Sécurité des OS

Grégoire Roumache

Avril 2021

Table des matières

Remarques:

- j'ai regroupé la résolution des labos *pfsense* avec ceux du cours de sécurité des réseaux
- je n'ai pas fait de synthèse zabbix
- les labos powershell sont traités dans la synthèse du cours de progra os

1 Correction examen théorique de juin 2019

1. Que veut dire PAM ?
   (a) Pluggable Authentification Mechanism
   (b) Pluggable Authorisation Mechanism
   (c) **Pluggable Authentification Modules**
   (d) Pluggable Authorisation Modules
   (e) Aucune de ces réponses
2. Quel est le but de PAM ?
   (a) Centraliser l'authentification
   (b) Fournir une API de développement de modules spécifiques d'authentification
   (c) Permettre l'exécution de traitements spécifiques automatisés lors de l'authentification
   (d) **Les réponses A, B, C sont toutes correctes**
   (e) Les réponses A, B, C ne sont pas toutes correctes
3. Quel comportement engendre le contrôle `required` de PAM ?
   (a) **Tous les modules utilisant ce contrôle doivent passer avec succès pour que la vérification soit accordée. Le cas échéant l'utilisateur n'est averti qu'à la fin du traitement de la pile. Un échec empêche l'ouverture de session, les autres modules de la pile sont néanmoins exécutés.**

(b) Tous les modules utilisant ce contrôle doivent passer avec succès pour que la vérification soit accordée. Le cas échéant l'utilisateur n'est averti qu'à la fin du traitement de la pile. Un échec empêche l'ouverture de session, les autres modules de la pile ne sont pas exécutés.

(c) Tous les modules utilisant ce contrôle doivent passer avec succès pour que la vérification soit accordée. Le cas échéant l'utilisateur est averti directement. Un échec empêche l'ouverture de session, les autres modules de la pile ne sont pas exécutés.

(d) Au moins un module utilisant ce contrôle doit passer avec succès pour que la vérification soit accordée. Le cas échéant l'utilisateur n'est averti qu'à la fin du traitement de la pile. Un échec empêche l'ouverture de session, les autres modules de la pile sont néanmoins exécutés.

(e) Au moins un module utilisant ce contrôle doit passer avec succès pour que la vérification soit accordée. Le cas échéant l'utilisateur est averti directement. Un échec empêche l'ouverture de session, les autres modules de la pile sont néanmoins exécutés.

4. Sous PAM, quel groupe de gestion vérifie si le compte utilisateur est arrivé à expiration ?

   (a) session

   (b) auth

   (c) password

   (d) **account**

   (e) Aucune de ces réponses

5. Quel autre avantage est lié à l'utilisation de PAM ?

   (a) La possibilité d'utiliser la double authentification

   (b) La possibilité de développer de nouveaux modules dans de multiples langages

   (c) La possibilité d'utiliser PAM dans des environnements hétérogènes, sur des OS différents (Linux, Windows, MAC, ...)

   (d) Les réponses A, B, C sont toutes correctes

   (e) **Les réponses A, B, C ne sont pas toutes correctes**

   > Les réponses A et B sont correctes, pas la C.

6. Quelle action engendre le module `pam_security.so` ?

   (a) Autorise le login par le compte root excepté sur les terminaux listés dans `/etc/securetty`

   (b) Autorise le login par le compte root uniquement sur les terminaux listés dans `/etc/securetty`

   (c) **Interdit le login par le compte root excepté sur les terminaux listés dans** `/etc/securetty`

   (d) Interdit le login par le compte root uniquement sur les terminaux listés dans `/etc/securetty`

   (e) Aucune de ces réponses

7. Quelle action engendre le module `pam_cracklib.so` ?

   (a) S'assure que le mot de passe employé a été renouvelé dans les délais

   (b) **S'assure que le mot de passe employé présente un niveau de sécurité suffisant**

   (c) S'assure que le mot de passe employé est présent dans le fichier `/etc/passwd`

   (d) S'assure que le mot de passe employé n'a pas été corrompu

   (e) Aucune de ces réponses

8. Que veut dire LDAP ?

   (a) Lightweight Direct Access Protocol

   (b) Lightweight Direct Authentification Protocol

   (c) **Lightweight Directory Access Protocol**

(d) Lightweight Directory Authentification Protocol

(e) Aucune de ces réponses

9. LDAP est un protocole réseaux OSI de quelle couche ?

(a) couche 2

(b) couche 3

(c) couche 4

(d) **couche 5**

(e) couche 6

v · m	Couches du modèle OSI [masquer]
7. Application	BGP · DHCP · DNS · FTP · FTPS · FXP · Gemini · Gopher · H.323 · HTTP · HTTPS · IMAP · IPP · IRC · LDAP · LMTP · MODBUS · NFS · NNTP · POP · RDP · RTSP · SILC · SIMPLE · SIP · SMB-CIFS · SMTP · SNMP · SOAP · SSH · TCAP · Telnet · TFTP · VoIP · Web · WebDAV · XMPP
6. Présentation	AFP · ASCII · ASN.1 · HTML · MIME · NCP · TDI · TLS · TLV (en) · Unicode · UUCP · Vidéotex · XDR · XML
5. Session	AppleTalk · DTLS · NetBIOS · RPC · RSerPool · SOCKS
4. Transport	DCCP · RSVP · RTP · SCTP · SPX · TCP · UDP
3. Réseau	ARP · Babel · BOOTP · CLNP · ICMP · IGMP · IPv4 · IPv6 · IPX · IS-IS · NetBEUI · NDP · RIP · EIGRP · OSPF · RARP · X.25
2. Liaison	Anneau à jeton (token ring) · Anneau à jeton adressé (Token Bus) · ARINC 429 · AFDX · ATM · Bitnet · CAN · Ethernet · FDDI · Frame Relay · HDLC · I²C · IEEE 802.3ad (LACP) · IEEE 802.1aq (SPB) · LLC · LocalTalk · MIL-STD-1553 · PPP · STP · Wi-Fi · X.21
1. Physique	4B5B · ADSL · BHDn · Bluetooth · Câble coaxial · Codage bipolaire · CSMA/CA · CSMA/CD · DSSS · E-carrier · EIA-232 · EIA-422 · EIA-449 · EIA-485 · FHSS · HomeRF · IEEE 1394 (FireWire) · IrDA · ISDN · Manchester · Manchester différentiel · Miller · MLT-3 · NRZ · NRZI · NRZM · Paire torsadée · PDH · SDH · SDSL · SONET · T-carrier · USB · VDSL · VDSL2 · V.21-V.23 · V.42-V.90 · Wireless USB · 10BASE-T · 10BASE2 · 10BASE5 · 100BASE-TX · 1000BASE-T
Articles liés	Pile de protocoles · Modèle Internet · Couche 8

10. Pour établir une communication avec un serveur LDAP, le client doit obligatoirement fournir ?

(a) **L'adresse IP + le numéro de port du serveur**

(b) Un login et un mot de passe

(c) Le protocole d'authentification à utiliser

(d) Il doit fournir A + B + C (= les 3 réponses ci-dessus)

(e) Aucune de ces réponses

11. Sous LDAP, qu'est ce que le DIT ?

(a) Le protocole réseau de communication

(b) Le protocole d'authentification choisi par le client

(c) **L'arbre d'information de l'annuaire**

(d) Un noeud de la structure hiérarchique LDAP

(e) Aucune de ces réponses

> DIT = Directory Information Tree

12. Sous LDAP, qu'est-ce qu'un DN ?

(a) Un nom distinctif qui compose le RDN

(b) **Un nom distinctif qui décrit une entrée de l'annuaire**

(c) Un nom distinctif qui décrit la valeur d'une entrée
(d) Un nom distinctif qui décrit le type d'un attribut
(e) Aucune de ces réponses

> - DN = Distinguished Name, nom absolu, unique, identifiant une entrée dans l'arborescence
> - RDN = Relative Distinguished Name, nom d'un élément dans l'arborescence
> - DN d'un élément = concaténation de l'ensemble des RDN de ses ascendants hiérarchiques

13. Sous LDAP, pourquoi utiliser les classes ?

(a) Pour regrouper des entrées possédant les mêmes valeurs
(b) Pour éviter d'avoir des entrées redondantes
(c) Pour regrouper des DN identiques
(d) **Pour éviter de définir plusieurs fois les attributs d'une entrée**
(e) Aucune de ces réponses

14. Sous LDAP, quelle opération n'est pas permise ?

(a) Faire une recherche par critères
(b) Supprimer une entrée
(c) Modifier un DN
(d) Modifier une entrée
(e) **Toutes ces opérations sont permises**

15. Quel modèle ne fait pas partie des modèles LDAPv3 ?

(a) Stockage d'informations
(b) Nommage
(c) Fonctionnel
(d) Sécurisation/confidentialité
(e) **Ce sont tous des modèles LDAPv3**

16. Le type de syntaxe d'un attribut LDAP défini...

(a) Le type de donnée stockée (valeur)
(b) Le type de comportement lors d'une recherche
(c) Des contraintes sur les valeurs de l'attribut
(d) **Les réponses A, B, C sont correctes**
(e) Aucune réponse n'est correcte

17. Une classe utilisée comme modèle pour créer d'autres classes d'objets est appelée ?

(a) Générique
(b) Structurelle
(c) **Abstraite**
(d) Auxiliaire
(e) Globale

> - abstraite = on peut l'instancier et la modifier comme on veut
> - structurelle = nécessaire à la création
> - auxiliaire = classe fourre-tout

18. LDAP utilise les OIDs, qu'est-ce qu'un OID ?
    (a) Notation de synthèse abstraite qui définit les RDN
    (b) **Chaine numérique qui identifie de façon unique un objet**
    (c) Notation de synthèse abstraite qui définit les attributs d'un objet
    (d) Chaine numérique qui identifie de façon unique un serveur LDAP
    (e) Globale

> OID = Object ID (= object identifier)

19. L'exemple suivant: `uid=john.doe,ou=People,dc=example,dc=com`, montre ?
    (a) **Un DN**
    (b) Un RDN
    (c) Un OID
    (d) Un UIT
    (e) Un DIT

> UIT = /, sans doute une faute de frappe pour UID

20. LDIF est...
    (a) **Un format de fichier LDAP**
    (b) Un format de structure LDAP
    (c) Un format de base de données LDAP
    (d) Un format d'attribut LDAP
    (e) Aucune réponse n'est correcte

> LDIP = LDAP Data Interchange Format, les données sont sous forme d'un fichier texte

21. Quelle fonctionnalité ne fait pas partie du modèle de sécurisation LDAP ?
    (a) Authentification
    (b) Confidentialité
    (c) Intégrité
    (d) Autorisation
    (e) **Aucune réponse n'est correcte**

22. PPP est un protocole d'authentification de ?
    (a) Couche 2
    (b) Couche 3
    (c) Couche 4
    (d) Couche 5
    (e) **Aucune réponse n'est correcte**

23. Quelle fonctionnalité supplémentaire MS-CHAPv2 apporte par rapport à MS-CHAPv1 ?
    (a) Le chiffrement du login
    (b) Le chiffrement du mot de passe

(c) Le chiffrement du login et du mot de passe
(d) **L'authentification mutuelle**
(e) Aucune réponse n'est correcte

24. Quelle est la faille majeure de MS-CHAP ?

(a) Le mot de passe est transmis non-chiffré
(b) **Le mot de passe est transmis chiffré mais il peut être déchiffré**
(c) Il n'est pas compatible avec le protocole WPA2
(d) Le serveur utilise un port ouvert pour la réception des requêtes
(e) Aucune réponse n'est correcte

25. PEAP est ?

(a) Une méthode de chiffrement
(b) Un protocole d'échange de clé publique
(c) Un protocole d'authentification à 2 niveaux
(d) **Un protocole d'identification propriétaire Microsoft**
(e) Aucune réponse n'est correcte

> PEAP = Protected Extensible Authentication Protocol

26. AAA: quelle réponse n'en fait pas partie ?

(a) Authentification
(b) Gestion des autorisations
(c) Enregistrement de l'historique (log)
(d) **Contrôle de l'intégrité**
(e) Aucune réponse n'est correcte

> Protocole AAA = Authentication, Authorization, Accounting/Auditing

27. À quoi correspond le x dans l'extension des fichiers scripts `powershell.psx` ?

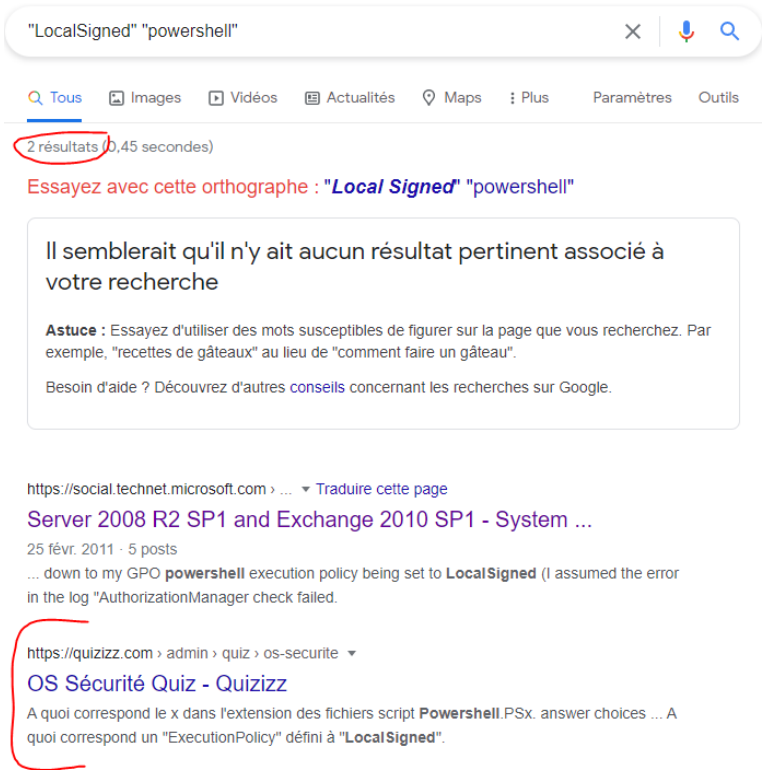
(a) Au niveau de la politique d'exécution du script
(b) **À la version de Powershell minimum compatible**
(c) Au niveau de cryptage de la signature du script
(d) À la version de Powershell maximale compatible
(e) Aucune réponse n'est correcte

28. À quoi correspond un `ExecutionPolicy` défini à `Restricted` ?

(a) Seuls les scripts locaux peuvent être exécutés
(b) Seuls les scripts locaux signés peuvent être exécutés
(c) Les scripts téléchargés doivent être signés peuvent être exécutés
(d) Tous les scripts doivent être signés peuvent être exécutés
(e) **Aucune réponse n'est correcte**

> `Restricted` = bloque l'exécution de tous les scripts

29. À quoi correspond un `ExecutionPolicy` défini à `LocalSigned` ?
    (a) Seuls les scripts locaux peuvent être exécutés
    (b) Seuls les scripts locaux signés peuvent être exécutés
    (c) Les scripts téléchargés doivent être signés peuvent être exécutés
    (d) Tous les scripts doivent être signés peuvent être exécutés
    (e) **Aucune réponse n'est correcte**



30. Un script signé est également ?
    (a) Chiffré par clé symétrique
    (b) Chiffré par clé asymétrique
    (c) Chiffré par clé privée
    (d) Chiffré par clé publique
    (e) **Il n'est pas chiffré**

31. Veeam Backup & Replication est conçu pour ?
    (a) **Les environnements virtualisés**
    (b) Les environnements physiques
    (c) Les environnements Windows uniquement
    (d) Les environnements Unix uniquement
    (e) Aucune réponse n'est correcte

32. Sur la machine à sauvegarder, Veeam Backup & Replication a besoin d'installer ?
    (a) Un agent source-side

(b) Un agent target-side

(c) Un agent source-side et un agent target-side

(d) Un agent Veeam Backup Proxy

(e) **Aucune réponse n'est correcte**

33. L'élément Veeam Backup Repository de l'architecture Veeam B&R sert à ?

(a) Répondre aux requêtes de restauration

(b) Installer les agents sur les hôtes à sauvegarder

(c) **Sauvegarder les données de backup**

(d) Administrer l'architecture Veeam B&R

(e) Aucune réponse n'est correcte

34. Lors d'un snapshot...

(a) On fait une copie du disque dur et on la bloque en écriture

(b) **On bloque le disque dur en écriture et on enregistre les modifications sur un disque dur secondaire**

(c) On bloque le disque dur en écriture pendant la création du backup

(d) Les modifications sont enregistrées sur le disque dur mais on attend la fin du backup pour les valider

(e) Aucune réponse n'est correcte

35. Lors d'un Resersed Incremental Backup ?

(a) **Le dernier point de sauvegarde est toujours complet**

(b) Il est nécessaire de faire périodiquement une sauvegarde complète

(c) On ne peut effacer les sauvegardes intermédiaires qu'après une sauvegarde complète

(d) La politique de rétention varie en fonction de la périodicité de la sauvegarde complète

(e) Aucune réponse n'est correcte

36. La déduplication est ?

(a) Un système qui permet de faire une copie d'une machine, cela permet la redondance de machine et la haute disponibilité

(b) **Un système qui permet de vérifier si un bloc de données est déjà sauvegardé et ainsi éviter la redondance**

(c) Un système qui permet de faire une copie des données sauvegardées. Cela permet la perte de données en cas de panne du serveur de stockage

(d) Un système qui virtualise une machine physique permettant ainsi de faire des tests sans toucher à la machine en production

(e) Aucune réponse n'est correcte

37. Le monitoring ne permet pas la mesure ?

(a) des performances

(b) de la disponibilité

(c) **de l'intégrité**

(d) des modifications

(e) le monitoring permet la mesure de A, B, C, D

38. SNMP est un protocole...

(a) De surveillance de composants informatiques (ventilateur, sonde, ...)

(b) De contrôle à distance d'équipement informatique

(c) **De surveillance d'équipement réseau**

(d) De surveillance d'application de type Java

(e) Les réponses A, B, C, D sont toutes correctes

39. Un proxy Zabbix ?

(a) **Peut collecter des données de performance et de disponibilité au nom du serveur Zabbix**

(b) Est déployé sur des cibles de surveillance pour superviser activement les ressources locales et les applications, et envoyer les données collectées au serveur Zabbix

(c) Est le composant central auquel les agents envoient leur disponibilité, les informations d'intégrité et les statistiques

(d) Est un système de stockage base de données de toutes les informations de configuration ainsi que des données collectées par Zabbix

(e) Les réponses A, B, C, D sont toutes correctes

40. Un élément Zabbix est ?

(a) Un équipement sur le réseau que vous souhaitez surveiller, avec adresse IP/DNS

(b) Une expression logique qui définit un seuil de problème et qui est utilisée pour "évaluer" les données reçues dans les éléments

(c) Une occurence unique de quelque chose qui mérite l'attention, comme un changement d'état de déclenchement, un enregistrement automatique d'agent ou une découverte d'agent

(d) **Une donnée particulière que vous voulez recevoir d'un hôte, une métrique de données**

(e) Aucune réponse n'est correcte

2 PAM - labo 3

- Créer un utilisateur et supprimer son mdp: `adduser toto && passwd -d toto`
- **centos** - interdire la connexion des utilisateurs sans mdp en supprimant *nullok*: `nano /etc/pam.d/system-auth`

  ```
  auth sufficient pam_unix.so nullok try_first_pass
  ```

- **debian** - modifier la politique de mot de passe:
  - `apt install libpam-cracklib`
  - `nano /etc/pam.d/common-passwd` (ajouter cette ligne)

    ```
    password required pam_cracklib.so retry=3 minlen=X difok=Y
    ```

- **centos** - empêcher les utilisateurs de se connecter et afficher un message quand ils essaient:
  - `echo "Only root can login T_T" > /etc/nologin`
  - `nano /etc/pam.d/login`

    ```
    account required pam_nologin.so
    ```

- **debian** - idem sous debian:
  - `echo "Only root can login T_T" > /etc/nologin`
  - `nano /etc/pam.d/login`

    ```
    auth requisite pam_nologin.so.
    ```

- **debian** - ajouter une règle pour créer le dossier perso d'un utilisateur qui n'en a pas:
  - `nano /etc/pam.d/common-session`

    ```
    session required pam_mkhomedir.so
    ```

  - `su <user>`
- **debian** - ajouter une règle pour que les changements de mdp des utilisateurs soient enregistrés:
  - `nano /etc/pam.d/common-password`

    ```
    password required pam_pwhistory
    ```

  Remarque: le changement est enregistré dans le dossier `/etc/security/opasswd`
- **debian** - ajouter un délai de 10 sec après l'échec d'une tentative de connexion:
  - `nano /etc/pam/common-auth`

    ```
    auth required pam_faildelay.so debug delay=10000000
    ```

- **debian** - définir une plage horaire de connexion ssh pour un utilisateur:
  - `nano /etc/security/time.conf`

    ```
    <service>;<terminal>;<utilisateur>;<time_range>
    sshd;*;<user>;!Wd       # ssh interdit à l'utilisateur le WE
    *;*;*;!Al1300-1400      # Wk = weekday, Wd = week-end, Al = any day
                            # 1300-1400 = 13-14h
    ```

3 LDAP - labo 4

- Installation/préparation:

```
# installer les paquets
yum -y install openldap compat-openldap openldap-clients openldap-servers \
    openldap-servers-sql openldap-devel

systemctl start slapd   # lance le service
systemctl enable slapd  # le service se lance au démarrage du système

netstat -antup | grep -i 389    # vérification: port ldap = 389

# -h <schéma_mdp> -s <nouveau_mdp>
slappasswd -h {SSHA} -s ldppassword > /etc/openldap/slapd.d/db.ldif
```

- `cd /etc/openldap/slapd.d/`
- Créer/modifier le fichier `db.ldif` pour modifier les variables `olcSuffix`, `olcRootDN` et `olcRootPW`:

```
# fichier à modifier in fine: ./cn=config/olcDatabase={2}hdb.ldif
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix              # suffixe de la db (= nom de domaine)
olcSuffix: dc=greg,dc=local     # greg.local

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN                      # root distinguished name (= root user)
olcRootDN: cn=ldapadm,dc=greg,dc=local  # root = ldapadm (nom standard ?)

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW                                  # root's password
olcRootPW: {SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3   # hash obtenu avec "slappasswd"
```

Remarque: on ne fait pas les modifications directement dans le fichier car elles seraient perdues à chaque fois qu'on lance `ldapmodify`.

- Envoyer les configurations au serveur ldap: `ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif`
- Créer le fichier `monitor.ldif` pour modifier la variable `olcAccess`:

```
# fichier à modifier in fine: ./cn=config/olcDatabase={1}monitor.ldif
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess:
    {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
    read by dn.base="cn=ldapadm,dc=greg,dc=local"
    read by * none
```

Syntaxe:

```
olcAccess: to [ressource]
    by [à qui] [type d'accès autorisé]
    by [à qui] [type d'accès autorisé]
```

- Envoyer les configurations au serveur ldap: `ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif`
- Copier la config de db et modifier le propriétaire:
  - `cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG`
  - `chown ldap:ldap /var/lib/ldap/*`
- Ajouter les schémas ldap *cosine* et *nis* (= schémas des tables de la db ldap)[1]:
  - `ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif`
  - `ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif`
  - `ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif`
- Créer le fichier `base.ldif` pour créer la base du directory ldap:

```
dn: dc=greg,dc=local
dc: greg
objectClass: top
objectClass: domain

dn: cn=ldapadm,dc=greg,dc=local
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

dn: ou=People,dc=greg,dc=local
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=greg,dc=local
objectClass: organizationalUnit
ou: Group
```

- Ajouter la base au domaine ldap: `ldapadd -x -W -D "cn=ldapadm,dc=greg,dc=local" -f base.ldif`
- Créer le fichier `test01.ldif` pour créer un utilisateur *test01*:

```
dn: uid=test01,ou=People,dc=greg,dc=local
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: test01
uid: test01
uidNumber: 9999
gidNumber: 100
homeDirectory: /home/test01
loginShell: /bin/bash
gecos: test01 [Admin (at) greg]
userPassword: {crypt}x
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

[1] `https://ldap.com/understanding-ldap-schema/`

- Ajouter l'utilisateur: `ldapadd -x -W -D "cn=ldapadm,dc=greg,dc=local" -f test01.ldif`
- Changer son mdp:

```
ldappasswd -s tttttt -W -D "cn=ldapadm,dc=greg,dc=local" \
    -x "uid=test01,ou=People,dc=greg,dc=local"
```

- Vérification: `ldapsearch -x cn=test01 -b dc=greg,dc=local`
- Ajouter le service ldap au parefeu:
  - `firewall-cmd -permanent -add-service=ldap`
  - `firewall-cmd -reload`
- Modifier le fichier de log de ldap: `nano /etc/rsyslog.conf`

```
local4.* /var/log/ldap.log
```

  Remarque: après, relancer le service: `systemctl restart rsyslog`

- Configuration/vérification sur un client ldap:

```
# installation
yum install -y openldap-clients nss-pam-ldapd

# Enregistrer le client sur le serveur en SSO (SSO = single sign on)
authconfig --enableldap --enableldapauth --ldapserver=<ip_serveur_ldap> \
    --ldapbasedn="dc=greg,dc=local" --enablemkhomedir --update

systemctl restart nslcd     # redémarre le service ldap client

getent passwd test01        # vérification (1)
su test01                   # vérification (2)
```

4 LDAP - labo 5

- Installation ldap sur debian:
  - `apt-get install slapd ldap-utils`
  - `dpkg-reconfigure slapd`

```
Omettre la configuration OpenLDAP ?             Non
Nome de domaine DNS:                            henallux.local
Nom de l'organization ?                         Henallux
Mot de passe administrateur:                    tttttt
Confirmez le mot de passe:                      tttttt
Module de base de données à utiliser:           MDB
Supprimer la db lors de la purge du paquet ?    Oui
Faut-il déplacer l'ancienne base de données ?   Oui
```

- Modifier les variables d'environnement de base de ldap: `nano /etc/ldap/ldap.conf`

```
BASE    dc=henallux,dc=local
URI     ldap://<ip_machine>/    # on peut utiliser: 127.0.0.1
```

- Vérification: `ldapsearch -xLLL`
- Créer un répertoire `/root/ldap/conf` pour centraliser les fichiers de configuration:
  - `mkdir -p /root/ldap/conf`
  - `cd /root/ldap/conf`
- Donner accès à l'admin à la config: `nano /root/ldap/conf/access-conf-admin.ldif`

```
dn: olcDatabase={0}config,cn=config
changeType: modify
add: olcAccess
olcAccess: to * by dn.exact=cn=admin,dc=henallux,dc=local manage by * break
```

  Envoyer au serveur ldap: `ldapmodify -Y external -f access-conf-admin.ldif -H ldapi:///`
  - `-Y <mécanisme_d_authentification>` = spécifie la méthode d'authentification
  - `-H ldapi:///` = ???
- Interroger le serveur ldap avec la commande: `ldapsearch`

  Exemple: `ldapsearch -D cn=admin,dc=henallux,dc=local -w tttttt`
  - `-D <utilisateur>` = utilisateur qui va se connecter/faire la recherche
  - `-w <mdp>` = mdp de l'utilisateur
  - `-W` = demande le mdp après avoir lancé la commande
  - `-y <fichier_mdp>` = connexion avec le mdp contenu dans un fichier
  - `-b <search_base>` = endroit où on fait la recherche
  - `-H ldap://<ip_ldap>` = connexion à un serveur ldap distant
- Configurer les logs:

- Configuration actuelle des logs: `ldapsearch -Y external -H ldapi:/// -b cn=config \ "(objectClass=olcGlobal)" olcLogLevel -LLL > log.ldif`
- Niveaux de logs:

```
-1   = enable all debugging
0    = no debugging
1    = trace function calls
2    = debug packet handling
4    = heavy trace debugging
8    = connection management
16   = print out packets sent and received
32   = search filter processing
64   = configuration file processing
128  = access control list processing
256  = stats log connections/operations/results
512  = stats log entries sent
1024 = print communication with shell backends
2048 = print entry parsing debugging
```

- Modifier le niveau de log: `nano log.ldif`

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: 256
```

- Envoyer la config au serveur ldap: `ldapmodify -Y EXTERNAL -H ldapi:/// -f log.ldif`
- Modifier le fichier de log de ldap: `nano /etc/rsyslog.conf`

```
LOCAL4.* -/var/log/slapd.log
```

- Redémarrer le service: `systemctl restart rsyslog`

- Les "overlays" (= modules/plugin supplémentaire)
  - Fichier d'installation d'overlay:

```
dn: cn=module,cn=config
cn: module
objectclass: olcModuleList
objectclass: top
olcmoduleload: <nom_module>.la
olcmodulepath: /usr/lib/ldap
```

  - Envoyer le fichier au serveur ldap: `ldapadd -Y EXTERNAL -H ldapi:/// -f <fichier>.ldif`
  - Fichier de conf d'overlay (ex: memberOf):

```
n: olcOverlay=memberof,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: olcConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
```

  - Envoyer le fichier au serveur ldap: `ldapadd -Y EXTERNAL -H ldapi:/// -f <fichier>.ldif`

- Vérification:
  - `tree /etc/ldap/slapd.d/`
  - `ldapsearch -QLLLY EXTERNAL -H ldapi:/// -b "cn=config" "Objectclass=olcmemberOf"`

- Structure de l'annuaire ldap:

```
dc=henallux,dc=local
├── ou=group,dc=henallux,dc=local
│   ├── ou=techinfo,ou=group,dc=henallux,dc=local
│   └── ou=security,ou=group,dc=henallux,dc=local
│   ou=people,dc=henallux,dc=local
│   ├── ou=administration,ou=people,dc=henallux,dc=local
│   └── ou=profs,ou=people,dc=henallux,dc=local
├── ou=section,dc=henallux,dc=local
└── ou=system,dc=henallux,dc=local
```

- Créer les OU (= organizational unit) (pas complet pour prendre moins de place):

```
dn: ou=people,dc=henallux,dc=local
ou: people
objectClass: organizationalUnit

dn: ou=section,dc=henallux,dc=local
ou: section
objectClass: organizationalUnit

dn: ou=group,dc=henallux,dc=local
ou: group
objectClass: organizationalUnit

dn: ou=system,dc=henallux,dc=local
ou: system
objectClass: organizationalUnit

dn: ou=administration,ou=people,dc=henallux,dc=local
ou: administration
objectClass: organizationalUnit
```

Envoyer au serveur: `ldapadd -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Créer un utilisateur:

```
dn: uid=olivier,ou=administration,ou=people,dc=henallux,dc=local
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: olivier
sn: olivier
givenName: Olivier
cn: Olivier
displayName: Olivier
userPassword: tttttt
mail: olivier@example.com
title: Admin
initials: N
```

Envoyer au serveur: `ldapadd -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Il y a 2 types de groupes:
  - `posixgroup`, équivalent à un groupe unix
  - `groupofnames`, équivalent à un groupe AD (problème: il doit toujours y avoir min 1 membre)
- Créer un groupe:

```
dn: cn=secugrpa,ou=security,ou=group,dc=henallux,dc=local
cn: secugrpa
description: Securite Groupe A
objectClass: groupOfNames
member: cn=admin,dc=henallux,dc=local

dn: cn=secugrpb,ou=security,ou=group,dc=henallux,dc=local
cn: secugrpb
description: Securite Groupe B
objectClass: groupOfNames
member: cn=admin,dc=henallux,dc=local
```

- Ajouter un membre à un groupe:

```
dn: cn=secugrpa,ou=security,ou=group,dc=henallux,dc=local
changetype: modify
add: member
member: uid=olivier,ou=administration,ou=people,dc=henallux,dc=local
```

- Créer les comptes systèmes `viewer` et `writer` qui peuvent lire/écrire dans l'annuaire:

```
dn: cn=viewer,ou=system,dc=henallux,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: viewer
description: LDAP viewer
userPassword: tttttt

dn: cn=writer,ou=system,dc=henallux,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: writer
description: LDAP Writer
userPassword: tttttt
```

- Afficher les ACL:

```
ldapsearch -xW -H ldap://localhost -D cn=admin,dc=henallux,dc=local \
    -b "cn=config" "olcDatabase={1}mdb" olcaccess
```

- Modifier les ACL:

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: to attrs=userPassword by self write
    by anonymous auth
    by dn="cn=writer,ou=system,dc=henallux,dc=local" write
    by dn="cn=viewer,ou=system,dc=henallux,dc=local" read
    by dn="cn=admin,dc=henallux,dc=local" write
    by * none
olcAccess: to dn.base="dc=henallux,dc=local" by users read
```

```
olcAccess: to * by self write
    by dn="cn=admin,dc=henallux,dc=local" write
    by * read by anonymous none
```

Envoyer au serveur: `ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f acl.ldif`

- Modifier une OU:

```
dn: ou=test,ou=people,dc=henallux,dc=local
changetype: modrdn
newrdn: ou=retest
deleteoldrdn: 1
```

Envoyer au serveur: `ldapmodify -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Déplacer une OU:

```
dn: ou=retest,ou=people,dc=henallux,dc=local
changetype: modrdn
newrdn: ou=retest
deleteoldrdn: 1
newsuperior: ou=techinfo,ou=group,dc=henallux,dc=local
```

Envoyer au serveur: `ldapmodify -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Supprimer une OU (elle doit être vide) – méthode 1:

```
dn: ou=retest,ou=techinfo,ou=group,dc=henallux,dc=local
changetype: delete
```

Envoyer au serveur: `ldapmodify -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Supprimer une OU (elle doit être vide) – méthode 2:

```
ou=retest,ou=techinfo,ou=group,dc=henallux,dc=local
```

Envoyer au serveur: `ldapdelete -cxWD cn=admin,dc=henallux,dc=local -f <fichier>.ldif`

- Déplacer un utilisateur:

```
dn: uid=jean,ou=administration,ou=people,dc=henallux,dc=local
changetype: modrdn
newrdn: uid=jean
deleteoldrdn: 1
newsuperior: ou=profs,ou=people,dc=henallux,dc=local
```

- Déplacer un groupe:

```
dn: cn=secugrpa,ou=security,ou=group,dc=henallux,dc=local
changetype: modrdn
newrdn: cn=secugrpa
deleteoldrdn: 1
newsuperior: ou=techinfo,ou=group,dc=henallux,dc=local
```

- Renommer un utilisateur:

```
dn: uid=jean,ou=profs,ou=people,dc=henallux,dc=local
changetype: modrdn
newrdn: uid=pierre
deleteoldrdn: 1
```

- Renommer un groupe:

```
dn: cn=secugrpa,ou=techinfo,ou=group,dc=henallux,dc=local
changetype: modrdn
newrdn: cn=tigrpb
deleteoldrdn: 1
```

- Supprimer un utilisateur – méthode 1:

```
dn: uid=pierre,ou=profs,ou=people,dc=henallux,dc=local
changetype: delete
```

- Supprimer un utilisateur – méthode 2 (directement en ligne de commande):

```
ldapdelete -cxWD cn=admin,dc=henallux,dc=local \
    uid=pierre,ou=profs,ou=people,dc=henallux,dc=local
```

- Supprimer un groupe – méthode 1:

```
dn: cn=tigrpb,ou=techinfo,ou=group,dc=henallux,dc=local
changetype: delete
```

- Supprimer un groupe – méthode 2 (directement en ligne de commande):

```
ldapdelete -cxWD cn=admin,dc=henallux,dc=local \
    cn=tigrpb,ou=techinfo,ou=group,dc=henallux,dc=local
```

- Ajouter un attribut à un utilisateur:

```
dn: uid=olivier,ou=administration,ou=people,dc=henallux,dc=local
changetype: modify
add: localityName
localityName: Namur
```

- Modification d'attribut utilisateur:

```
dn: uid=carl,ou=administration,ou=people,dc=henallux,dc=local
changetype: modify
replace: UserPassword
UserPassword: rrrrrr
```

- Modification de mot de passe utilisateur:

```
ldappasswd  -WS -H ldap://localhost
    -D "uid=olivier,ou=administration,ou=people,dc=henallux,dc=local"
```

- Modification d'attribut groupe:

```
dn: uid=olivier,ou=administration,ou=people,dc=henallux,dc=local
changetype: modify
replace: localityName
localityName: Bruxelles
```

- Supprimer un attribut utilisateur:

```
dn: uid=olivier,ou=administration,ou=people,dc=henallux,dc=local
changetype: modify
delete: localityName
```

- Supprimer un attribut groupe:

```
dn: cn=tigrpa,ou=techinfo,ou=group,dc=henallux,dc=local
changetype: modify
delete: member
member: uid=carl,ou=administration,ou=people,dc=henallux,dc=local
```