da diversi servizi per poter effettuare autenticazioni verso Active Directory.

L'evoluzione del modulo Winbind ha seguito l'evolversi di Windows integrandosi dapprima con NTLM e successivamente con AD per mezzo di Kerberos.

## Le ACL: cosa sono e perché le installiamo

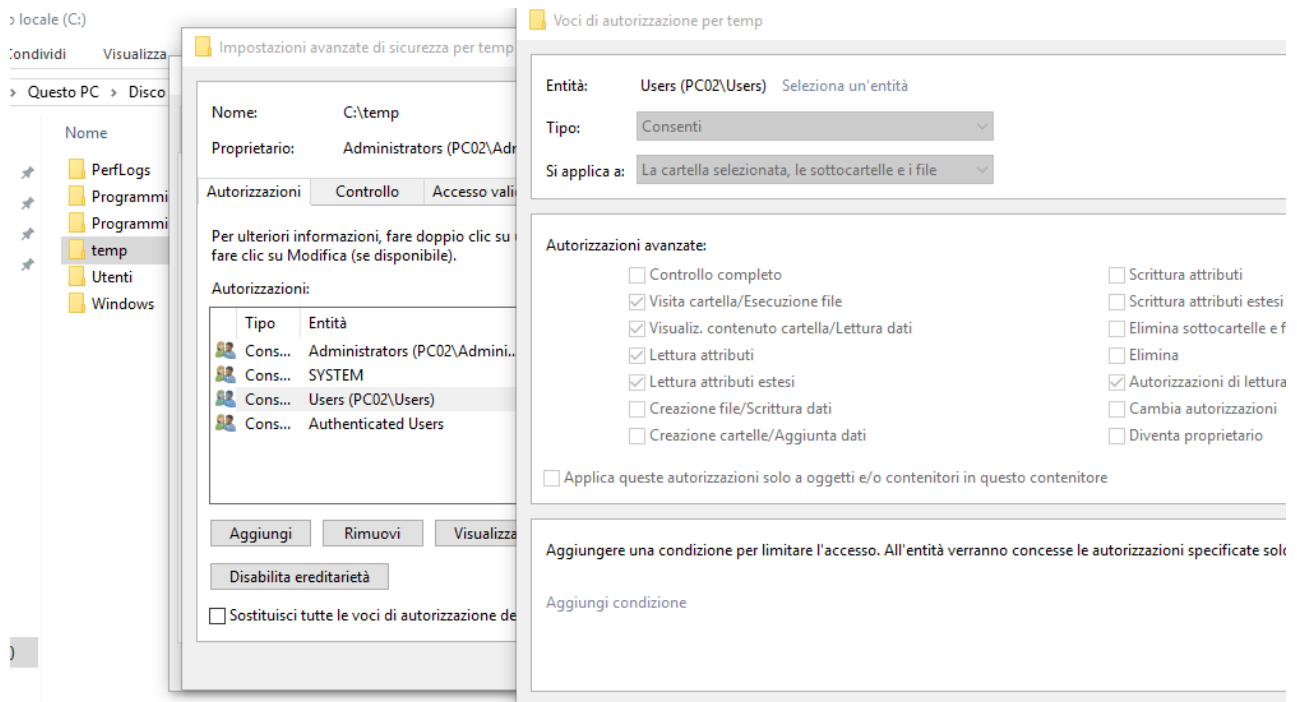
Linux ha una gestione semplice dei permessi su file



```
drwxr-xr-x 5 root root 4096 gen 4 11:42 .
drwxr-xr-x 23 root root 4096 dic 28 17:16 ..
drwxr-xr-x 17 administrator administrator 4096 gen 27 16:07 administrator
drwxr-s-- 3 root users 4096 gen 4 13:26 EXAMPLE
drwxr-xr-x 4 root root 4096 gen 2 22:23 samba
root@DC01: /home#
```

Windows ha una gestione dei permessi piu' complessa:





E' possibile aggiungere le ACL (access control list) e attributi estesi anche su Linux.

Gli attributi permettono di aggiungere dei metadati ai file che permettono di aggiungere informazioni ai file. Le ACL permettono di estendere i permessi ai file e vengono implementato attraverso gli attributi aggiunti ai file.

Per installare gli attributi e le acl procediamo nel seguente modo:

```
sudo apt install acl attr
```

poi andiamo a configurare fstab per abilitare una partizione con attributi estesi

```
sudo nano /etc/fstab
```

```
/dev/sda1/      ext4  user_xattr,acl,barrier=1,defaults 0 1
```

acl - per abilitare le ACL estese provenienti dal mondo Microsoft

user\_xattr - per abilitare l'ereditarietà degli attributi (tra cartella padre e le sottocartelle/file)

Per abilitare la modifica dobbiamo riavviare il server.

## Verifichiamo il funzionamento degli attributi e delle ACL estese.

Creiamo un file vuoto con il comando touch

```
sudo touch testing_acl.txt
```

Assegniamo l'attributo user.test il valore test

```
sudo setfattr -n user.test -v test testing_acl.txt
```

verifichiamo

```
sudo getfattr -d testing_acl.txt
```

```
sudo setfattr -n security.test -v test2 testing_acl.txt
```

```
sudo getfattr -n security.test -d testing_acl.txt
```

[http://wiki.linuxquestions.org/wiki/Extended\\_attributes](http://wiki.linuxquestions.org/wiki/Extended_attributes)

Con le ACL posso settare i permessi per singolo utente o gruppo. Nell'esempio assegno al gruppo adm i permessi di scrittura lettura e esecuzione.

```
sudo setfacl -m g:adm:rwx testing_acl.txt
sudo getfacl testing_acl.txt
```

## Il dominio Active Directory che vogliamo configurare

<https://blogging.dragon.org.uk/samba4-ad-dc-on-ubuntu-14-04/>

Per prima cosa dobbiamo definire le informazioni del dominio Active Directory che vogliamo creare:

**AD DC Hostname:** LDC01 (nome del nostro server)

**AD DNS Domain Name:** LDC01.example.local (nome e dominio)

**Kerberos Realm:** LDC01.EXAMPLE.LOCAL (nome e dominio è maiuscolo)

**Domain Name/NetBIOS Name:** example (nome netbios)

**IP Address:** 10.11.12.200 (indirizzo Ip del nostro server)

**Forwarder DNS Server:** 10.11.12.200 (indirizzo Ip del server a cui forwardare le richieste DNS)

**Gateway:** 10.11.12.2 (gateway)

**Subnet Mask:** 255.255.255.0 (netmask)

**Server Role:** Primary Domain Controller (PDC) (ruolo del server)

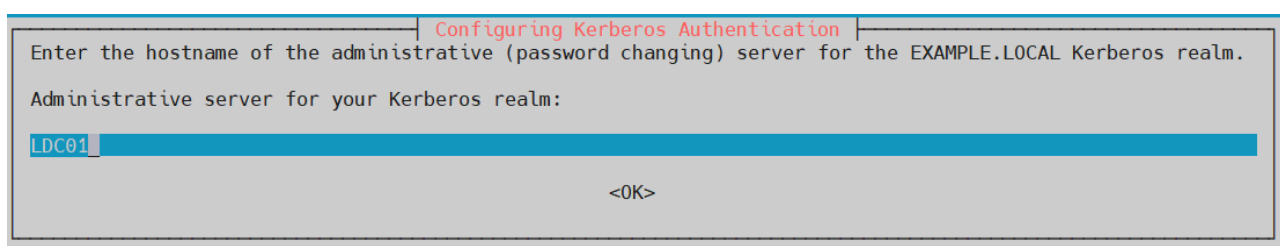
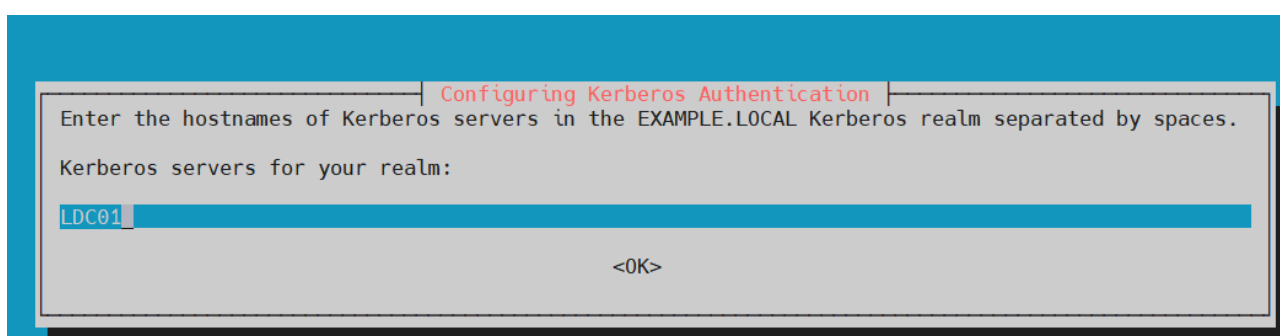
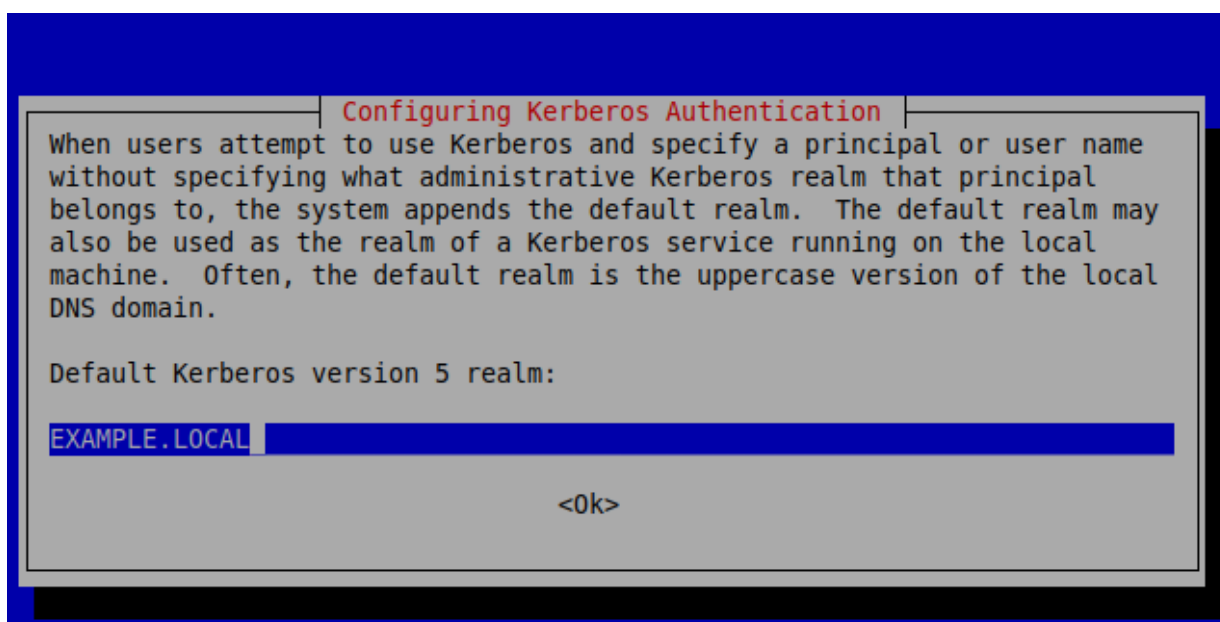
**Domain Admin Password:** Admin1234! (password)

**Backend DNS:** BIND9 DLZ (chi gestisce il DNS)

[https://wiki.samba.org/index.php/BIND9\\_DLZ\\_DNS\\_Back\\_End](https://wiki.samba.org/index.php/BIND9_DLZ_DNS_Back_End)

```
sudo apt-get install samba smbclient build-essential libacl1-dev
libattr1-dev libblkid-dev libreadline-dev python3-dev libpam0g-dev
python3-dnspython gdb pkg-config libpopt-dev libldap2-dev dnsutils
libbsd-dev krb5-user docbook-xsl libcups2-dev ldb-tools winbind libnss-
winbind libpam-winbind
```

Dopo aver eseguito i comandi viene eseguito un wizard che chiede alcune informazioni relative al dominio.



Cancelliamo il file di configurazione

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

Eseguiamo il comando per creare il nostro dominio in modalità iterativa

```
(samba-tool domain provision --use-rfc2307 --realm=EXAMPLE.LOCAL --domain=EXAMPLE --dns-backend=BIND9_DLZ --adminpass=Admin1234!)
```

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

Realm: **EXAMPLE.LOCAL**

Domain [EXAMPLE]:

Server Role (dc, member, standalone) [dc]:

DNS backend (SAMBA\_INTERNAL, BIND9\_FLATFILE, BIND9\_DLZ, NONE) [SAMBA\_INTERNAL]: **BIND9\_DLZ**

Administrator password:

Retype password:

Looking up IPv4 addresses

Looking up IPv6 addresses

No IPv6 address will be assigned

Setting up share.ldb

Setting up secrets.ldb

Setting up the registry

Setting up the privileges database

Setting up idmap db

Setting up SAM db

Setting up sam.ldb partitions and settings

Setting up sam.ldb rootDSE

Pre-loading the Samba 4 and AD schema

Adding DomainDN: DC=example,DC=local

Adding configuration container

Setting up sam.ldb schema

Setting up sam.ldb configuration data

Setting up display specifiers

Modifying display specifiers

Adding users container

Modifying users container

Adding computers container

Modifying computers container

Setting up sam.ldb data

Setting up well known security principals

Setting up sam.ldb users and groups

Setting up self join

Adding DNS accounts

Creating CN=MicrosoftDNS,CN=System,DC=example,DC=local

Creating DomainDnsZones and ForestDnsZones partitions

Populating DomainDnsZones and ForestDnsZones partitions

See /var/lib/samba/private/named.conf for an example configuration include file for BIND

and /var/lib/samba/private/named.txt for further documentation required for secure DNS updates

Setting up sam.ldb rootDSE marking as synchronized

Fixing provision GUIDs

A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/samba/private/krb5.conf

Setting up fake yp server settings

Once the above files are installed, your Samba4 server will be ready to use

Server Role: active directory domain controller

Hostname: LDC01

NetBIOS Domain: EXAMPLE

DNS Domain: example.local

DOMAIN SID: S-1-5-21-3981063959-2489711124-570155663

## Apriamo il file di configurazione principale di samba

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

# Global parameters

```

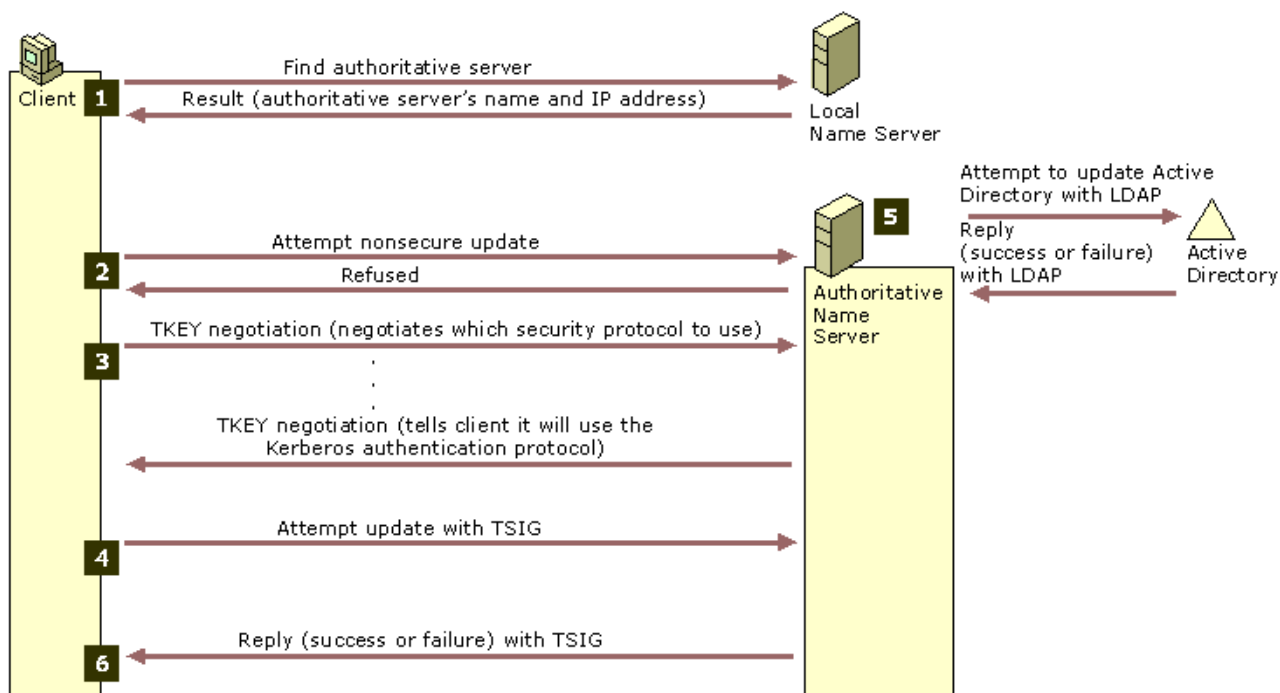
[global]
    workgroup = EXAMPLE
    realm = EXAMPLE.LOCAL
    netbios name = LDC01
    server role = active directory domain controller
    server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc, drepl, winbindd, ntp_signd, kcc, dnsupdate
    idmap_ldb:use rfc2307 = yes
    #Permette l'aggiornamento del DNS in modo dinamico
    allow dns updates = nonsecure and secure
    #Permette di effettuare il forward delle richieste dns
    dns forwarder = 192.168.153.200
    #Aumenta livello di log
    log level = 1 auth:5 winbind:5
    #Abilito act e attributi estesi
    vfs objects = dfs_samba4 acl_xattr
    map acl inherit = yes
    store dos attributes = yes
    #Abilito WinBind, modulo di autenticazione NTLM e Kerberos
    winbind use default domain = yes
    winbind enum users = yes
    winbind enum groups = yes
    winbind refresh tickets = yes
    ntlm auth = yes
[netlogon]
    path = /var/lib/samba/sysvol/example.local/scripts
    read only = No
[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

```

## Usiamo Bind con Dynamic DNS.

Un dinamic DNS è un DNS che può essere popolato dinamicamente, quando un client viene aggiunto al dominio.

Un client può aggiornare il DNS solo dopo essersi autenticato.



Per farlo Bind usa kerberos per aggiornare il DNS di Active directory tramite il comando nsupdate.

Aggiungiamo nel file di configurazione di Bind la seguente opzione

`key-gssapi-keytab "/var/lib/samba/private/dns.keytab";`

```
sudo nano /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
    recursion yes;           # enables recursive queries
    allow-recursion { trusted; }; # allows recursive queries from "trusted" clients
    listen-on { 192.168.153.200;127.0.0.1; }; # ns1 private IP address - listen on private network only
    allow-transfer { none; }; # disable zone transfers by default
    // forwarders {
    //     8.8.8.8;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
}
```

```
dnssec-validation auto;
```

```
auth-nxdomain yes; # conform to RFC1035
```

```
// Aggiungo il file generato da Samba per permettere il DNS dinamico  
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

```
};
```

Verifichiamo la versione di bind

```
sudo /usr/sbin/rndc --version
```

e verifichiamo che sia attiva la libreria giusta in base alla versione di bind

```
sudo nano /var/lib/samba/bind-dns/named.conf
```

```
dlz "AD DNS Zone" {  
    # For BIND 9.8.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9.so";  
  
    # For BIND 9.9.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_9.so";  
  
    # For BIND 9.10.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_10.so";  
  
    # For BIND 9.11.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_11.so";  
  
    # For BIND 9.12.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_12.so";  
  
    # For BIND 9.14.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_14.so";  
  
    # For BIND 9.16.x  
    # database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_16.so";  
    #  
    # For BIND 9.18.x  
    database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_18.so";  
};
```

A questo punto indichiamo a BIND che oltre ad usare i file di configurazione deve usare anche la configurazione di SAMBA.

```
sudo nano /etc/bind/named.conf
```

```
include "/etc/bind/named.conf.options";  
include "/var/lib/samba/bind-dns/named.conf";  
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.default-zones";
```

Dentro /var/lib/samba/private/dns.keytab sono presenti le chiavi per poter aggiornare il database dns. Poiché l'aggiornamento lo deve fare BIND deve poter accedere a queste chiavi. Quindi cambiamo i permessi al file dns.keytab

```
sudo chgrp bind /var/lib/samba/bind-dns/dns.keytab  
sudo chmod g+r /var/lib/samba/bind-dns/dns.keytab
```

## Modifichiamo la configurazione del servizio apparmor

Apparmor è un'applicazione che indica cosa può fare un processo

- From the profile we see 'r' (read), 'w' (write), 'm' (memory map as executable), 'k' (file locking), and 'l' (creation hard links). There are others not demonstrated in this profile, including (but not limited to) 'ix' (execute and inherit this profile), 'Px' (execute under another profile, after cleaning the environment), and 'Ux' (execute unconfined, after cleaning the environment)

Nella vecchia versione andava modificata la configurazione apparmor. Nel nuovo script viene modificata in automatico.

Vediamo la configurazione

```
sudo nano /etc/apparmor.d/usr.sbin.named
```

```
# Samba DLZ
/{usr/,}lib/{multiarch}/samba/bind9/*.so rm,
/{usr/,}lib/{multiarch}/samba/gensec/*.so rm,
/{usr/,}lib/{multiarch}/samba/ldb/*.so rm,
/{usr/,}lib/{multiarch}/ldb/modules/ldb/*.so rm,
/var/lib/samba/bind-dns/dns.keytab rk,
/var/lib/samba/bind-dns/named.conf r,
/var/lib/samba/bind-dns/dns/** rwk,
/var/lib/samba/private/dns.keytab rk,
/var/lib/samba/private/named.conf r,
/var/lib/samba/private/dns/** rwk,
/etc/samba/smb.conf r,
/dev/urandom rwmk,
owner /var/tmp/krb5_ * rwk,
```

Riavviamo il server

```
sudo reboot
```

## Verifichiamo che sia attivo il servizio samba-ad-dc

```
sudo service samba-ad-dc start
```

Failed to start samba-ad-dc.service: Unit samba-ad-dc.service is masked.

```
sudo rm /etc/systemd/system/samba-ad-dc.service
```

```
sudo systemctl enable samba-ad-dc
```

Synchronizing state of samba-ad-dc.service with SysV service script with /lib/systemd/systemd-sysv-install.

Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc

Avviamo il servizio Samba AD

```
sudo systemctl start samba-ad-dc
```

## Verifichiamo l'installazione e la configurazione del server Active Directory

```
smbclient -L localhost -U%
```



```
admin@LCD01:~$ smbclient -L localhost -U%

      Sharename      Type      Comment
      -----
      sysvol         Disk
      netlogon       Disk
      IPC$           IPC        IPC Service (Samba 4.15.13-Ubuntu)
SMB1 disabled -- no workgroup available
admin@LCD01:~$
```

```
smbclient //localhost/sysvol -UAdministrator -c 'ls'
```

```
admin@LCD01:~$ smbclient //localhost/sysvol -UAdministrator -c 'ls'
Password for [EXAMPLE\Administrator]:
.          D          0   Wed Apr  3 14:25:16 2024
..         D          0   Wed Apr  3 14:30:26 2024
example.local D          0   Wed Apr  3 14:25:13 2024

      20458536 blocks of size 1024. 9847724 blocks available
admin@LCD01:~$
```

```
host -t SRV _ldap._tcp.example.local.
```

```
administrator@DC01:~$ host -t SRV _ldap._tcp.example.local.
_ldap._tcp.example.local has SRV record 0 100 389 dc01.example.local.
```

```
host -t SRV _kerberos._udp.example.local.
```

```
administrator@DC01:~$ host -t SRV _kerberos._udp.example.local.
_kerberos._udp.example.local has SRV record 0 100 88 dc01.example.local.
```

```
host -t A ldc01.example.local.
```

```
admin@LCD01:~$ host -t A lcd01.example.local
lcd01.example.local has address 192.168.153.200
admin@LCD01:~$
```

Verifichiamo il funzionamento di kerberos

```
kinit administrator
```

Se non funziona assicurarsi che il dominio sia con i caratteri maiuscoli.

Se nel file /etc/krb5.conf non è presente il codice sotto, aggiungerlo

```
[libdefaults]
    default_realm = EXAMPLE.LOCAL
.....
[realms]
    EXAMPLE.LOCAL = {
        kdc = LDC01
```

```
admin_server=LDC01
}
```

<https://www.slideshare.net/AshwinPawar/krb5>

Andiamo a visualizzare la Ticket cache con il comando

*klist*

```
root@DC01:/etc# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EXAMPLE.LOCAL

Valid starting    Expires          Service principal
02/01/2018 11:10:33 02/01/2018 21:10:33  krbtgt/EXAMPLE.LOCAL@EXAMPLE.LOCAL
        renew until 03/01/2018 11:10:22
```

Se vogliamo svuotare la cache possiamo usare il comando

*kdestroy*

Andiamo adesso a controllare cosa c'è nel DNS di Active Directory

*samba-tool dns query ldc01 example.local @ ALL*

```
root@DC01:/etc# samba-tool dns query dc01 EXAMPLE.LOCAL @ ALL
debug_lookup_classname(auth_audit): Unknown class
GENSEC backend 'gssapi_spnego' registered
GENSEC backend 'gssapi_krb5' registered
GENSEC backend 'gssapi_krb5_sasl' registered
GENSEC backend 'spnego' registered
GENSEC backend 'schannel' registered
GENSEC backend 'naclrpc_as_system' registered
GENSEC backend 'sasl-EXTERNAL' registered
GENSEC backend 'ntlmssp' registered
GENSEC backend 'ntlmssp_resume_ccache' registered
GENSEC backend 'http_basic' registered
GENSEC backend 'http_ntlm' registered
GENSEC backend 'krb5' registered
GENSEC backend 'fake_gssapi_krb5' registered
Using binding ncacn_ip_tcp:dc01[,sign]
resolve_lmhosts: Attempting lmhosts lookup for name dc01<0x20>
resolve_lmhosts: Attempting lmhosts lookup for name dc01<0x20>
```

Se non funziona, modifichiamo hosts sostituendo ldc01 da 127.0.0.1 a 192.168.153.200 e rilanciamo il comando

Bisogna assicurarsi che ci sia 127.0.0.1 ldc01 altrimenti non funziona l'ssh

```

root@LDC01:/home/admin# samba-tool dns query ldc01 example.local @ ALL
GENSEC backend 'gssapi_spnego' registered
GENSEC backend 'gssapi_krb5' registered
GENSEC backend 'gssapi_krb5_sasl' registered
GENSEC backend 'spnego' registered
GENSEC backend 'schannel' registered
GENSEC backend 'naclrpc_as_system' registered
GENSEC backend 'sasl-EXTERNAL' registered
GENSEC backend 'ntlmssp' registered
GENSEC backend 'ntlmssp_resume_ccache' registered
GENSEC backend 'http_basic' registered
GENSEC backend 'http_ntlm' registered
GENSEC backend 'http_negotiate' registered
GENSEC backend 'krb5' registered
GENSEC backend 'fake_gssapi_krb5' registered
Starting GENSEC mechanism spnego
Starting GENSEC submechanism gssapi_krb5
Ticket in credentials cache for administrator@EXAMPLE.LOCAL will expire in 35930 secs
Name=, Records=3, Children=0
SOA: serial=11, refresh=900, retry=600, expire=86400, minttl=3600, ns=ldc01.example.local., email=hostmaster.example.local. (flags=6000000f0, serial=11, ttl=3600)
NS: ldc01.example.local. (flags=6000000f0, serial=1, ttl=900)
A: 192.168.153.200 (flags=6000000f0, serial=1, ttl=900)
Name=_msdcs, Records=0, Children=0
Name=_sites, Records=0, Children=1
Name=_tcp, Records=0, Children=4
Name=_udp, Records=0, Children=2
Name=DomainDnsZones, Records=0, Children=2
Name=ForestDnsZones, Records=0, Children=2
Name=ldc01, Records=1, Children=0
A: 192.168.153.200 (flags=f0, serial=1, ttl=900)

```

Verifichiamo l'autenticazione con il protocollo NTLM

```
sudo ntlm_auth --request-nt-key --username=administrator
```

## Comandi samba-tool

<https://www.tecmint.com/manage-samba4-active-directory-linux-command-line/>

Il dominio da noi creato può essere gestito tramite il comando samba-tool.

```
samba-tool -h
```

## Gestiamo gli utenti in AD

```

sudo samba-tool user create utente01 --given-name=utente --
surname=01
sudo samba-tool user create utente02 --given-name=utente --
surname=02
sudo samba-tool user create utente03 --given-name=utente --
surname=03

```

```

sudo samba-tool user list
sudo samba-tool user delete utente02
sudo samba-tool user disable utente03
sudo samba-tool user enable utente03

```

## Gestiamo i gruppi in AD

```

sudo samba-tool group list
sudo samba-tool group add gruppo-utenti
sudo samba-tool group addmembers "gruppo-utenti" utente01
sudo samba-tool group addmembers "gruppo-utenti" utente03

```

```
sudo samba-tool group listmembers
```

## Creazione di cartelle e home per gli utenti

[https://wiki.samba.org/index.php/User\\_Home\\_Folders](https://wiki.samba.org/index.php/User_Home_Folders)

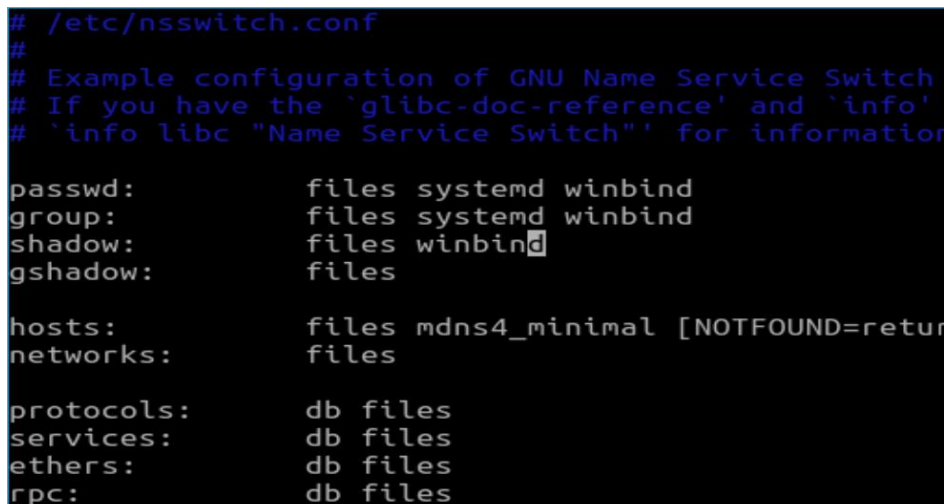
Vogliamo fare in modo che gli utenti del dominio abbiano la propria cartella home dove depositare i file personali.

Dobbiamo per prima cosa far capire al SO dove andare a prendere gli utenti e i gruppi. Questo viene fatto tramite la funzionalità Name Service Switch. Questo non è un servizio.

```
sudo getent passwd
```

Modifichiamo il file `/etc/nsswitch.conf` sostituendo `systemd` con `winbind`

```
cat /etc/nsswitch.conf
```



```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch
# If you have the `glibc-doc-reference' and `info'
# `info libc "Name Service Switch"' for information

passwd:          files systemd winbind
group:           files systemd winbind
shadow:         files winbind
gshadow:        files

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

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

Autenticiamoci con `wbinfo` con le credenziali del dominio (utente amministratore del dominio)

```
sudo wbinfo --krb5auth=administrator
```

Verifichiamo che gli utenti e i gruppi del dominio

```
sudo wbinfo -u
```

```
sudo wbinfo -g
```

e verifichiamo che gli utenti e i gruppi possano essere visti in ambiente linux

```
getent passwd
```

```
getent group
```

Se gli utenti non vengono visti in ambiente linux non possiamo gestire i permessi nelle cartelle.

## Aggiungiamo le condivisioni smb

Creiamo la cartella in cui mette le home degli utenti e gli assegniamo i permessi giusti.

Gli utenti devono poter accedere solo alla propria HOME (`/home/EXAMPLE/nome.cognome`)

```
mkdir -p /home/EXAMPLE/  
chgrp -R "Domain Users" /home/EXAMPLE/
```

Cambiamo i permessi per dare la possibilità agli utenti di creare le proprie cartelle con i propri permessi

```
chmod 2750 /home/EXAMPLE/
```

Apriamo il file di configurazione dei samba

```
/etc/samba/smb.conf
```

Andiamo nella sezione Users

```
[users]  
path = /home/EXAMPLE/  
read only = no  
force create mode = 0600  
force directory mode = 0700
```

Aggiorniamo la configurazione di samba

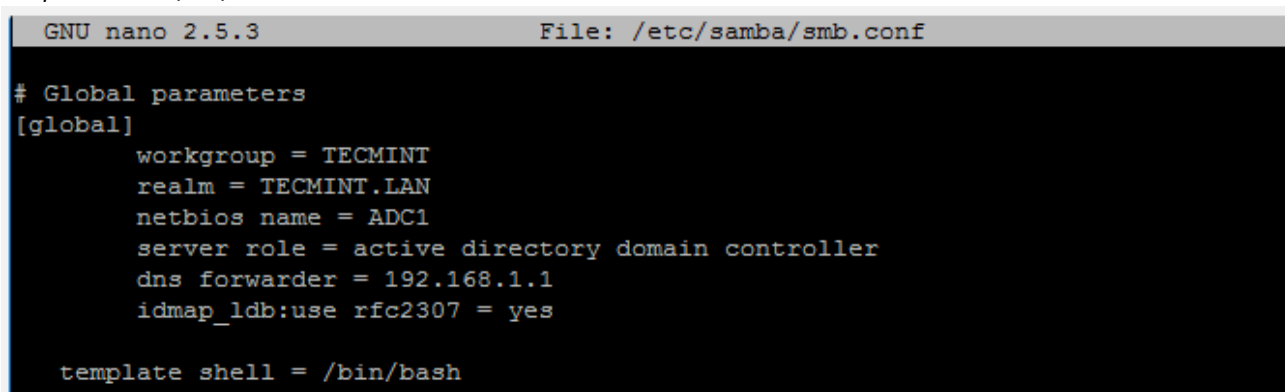
```
smbcontrol all reload-config
```

[https://wiki.samba.org/index.php/Setting\\_up\\_a\\_Share\\_Using\\_Windows\\_ACLs](https://wiki.samba.org/index.php/Setting_up_a_Share_Using_Windows_ACLs)

## Abilitiamo l'accesso alla home

Modifichiamo Samba per definire la shell di default per chi si collega via ssh

```
template shell = /bin/bash
```



```
GNU nano 2.5.3 File: /etc/samba/smb.conf  
  
# Global parameters  
[global]  
    workgroup = TECMINT  
    realm = TECMINT.LAN  
    netbios name = ADC1  
    server role = active directory domain controller  
    dns forwarder = 192.168.1.1  
    idmap_ldb:use rfc2307 = yes  
  
    template shell = /bin/bash
```

Riaggiorniamo la configurazione di samba con

```
sudo smbcontrol all reload-config
```

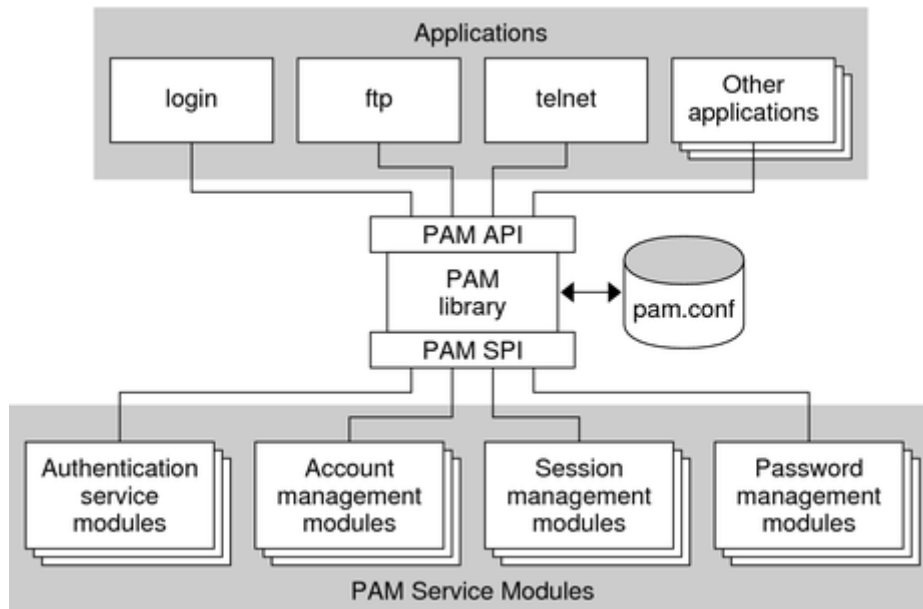
Per verificare se è stata condivisa la cartella users eseguiamo

```
smbclient -L localhost -U%
```

## Autenticazione local PAM

[https://it.wikipedia.org/wiki/Pluggable\\_authentication\\_modules](https://it.wikipedia.org/wiki/Pluggable_authentication_modules)

Il Pluggable Authentication Modules (in acronimo PAM) è un meccanismo per integrare più schemi di autenticazione a basso livello in un'unica Application Programming Interface (API) ad alto livello, permettendo ai programmi che necessitano di una forma di autenticazione, di essere scritti indipendentemente dallo schema di autenticazione sottostante utilizzato.



v

Usiamo PAM per automatizzare la creazione dell'homepage quando l'utente si collega in ssh

[https://www.systutorials.com/docs/linux/man/8-pam\\_mkhomedir/](https://www.systutorials.com/docs/linux/man/8-pam_mkhomedir/)

Il modulo pam gestisce l'autenticazione degli utenti per il servizio sshd

Vediamo la configurazione di pam

Se l'utente02 prova a collegarsi al server in ssh viene fuori il seguente errore perché non esiste la homedirectory. La homedirectory è dentro il file di configurazione di samba.

```
Last login: Tue Jan 30 22:19:29 2018 from 192.168.80.1
Could not chdir to home directory /home/EXAMPLE/utente02: No such file or directory
EXAMPLE\utente02@DC01:/$
```

## Modifichiamo PAM per creare la homedirectory in automatico

Installiamo il modulo di pam che si occupa di fare il mount automatico

```
sudo apt-get install libpam-mount
```

Andiamo a modificare la configurazione di pam per creare la home directory in automatico

```
sudo vim /etc/pam.d/common-session
```

Aggiungiamo alla fine del file la seguente opzione

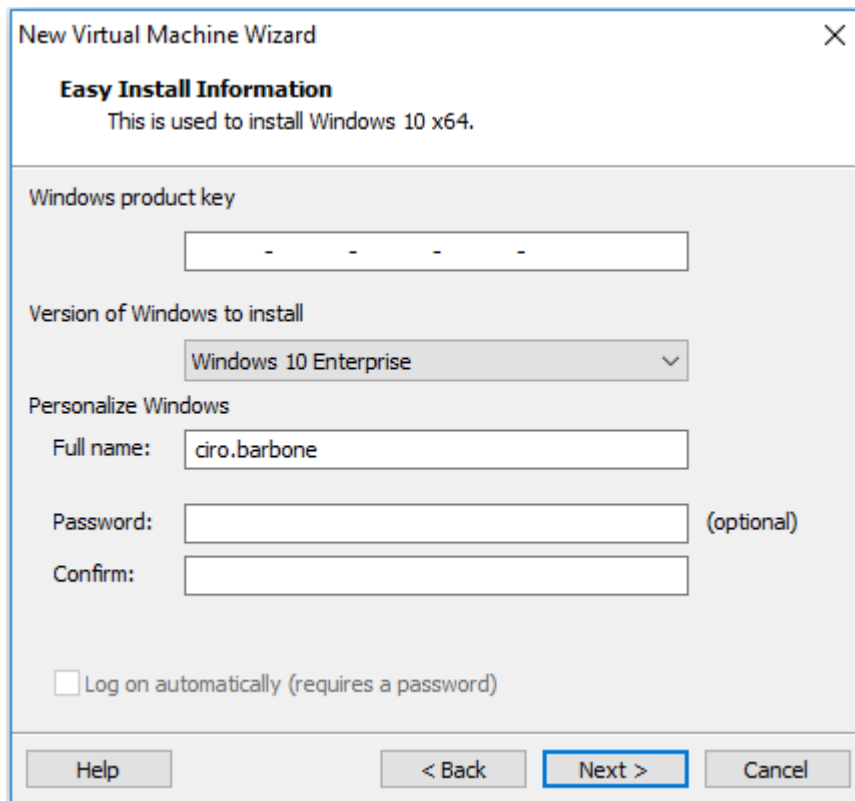
```
session required    pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

assicuresi che ci sia anche questa

```
session optional    pam_mount.so
```

Accediamo in ssh per verificare se la configurazione funziona.

Installiamo il nostro client Windows 10



The image shows a screenshot of the 'New Virtual Machine Wizard' window, specifically the 'Easy Install Information' step. The window has a title bar with the text 'New Virtual Machine Wizard' and a close button (X) in the top right corner. Below the title bar, the section is titled 'Easy Install Information' with a subtitle 'This is used to install Windows 10 x64.'.

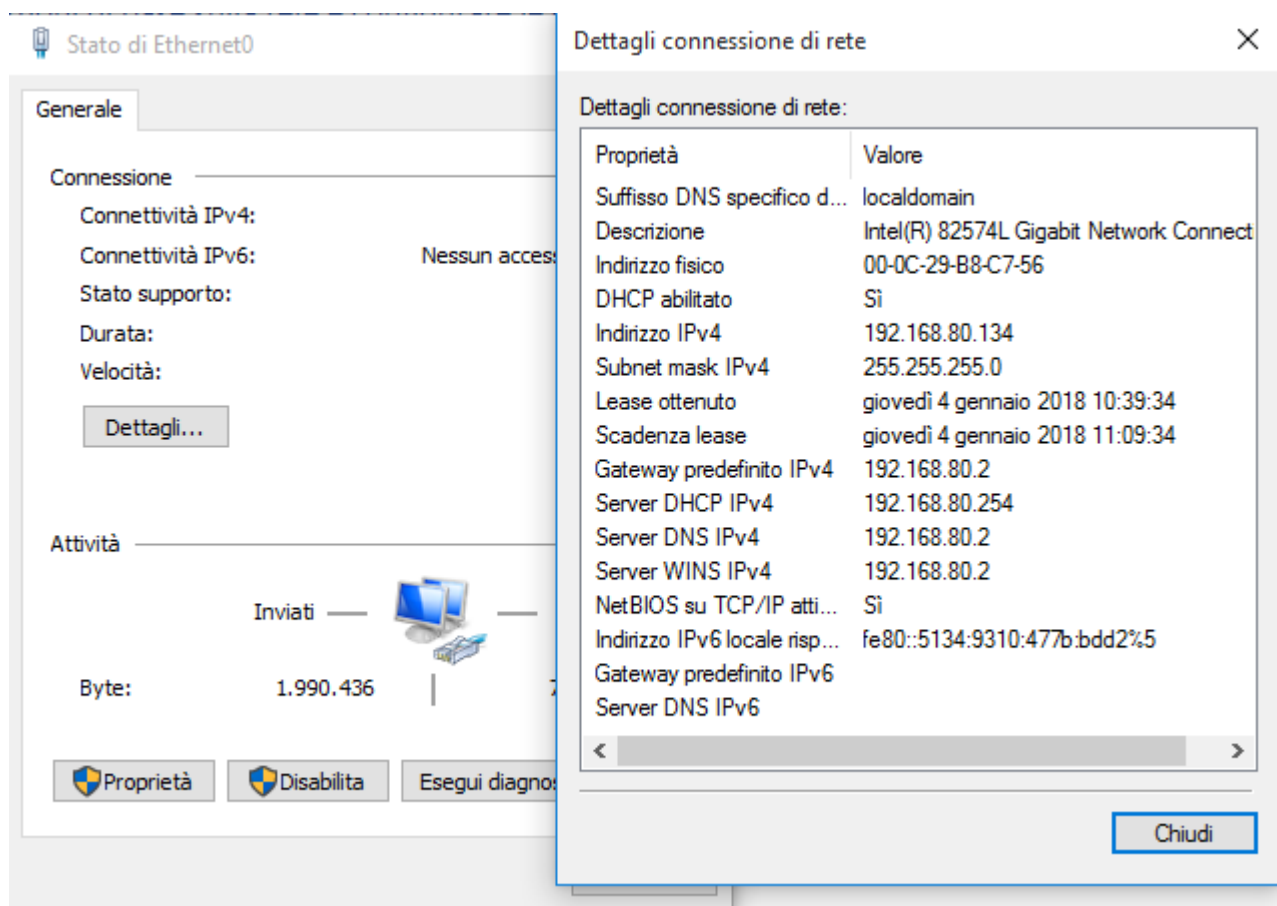
The main content area contains the following fields and options:

- Windows product key:** A text input field with four dashes ( - - - - ) as a placeholder.
- Version of Windows to install:** A dropdown menu currently showing 'Windows 10 Enterprise' with a downward arrow.
- Personalize Windows:**
  - Full name:** A text input field containing 'ciro.barbone'.
  - Password:** A text input field, followed by the text '(optional)'.
  - Confirm:** A text input field.
- Log on automatically:** A checkbox labeled 'Log on automatically (requires a password)' which is currently unchecked.

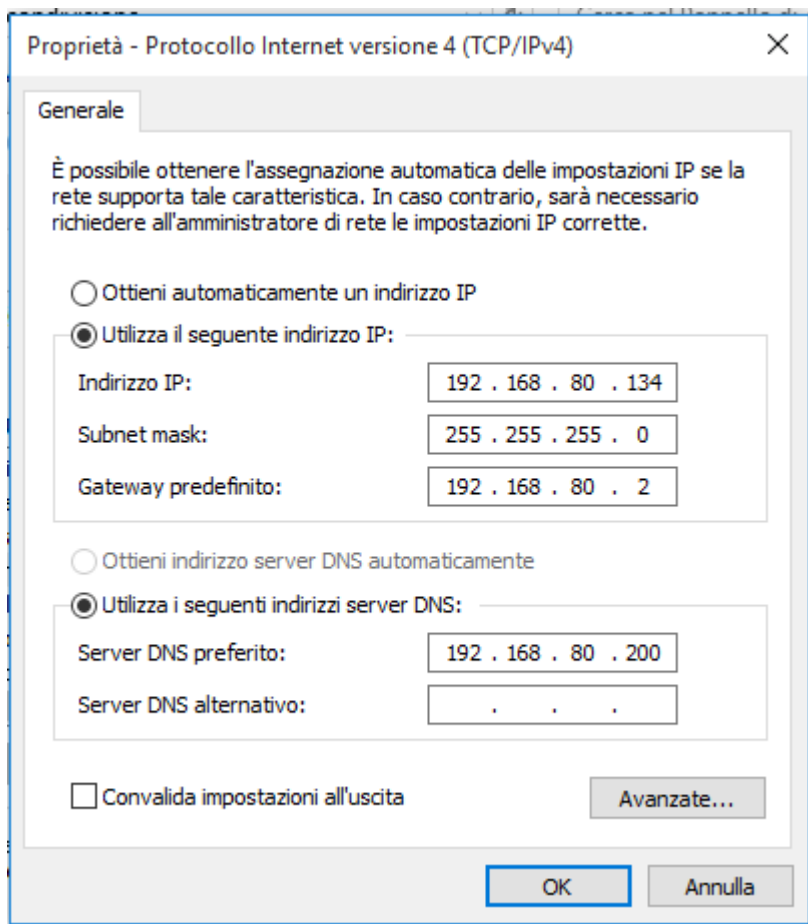
At the bottom of the window, there are four buttons: 'Help', '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Vediamo la configurazione della macchina windows 10





Cambiamo la configurazione della rete prima di inserirlo nel dominio. La cosa importante è il DNS.



Verifichiamo la configurazione di rete tramite comandi

*Ipconfig*

```
C:\Users\Administrator>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet0:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::5134:9310:477b:bdd2%5
    Indirizzo IPv4. . . . . : 192.168.80.134
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.80.2

Scheda Tunnel isatap.{FD2380DF-50B7-498E-A304-3C10D0BC3E69}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

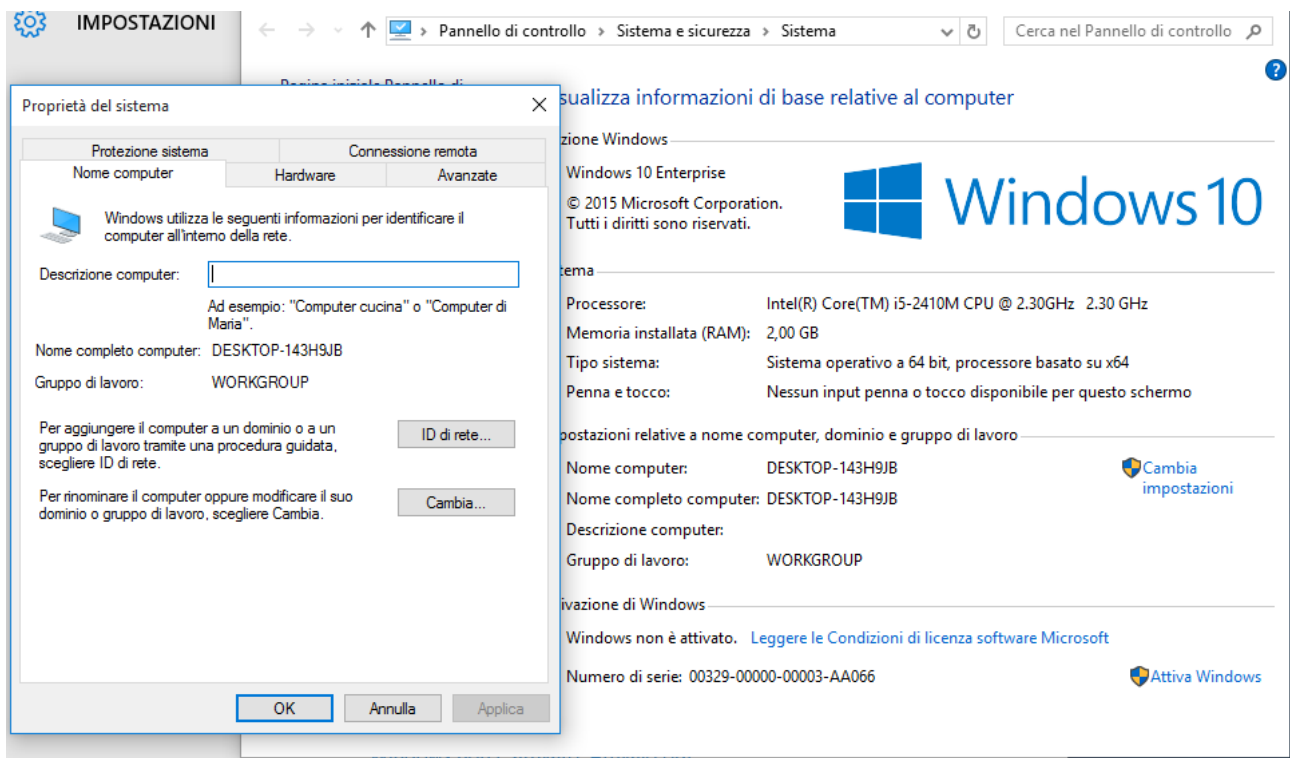
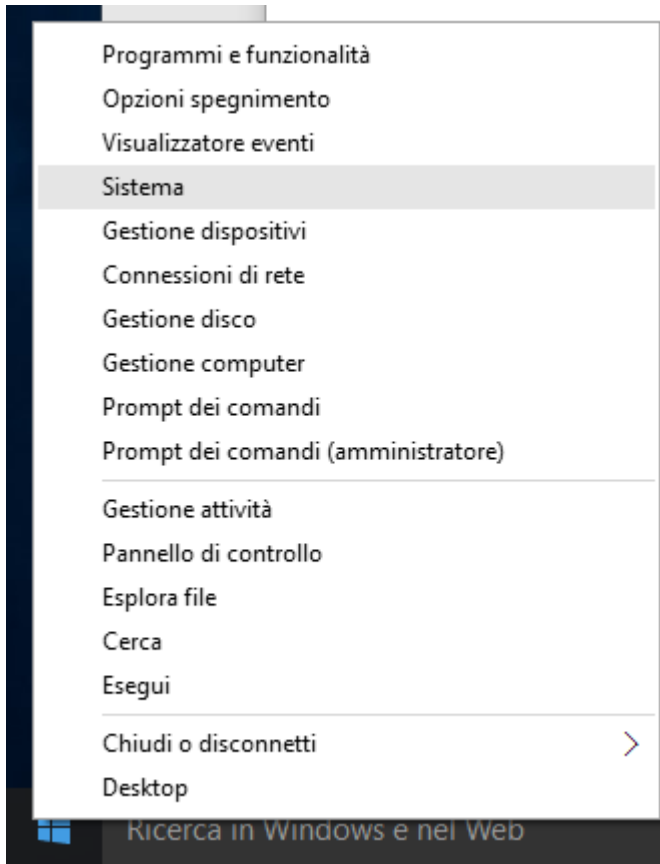
Scheda Tunnel Connessione alla rete locale (LAN)* 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:9d38:6abd:34fa:4753:68d9:c1f9
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::34fa:4753:68d9:c1f9%3
    Gateway predefinito . . . . . : ::
```

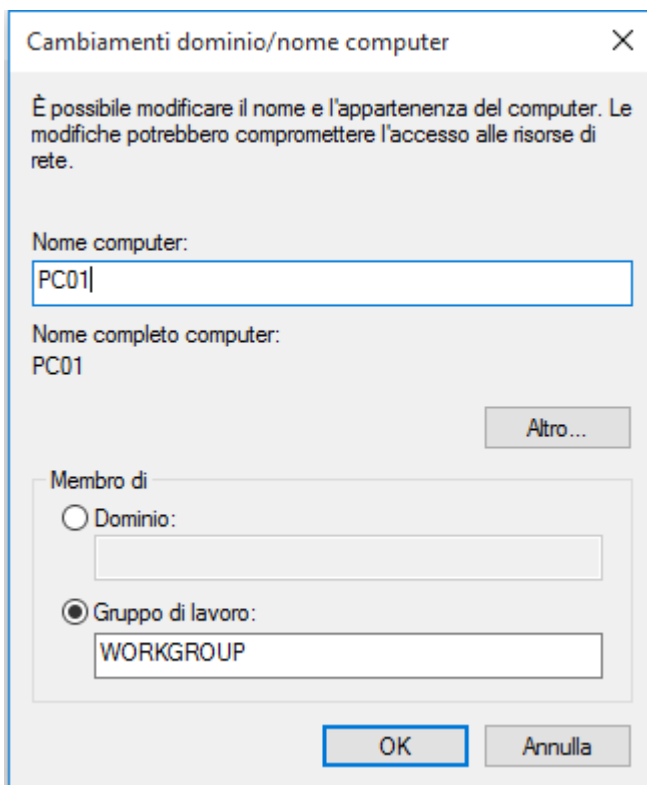
*Ipconfig /all*

*Route print*

Cambiamo il nome del computer prima di inserirlo nel dominio

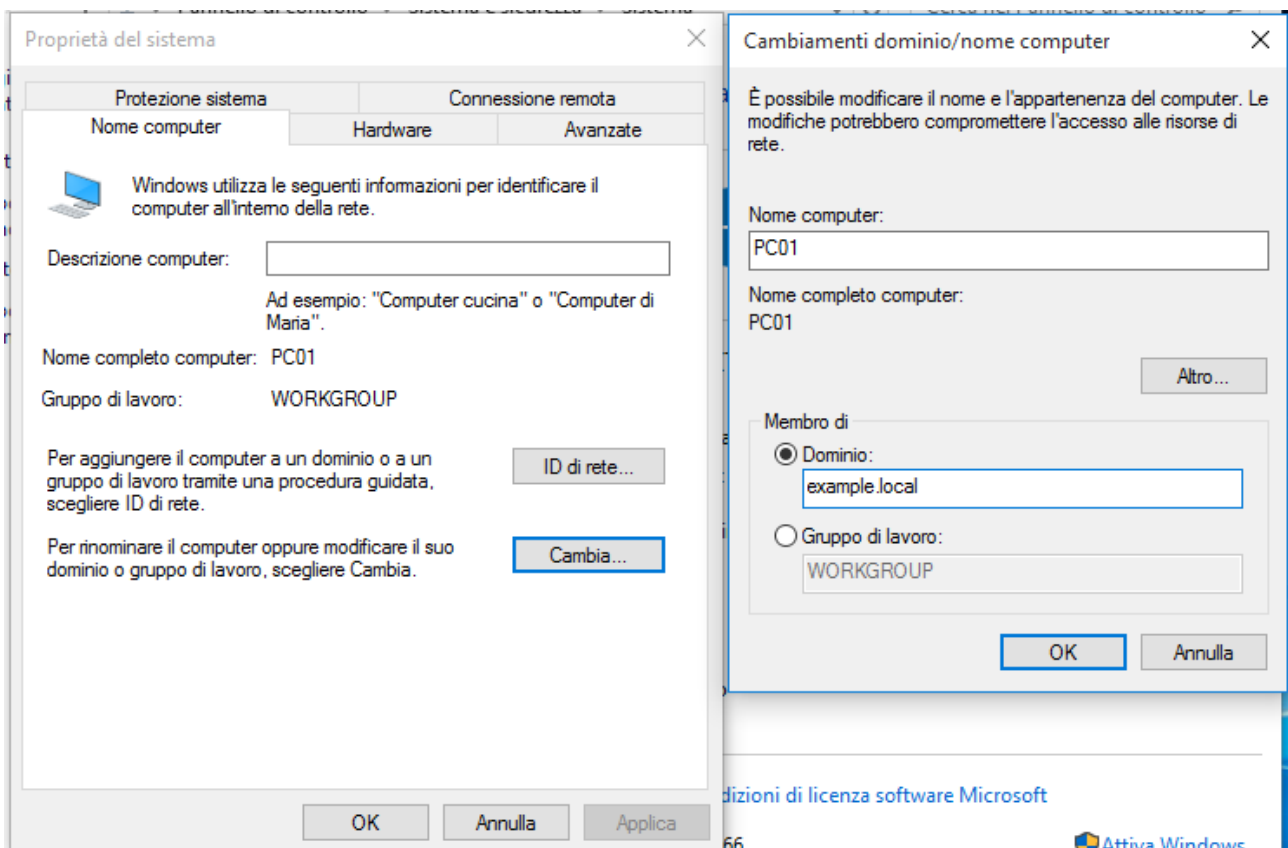


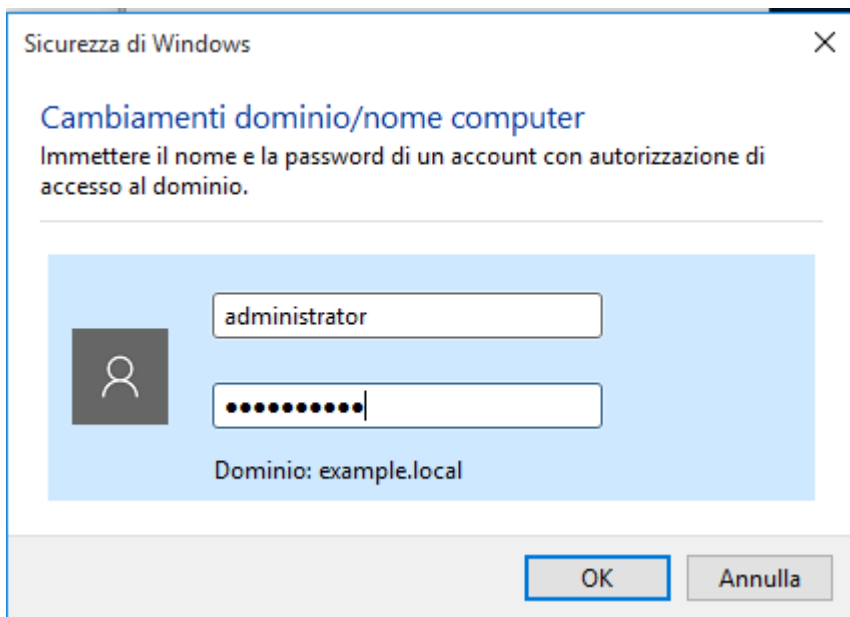
Rinominiamo il computer in PC01



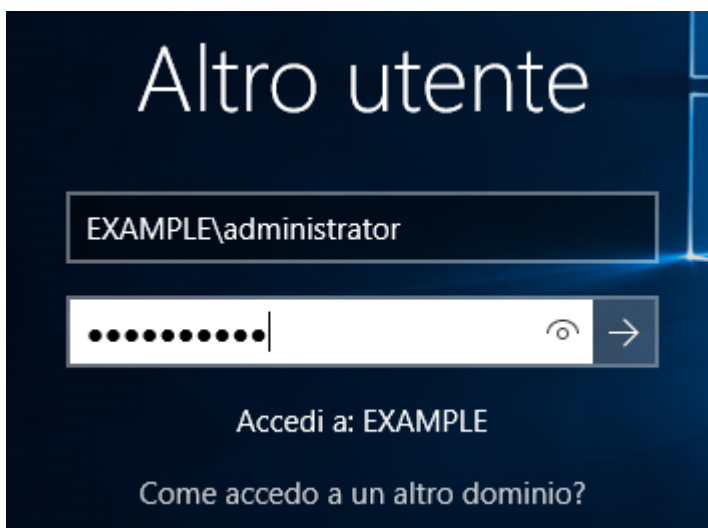
Riavviamo il computer.

Inseriamo il computer nel dominio





Effettuiamo il primo accesso al computer con le credenziali del dominio



Verifichiamo se funziona il DNS dinamico

```
ipconfig /registerdns
```

Andare a vedere /var/log/syslog del domain controller

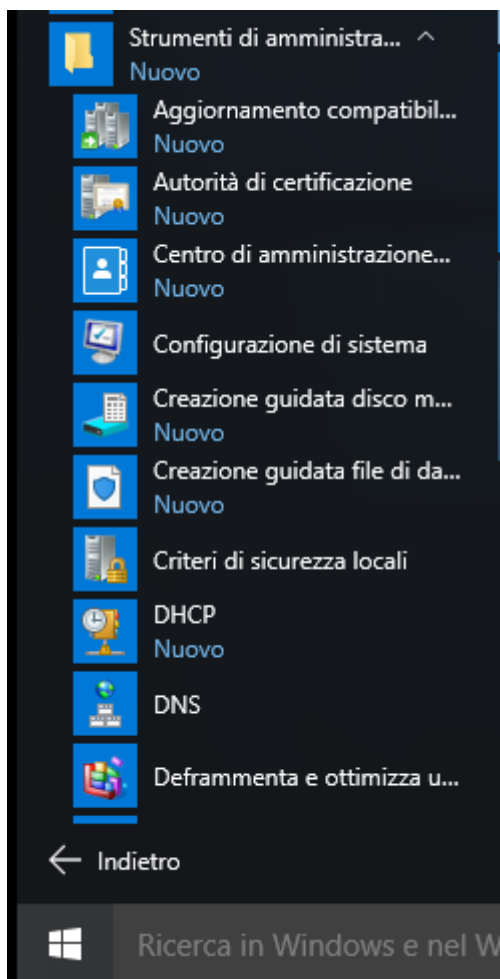
## Installiamo RSAT Strumenti di amministrazione remota per AD

Oltre a samba-tools è possibile usare gli strumenti di amministrazione remota per gestire il dominio Active directory. Questi strumenti si installano su un client windows.

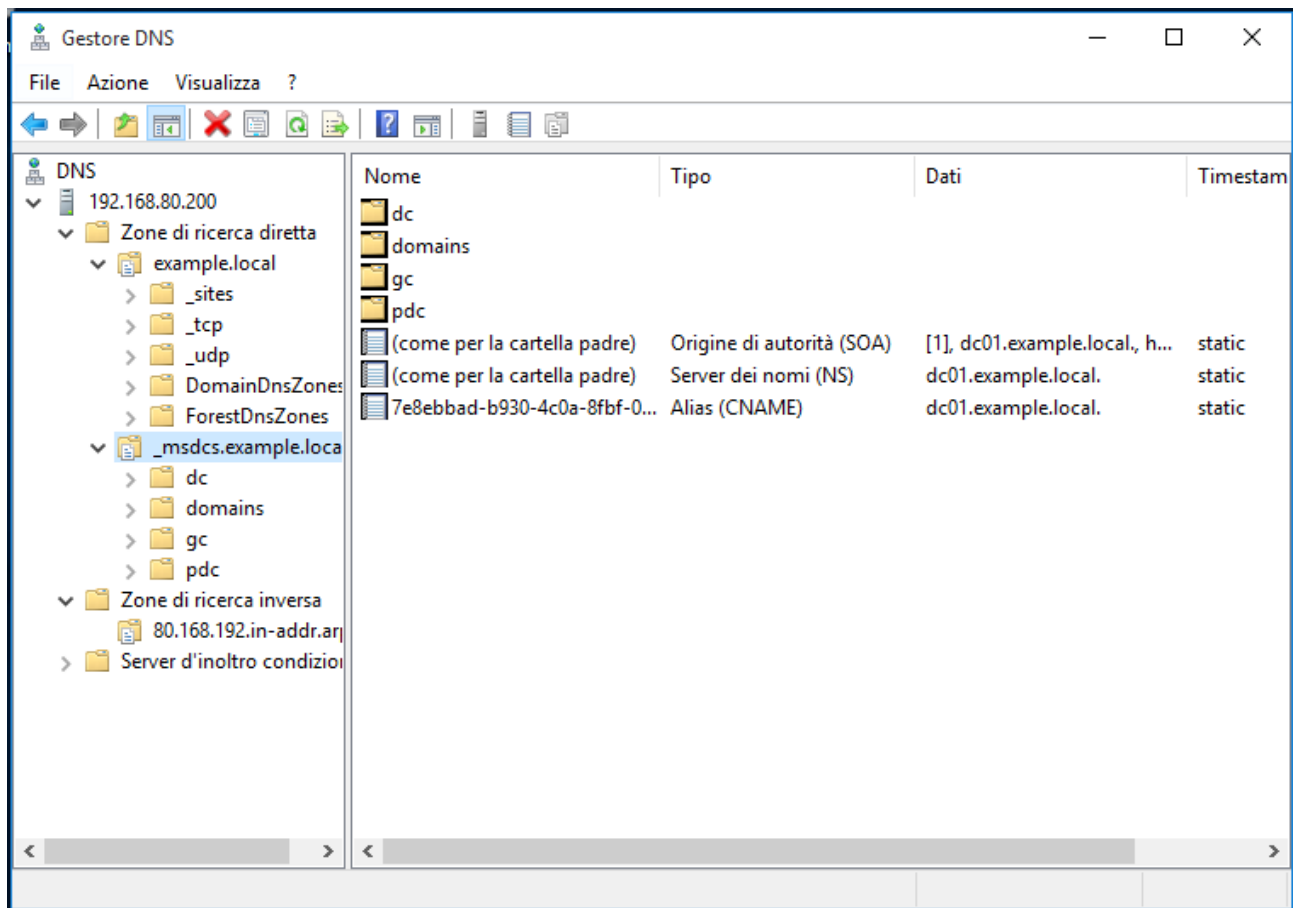
Windows10RSAT

<https://www.microsoft.com/it-IT/download/details.aspx?id=45520>

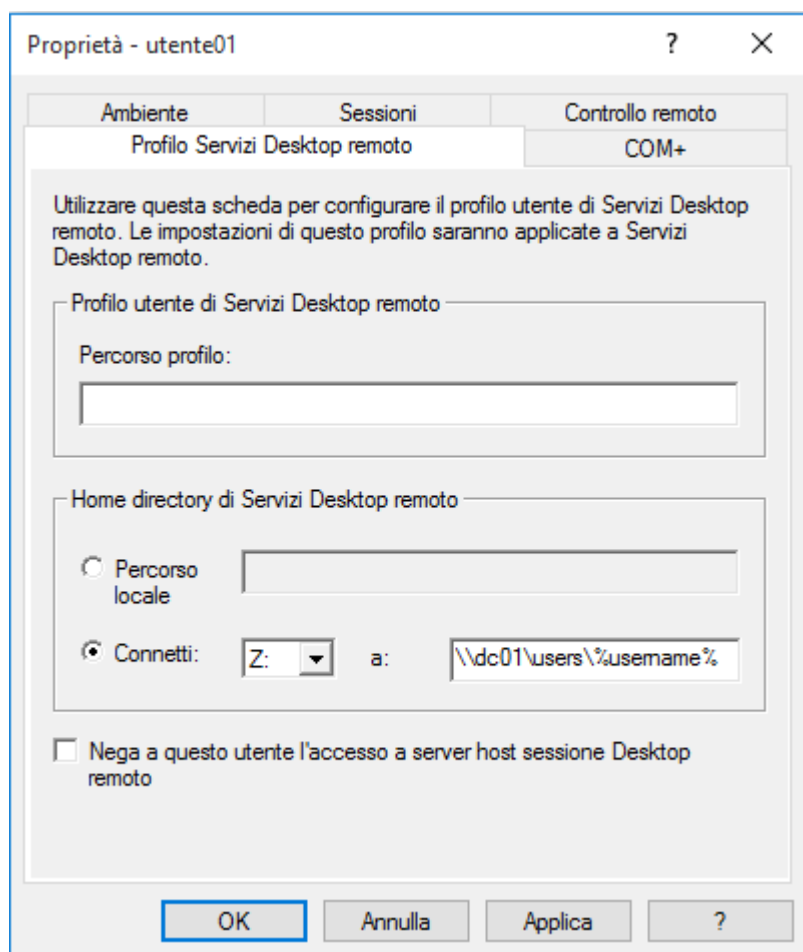
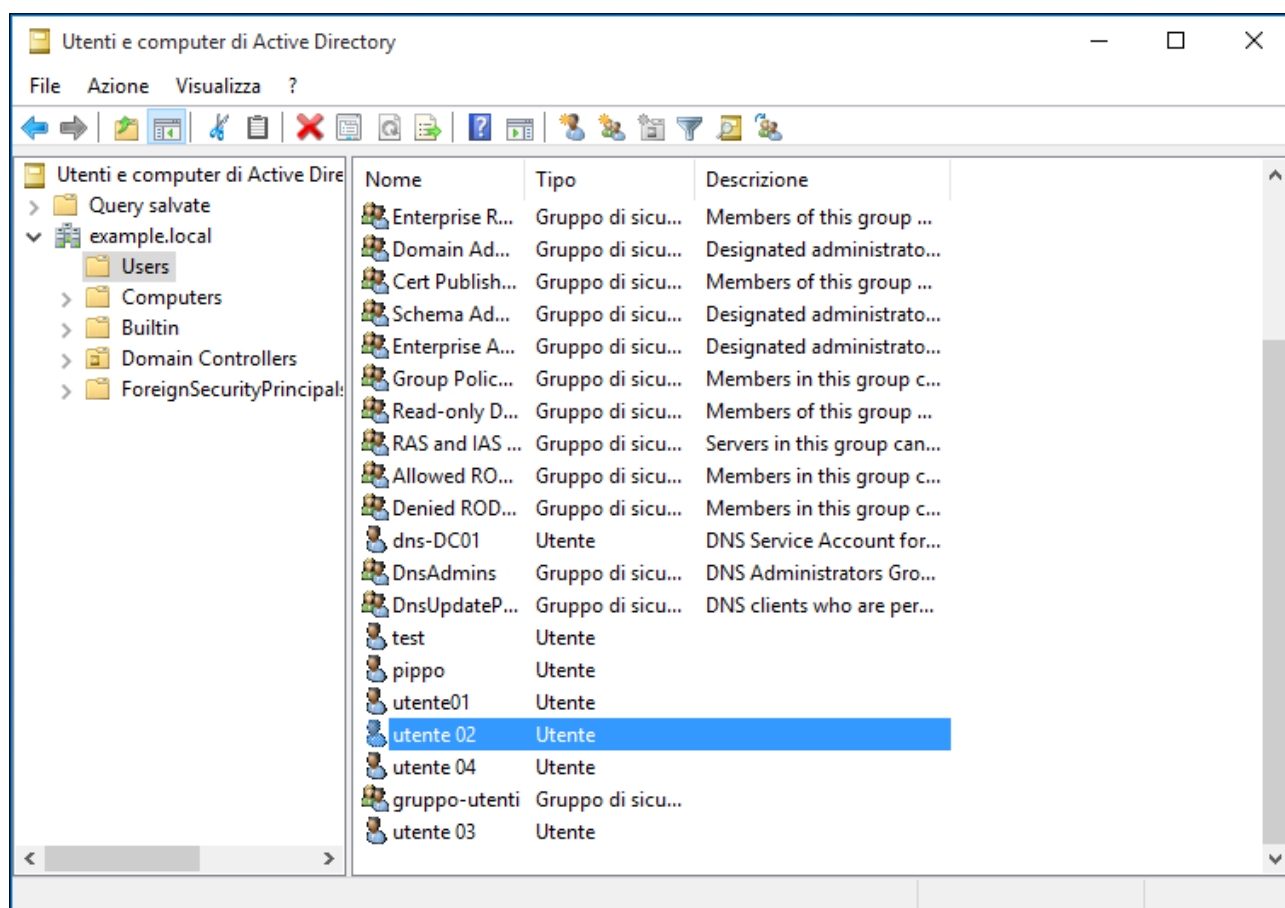
Dopo l'installazione bisogna riavviare il PC. Ci colleghiamo con le credenziali di Administrator del dominio example.local



Gestione del DNS

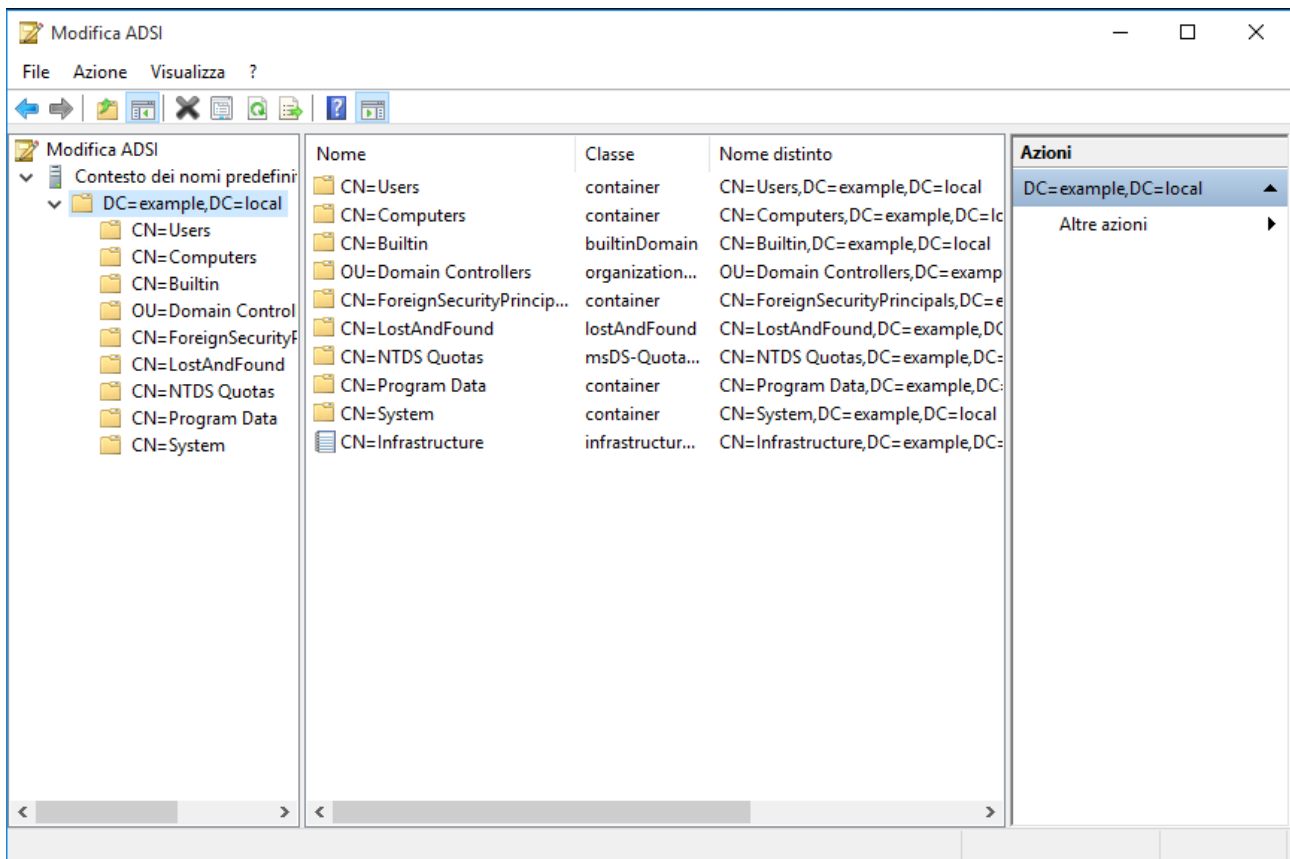


Gestione degli oggetti del dominio





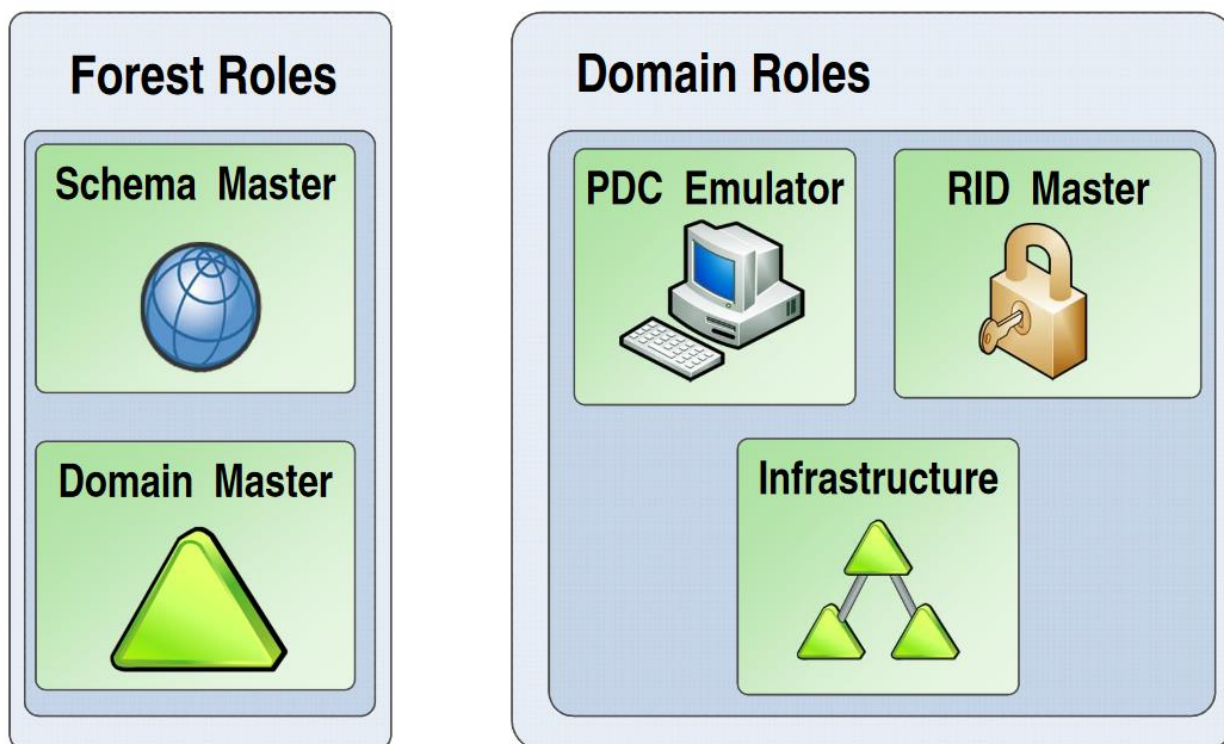
## Editor degli oggetti di Active Directory



## Ruoli FSMO (Flexible Single Master Operation)

Active Directory nasce per avere più domain controller. Per prevenire certi aggiornamenti che potrebbero creare conflitti esistono gli Operation Masters. Posso distribuire i ruoli a Domain controller differenti.

Visto che il ruolo di Operation Master può essere spostato da un server all'altro questo deve essere flessibile e può esistere un solo Operation Master.



I ruoli FSMO sono:

**Schema Master** – Questo ruolo ha il controllo completo sugli aggiornamenti dello schema. Gli aggiornamenti effettuati allo schema di Active Directory sullo Schema Master sono replicati sugli altri domain controller nel dominio. Per ogni Foresta può esistere un solo Schema Master.

**Domain Naming Master** – Questo ruolo si occupa dell'aggiunta o rimozione di domini da una foresta.

**Infrastructure Master** – Il ruolo di Infrastructure Master è il responsabile degli aggiornamenti degli oggetti SID e DN.

**PDC Emulator** – Uno dei ruoli più importanti è il PDC Emulator. Se stai utilizzando un ambiente in cui sono inseriti ancora dei server Windows NT4 BDC (Backup Domain Controller) questo ruolo emula il PDC (Primary Domain Controller). Se stai utilizzando Domain Controller con server windows 2000 / 2003 questo ruolo non è importante. Il PDC Emulator si occupa di modifiche password, blocco account e log password errate. Può esistere un solo PDC Emulator per dominio.

**RID Master** – Il RID (Relative Identifier) Master ha due ruoli: il primo è responsabile della gestione dei RID pools sui DC. Quando un DC viene avviato gli viene dato un set di RID per inserire gli oggetti creati su di esso. Quando questi finiscono il RID Master gli conferisce un nuovo blocco di RID. I RID sono usati come SID per i domini per creare un unico SID per i nuovi oggetti. Il RID Master gestisce anche il movimento di oggetti tra un dominio e un altro. Può esistere un solo RID master per Foresta [dcdiag /test:ridmanager /v](#)

Master operazioni

?

×

RID

Controller di dominio primario

Infrastruttura

Il master operazioni gestisce le allocazioni dei pool di RID ad altri controller di dominio. Un solo server del dominio ha questo compito.

Master operazioni:

DC01.example.local

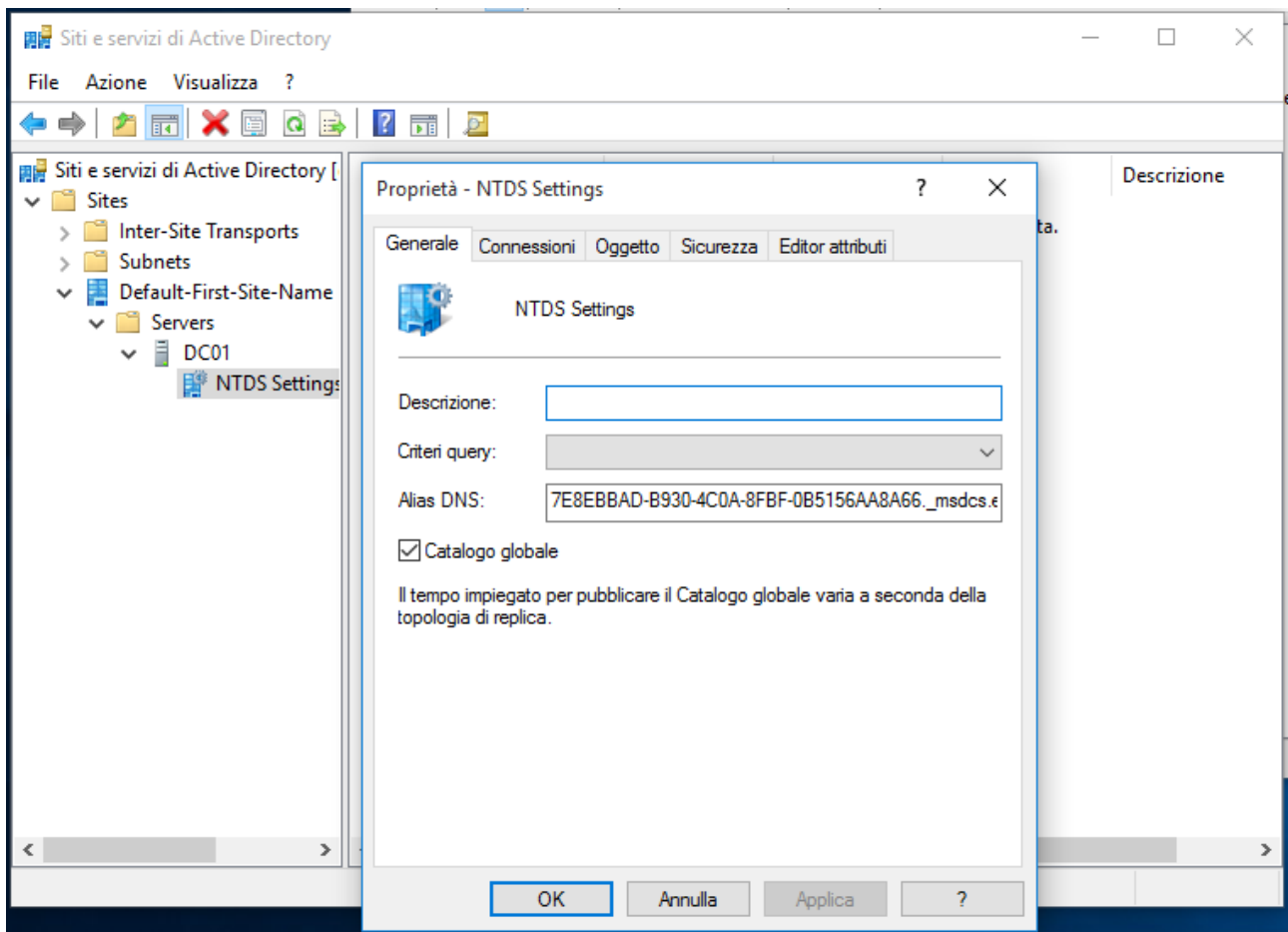
Per trasferire il ruolo di master operazioni al seguente computer, scegliere Cambia.

Cambia...

dc01.example.local

Chiudi

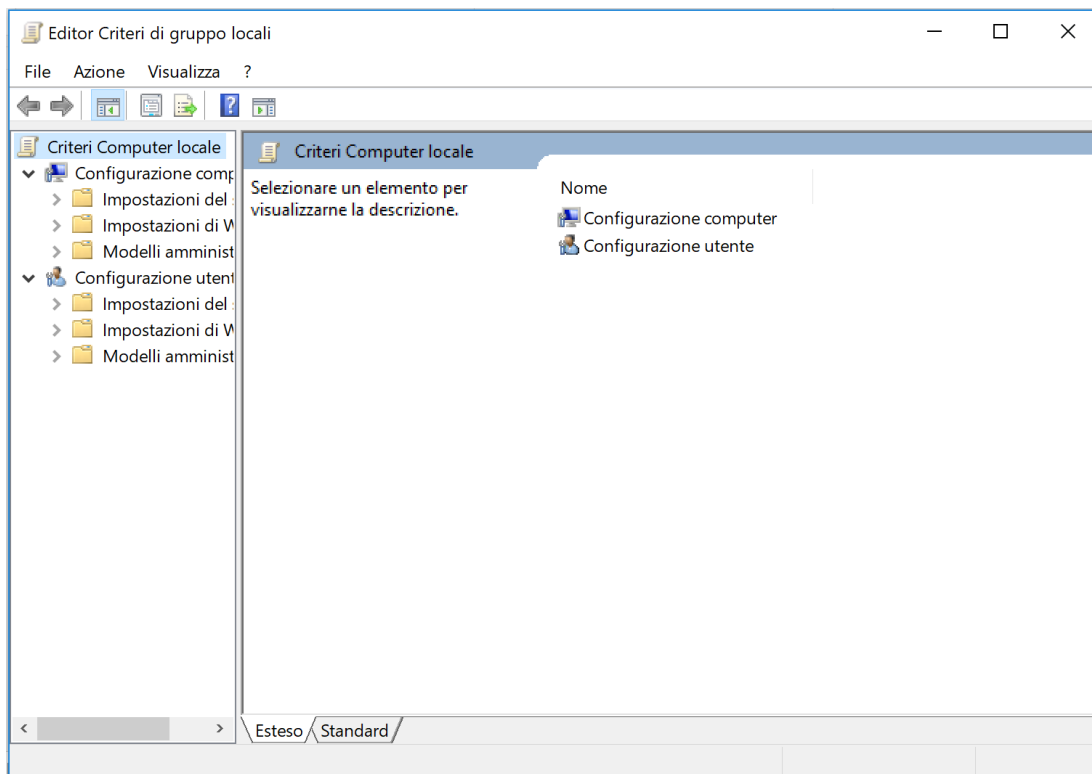
Annulla



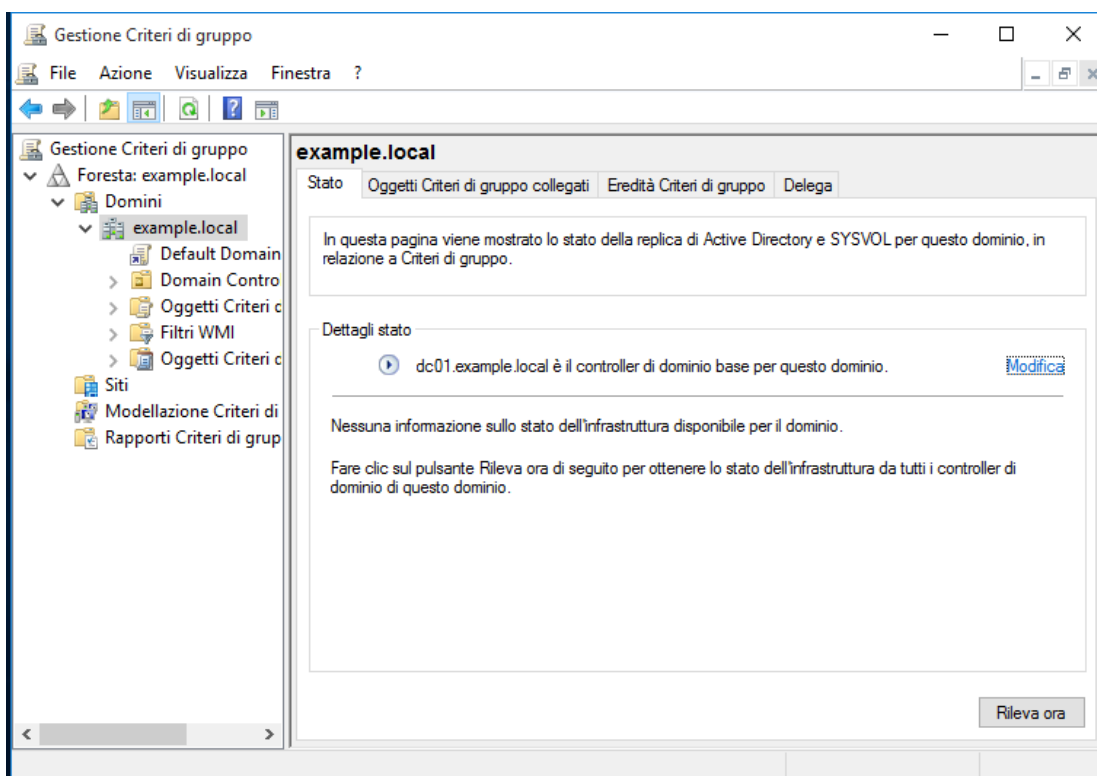
## Group Policy

Ogni computer può essere personalizzato usando le mmc local policy

Eseguiamo il comando gpedit.msc



Invece di usare le policy locali è possibile gestire le policy in modo centralizzato, usando le group policy.



Mappiamo delle cartelle con le Policy.

Dove vanno a finire le policy?

<\\dc01\\sysvol\\example.local\\Policies\\{6AC1786C-016F-11D2-945F-00C04FB984F9}>

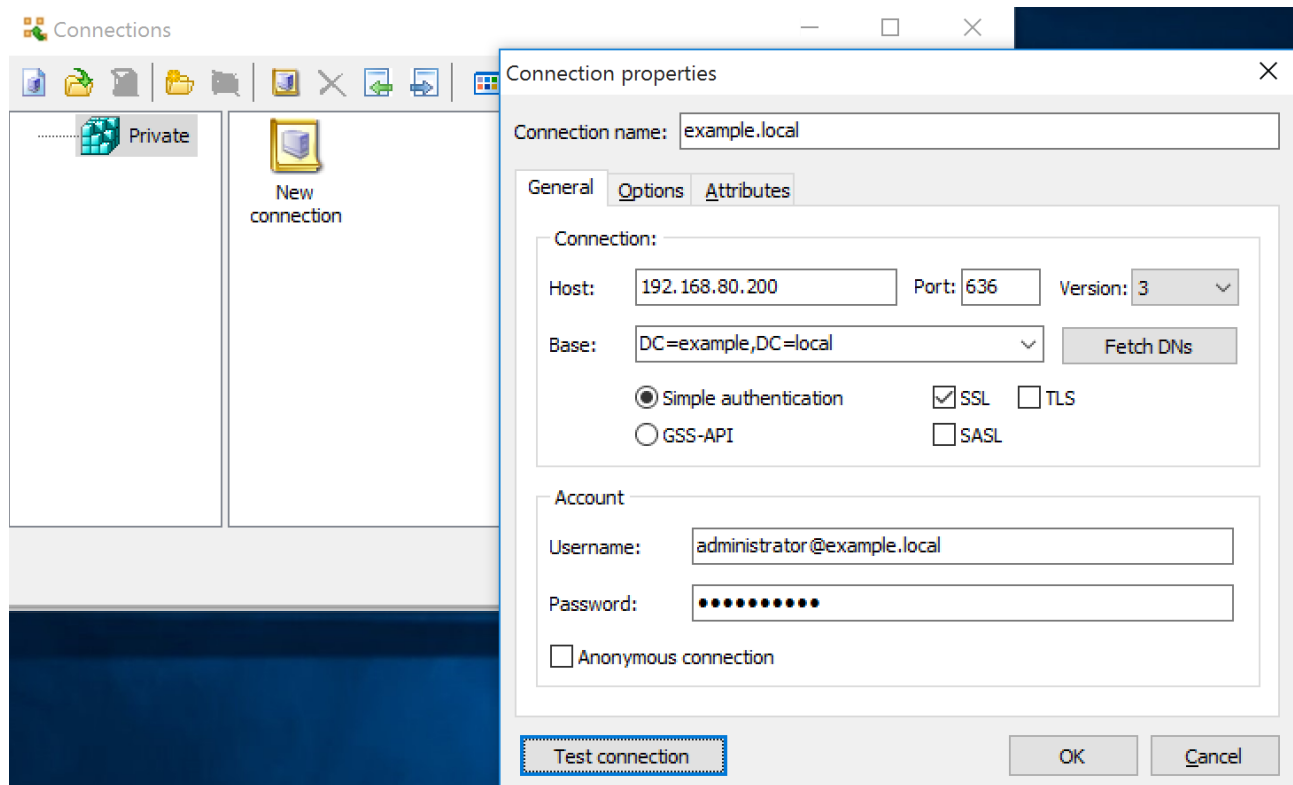
Le loopback policy permettono di elaborare le policy di computer e utenti presenti in OU differenti.

Computer Configuration/Administrative Templates/System/Group Policy

## LdapAdmin

LdapAdmin non richiede nessuna installazione.

Dopo averlo eseguito creiamo una nuova connessione.



## Query Ldap

<https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

| Operator | Meaning                                    |
|----------|--|
| =        | Equality                                   |
| >=       | Greater than or equal to (lexicographical) |
| <=       | Less than or equal to (lexicographical)    |

| Operator | Meaning                                |
|----------|--|
| &        | AND, all conditions must be met        |
|          | OR, any of the conditions must be met  |
| !        | NOT, the clause must evaluate to False |

## Esempi di Filtri

| Query  | LDAP Filter   |
|--|---|
| All user objects                               | (&(objectCategory=person)(objectClass=user))  |
| All user objects (Note 1)                      | (sAMAccountType=805306368)  |
| All computer objects                           | (objectCategory=computer)   |
| All contact objects                            | (objectClass=contact)   |
| All group objects                              | (objectCategory=group)  |
| All organizational unit objects                | (objectCategory=organizationalUnit)   |
| All container objects                          | (objectCategory=container)  |
| All builtin container objects                  | (objectCategory=builtinDomain)  |
| All domain objects                             | (objectCategory=domain)   |
| Computer objects with no description           | (&(objectCategory=computer)(!(description=*)))  |
| Group objects with a description               | (&(objectCategory=group)(description=*))  |
| Users with cn starting with "Joe"              | (&(objectCategory=person)(objectClass=user)(cn=Joe*))   |
| Phone numbers in form (xxx) xxx-xxx            | (telephoneNumber=(*)*-*)  |
| Groups with cn starting with "Test" or "Admin" | (&(objectCategory=group)( (cn=Test*)(cn=Admin*)))   |
| All users with both a first and last name.     | (&(objectCategory=person)(objectClass=user)(givenName=*)(sn=*))   |
| All users with direct reports but no manager   | (&(objectCategory=person)(objectClass=user)(directReports=*)(!(manager=*))                                    |
| All users with specified email address         | (&(objectCategory=person)(objectClass=user)( (proxyAddresses=*:jsmith@company.com)(mail=jsmith@company.com))) |

|  |  |
|--|--|
| All users with Logon Script: field occupied  | (&(objectCategory=person)(objectClass=user)(scriptPath=*))                                       |
| Objects with sAMAccountName that begins with "x", "y", or "z"                        | (sAMAccountName>=x)  |
| Objects with sAMAccountName that begins with "a" or any number or symbol except "\$" | (&(sAMAccountName<=a)(!(sAMAccountName=\$*)))  |
| All users with "Do not require kerberos preauthentication" enabled                   | (&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=4194304)) |
| Accounts trusted for delegation (unconstrained delegation)                           | (userAccountControl:1.2.840.113556.1.4.803:=524288)  |
| Accounts that are sensitive and not trusted for delegation                           | (userAccountControl:1.2.840.113556.1.4.803:=1048576)   |
| All users with "primary" group other than "Domain Users"                             | (&(objectCategory=person)(objectClass=user)(!(primaryGroupID=513)))                              |
| All servers  | (&(objectCategory=computer)(operatingSystem=*server*))   |
| All objects protected by AdminSDHolder   | (adminCount=1)   |
| All trusts established with a domain   | (objectClass=trustedDomain)  |
| All Group Policy objects   | (objectCategory=groupPolicyContainer)  |
| All service connection point objects   | (objectClass=serviceConnectionPoint)   |



Search











Path: DC=example,DC=local Browse...

Search Custom Options Regular Expressions

Filter: (&(objectCategory=person)(objectClass=user)) Start Clear all

Save Delete

(&(objectCategory=person)(objectClass=user)) x

| DN  |  |
|---|--|
|  CN=Administrator,CN=Users,DC=example,DC=local |  |
|  CN=utente 02,CN=Users,DC=example,DC=local     |  |
|  CN=utente 03,CN=Users,DC=example,DC=local     |  |
|  CN=utente 04,CN=Users,DC=example,DC=local     |  |
|  CN=dns-DC01,CN=Users,DC=example,DC=local      |  |
|  CN=utente01,CN=Users,DC=example,DC=local      |  |
|  CN=krbtgt,CN=Users,DC=example,DC=local        |  |
|  CN=Guest,CN=Users,DC=example,DC=local         |  |
|  CN=pippo,CN=Users,DC=example,DC=local         |  |
|  CN=test,CN=Users,DC=example,DC=local        |  |
|   |  |
|   |  |
|   |  |

Server: 192.168.80.200 10 object(s) retrieved.

## Vediamo lo schema

Gli attributi e le classi

Schema Viewer

Search: person

☐ Whole words only

person

nTFRSSettings

nTFRSSubscriber

nTFRSSubscriptions

oncRpc

organization

organizationalPerson

organizationalRole

organizationalUnit

packageRegistration

person

physicalLocation

pkiCertificateTemplate

pkiEnrollmentService

posixAccount

posixGroup

printQueue

queryPolicy

remoteMailRecipient

remoteStorageServicePoin

residentialPerson

rFC822LocalPart

rIDManager

rIDSet

room

rpcContainer

rpcEntry

**Name: person**

Description:

Oid: 2.5.6.6

Kind: Structural

Superior: [top](#)

Must:

Inherited from: [top](#)

[instanceType](#)

[nTSecurityDescriptor](#)

[objectCategory](#)

[objectClass](#)

May:

[attributeCertificateAttribute](#)

[seeAlso](#)

[serialNumber](#)

[sn](#)

[telephoneNumber](#)

[userPassword](#)

Inherited from: [top](#)

[adminDescription](#)

[adminDisplayName](#)

[allowedAttributes](#)

[allowedAttributesEffective](#)

[allowedChildClasses](#)

[allowedChildClassesEffective](#)

[bridgeheadServerListBL](#)

Server: 192.168.80.200

Object Classes

person

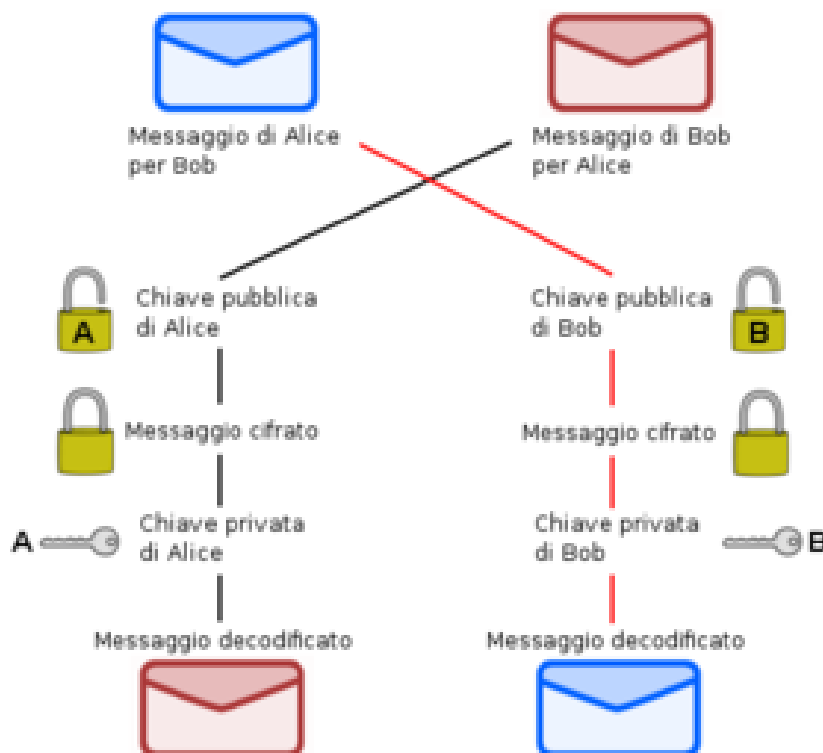
## Crittografia Asimmetrica

La crittografia Asimmetrica si basa su 2 chiavi:

- La chiave pubblica, che deve essere distribuita;
- La chiave privata, appunto personale e segreta;

Due degli usi più conosciuti della crittografia asimmetrica sono:

- crittografia a chiave pubblica, nel quale i messaggi sono crittografati con la chiave pubblica del destinatario. Il messaggio non può essere decriptato da chi non possiede la chiave privata corrispondente, che viene così presupposto di essere il proprietario di quella chiave e la persona associata con la chiave pubblica. Questo è utilizzato nel tentativo di garantire la riservatezza;
- firma digitale, in cui un messaggio viene firmato con la chiave privata del mittente e può essere verificato da chiunque abbia accesso alla chiave pubblica del mittente. Questa verifica dimostra che il mittente ha avuto accesso alla chiave privata ed è pertanto probabile che sia la persona associata alla chiave pubblica. Questo assicura anche che il messaggio non è stato manomesso, ogni manipolazione del messaggio comporterà modifiche al digest, che altrimenti rimarrebbe invariato tra il mittente e ricevente

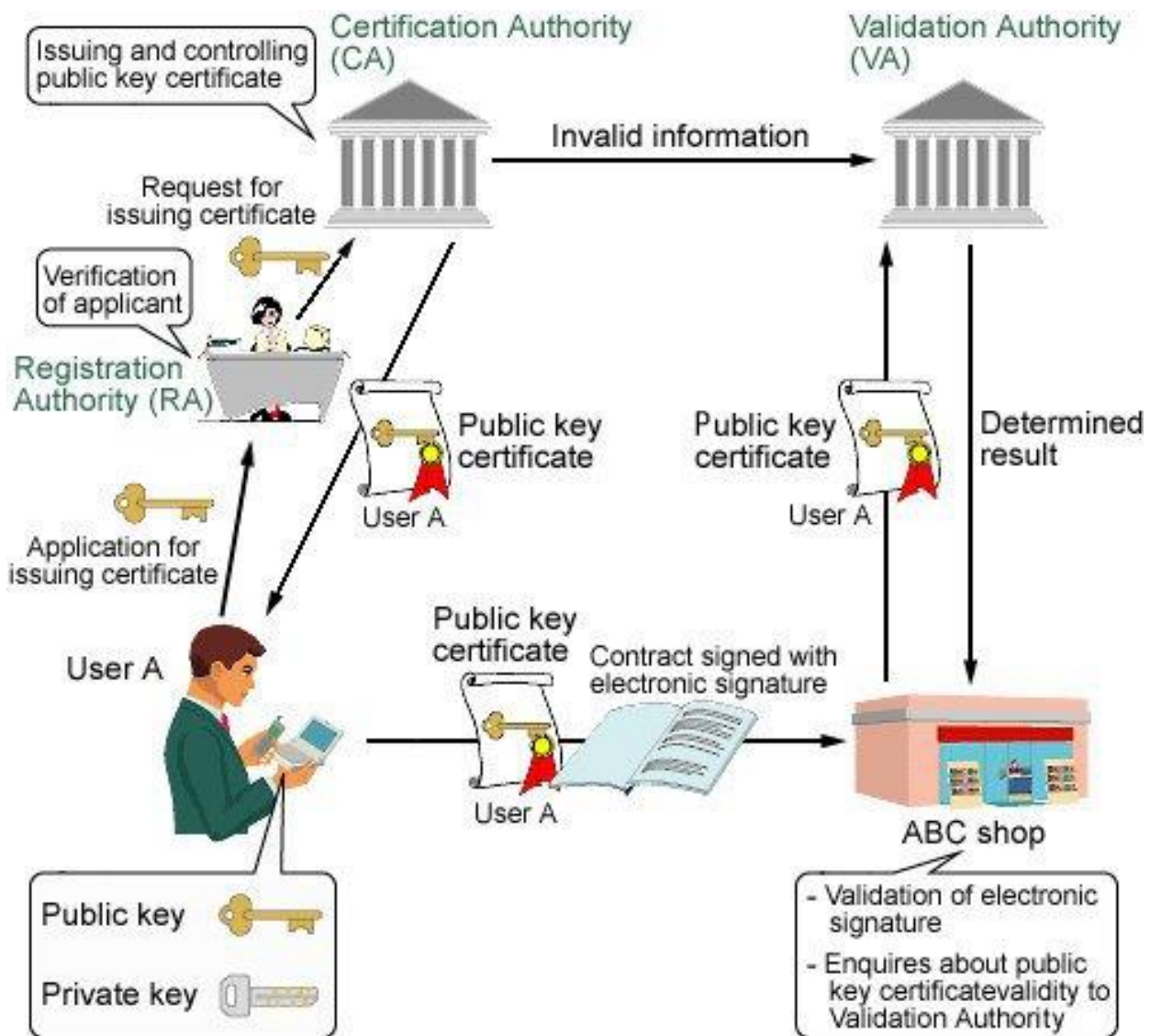


## Certification authority

E' un soggetto abilitato a rilasciare certificati digitali tramite una procedura standard.

Le CA usano una infrastruttura a chiave pubblica (PKI) organizzata nel seguente modo:

- Sistema di Certification authority (CA): root CA
- Sistema di Registration authority (RA): registrazione e autenticazione degli utenti che richiedono un certificato
- Certificate Server (VA) che attesta la corrispondenza certificato/entità della CA



Alice e Bob vogliono scambiarsi messaggi firmati e crittografati; a tale scopo entrambi creano la loro coppia di chiavi e pubblicano quelle pubbliche su un keyserver. Quindi Alice scrive un messaggio per Bob, lo firma con la propria chiave privata e lo cripta con la chiave pubblica di Bob, quindi il messaggio viene inviato. In ricezione Bob decripta il messaggio con la propria chiave privata e verifica la firma con la chiave pubblica intestata ad Alice. Bob a questo punto sa due cose:

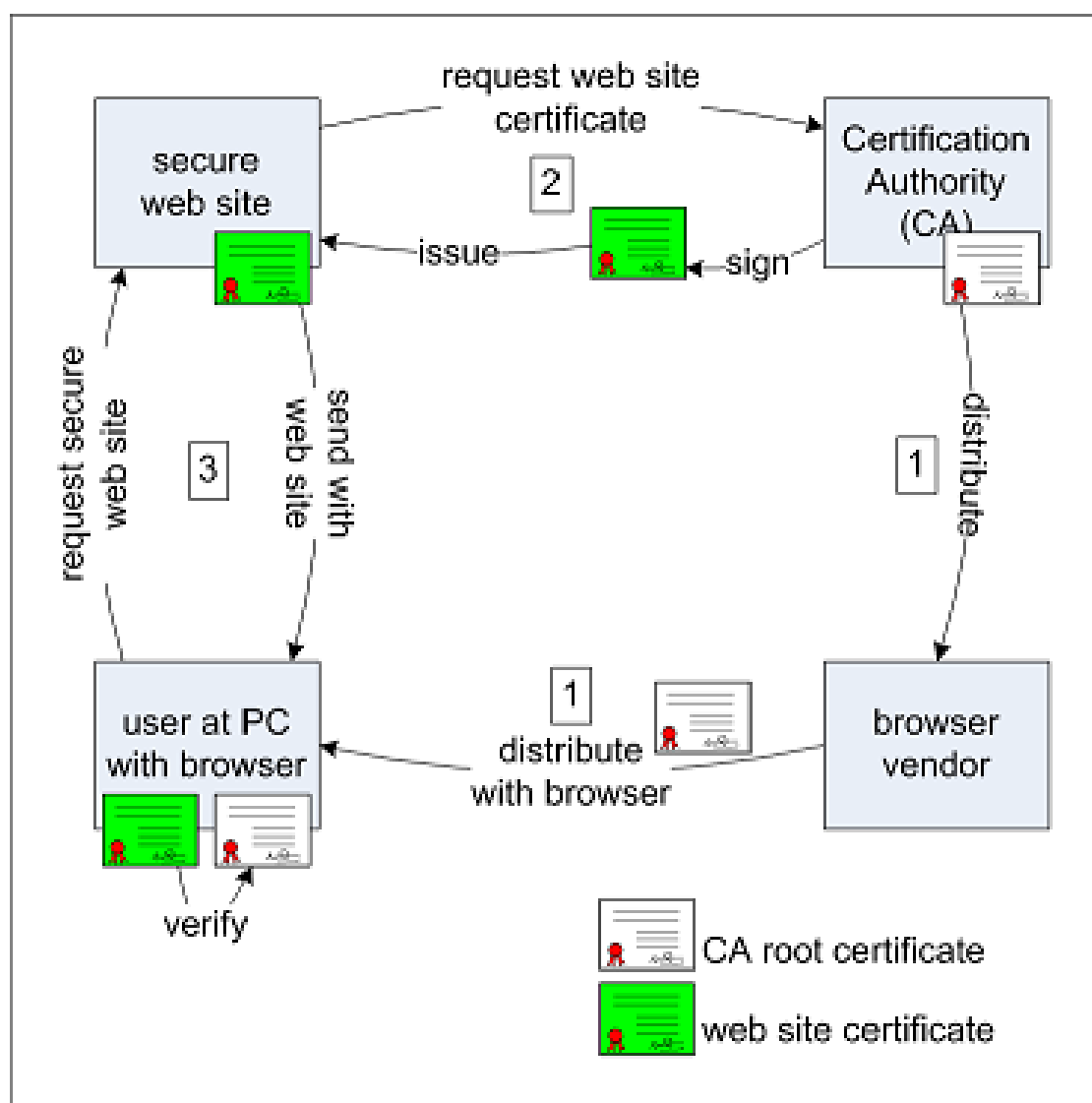
- il messaggio era diretto a lui perché è riuscito a decifrarlo con la propria chiave privata
- il messaggio è stato firmato con la chiave privata relativa alla chiave pubblica che lui ha usato per verificare la firma.

Nel contempo Bob non ha alcuna garanzia che la chiave sia realmente di proprietà di Alice. Continuando l'esempio, supponiamo che una terza persona, Mallory, riesca ad intercettare la comunicazione in cui Bob ottiene la chiave di Alice e riesca a sostituirla con la sua chiave pubblica in cui si spaccia per Alice. Bob non ha alcun modo per scoprire l'inganno. Per risolvere situazioni di questo tipo nascono le CA che si fanno

carico di verificare e garantire la corrispondenza fra chiave e proprietario. Quando un utente richiede un certificato, la CA verifica la sua identità, quindi crea un Documento digitale firmato con la chiave privata della CA e pubblicato. Nell'esempio precedente supponiamo che Alice e Bob si facciano firmare le loro chiavi da una CA che entrambi ritengono attendibile. In questo caso l'attacco di Mallory non è più possibile in quanto non è in grado di riprodurre la firma della CA.

La CA root si trova al vertice della certification authority. Questa certifica le Sub-CA. La CA root si genera da sola la chiave privata e pubblica e genera e gestisce i certificati per gli altri.

Cosa succede quando visualizziamo un sito web con certificato SSL



Tramite la mmc Certificati è possibile visualizzare le CA root riconosciute dal proprio computer.

Alcuni browser non usano il repository di Windows.

Console1 - [Radice console\Certificati - Utente corrente\Autorità di certificazione radice attendibili\Certificati]

FileAzioneVisualizzaPreferitiFinestra?

Radice console

- ▼ Certificati - Utente corrente
  - ▼ Personale
    - Certificati
  - ▼ Autorità di certificazione
    - Certificati
  - > Attendibilità per l'organi...
  - > Autorità di certificazione
  - > Oggetto utente Active D...
  - > Autori attendibili
  - > Certificati non disponibi...
  - > Autorità di certificazione
  - > Persone attendibili
  - > Emittenti per autenticazi...
  - > Altri utenti
  - > Local NonRemovable Ce...
  - > MSIEHistoryJournal
  - > Radici attendibili smart c...

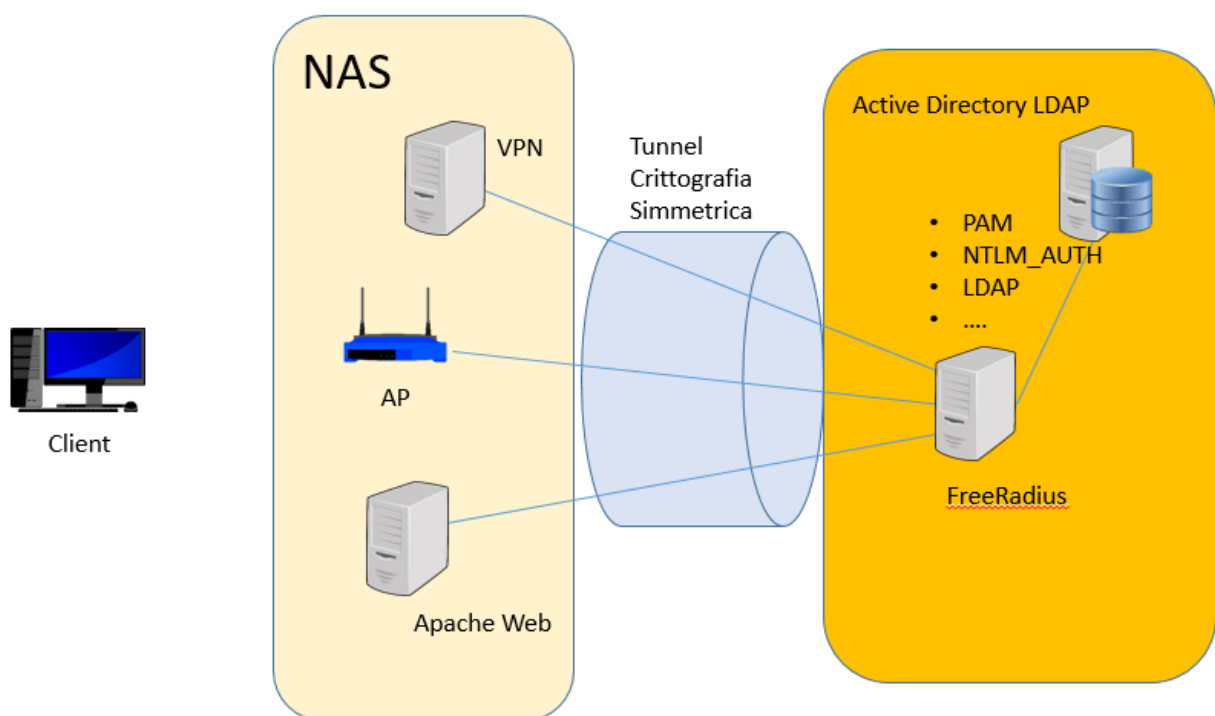
| Rilasciato a                          | Emesso da                                | Data scadenza | Scopi |
|---------------------------------------|--|---------------|-------|
| Actalis Authentication Root CA        | Actalis Authentication Root CA           | 22/09/2030    | Auter |
| AddTrust External CA Root             | AddTrust External CA Root                | 30/05/2020    | Auter |
| Altus Local client Certificate Aut... | Altus Local client Certificate Author... | 17/09/2037    | <Tut  |
| Baltimore CyberTrust Root             | Baltimore CyberTrust Root                | 13/05/2025    | Auter |
| Certum CA                             | Certum CA                                | 11/06/2027    | Auter |
| Certum Trusted Network CA             | Certum Trusted Network CA                | 31/12/2029    | Auter |
| Class 3 Public Primary Certificati... | Class 3 Public Primary Certification ... | 02/08/2028    | Posta |
| COMODO RSA Certification Aut...       | COMODO RSA Certification Autho...        | 19/01/2038    | Auter |
| Copyright (c) 1997 Microsoft Corp.    | Copyright (c) 1997 Microsoft Corp.       | 31/12/1999    | Time: |
| DigiCert Assured ID Root CA           | DigiCert Assured ID Root CA              | 10/11/2031    | Auter |
| DigiCert Global Root CA               | DigiCert Global Root CA                  | 10/11/2031    | Auter |
| DigiCert Global Root G2               | DigiCert Global Root G2                  | 15/01/2038    | Auter |
| DigiCert High Assurance EV Roo...     | DigiCert High Assurance EV Root CA       | 10/11/2031    | Auter |
| DST Root CA X3                        | DST Root CA X3                           | 30/09/2021    | Posta |
| Entrust Root Certification Autho...   | Entrust Root Certification Authority     | 27/11/2026    | Auter |
| Entrust Root Certification Autho...   | Entrust Root Certification Authorit...   | 07/12/2030    | Auter |
| Equifax Secure Certificate Autho...   | Equifax Secure Certificate Authority     | 22/08/2018    | Posta |

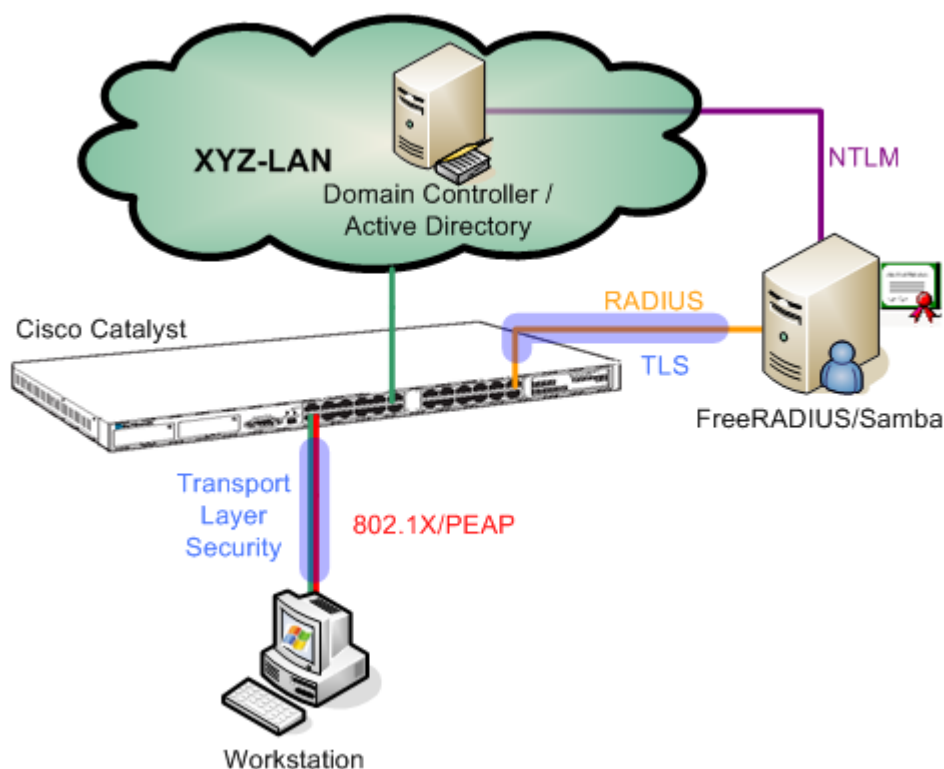
L'archivio Autorità di certificazione radice attendibili contiene 49 certificati.

## 4 - Il servizio Radius Server

RADIUS (Remote Authentication Dial-In User Service) è un protocollo AAA (authentication, authorization, accounting) utilizzato in applicazioni di accesso alle reti.

Le parti che costituiscono l'architettura RADIUS sono un server di accesso alla rete , comunemente indicato con la sigla NAS (Network Access Server) e un server che si occupa di effettuare l'autenticazione dell'utente sulla rete , il server RADIUS appunto. Solitamente il NAS è un router o Access Point collegato direttamente al server RADIUS che si occupa di controllare il pacchetto contenente le credenziali di accesso dell'utente (username e password). Tali credenziali vengono confrontate con quelle esistenti in un database relativamente all'utente : in caso di matching l'utente autenticato può accedere ai servizi della rete , in caso contrario il protocollo prevede la notifica di un messaggio di errore. La comunicazione fra il NAS ed il server RADIUS è crittografata usando una chiave segreta condivisa da entrambi (secret key) che deve essere opportunamente creata sia sul NAS che sul server RADIUS e mantenuta riservata.





Uno dei compiti del NAS può essere quello di assegnare al client remoto, dopo l'avvenuta convalida delle credenziali di accesso alla rete dell'utente, un indirizzo IP compatibile con il range di IP disponibili (il NAS spesso funge da server DHCP, funzionalità questa integrata in molti routers presenti sul mercato).

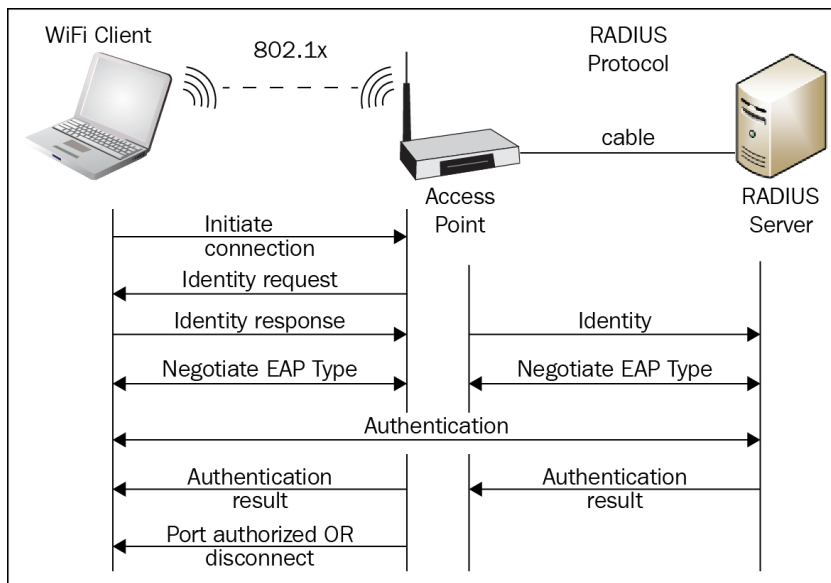
I protocolli di autenticazione dell'utente remoto sul server RADIUS storici sono:

- PAP (password authentication protocol): Il metodo utilizzato dal protocollo PAP è di tipo 2-way handshake. Quando la connessione è stabilita viene inviata da parte del client una coppia Username e Password. Il server confronta i dati ricevuti con quelli nel proprio database quindi autentica o rifiuta il client.
- CHAP (challenge handshake authentication protocol): Il protocollo CHAP utilizza un metodo 3-way handshake per verificare l'identità del client e questo processo può essere ripetuto più volte lungo la durata della connessione. Una volta stabilito il collegamento il server invia una stringa contenente dei caratteri ed il proprio nome, chiamata "challenge". Il client invia in risposta una stringa calcolata tramite una funzione hash one-way. Il server controlla che l'hash generato anch'esso tramite la stessa funzione one-way e se corretto autentica il client altrimenti termina la connessione.

Il database delle utenze che fornisce il servizio di backend come supporto al server RADIUS può essere sia un semplice file di testo (ad es il file /etc/passwd di UNIX) sia un DB dedicato come LDAP o un altro database (PostgreSQL, MySQL).

Per i problemi di sicurezza insiti nei protocolli PAP e CHAP è stato definito il protocollo Extensible Authentication Protocol (EAP) che rende RADIUS capace di lavorare con una varietà di schemi di autenticazione, inclusi chiave pubblica, Kerberos e smart card.





L'access point, ad esempio, agisce da traduttore EAP-RADIUS tra il client wireless e il RADIUS server, utilizzando il protocollo EAP per la comunicazione con il client e il protocollo RADIUS per la comunicazione con il server RADIUS. L'access point incapsula quindi le informazioni (come lo username o la chiave pubblica) in un pacchetto RADIUS che inoltra al server RADIUS. Quando il server rimanda una delle possibili risposte (Access-Accept/Reject/Challenge), l'access point spacchetta il pacchetto RADIUS e inoltra la risposta al client in un pacchetto EAP.

<https://aswinchandran.wordpress.com/eap/>

Di seguito alcuni protocolli metodi di autenticazione EAP:


- **EAP-MD5:** MD5-Challenge requires username/password, and is equivalent to the PPP CHAP protocol [RFC1994]. This method does not provide dictionary attack resistance, mutual authentication, or key derivation, and has therefore little use in a wireless authentication environment.
- **Lightweight EAP (LEAP):** A username/password combination is sent to a Authentication Server (RADIUS) for authentication. Leap is a proprietary protocol developed by Cisco, and is not considered secure. Cisco is phasing out LEAP in favor of PEAP. The closest thing to a published standard can be found [here](#).
- **EAP-TLS:** Creates a TLS (**Transport Layer Security**) session within EAP, between the Supplicant and the Authentication Server. Both the server and the client(s) need a valid (x509) certificate, and therefore a PKI. This method provides authentication both ways. EAP-TLS is described in [RFC2716].
- **EAP-TTLS:** Sets up a encrypted TLS-tunnel for safe transport of authentication data. Within the TLS tunnel, (any) other authentication methods may be used. Developed by Funk Software and Meetinghouse, and is currently an IETF draft.
- **Protected EAP (PEAP):** Uses, as EAP-TTLS, an encrypted TLS-tunnel. Supplicant certificates for both EAP-TTLS and EAP-PEAP are optional, but server (AS) certificates are required. Developed by Microsoft, Cisco, and RSA Security, and is currently an IETF draft.

- *EAP-MSCHAPv2*: Requires username/password, and is basically an EAP encapsulation of MS-CHAP-v2 [\[RFC2759\]](#). Usually used inside of a PEAP-encrypted tunnel. Developed by Microsoft, and is currently an IETF draft.

Nell'infrastruttura wireless di Ateneo viene usato PEAP con MS-CHAPv2 . PEAP richiede che sul server Radius sia presente un certificato valido.

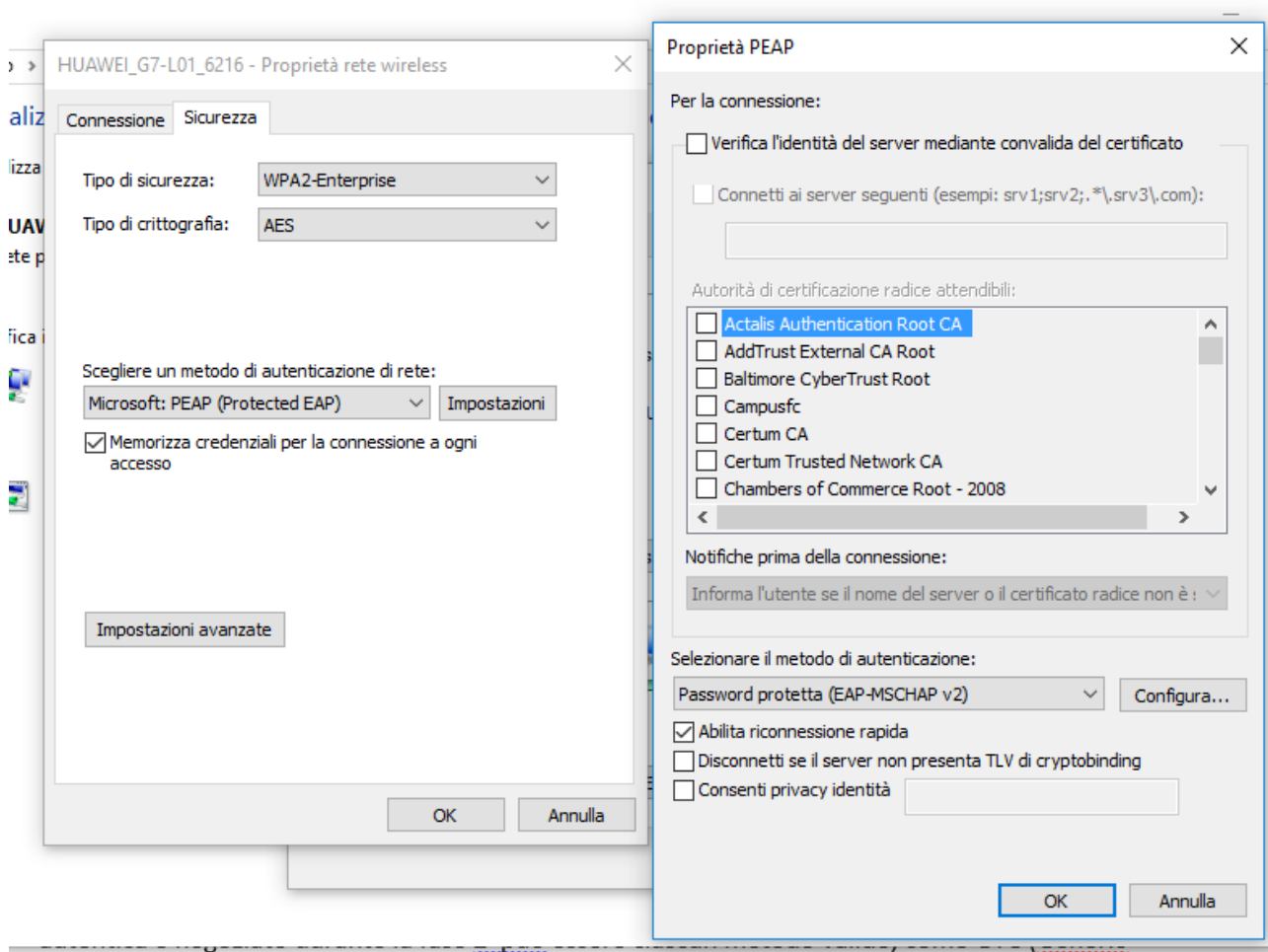
- Nella fase 1 il client autentica il server e usa un TLS handshake per creare un tunnel crittato.
- Nella fase 2 il server autentica l'utente (o le credenziali della macchina) utilizzando un protocollo di autenticazione eap. L'autenticazione eap è protetta dal tunnel crittato creato in fase 1. Il tipo di autentica è negoziato durante la fase 2 può essere ciascun metodo valido, come GTC (Generic Token Card) oppure MS-CHAPv2.

## Comparison chart

| <div>  Edit         </div> <div>WPA2</div> <div>WPA3</div> |   |
|---|---|
| <b>Stands For</b>   | <div>Wi-Fi Protected Access 2</div> <div>Wi-Fi Protected Access 3</div>   |
| <b>What Is It?</b>  | <div>           A security protocol developed by the Wi-Fi Alliance in 2004 for use in securing wireless networks; designed to replace the <a href="#">WEP</a> and <a href="#">WPA</a> protocols.         </div> <div>           Released in 2018, WPA3 is the next generation of WPA and has better security features. It protects against weak passwords that can be cracked relatively easily via guessing.         </div> |
| <b>Methods</b>  | <div>           Unlike WEP and WPA, WPA2 uses the AES standard instead of the RC4 stream cipher. CCMP replaces WPA's TKIP.         </div> <div>           128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise) and forward secrecy. WPA3 also replaces the Pre-Shared Key (PSK) exchange with Simultaneous Authentication of Equals, a more secure way to do initial key exchange.         </div>            |
| <b>Secure and Recommended?</b>  | <div>           WPA2 is recommended over WEP and WPA, and is more secure when Wi-Fi Protected Setup (WPS) is disabled. It is not recommended over <a href="#">WPA3</a>.         </div> <div>           Yes, WPA3 is more secure than WPA2 in ways discussed in the essay below.         </div>  |
| <b>Protected Management Frames (PMF)</b>  | <div>           WPA2 mandates support of PMF since early 2018. Older <a href="#">routers</a> with unpatched firmware may not support PMF.         </div> <div>           WPA3 mandates use of Protected Management Frames (PMF)         </div>  |

## Ambiente di test

L'obiettivo è realizzare un'infrastruttura Radius con autenticazione PEAP



## Installazione FreeRadius

Nel laboratorio Installiamo il pacchetto freeradius e poi andiamo a configurare PEAP

```
sudo apt-get -y install freeradius
```

Poi installiamo easy-rsa per generare un certificato autosegnato.

```
sudo apt install easy-rsa
sudo mkdir /etc/freeradius/certs
sudo cp -R /usr/share/easy-rsa /etc/freeradius/certs/
cd /etc/freeradius/certs/easy-rsa
```

Generiamo il certificato della CA e dei server. Quando vengono richieste le password inserire la solita Admin1234!

```
./easyrsa init-pki
./easyrsa build-ca
./easyrsa gen-crl
```

Creiamo il certificato per il server Radius usando la CA

```
./easyrsa build-server-full server
```

Vengono creati i seguenti file

```
/etc/freeradius/certs/easy-rsa/pki/ca.crt
/etc/freeradius/certs/easy-rsa/pki/issued/server.crt
/etc/freeradius/certs/easy-rsa/pki/private/server.key
```

I files di configurazione sono sotto la directory /etc/freeradius/3.0 ed il file fondamentali sono 2:

- radiusd.conf : contiene le direttive relative al tipo di autenticazione ed autorizzazione utilizzati dal vostro server RADIUS
- clients.conf : contiene i dati del server NAS (compreso il secret key che serve per la comunicazione crittografata con il server RADIUS)

Configuriamo freeradius per accettare i certificati. Modifichiamo il file mods-enabled/eap e indichiamo il file contenente la password (vuoto) il file che contiene la chiave privata del certificato e il certificato sia del server che della CA.

Sempre nello stesso file modifichiamo il peap e mschapv2

```
peap {

    private_key_password = Admin1234!
    private_key_file = /etc/freeradius/certs/easy-rsa/pki/private/server.key
    certificate_file = /etc/freeradius/certs/easy-rsa/pki/issued/server.crt

    ca_file = /etc/freeradius/certs/easy-rsa/pki/ca.crt
```

Assegniamo i permessi giusti

```
sudo usermod -a -G winbindd_priv freerad
sudo chgrp winbindd_priv /var/lib/samba/winbindd_privileged/
```

configuriamo FreeRadius per usare ntlm\_auth per verificare le credenziali degli utenti

Modifichiamo il file

```
sudo vim /etc/freeradius/3.0/mods-available/mschap
```

aggiungendo

```
with_ntdomain_hack=yes
```

necessario per correggere un errore dovuto alla formato di challenge/response tra radius e Domain controller.

E abilitiamo l'autenticazione con ntlm aggiungendo la seguente stringa

```
mschap {
    ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --domain=EXAMPLE --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"
```

Nel file

```
/etc/freeradius/3.0/mods-available/eap:
```

~~Impostiamo il tipo di autenticazione PEAP~~

```
default_eap_type=peap
```

~~Poi nella sezione tls-config-tls-common~~

```
random_file=/dev/urandom
```

Permettiamo all'utente freerad di poter eseguire richieste winbind

```
usermod -a -G winbindd_priv freerad
```

## Verifichiamo il funzionamento dell'autenticazione

```
ntlm_auth --request-nt-key --domain=EXAMPLE --username=utente01 --  
password=Admin1234!
```

## Verifichiamo il funzionamento di freeradius

Bisogna prima spegnere il servizio che è partito con l'installazione di freeradius

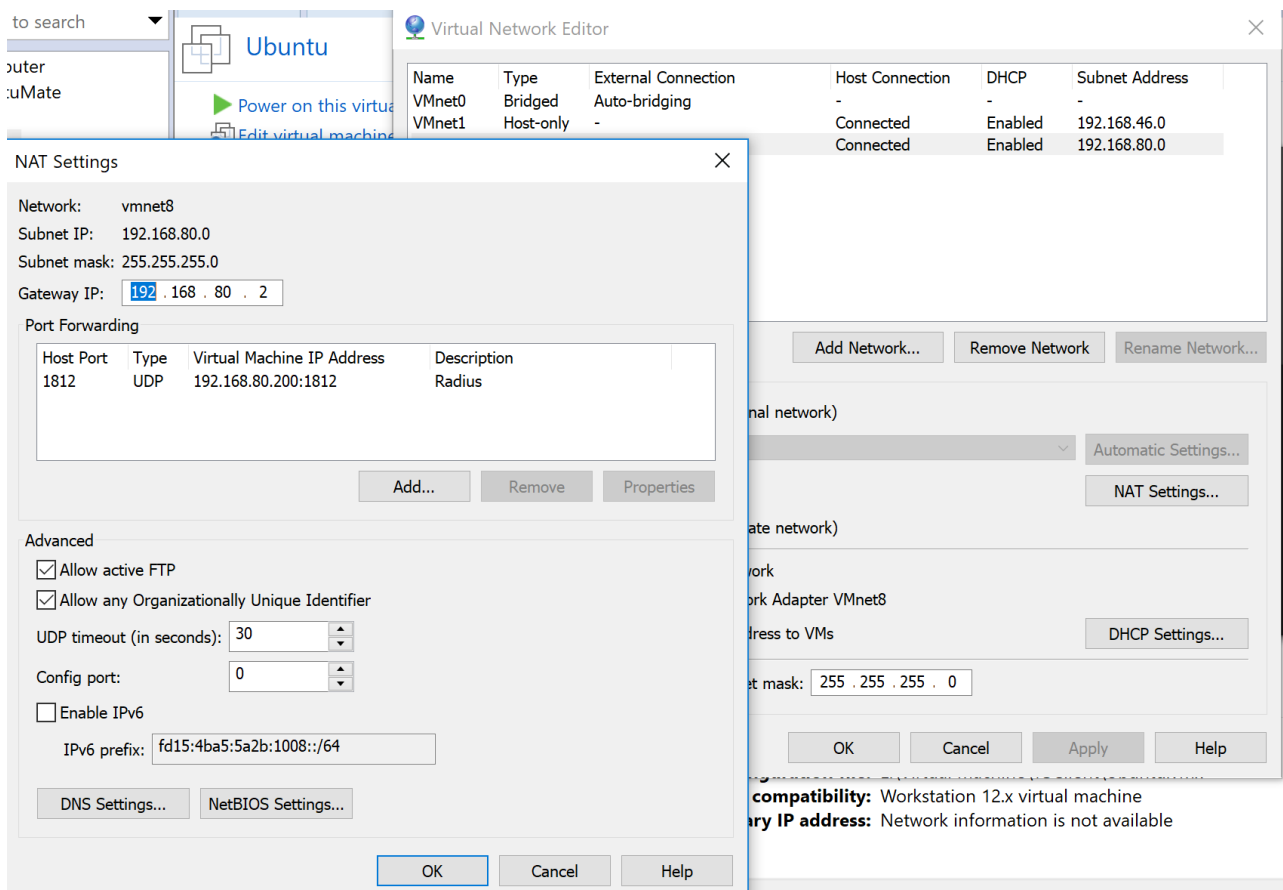
```
systemctl stop freeradius
```

Adesso si può eseguire freeradius in modalità debug

```
freeradius -X
```

```
radtest -t mschap utente01 Admin1234! localhost 123 testing123
```

## Destination NAT con VmWare Workstation



Ricordiamo che VmWare Workstation gira su Windows 10 e questo ha un firewall che blocca le richieste dall'esterno. Per semplicità disabilitiamo il firewall di windows.

Configuriamo l'Access Point per usare l'autenticazione WAP/WPA2 con Radius.

La password è 123456789012

### Wireless -- Security

This page allows you to configure security features of the wireless LAN. A network key is required to authenticate to this wireless network. Click "Save/Apply" to configure the wireless security options.

|                           |               |
|---------------------------|---------------|
| Network Authentication:   | WPA/WPA2      |
| WPA2 Preauthentication:   | Disabled      |
| Network Re-auth Interval: | 36000         |
| WPA Group Rekey Interval: | 0             |
| RADIUS Server IP Address: | 192.168.216.7 |
| RADIUS Port:              | 1812          |
| RADIUS Key:               | ••••••••••    |
| WPA Encryption:           | AES           |
| WEP Encryption:           | Disabled      |

Configuriamo Freeradius per accettare richieste di autenticazione da parte dell'Access Point.

Apriamo il nostro file client.conf e aggiungiamo l'indirizzo Ip dell'Access Point e la password.

```
client 192.168.126.199 {  
    secret      = 123456789012  
    shortname    = asus  
}
```

```
sudo rm -f /etc/resolv.conf
```

```
sudo ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

```
reboot
```

Per sistemare

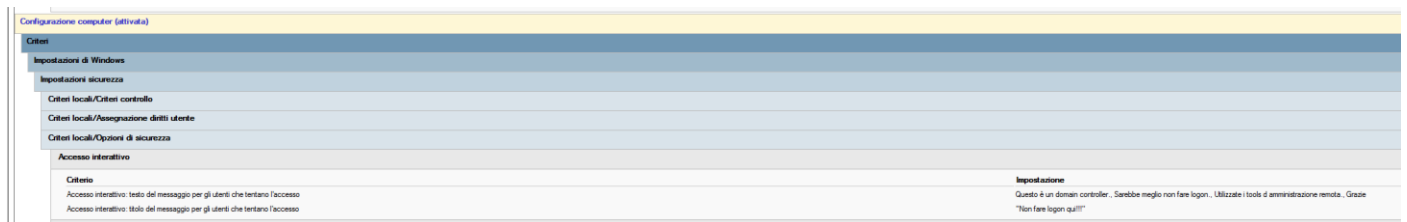
Verificare apparmor se sta funzionando

Andare in /etc/network/interfaces

E modificare il file

```
dns-nameservers 10.11.12.200
```

```
sudo ip addr flush interface-name  
sudo systemctl restart networking
```



[https://www.coretech.it/it/service/knowledge\\_base/Programmazione/Ubuntu/Ubuntu-Server-come-AD-domain-controller.php](https://www.coretech.it/it/service/knowledge_base/Programmazione/Ubuntu/Ubuntu-Server-come-AD-domain-controller.php)