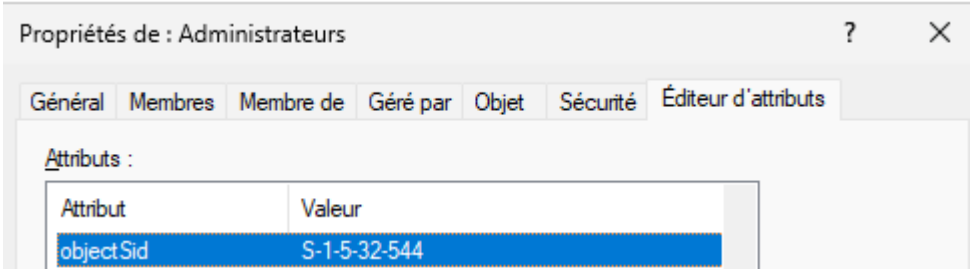
Le groupe Administrateurs

(environnement Active Directory)

Le groupe « Administrateurs »

Le groupe « Administrateurs » :

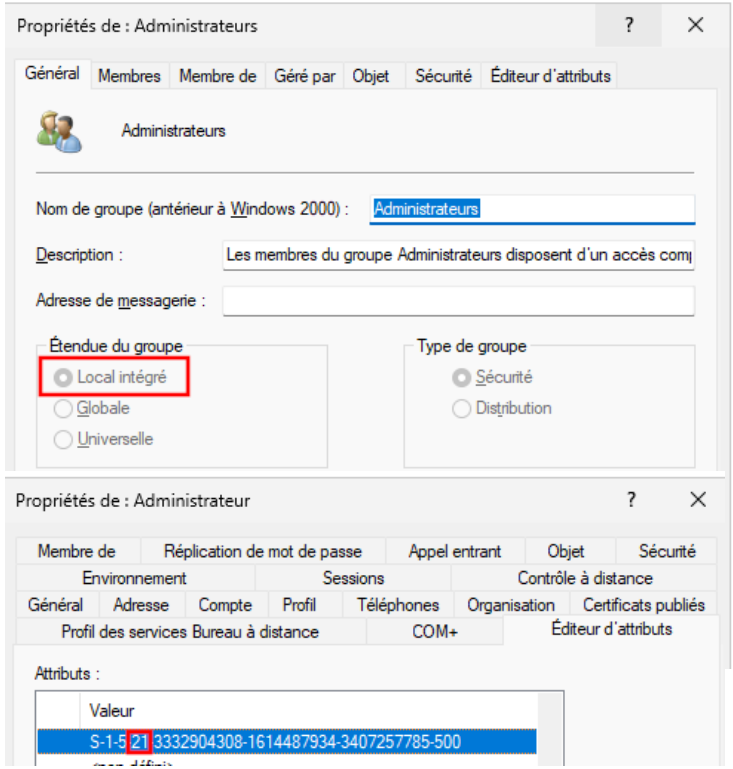
- Est un groupe local, présent sur tout système Windows (client ou serveur)
- Tout objet membre de ce groupe, dispose des privilèges les plus élevés sur la machine
- Son SID est donc un SID local : S-1-5-32-**544**



Le groupe « Administrateurs » > AD

Dans le contexte « Active Directory », malgré sa présence dans la console de gestion des utilisateurs et ordinateurs AD :

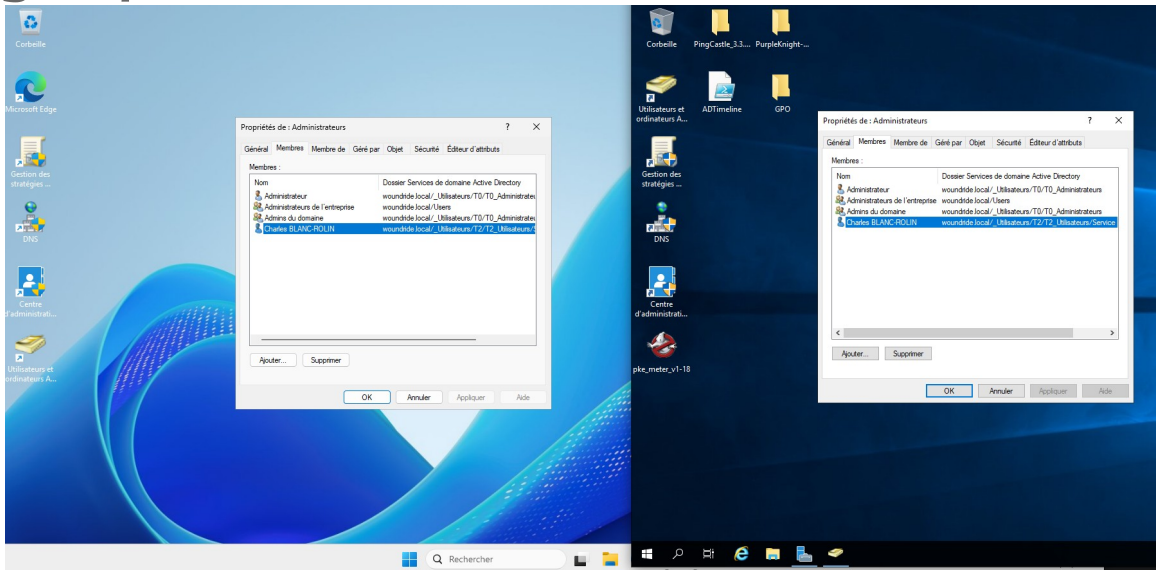
- Il reste un **groupe local**, contrairement à certaines croyances et au compte « administrateur », qui lui, devient un compte **utilisateur du domaine**
- Il est bien distinct du groupe « Admins du domaine »
- Il devient un groupe partagé entre les différents DC



Ajouts d'objets dans le groupe « Administrateurs »

Lorsqu'un objet est ajouté dans le groupe « Administrateurs » d'un DC :

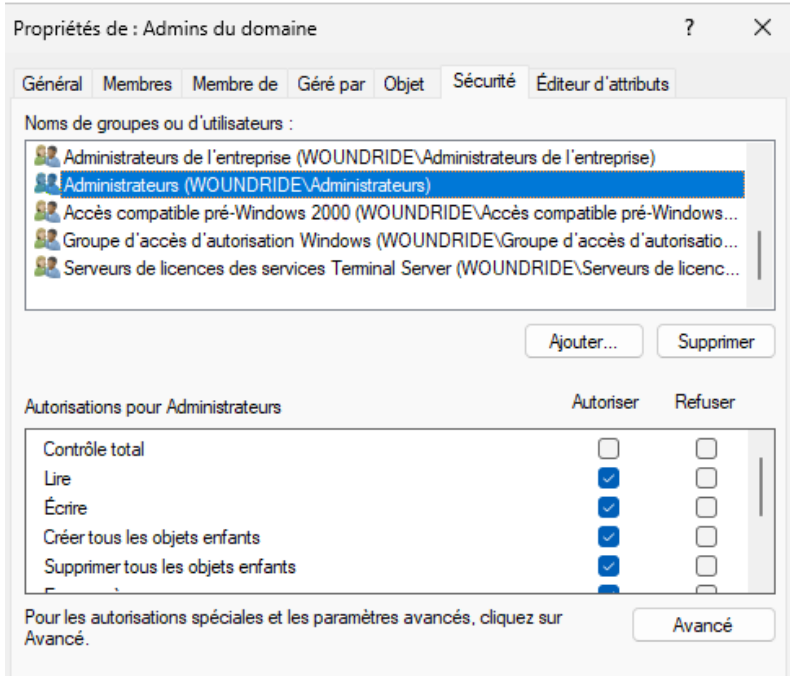
- Une synchronisation est faite entre les DC
- On retrouve donc l'objet ajouté dans le groupe « Administrateurs » du DC N°1, présent dans le groupe « Administrateurs » du DC N°2



« Administrateurs » VS « Admins du domaine »

Malgré leurs noms assez proches, ces groupes présentent des différences :

- « Administrateurs » dispose des privilèges les plus élevés pour l'administration des DC
- « Admins du domaine » dispose des privilèges les plus élevés pour l'administration de l'annuaire Active Directory (configuration, gestion des objets, des GPO...)
- Le groupe « Administrateurs », dispose des droits d'écriture, sur le groupe « Admins du domaine ». Ses membres ne peuvent donc pas administrer « directement » l'AD, mais seulement les DC. Ils peuvent en revanche se promouvoir eux-mêmes « Admins du domaine » .

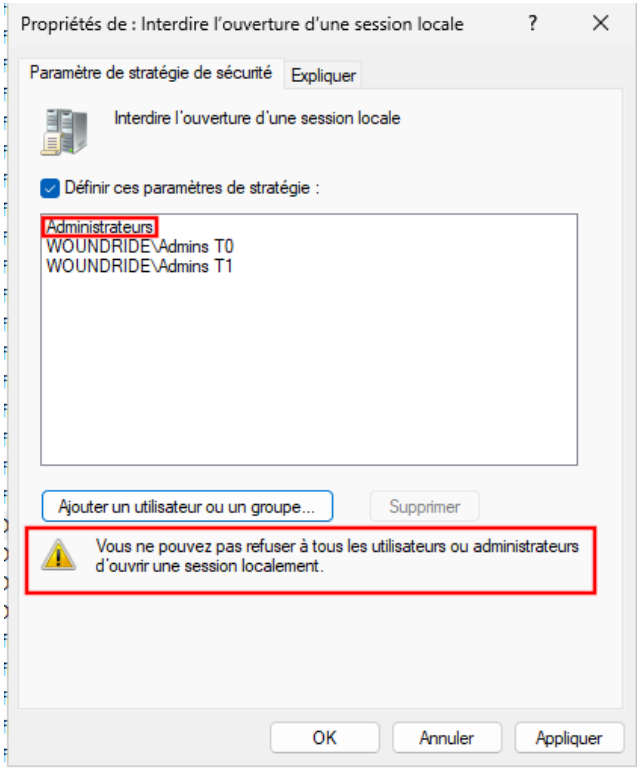


Difficultés dans l'application du Tiering model

La restriction d'ouverture de sessions via GPO n'est pas possible pour le groupe « Administrateurs » :

Pourquoi ?

- Car il s'agit d'un groupe local identique sur tous les ordinateurs Windows (PC ou serveurs).
- Son SID est donc le même sur les DC que sur toutes les machines du domaines.
- Interdire l'ouverture de session locale au groupe « Administrateurs » local revient à dire, plus d'administration possible des machines du domaines
- L'Active Directory vous en empêchera de toute façon !



Les membres du groupe « Administrateurs » > un vrai danger

Lorsqu'un objet est ajouté dans le groupe « Administrateurs » d'un DC :

- Il devient indirectement un administrateur du domaine puisqu'il peut se placer lui même dans le groupe « Admins de domaine ».

- S'il n'est pas membre du groupe « Admins de domaine » initialement, ou membre d'un groupe restreint du domaine (comme Admins T0 vu précédemment), il pourra ouvrir une session locale sur un PC du Tier 2.

- Si le PC du T2 est compromis, l'attaquant pourra devenir en quelques secondes, administrateur du domaine et compromettre l'ensemble du SI.

Illustration de ce risque majeur

L'ordinateur PC11 appartient à l'UO T2 (ordinateurs), sur laquelle la restriction d'ouverture de session s'applique aux administrateurs T1 et T0 :

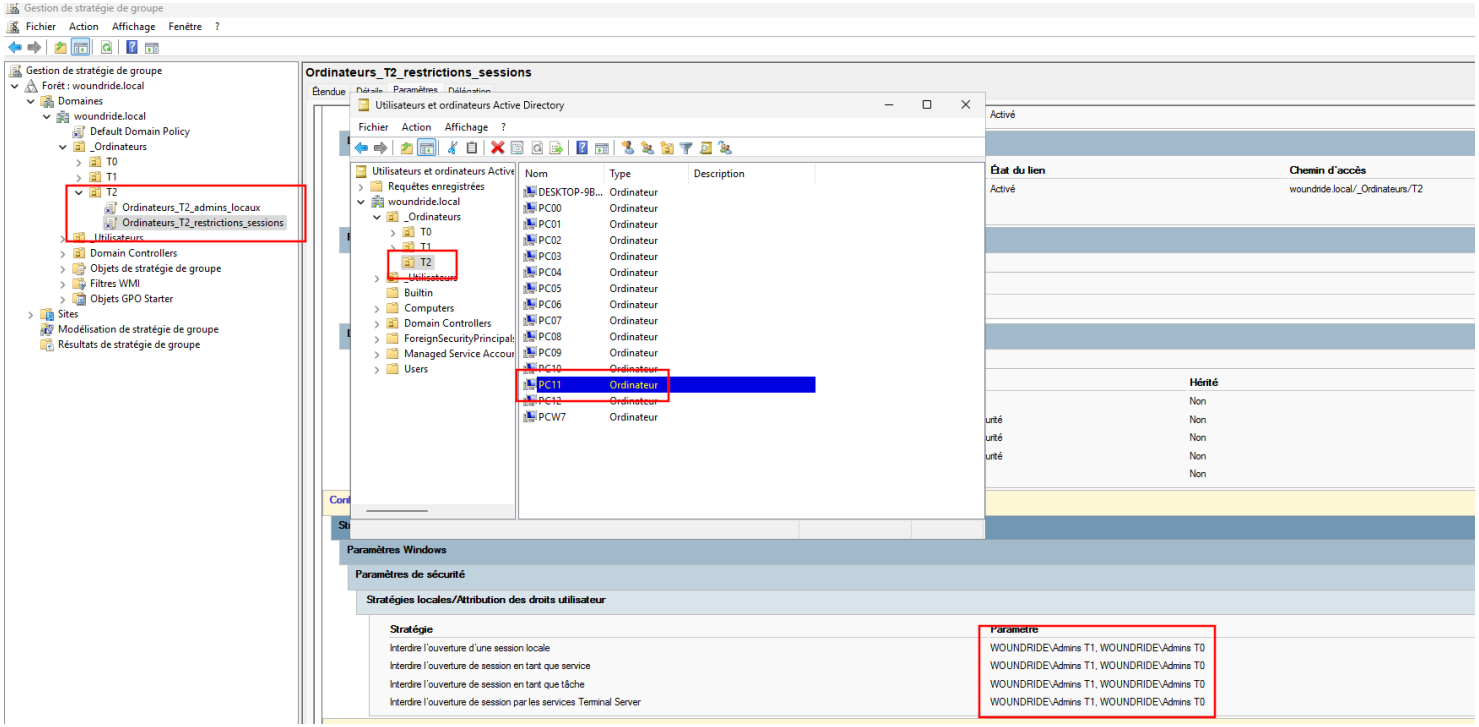
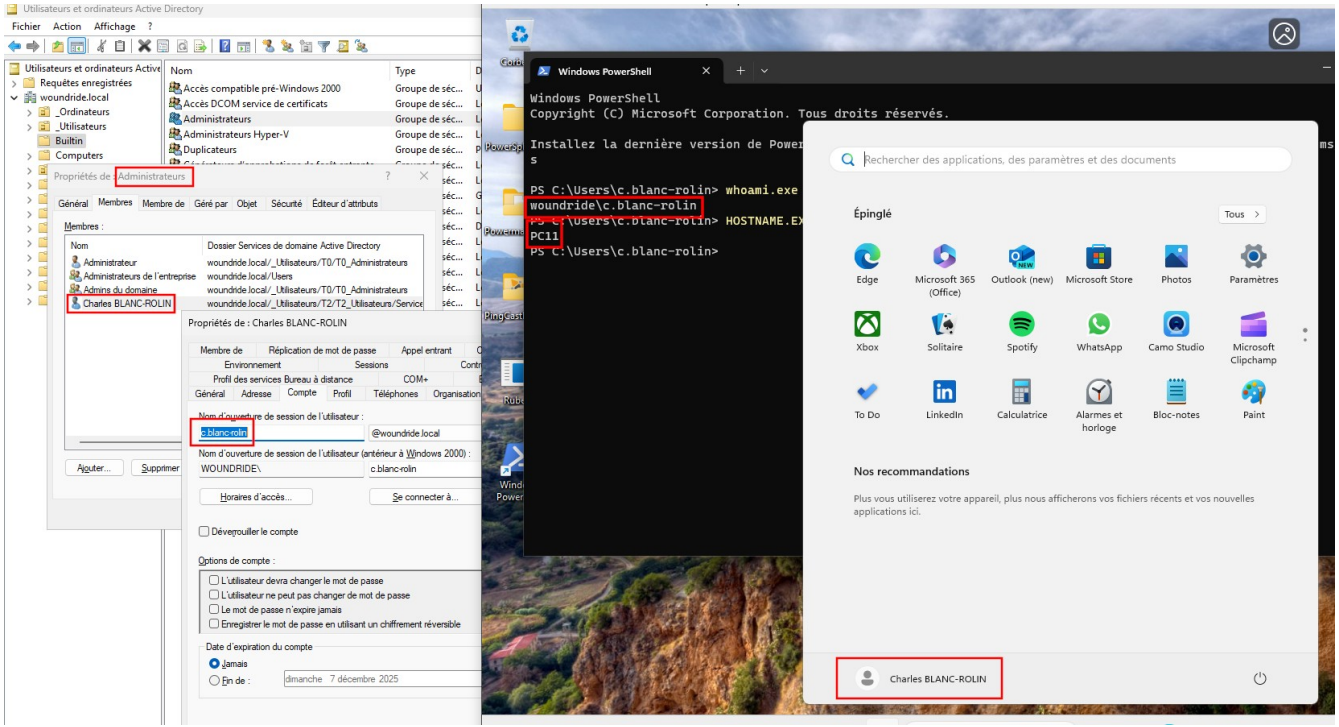


Illustration de ce risque majeur

Le compte c.blanc-rolin est membre du groupe « Administrateurs » (devant être considéré comme T0) et peut ouvrir une session locale sur PC11 :



Ressources et outils utilisés

- Comptes protégés et groupes dans Active Directory
  https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory

- Active Directory security groups
  https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

- Guide ANSSI – Administration sécurisée de l'AD
  https://cyber.gouv.fr/sites/default/files/document/anssi-guide-admin_securisee_si_ad_v1-0%20%283%29.pdf

- Security identifiers
  https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers