TUTORIEL · ANNUAIRES ET AUTHENTIFICATION

LDAP

Configuration et mise en pratique avec OpenLDAP

Samuel Vermeulen — SV Formations

Licence CC BY-NC 4.0 — partage et diffusion autorisés à des fins non commerciales, avec mention de l'auteur.

PROGRAMME

Six étapes, de la théorie au TP

01

Comprendre LDAP

Protocole, ports, rôle de l’annuaire

02

Structurer l’annuaire

DIT, DN, schémas, format LDIF

03

Installer OpenLDAP

slapd, ldap-utils, cn=config

04

Peupler et interroger

ldapadd, ldapsearch, filtres

05

Sécuriser

TLS, ACL, hachage des mots de passe

06

Intégrer et dépanner

SSSD, applications, codes d’erreur

CC BY-NC 4.0

COMPRENDRE LDAP

Qu’est-ce que LDAP ?

Lightweight Directory Access Protocol : un protocole standard pour lire et écrire dans un annuaire — une base optimisée pour la lecture, qui centralise comptes, groupes et ressources.

389

LDAP en clair, ou chiffré via StartTLS

636

LDAPS : TLS dès la connexion

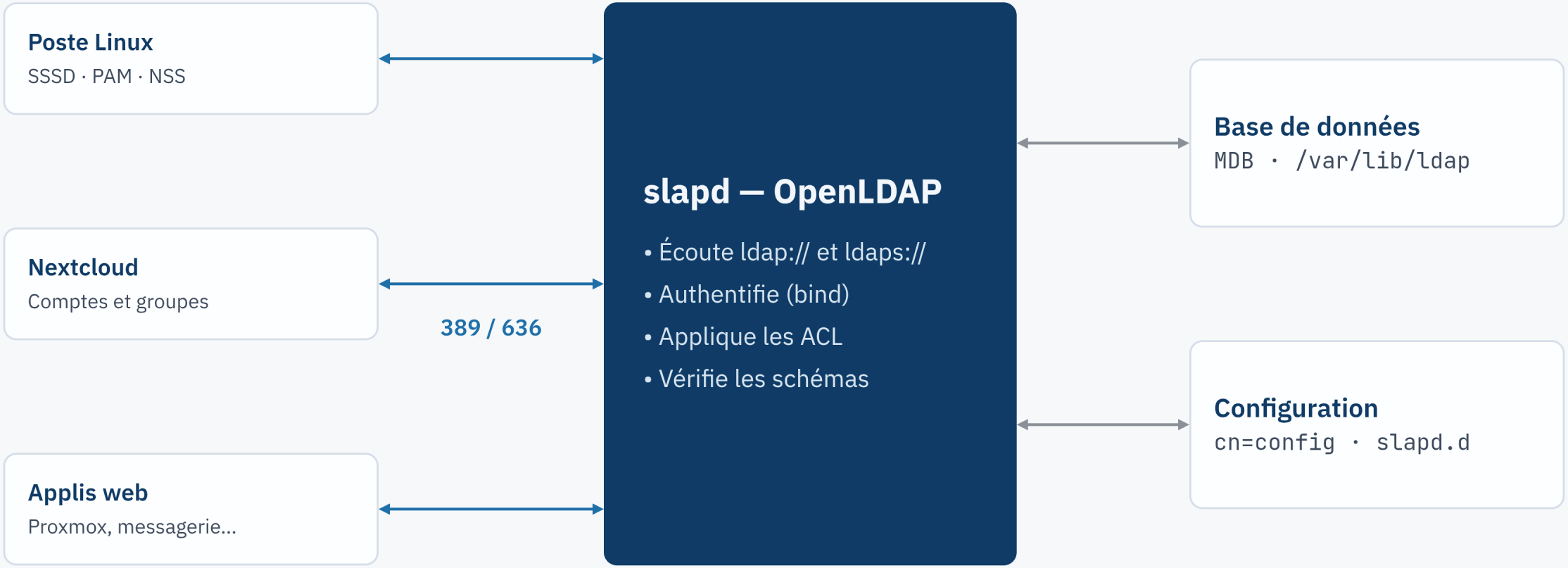
v3

Version actuelle du protocole (RFC 4511)

CC BY-NC 4.0

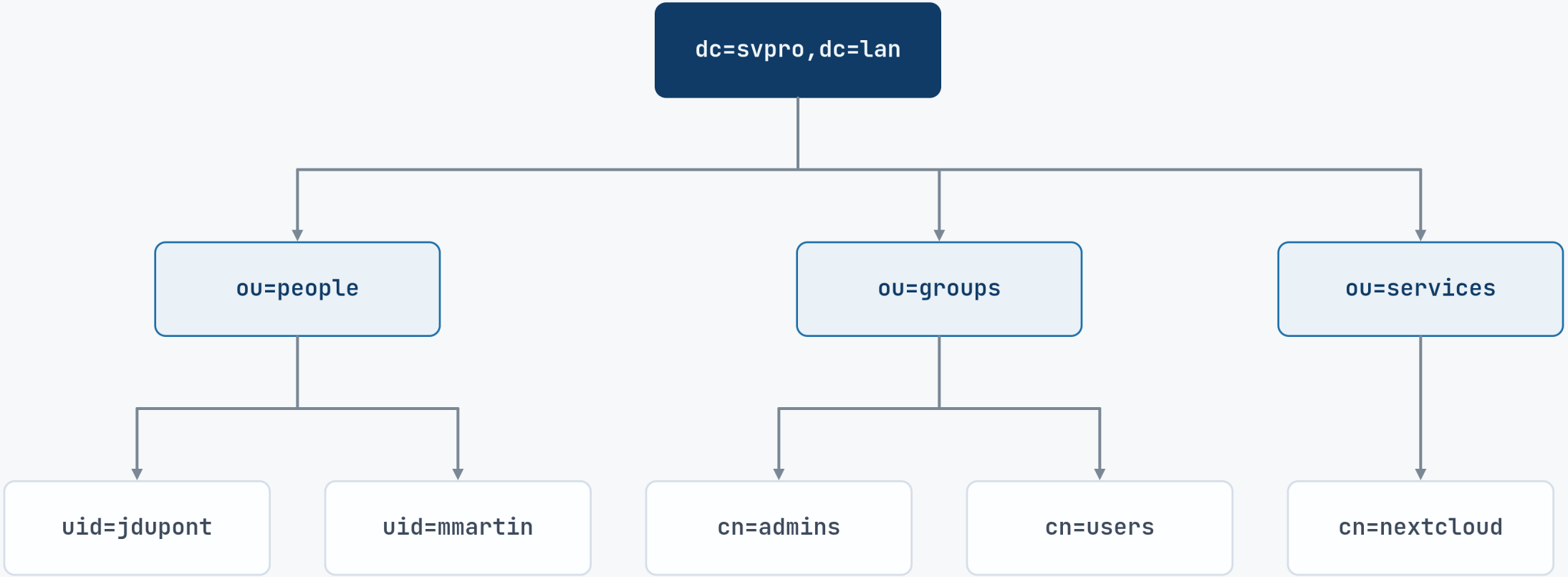
COMPRENDRE LDAP

Architecture client – serveur



CC BY-NC 4.0

L'annuaire est un arbre : le DIT



CC BY-NC 4.0

Le vocabulaire indispensable

Terme	Rôle	Exemple
DN	Nom unique et complet d'une entrée	uid=jdupont,ou=people,dc=svpro,dc=lan
RDN	Partie gauche du DN, unique sous son parent	uid=jdupont
Suffixe	Racine de l'arbre (base DN)	dc=svpro,dc=lan
objectClass	Classe qui fixe les attributs requis et permis	inetOrgPerson, posixAccount
Attribut	Paire type : valeur d'une entrée	mail: jean.dupont@svpro.lan
Schéma	Ensemble des classes et attributs connus	core, cosine, nis, inetorgperson

CC BY-NC 4.0

Le format LDIF décrit les entrées

```
# jdupont.ldif
dn: uid=jdupont,ou=people,dc=svpro,dc=lan
objectClass: inetOrgPerson
objectClass: posixAccount
uid: jdupont
cn: Jean Dupont
sn: Dupont
mail: jean.dupont@svpro.lan
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/jdupont
loginShell: /bin/bash
```

`dn`

Identifie l'entrée ; toujours la première ligne.

`objectClass`

Une ou plusieurs classes, qui imposent les attributs requis.

`Ligne vide`

Sépare deux entrées dans un même fichier.

CC BY-NC 4.0

MISE EN PRATIQUE

Passons au lab

Debian 12 ou 13, OpenLDAP (slapd 2.5+), domaine svpro.lan, serveur ldap.svpro.lan

CC BY-NC 4.0

Installation sur Debian

```
# 1. Installer le serveur et les outils
sudo apt update
sudo apt install slapd ldap-utils

# 2. Reconfigurer proprement
sudo dpkg-reconfigure slapd

# 3. Vérifier
sudo systemctl status slapd
sudo slapcat
```

Réponses à dpkg-reconfigure

Question	Réponse
Omettre la configuration ?	Non
Nom de domaine DNS	svpro.lan
Organisation	SV Pro
Mot de passe admin	••••••••
Purger la base avec le paquet ?	Non
Déplacer l'ancienne base ?	Oui

CC BY-NC 4.0

Configurer via cn=config

```
# Lister la configuration (socket local, root)
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// \
  -b cn=config dn

# loglevel.ldif
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats

sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f loglevel.ldif
```

Configuration dynamique

Tout est stocké dans l'arbre cn=config. Les changements s'appliquent sans redémarrer slapd.

⚠

Attention

Ne modifiez jamais les fichiers de /etc/ldap/slapd.d à la main : passez toujours par ldapmodify.

CC BY-NC 4.0

PEUPLER ET INTERROGER

Créer la structure, puis les comptes

```
# base.ldif
dn: ou=people,dc=svpro,dc=lan
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=svpro,dc=lan
objectClass: organizationalUnit
ou: groups

dn: cn=users,ou=groups,dc=svpro,dc=lan
objectClass: posixGroup
cn: users
gidNumber: 10000
```

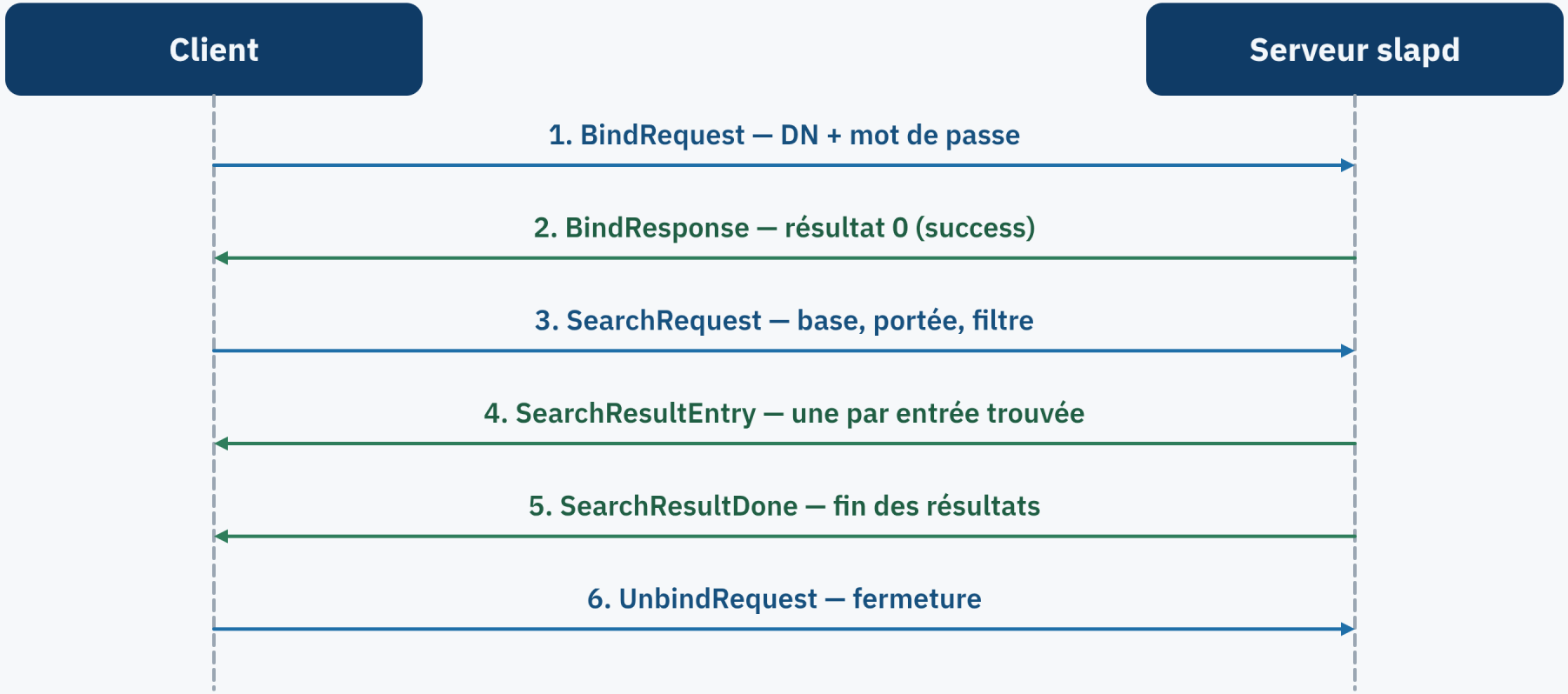
```
# Importer
ldapadd -x -W \
  -D cn=admin,dc=svpro,dc=lan \
  -f base.ldif

ldapadd -x -W -D cn=admin,dc=svpro,dc=lan \
  -f jdupont.ldif

# Définir le mot de passe
ldappasswd -x -W -S \
  -D cn=admin,dc=svpro,dc=lan \
  uid=jdupont,ou=people,dc=svpro,dc=lan
```


CC BY-NC 4.0

Une requête LDAP, pas à pas



CC BY-NC 4.0

Interroger avec ldapsearch

```
ldapsearch -x -LLL -H ldap://ldap.svpro.lan \
  -b ou=people,dc=svpro,dc=lan -s sub \
  "(&(objectClass=posixAccount)(loginShell=/bin/bash))" uid mail
```

Option	Effet
-x	Bind simple
-LLL	LDIF sans commentaires
-H	URI du serveur
-b	Base de la recherche
-s	Portée : base, one, sub
-D / -W	DN et mot de passe

Filtre	Type
(uid=jdupont)	Égalité
(cn=Jean*)	Sous-chaîne
(mail=*)	Présence
(&(...)(...))	ET logique
(|(...)(...))	OU logique
(!(...))	Négation

CC BY-NC 4.0

SÉCURISER

Trois réflexes de sécurité

Chiffrer

StartTLS sur 389 ou LDAPS sur 636. Côté client : ldapsearch -ZZ impose TLS.

Contrôler

Les ACL olcAccess définissent qui lit ou modifie quoi, de la règle la plus précise à la plus générale.

Hacher

Jamais de mot de passe en clair : {SSHA} par défaut, {ARGON2} via le module pw-argon2.

```
# acl.ldif — appliqué avec ldapmodify -Y EXTERNAL -H ldapi:///
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to * by users read by * none
```


CC BY-NC 4.0

Authentifier un poste Linux avec SSSD




```
# /etc/sssd/sssd.conf (chmod 600)
[sssd]
services = nss, pam
domains = svpro

[domain/svpro]
id_provider = ldap
auth_provider = ldap
ldap_uri = ldaps://ldap.svpro.lan
ldap_search_base = dc=svpro,dc=lan
```

```
# Paquets client
sudo apt install sssd-ldap \
  libpam-sss libnss-sss

# Créer le home au 1er login
sudo pam-auth-update \
  --enable mkhomedir

# Tester
getent passwd jdupont
```


CC BY-NC 4.0

INTÉGRER ET DÉPANNER

Raccorder les applications

Nextcloud

Application « LDAP user and group backend » : bind avec un compte de service, filtres d'utilisateurs et de groupes.

YunoHost

S'appuie nativement sur OpenLDAP (slapd) pour tous ses comptes : une bonne base d'observation.

Proxmox VE

Ajout d'un royaume LDAP : Datacenter › Permissions › Realms, puis synchronisation.

Bonne pratique

Un DN de service dédié, en lecture seule, par application — jamais cn=admin.

CC BY-NC 4.0

Lire les codes d’erreur

Code	Nom	Cause probable et piste
49	invalidCredentials	DN ou mot de passe erroné : vérifier le DN complet passé à -D
32	noSuchObject	Base ou entrée inexistante : vérifier -b, contrôler avec slapcat
50	insufficientAccessRights	Les ACL refusent l’opération : revoir olcAccess
65	objectClassViolation	Attribut obligatoire absent ou non permis par les classes
68	entryAlreadyExists	Le DN existe déjà : utiliser ldapmodify plutôt que ldapadd
-1	Can’t contact LDAP server	Service, port ou pare-feu : systemctl status slapd, ss -tlnp

Journaux du serveur : journalctl -u slapd -f avec olcLogLevel: stats

CC BY-NC 4.0

TRAVAUX PRATIQUES

À vous de jouer

01 Installer slapd et fixer le suffixe dc=svpro,dc=lan	**02** Créer ou=people et ou=groups, puis trois utilisateurs
03 Lister les comptes dont le shell est /bin/bash	**04** Ajouter une ACL protégeant userPassword
05 Activer StartTLS et tester avec ldapsearch -ZZ	**06** Raccorder un client Debian avec SSSD

Critère de réussite : **getent passwd jdupont** répond sur le client et **ssh jdupont@client** fonctionne.

CC BY-NC 4.0



Merci !

LICENCE DE DIFFUSION

Ce support est publié sous licence **Creative Commons Attribution – Pas d'Utilisation Commerciale 4.0 International (CC BY-NC 4.0)**.

Vous pouvez le copier, le partager et l'adapter à des fins **non commerciales**, en citant l'auteur : Samuel Vermeulen — SV Formations.

creativecommons.org/licenses/by-nc/4.0/deed.fr

© 2026 Samuel Vermeulen