DECEPTION COMPONENT GENERATOR

(Samba over LDAP authentication)

Gloria Pelucchini, Leonardo Lembo, Stefano Paparella, Alessio Troffei

LA SCELTA DEL PROGETTO

- Attacchi crescenti
- Cambio di visione ai problemi

LA DECEPTION TECHNOLOGY

- Inganna i criminali che prendono di mira la rete di un'organizzazione.
- Distoglie l'attenzione dell'aggressore dalle vere risorse dell'organizzazione.

GLI STRUMENTI DELLA DECEPTION TECHNOLOGY

HONEYPOT

- Primo strumento della Deception Technology.
- Capacità statiche e limitate

STRUMENTI PIU' SOFISTICATI

- HoneyNet
- HoneyCredential
- HoneyToken

DECEPTION PLATFORM

LA PRIMA SOLUZIONE: VM

La Macchina Virtuale

<u>Isolamento completo:</u>
Evita di contaminare le altre macchine su host condiviso.

<u>Sviluppo interattivo:</u>
Grazie alla possibilità di fare snapshot.

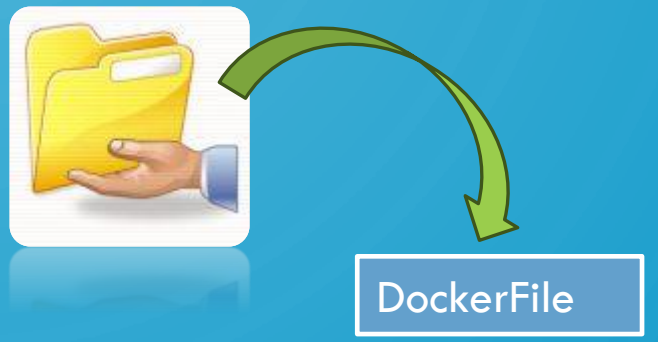
ISO di installazione di Debian

LA SECONDA SOLUZIONE: Docker

Ci sono due modi per l' installazione dell'immagine del SO Debian:

docker hub

```
docker run --name=CybersecProject
-it debian:stable-slim /bin/bash
```




```
docker build -t CybersecProject
/path/to/Dockerfile
```

```
docker run –it CybersecProject /bin/bash
```

Comandi fondamentali:

Utilizzo dell'immagine del container creato.

EXPORT

Una volta terminato il lavoro, si può esportare seguendo questo comando:

```
docker export --output="<PATH>/image.tar" CybersecProject
```

IMPORT

Una volta ricevuta l'immagine, la si può importare seguendo questi comandi:

```
docker import <PATH>/image.tar
```

```
docker images
```

```
docker run –it 4af0 /bin/bash
```

Comandi fondamentali:

RIAVVIO CONTAINER

Ci permette di poter operare ancora sullo stesso container, che abbiamo prima avviato su Docker Desktop.

```
docker exec -it CybersecProject bash
```

CHIUSURA CONTAINER

Tramite il comando di cui sotto e stoppandolo da Docker Desktop (su Windows):

```
exit
```

PERCHE' DUE SOLUZIONI?

VIRTUAL MACHINE

Astrazione del sistema operativo quindi possibile consegna con albero LDAP popolato.

DOCKER

- Astrazione dei processi
- Generazione randomica del SID di Samba

  Impossibilità di riconoscere utenti precedentemente creati e quindi di accedere alle loro cartelle.

L
LIGHTWEIGHT

D
DIRECTORY

A
ACCESS

P
PROTOCOL

DSA

DIRECTORY
SYSTEM AGENT

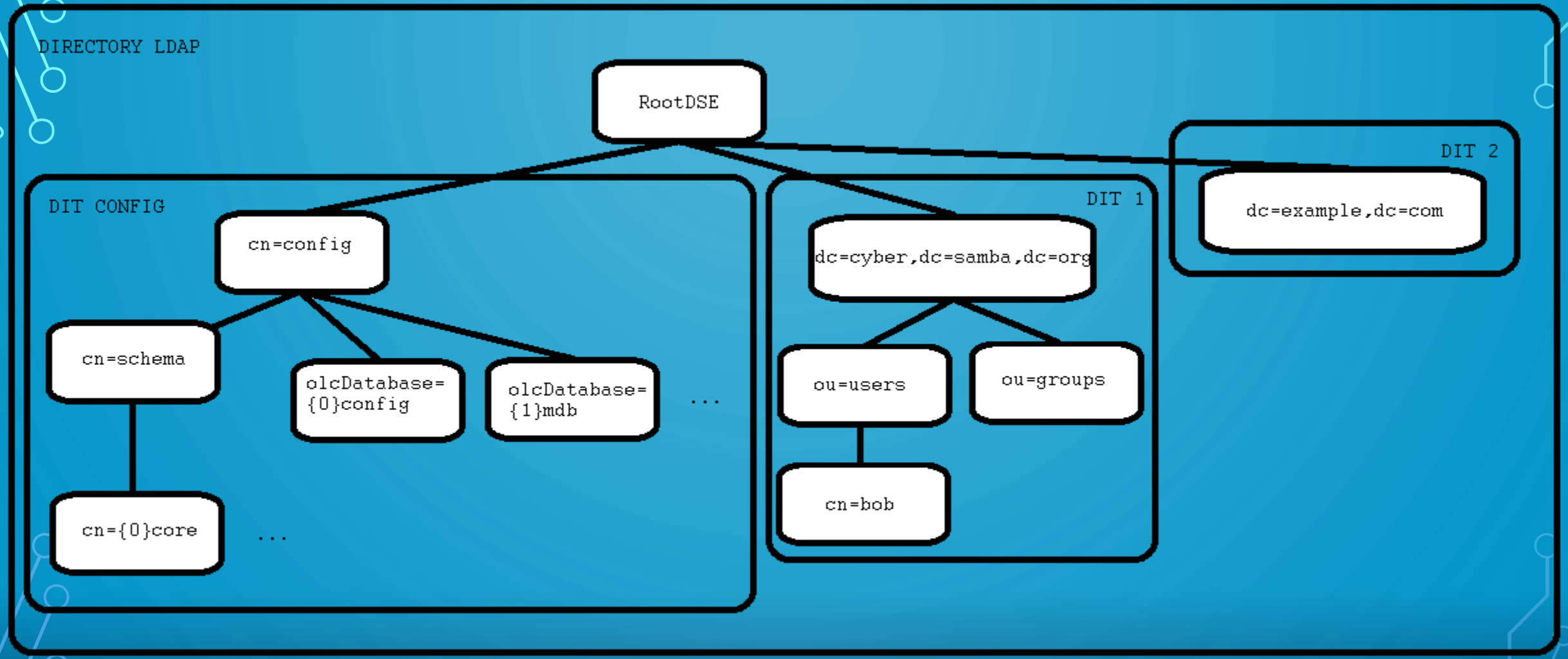
DUA

DIRECTORY
USER AGENT

DIT

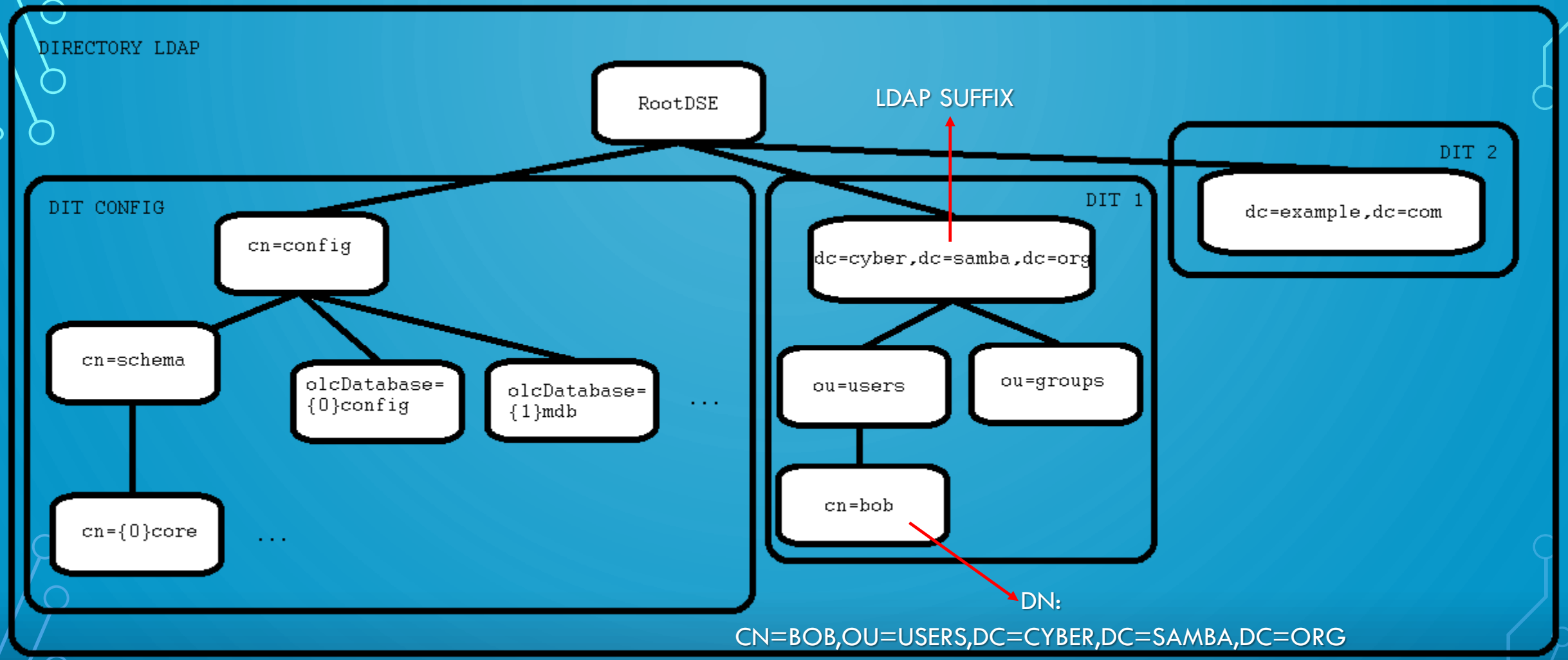
DIRECTORY
INFORMATION TREE

DIRECTORY LDAP



DC=DOMAIN COMPONENTS | OU=ORGANIZATIONAL UNIT | CN=COMMON NAME

DIRECTORY LDAP



DC=DOMAIN COMPONENTS | OU=ORGANIZATIONAL UNIT | CN=COMMON NAME

METODI DI AUTENTICAZIONE

SIMPLE (SSO)

- Anonimo
- Non Autenticato
- User/Password Autenticato

SASL

Qualsiasi Framework SASL:

- Meccanismi basati su Kerberos
- EXTERNAL
- Altri meccanismi di Auth..

SLAPD
Standalone LDAP Daemon

Configurazione:

- dpkg-reconfigure slapd -

/var/lib/ldap/*

```
Prompt dei comandi - docker  run --name=CybersecProject -p 389:389 -it debian:stable-slim /bin/bash
root@7a63fcd5e1f6:/# tree /var/lib/ldap/
/var/lib/ldap/
|-- data.mdb
`-- lock.mdb
```

/etc/ldap/*

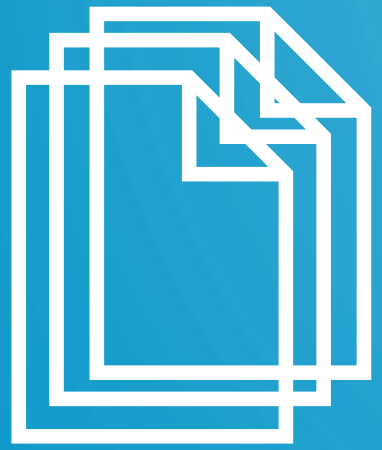
```
Prompt dei comandi - docker  run --name=CybersecProject -p 389:389 -it debian:stable-slim /bin/bash
root@7a63fcd5e1f6:/# tree /etc/ldap/
/etc/ldap/
|-- ldap.conf
|-- sasl2
|-- schema
|   |-- README
|   |-- collective.ldif
|   |-- collective.schema
|   |-- corba.ldif
|   |-- corba.schema
|   |-- core.ldif
|   |-- core.schema
|   |-- cosine.ldif
|   |-- cosine.schema
|   `--    ...
|
`-- slapd.d
    |-- cn=config
    |   |-- cn=module{0}.ldif
    |   |-- cn=schema
    |   |   |-- cn={0}core.ldif
    |   |   |-- cn={1}cosine.ldif
    |   |   |-- cn={2}nis.ldif
    |   |   `-- cn={3}inetorgperson.ldif
    |   |-- cn=schema.ldif
    |   |-- olcDatabase={-1}frontend.ldif
    |   |-- olcDatabase={0}config.ldif
    |   `-- olcDatabase={1}mdb.ldif
    `-- cn=config.ldif
```

Diverse tecnologie per il Backend

- BDB
- HDB
- MDB

LDAP SCHEMA

Necessari per definire la struttura delle entry LDAP



PREINSTALLATI:

core.ldif

cosine.ldif

inetorgperson.ldif

nis.ldif

…

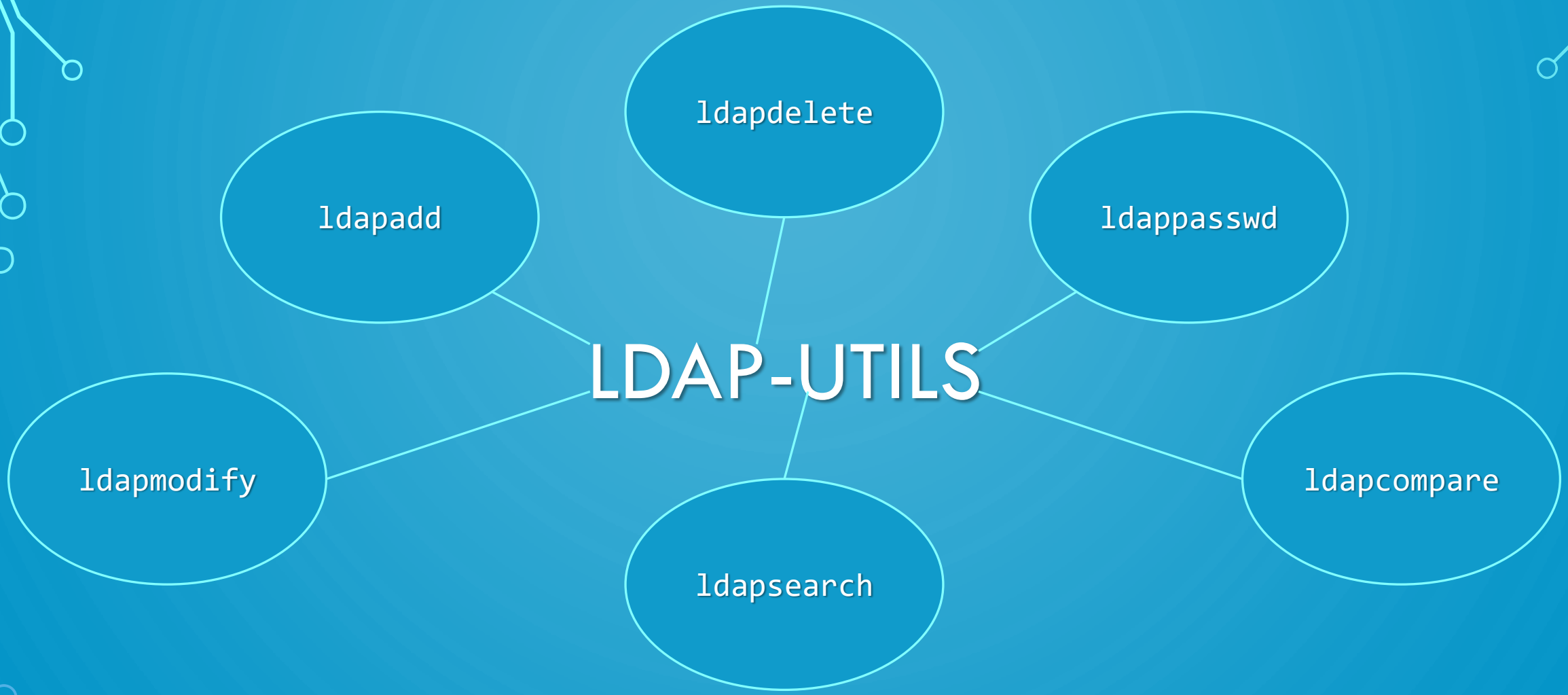
DA INSTALLARE:

samba.schema

COMANDI:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H
ldap:///cn={12}samba,cn=schema,cn=config -l cn=samba.ldif
```

```
ldapadd -Q -Y EXTERNAL -H ldapi:// -f cn\=samba.ldif
```



ESEMPI DI UTILIZZO

```
ldapsearch -x -b <search_base> -H ldap://127.0.0.1 -D <bind_dn> -W
```

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config
```

LIBNSS-SLAPD

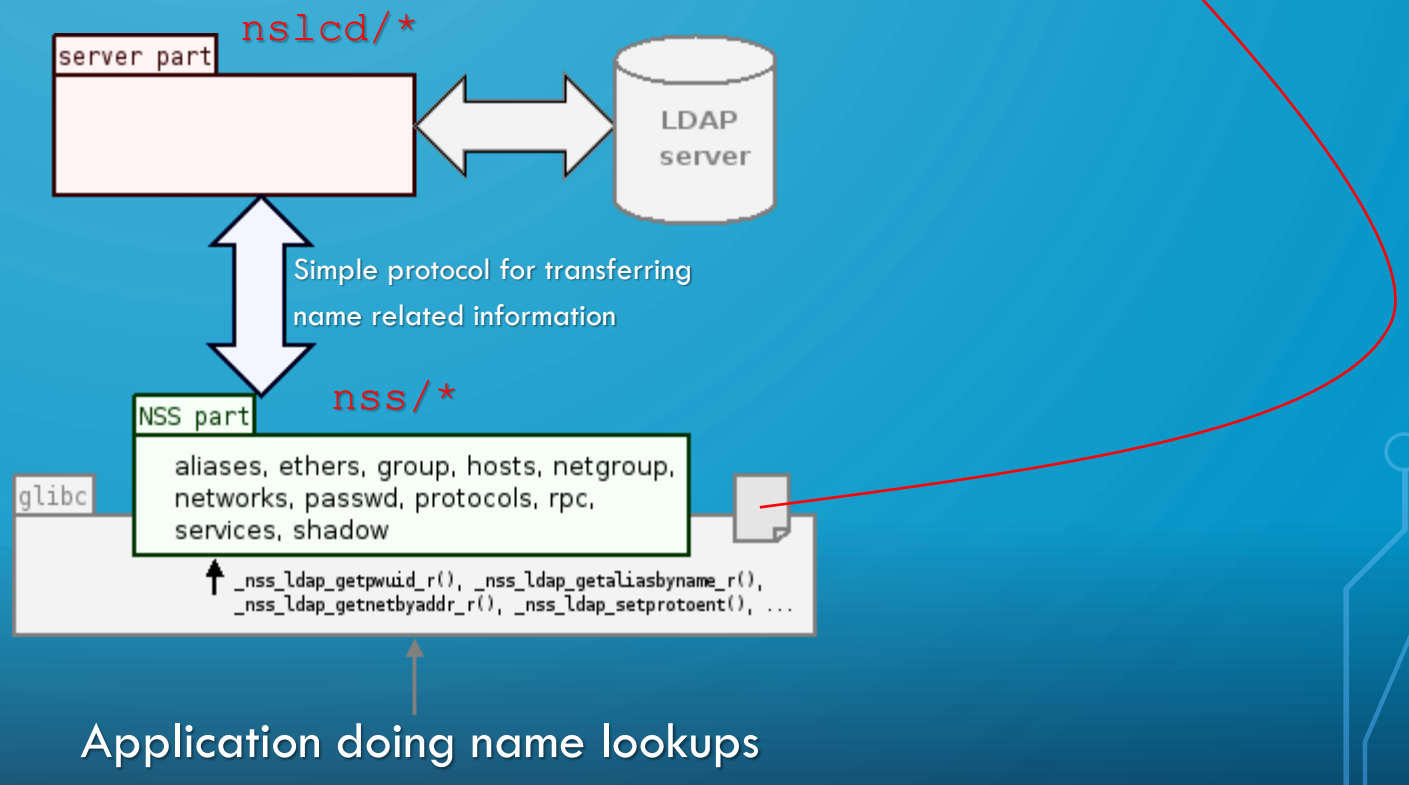
Per abilitare LDAP lookup per group, passwd e shadow

LDAP server URI: ldapi:///

Prompt dei comandi - docker run --name=CybersecProject -p 389:389 -it debian:stable-slim /bin/bash

```
  GNU nano 7.2
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.

passwd:         files ldap
group:          files ldap
shadow:         files ldap
```



SAMBA

Suite di applicazioni Unix.

Opera su protocollo SMB.

Permette ai server di comunicare con lo stesso protocollo di rete dei prodotti Microsoft.

Consente la condivisione di FS e stampanti tra client e server.

```
sudo apt-get install samba
```

CONFIGURAZIONE SAMBA – IL FILE SMB.CONF

Due **tipi fondamentali** di opzioni di configurazione

GLOBAL

- Sezione **[global]**
- Definiscono i **comportamenti generali** di Samba
  - Parametri di configurazione
  - Opzioni di default per gli share
- Dev'essere **SEMPRE** presente

SHARE

- Tre tipi di share:
  - Pubblico **[public]**
  - Privato **[homes]**
  - Gruppo **[nome_gruppo]**
- Definiscono il comportamento dello specifico share
- Se appaiono in **[global]**, contano come impostazioni di default

OPZIONI GLOBALI – OPZIONI DI BASE

```
server role = standalone server
```

```
unix password sync = yes
```

```
usershare allow guests = no
```

OPZIONI GLOBALI – OPZIONI DI BASE

server role = standalone server

unix password sync = yes

usershare allow guests = no

OPZIONI GLOBALI – OPZIONI DI BASE

server role = standalone server

unix password sync = yes

usershare allow guests = no

SMBLDAP-TOOLS

- Installazione: **apt-get install smbldap-tools**
- Configurazione: **smbldap-config**
  - **SID**
  - **HomeDir** degli utenti
  - **sambaDomain** (= WORKGROUP)

} Valori di default

  - configurazione dello **SlaveLDAP** e del **MasterLDAP** (stessi IP e admin)
  - Impostazione dei suffissi
    - **suffix**
    - **groups**
    - **users**
    - **machines**
    - **idmap**

FINALIZZARE IL COLLEGAMENTO A LDAP

```
# Configurazione ldap per samba
   passdb backend = ldapsam:"ldap://127.0.0.1"
   ldap suffix = dc=cyber,dc=samba,dc=org
   ldap user suffix = ou=users
   ldap group suffix = ou=groups
   ldap machine suffix = ou=computers
   ldap idmap suffix = ou=idmap
   ldap admin dn = cn=admin,dc=cyber,dc=samba,dc=org
   ldap ssl = no
   ldap passwd sync = yes

   add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

GESTIRE UTENTI E GRUPPI

• Creazione **utente**	**smbldap-useradd –m –P –a ste –s «»**
• Cancellazione **utente**	**smbldap-userdel –r ste**
• Creazione **gruppo**	**smbldap-groupadd ProgCyb**
• Cancellazione **gruppo**	**smbldap-groupdel ProgCyb**
• **Inserimento** di un utente nel gruppo	**smbldap-groupmod –m ste, usr2 ProgCyb**
• **Visualizzazione** di un utente	**smbldap-usershow ste**

OPZIONI DI SHARE…

PRIVATO – [homes]

```
[homes]
   comment = Home Directories
   browseable = yes

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
   read only = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
   create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
   directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# The following parameter makes sure that only "username" can connect
# to \\server\username
# This might need tweaking when using external authentication schemes
   valid users = %U
```

PUBBLICO – [public]

```
[public]
   comment = Public Directory
   path = /home/public
   public = yes
   read only = no
   browseable = yes
   guest ok = no
   force user = nobody
   force group = nogroup
```

…E LE CARTELLE CONDIVISE?

CARTELLE CONDIVISE – [nome_gruppo]

```
[ProgCyb]
   path = /home/ProgCyb
   read only = no
   browseable = yes
   valid users = @ProgCyb
```

SMBCLIENT – ACCESSO ALLO SHARE PRIVATO

```
stefano@10:/$ sudo smbclient //127.0.0.1/homes -U ste
Password for [WORKGROUP\ste]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Dec 14 12:18:40 2023
  ..                                  D        0  Thu Dec 14 12:18:28 2023
  .face.icon                          H     5290  Wed Jul 12 11:49:12 2023
  .bashrc                             H     3526  Sun Apr 23 23:23:06 2023
  .face                               H     5290  Wed Jul 12 11:49:12 2023
  Desktop                             D        0  Thu Dec 14 12:19:10 2023
  .profile                            H      807  Sun Apr 23 23:23:06 2023
  .bash_logout                        H      220  Sun Apr 23 23:23:06 2023

                50303512 blocks of size 1024. 39779208 blocks available
smb: \>
```

SMBCLIENT – ACCESSO ALLO SHARE PUBBLICO

```
stefano@10:/$ sudo smbclient //127.0.0.1/public -U ste
Password for [WORKGROUP\ste]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Dec 14 12:27:52 2023
  ..                                  D        0  Thu Dec 14 12:18:28 2023
  README.txt                          N     3435  Thu Dec 14 12:27:51 2023

                50303512 blocks of size 1024. 39779208 blocks available
smb: \>
```

SMBCLIENT – ACCESSO ALLE CARTELLE CONDIVISE

```
stefano@10:/$ sudo smbclient //127.0.0.1/ProgCyb -U ste
Password for [WORKGROUP\ste]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Dec 14 11:36:08 2023
  ..                                  D        0  Thu Dec 14 12:18:28 2023
  video_tutorial_fotografia.docx      N    22983  Thu Dec 14 11:35:29 2023
  lista_spese_vacanza.pdf             N    53957  Thu Dec 14 11:35:29 2023
  foto_artistica.docx                 N    18024  Thu Dec 14 11:35:26 2023
  studio_fotografico.odt              N    15995  Thu Dec 14 11:35:26 2023
  Lavoro                              D        0  Thu Dec 14 11:36:08 2023

                50303512 blocks of size 1024. 39779208 blocks available
smb: \>
```

Se l'utente non fa parte del gruppo: **NT_STATUS_PERMISSION_DENIED**

PANORAMICA

Script di aggiunta utenti/gruppi e generazione filesystem fittizio

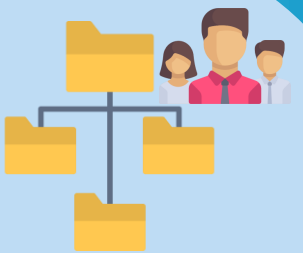
Pandoc

ClamAV

IMPLEMENTAZIONE DELL'INGANNO

Script Bash

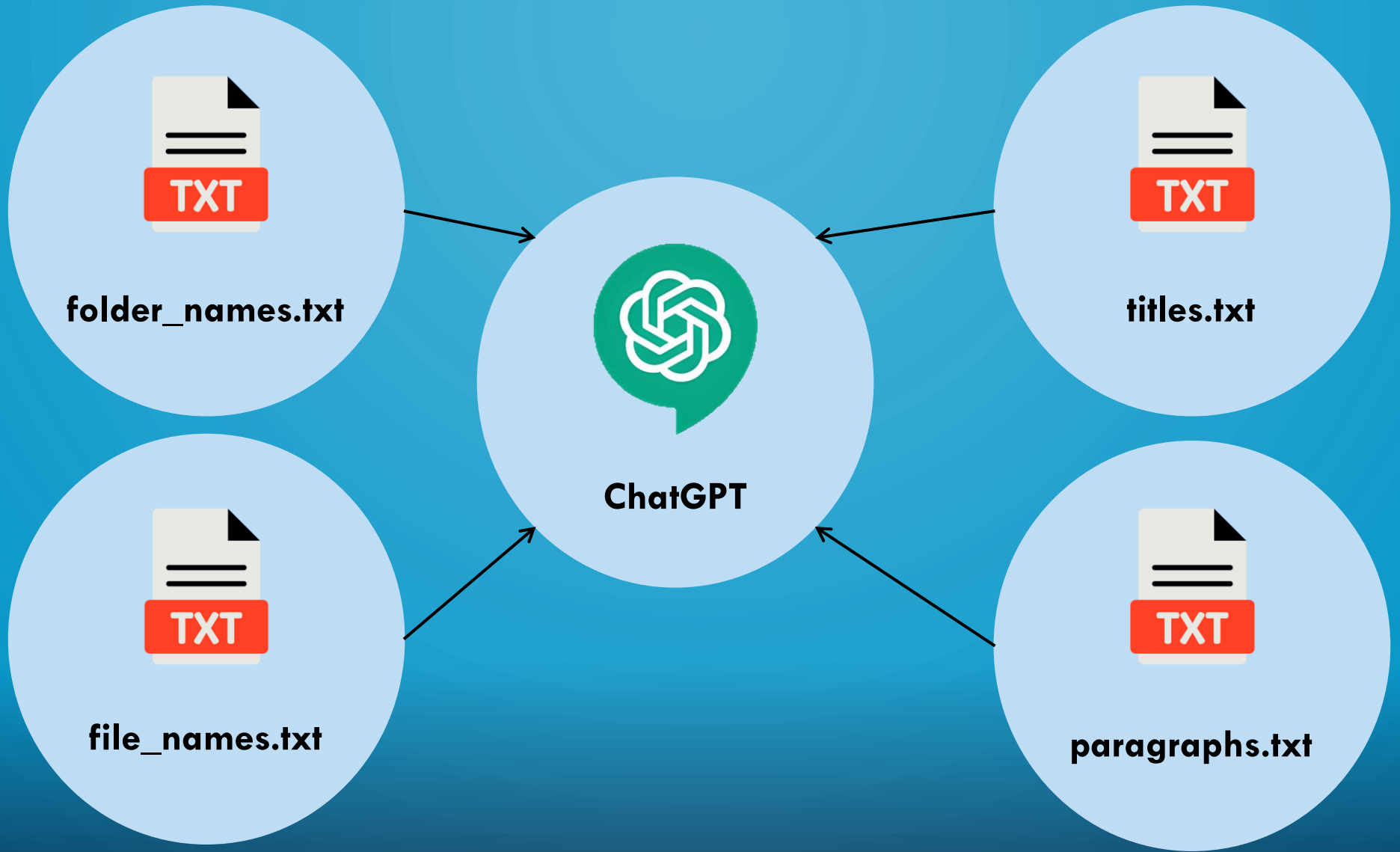
Generazione utenti e/o gruppi



Creazione e riempimento Samba share

Filesystem fittizio

GENERAZIONE DEI FILE TEMPORANEI E DEL FILESYSTEM



PERCHÉ NON USARE UN LLM LOCALE COME LLAMA?

LLaMA 2 – 7B

GPU: 6GB VRAM - RTX 3050, RTX 3060, GTX 1660, 2060, AMD 5700 XT.

RAM: Almeno 8 GB di RAM.

LLaMA 2 – 13B

GPU: 10GB VRAM - AMD 6900 XT, RTX 2060, 3060, 3080, A2000.

RAM: Almeno 16 GB di RAM.

LLaMA 2 – 70B

GPU: 40GB VRAM - A100 40GB, 2x3090, 2x4090, A40, RTX A6000, 8000.

RAM: Almeno 64 GB di RAM.

CPU: i9-10900K, i7-12700K, or Ryzen 9 5900x, AMD Ryzen Threadripper 3990X (64 cores e 128 threads).

PANDOC

Convertire in PDF:

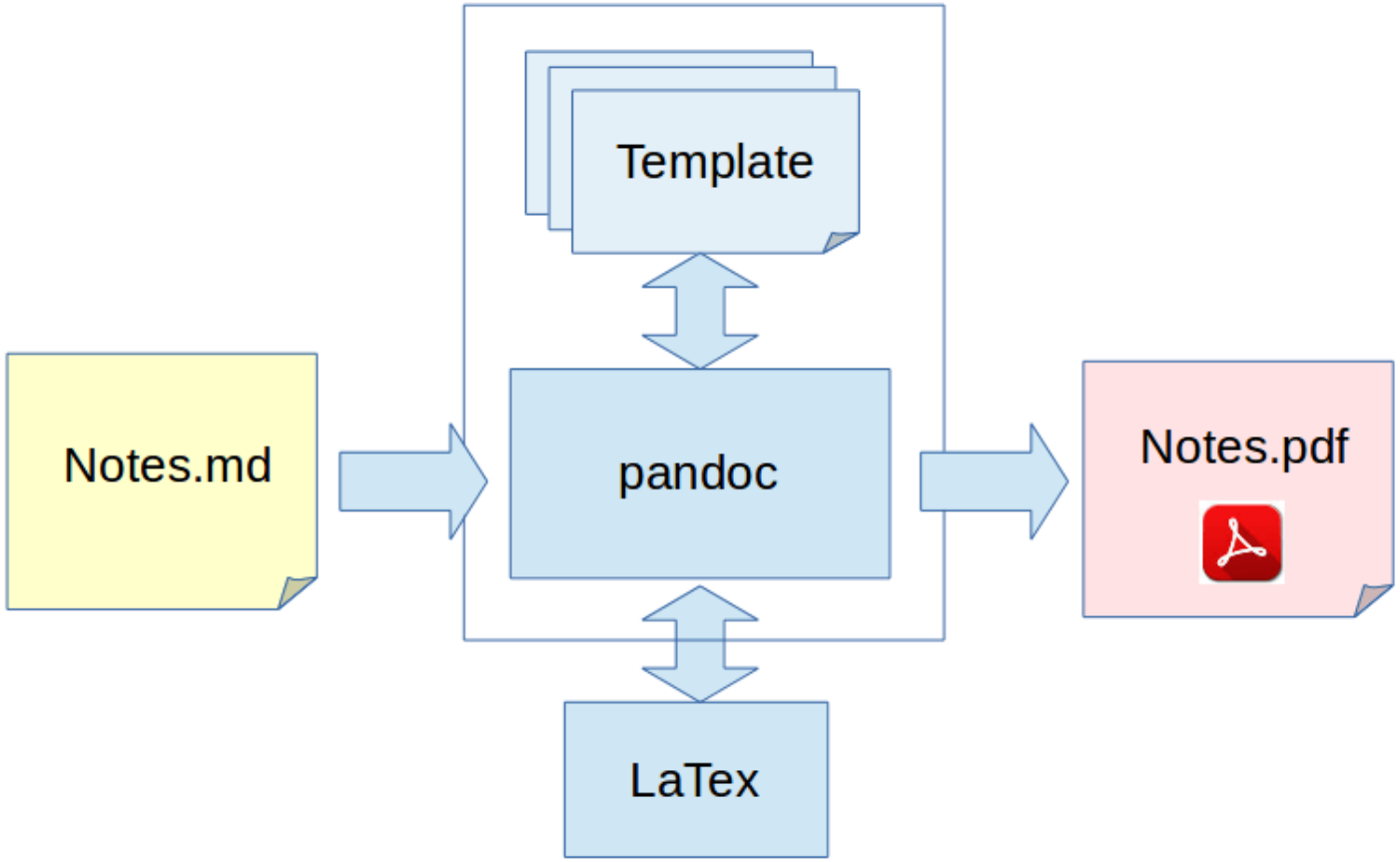
```
pandoc input.txt --pdf-engine=xelatex -o output.pdf
```

Convertire in documento Word:

```
pandoc -s input.txt -o output.docx
```

Convertire in OpenDocument:

```
pandoc input.txt -o output.odt
```



UTILIZZO DI PANDOC NEL PROGETTO

File temporaneo generato in markdown

Conversione in .pdf, .docx, .odt

Eliminazione file temporanei

CLAMAV

- Alto tasso di rilevazione;
- Supporta di numerosi tipi di file;
- Scansione in tempo reale;
- Elevata configurabilità;
- Pulizia automatica minacce;

UTILIZZO DI CLAMAV

Creazione filesystem dell'utente o gruppo

Aggiunta del percorso della cartella a ClamAV

Scansione in tempo reale

CONFIGURAZIONE DI CLAMAV

Config file di clamd (clamd.conf)

Systemd service file (clamav-onacc.service)

Script (detected.sh)

VM vs DOCKER – SCANSIONE CLAMAV

VM → Systemd

- Ambiente più complesso
- Necessità di creare un Systemd service file

```
sudo systemctl enable clamav-daemon.service
```

Docker → Cron

- Ambiente più snello
- Più semplice e permette di offrire lo stesso tipo di sicurezza

```
0 0 * * * /home/public/clamav_docker/clamscan.sh
```

GRAZIE PER L'ATTENZIONE!