ADeleg

Un outil de gestion des permissions d'un Active Directory

Aurélien Bordes – Matthieu Buffet

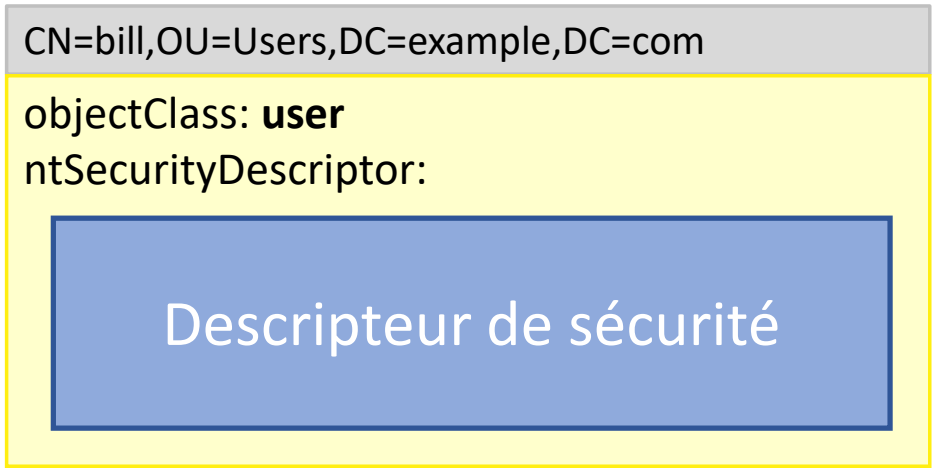
SSTIC – 1er juin 2022

Les objectifs d'ADeleg

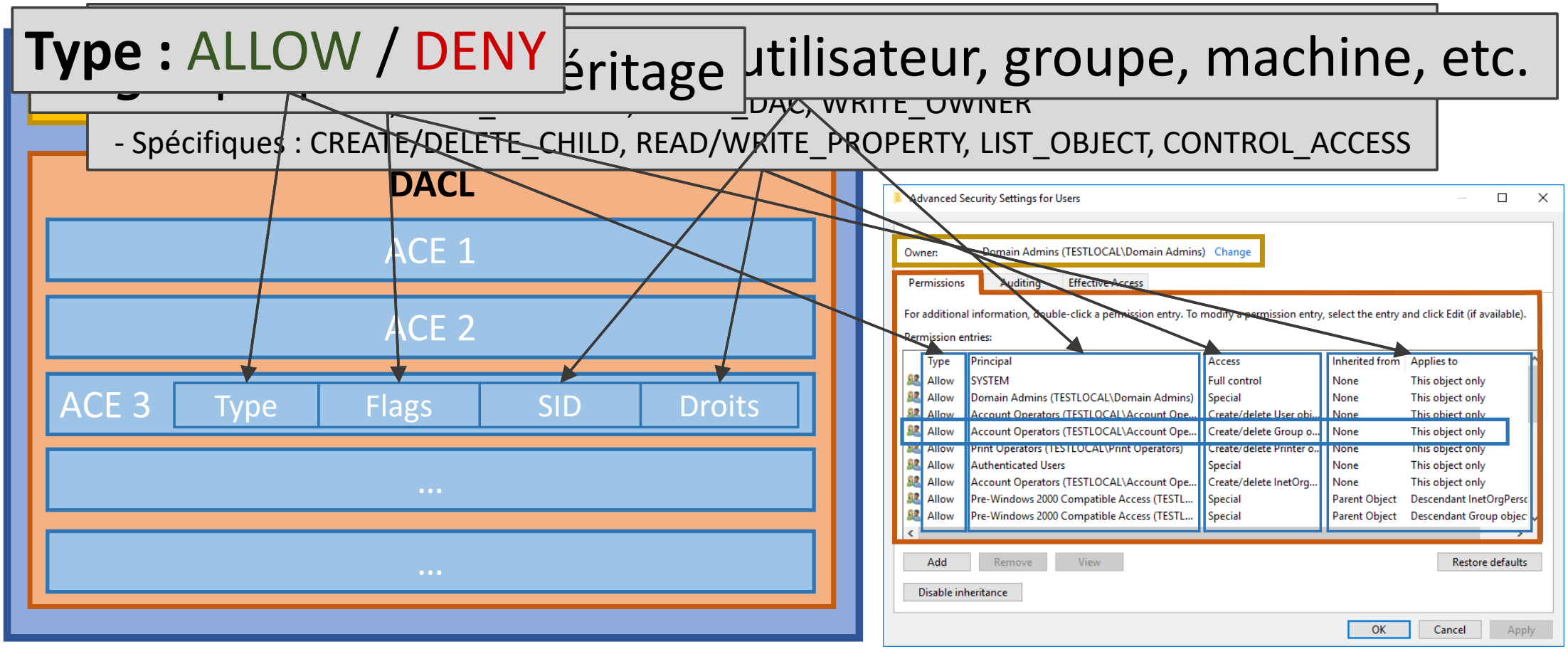
- ADeleg est outil qui permet de faciliter la gestion des permissions dans les annuaires Active Directory
- La gestion des permissions dans les AD peut-être difficile et complexe
- 3 cas d'utilisation d'ADeleg :
  - Peu ou pas de gestion des permissions car trop complexe
  - Erreurs dans les mises en place des permissions par les administrateurs
  - Voir et comprendre les permissions positionnées par les produits tiers

Contrôle d'accès dans l'Active Directory

- Le contrôle d'accès des objets d'un annuaire Active Directory repose sur le contrôle d'accès de Windows
- Chaque objet dispose d'un **descripteur de sécurité** indiquant, en autre, le **propriétaire** et les **autorisations d'accès** sur l'objet (suppression, lecteur/écriture d'attribut, énumération des fils, etc.)

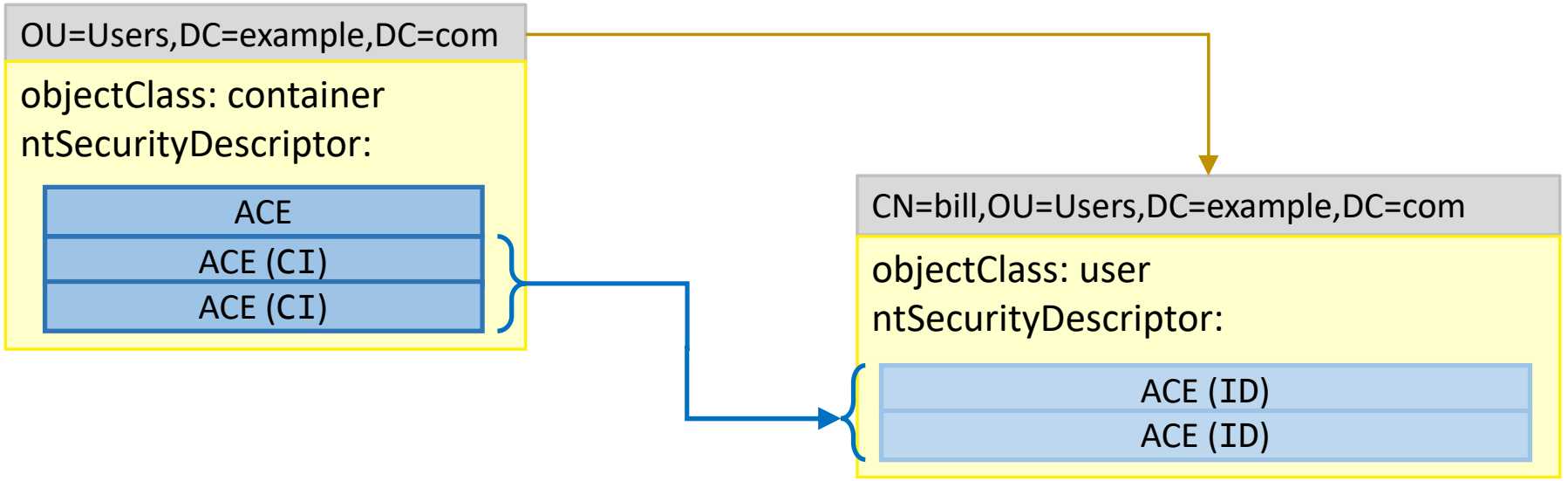


Descripteur de sécurité (simplifié)



Héritage des ACE

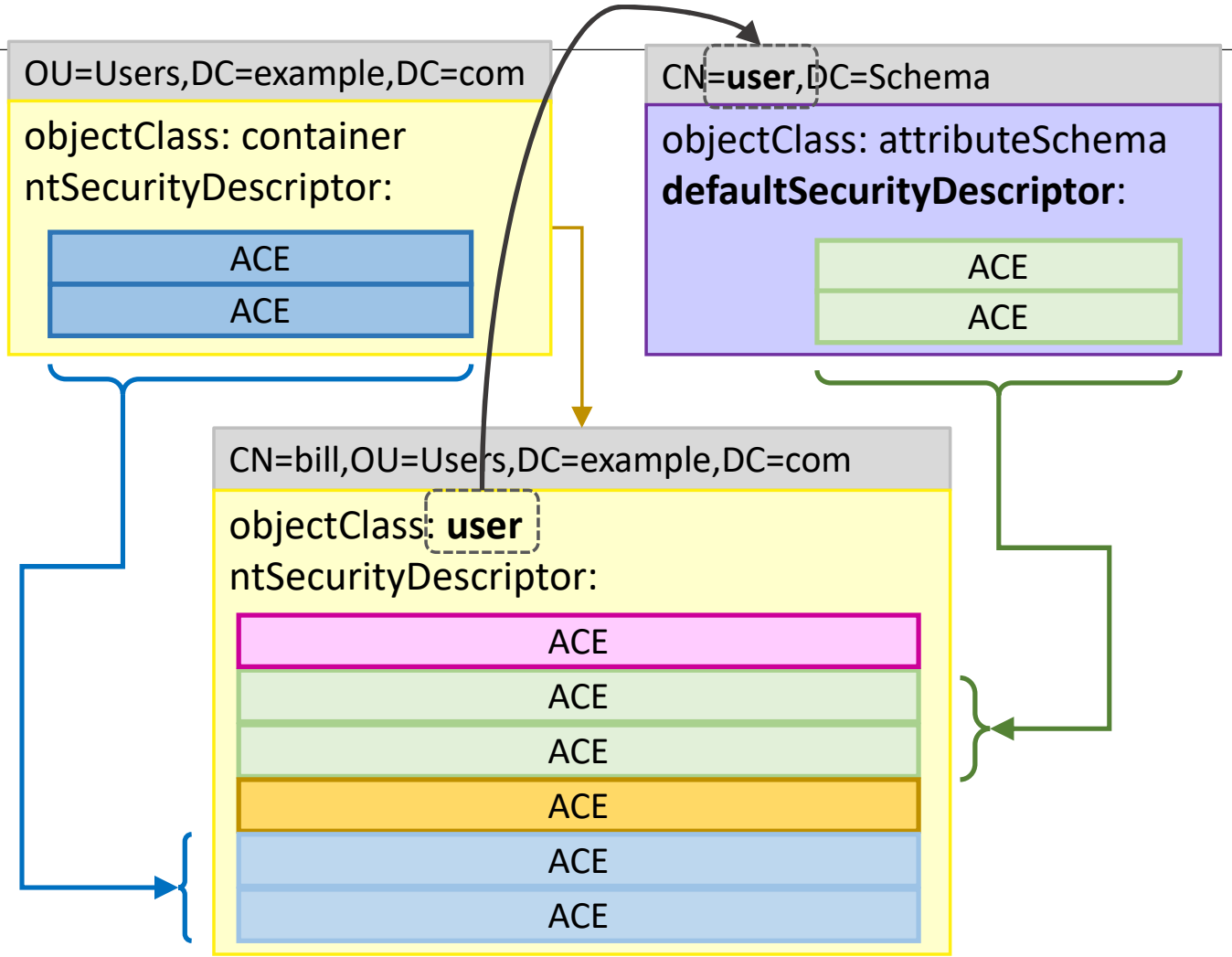
- L'Active Directory, de par son organisation hiérarchique, permet l'**héritage des permissions**
- Une ACE sur un objet, marquée comme « héritable » (CI), se voit dupliquée sur les fils de l'objet et les ACE sont alors marquées comme « héritées » (ID)
- La cohérence de l'héritage dans un AD est assurée par le « SDProp »

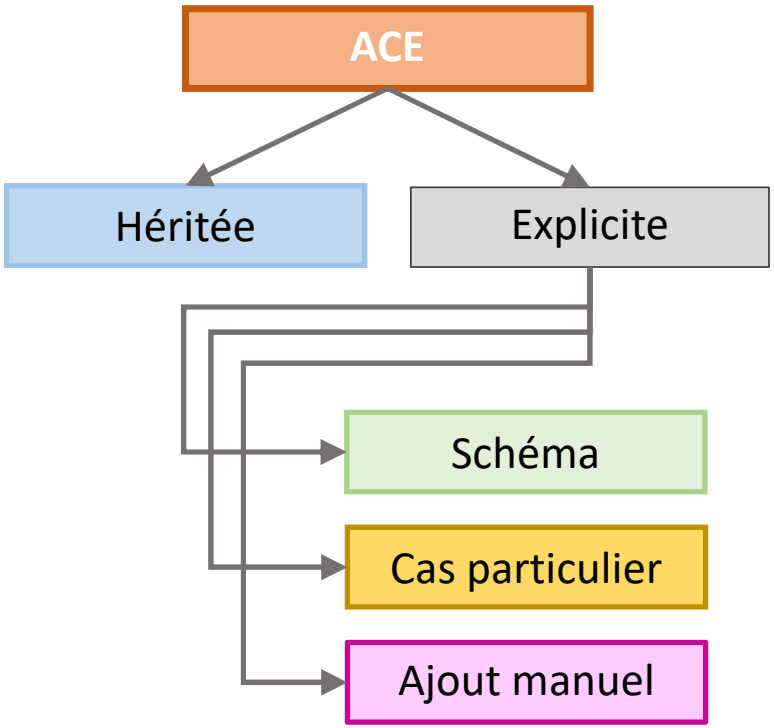


Permissions définies dans le schéma

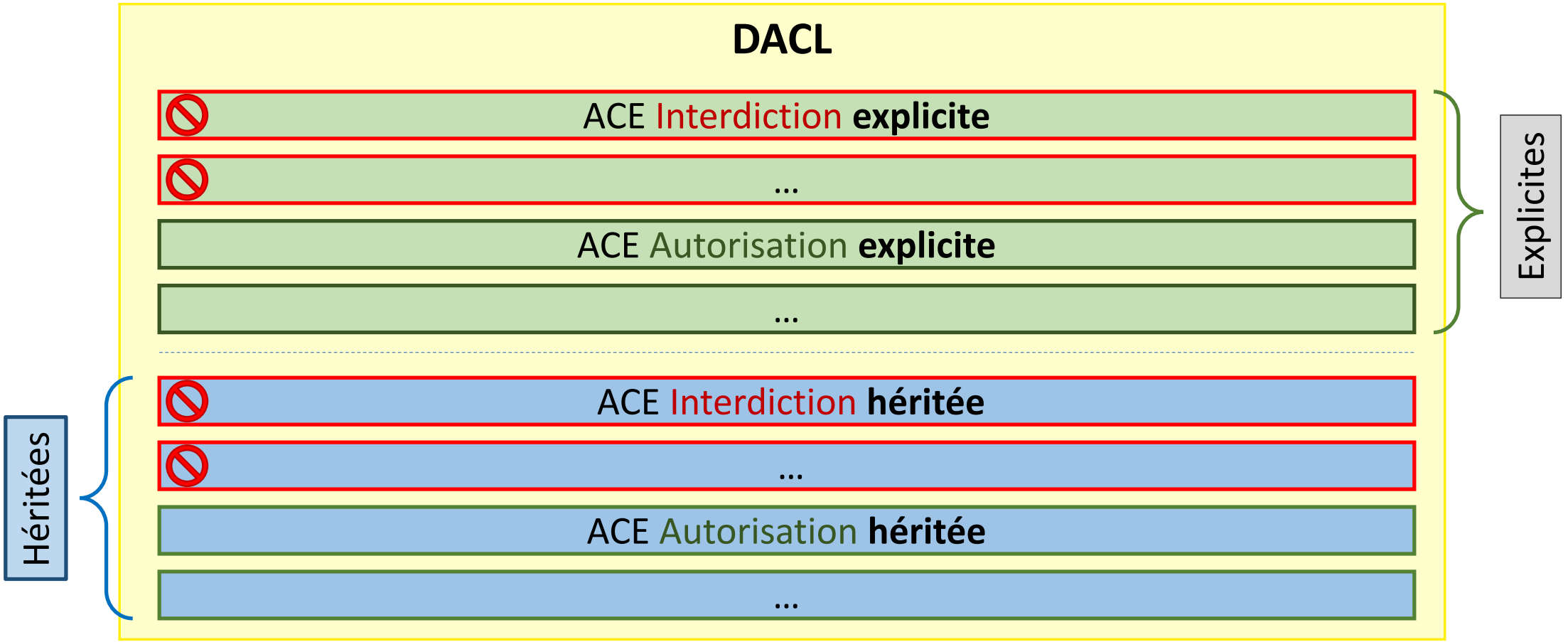
- La structure d'un annuaire est décrite dans le **schéma** qui définit :
  - Les types d'objets (**classes**)
  - Les propriétés des objets (**attributs**)
- Pour chaque classe d'objets (utilisateur, groupe, GPO, etc.), un descripteur de sécurité « par défaut » est défini
- Ce descripteur de sécurité par défaut est appliqué quand :
  - Un objet est créé
  - Les permissions sur un objet sont « réinitialisées »

Origines des ACE sur un objet





Ordre des ACE (ordre canonique)



Points d’analyse et erreurs possibles

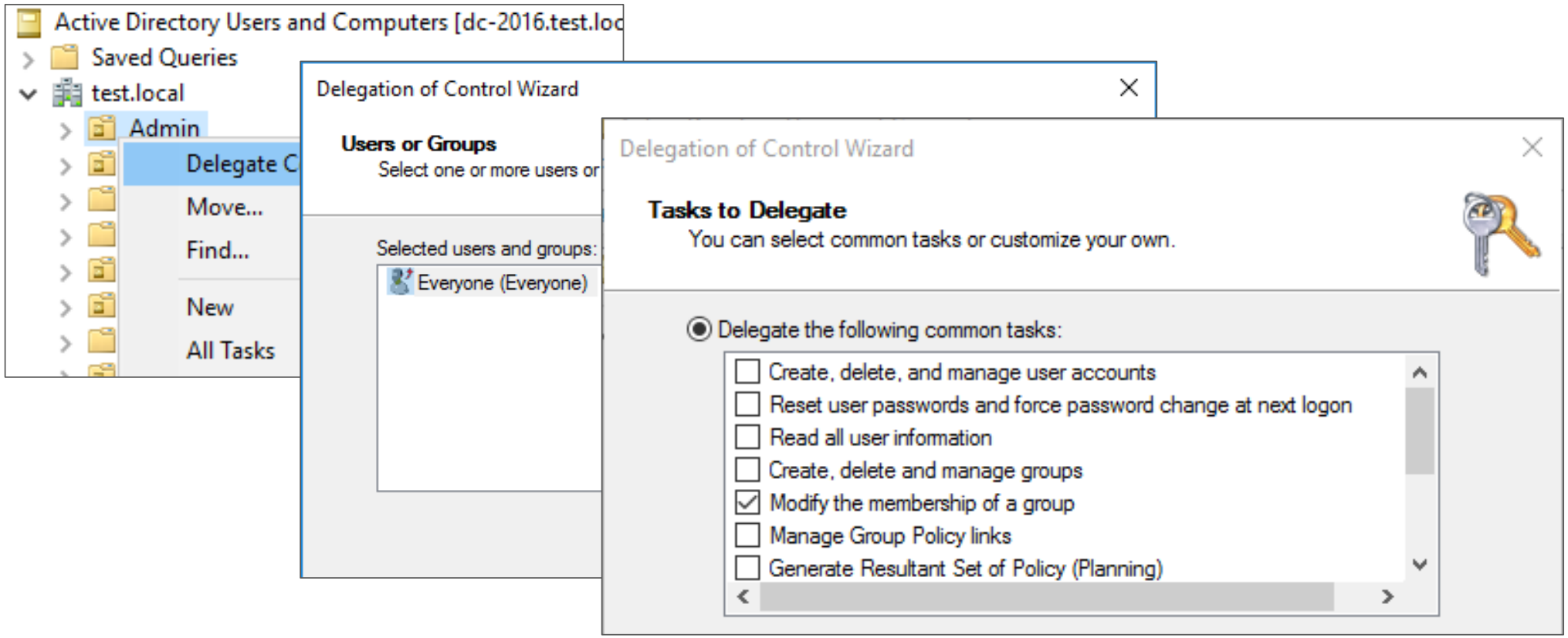
- Non respect de l’ordre canonique
- Modification des permissions par défaut dans le schéma
- ACE à destination d’un compte supprimé
- Blocage d’héritage
- Propriétaire modifié
- ACE explicite

Vidéo 1

La délégation d'administration

- Les délégations sont des opérations primordiales pour la sécurité de l'Active Directory
- L'objectif est de ne pas réaliser les opérations d'administration avec des comptes très privilégiés (*i.e.* Administrateurs du domaine)
- La délégation permet de limiter :
  - Les opérations d'administration (droits associés)
  - La portée (*scoping*)

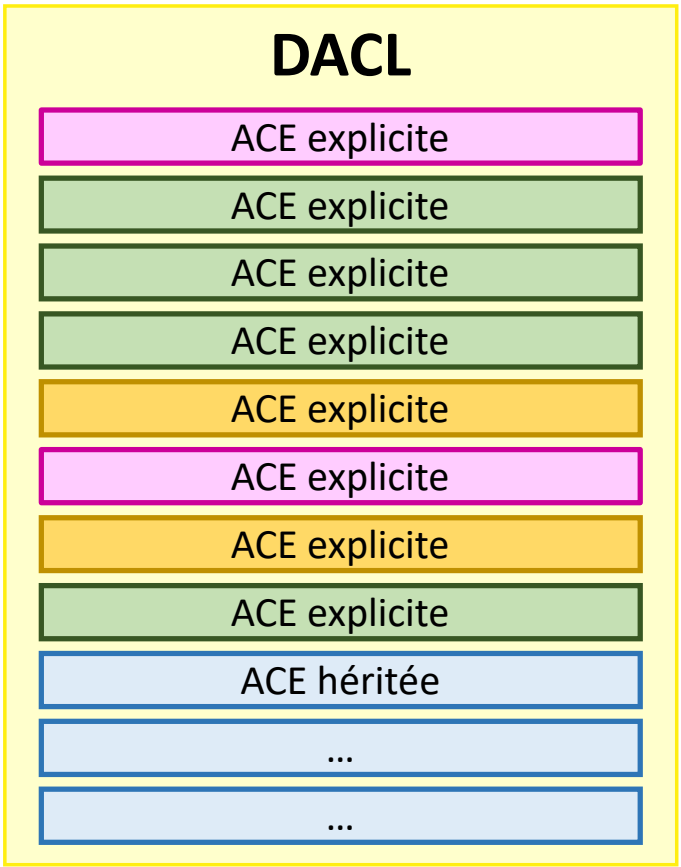
La délégation… Facile à faire

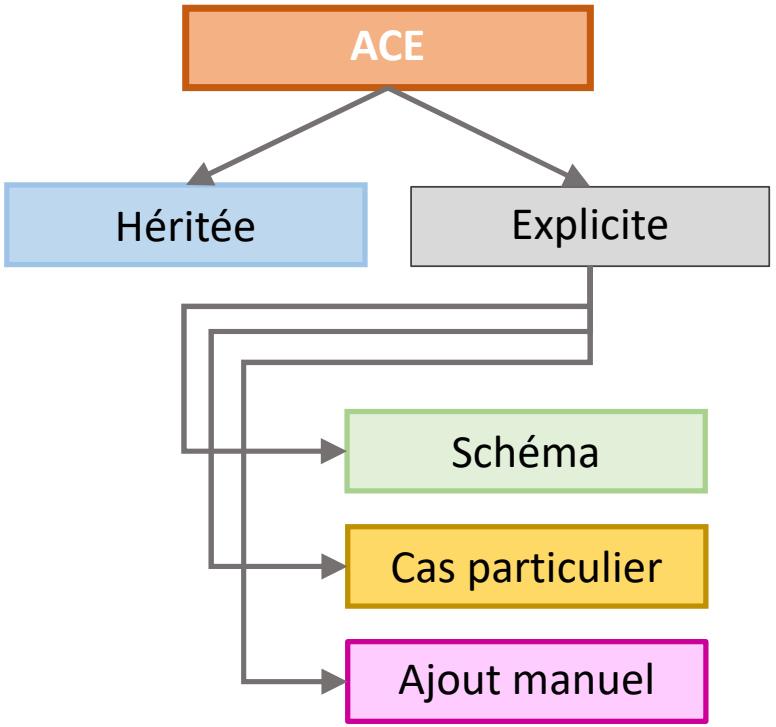


La délégation… Difficile à inventorier

```
Dn: OU=Admin,DC=test,DC=local
  distinguishedName: OU=Admin,DC=test,DC=local;
  name: Admin;
  nTSecurityDescriptor: O:DAD:AI (OA;;CCDC;4828cc14-1437-45bc-9b07-
    ad6f015e5f28;;AO)(OA;;CCDC;bf967a86-0de6-11d0-a285-00aa003049e2;;AO)(OA;;CCDC;bf967a9c-0de6-11d0-
    a285-00aa003049e2;;AO)(OA;;CCDC;bf967aa8-0de6-11d0-a285-00aa003049e2;;PO)(OA;;CCDC;bf967aba-0de6-
    11d0-a285-00aa003049e2;;AO)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DA)(A;;LCRPLORC;;;AU)
    (OA;CIIO;RPWP;bf9679c0-0de6-11d0-a285-00aa003049e2;bf967a9c-0de6-11d0-a285-00aa003049e2;WD)
    (A;;LCRPLORC;;;ED)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-
    5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;CO)(OA;CIIOID;SW;9b026da6-0d3c-465c-8bee-
    5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;PS)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-
    00a0c983f608;bf967a86-0de6-11d0-a285-00aa003049e2;ED)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-
    00a0c983f608;bf967a9c-0de6-11d0-a285-00aa003049e2;ED)(OA;CIIOID;RP;b7c69e6d-2cc7-11d2-854e-
    00a0c983f608;bf967aba-0de6-11d0-a285-00aa003049e2;ED)(OA;CIIOID;WP;ea1b7b93-5e48-46d5-bc6c-
    4df4fda78a35;bf967a86-0de6-11d0-a285-00aa003049e2;PS)(OA;CIIOID;LCRPLORC;;4828cc14-1437-45bc-9b07-
    ad6f015e5f28;RU)(OA;CIIOID;LCRPLORC;;bf967a9c-0de6-11d0-a285-
    00aa003049e2;RU)(OA;CIIOID;LCRPLORC;;bf967aba-0de6-11d0-a285-
    00aa003049e2;RU)(OA;CIID;RPWP;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;PS)(OA;CIID;RPWPCR;91e647de-
    d96f-4b70-9557-d63ff4f3ccd8;;PS)(A;CIID;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;EA)(A;CIID;LC;;;RU)
    (A;CIID;CCLCSWRPWPLOCRSDRCWDWO;;;BA);
```

Comment trouver une délégation ?





Vidéo 2

Modèle de délégation par ADeleg

- Les modèles d'administration AD (par exemple en *Tiering*) nécessitent la mise en place de délégations (permissions)
- ADeleg permet de mettre en place un modèle de délégation décrit dans des fichiers JSON :
  - Définition des droits des délégations (exemple : « *Reset user password without knowing their current one* »)
  - Définition des délégations (Qui / Où / Quoi)
- ADeleg calcule les ACE attendues et met en évidence les écarts par rapport au modèle

Exemple de délégations

```
{
   "name": "Reset user password without knowing their current one",
   "rights": [{
       "access_mask": "CONTROL_ACCESS",
       "object_type": "Reset Password",
    }, {
       "access_mask": "WRITE_PROPERTY",
       "object_type": "pwdLastSet",
    }]
}
```

Qui ? (samAccountName, SID)

Où ? (DN)

```
(OA;CIIO;WP;bf967a0a-0de6-11d0-a285-00aa003049e2;bf967aba-0de6-11d0-a285-00aa003049e2;S-1-5-21-298802938-646582368-2588077371-1104)
(OA;CIIO;CR;00299570-246d-11d0-a768-00aa006e0529;;S-1-5-21-298802938-646582368-2588077371-1104)
```

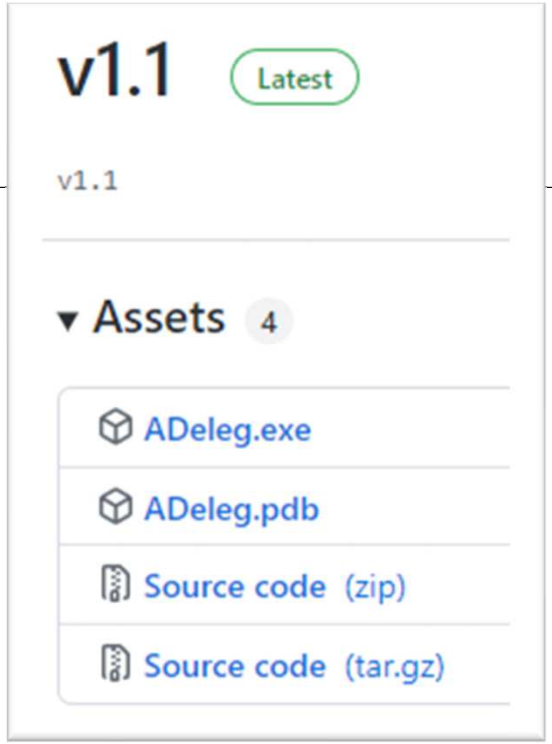
Quoi ? (Droit décrit ci-dessus)

```
[{
   "trustee": { "sam_account_name": "Tier2-Admins" },
   "resource": { "dn": "OU=Users,OU=Tier2,DC=example,DC=com" },
   "template": "Reset user password without knowing their current one"
}]
```

Vidéo 3

ADeleg

- https://github.com/mtth-bfft/adeleg



- Contributions bienvenues, à la fois sur le retour d'utilisation, sur le code ou sur les modèles de délégations qui sont fournis
- Si des besoins communs de modèle de délégation émergent, on les rajoutera (ouvrez une *issue*)

Questions ?

aurelien26@free.fr
matthieu@buffet.re