Administration sécurisée et Tiering

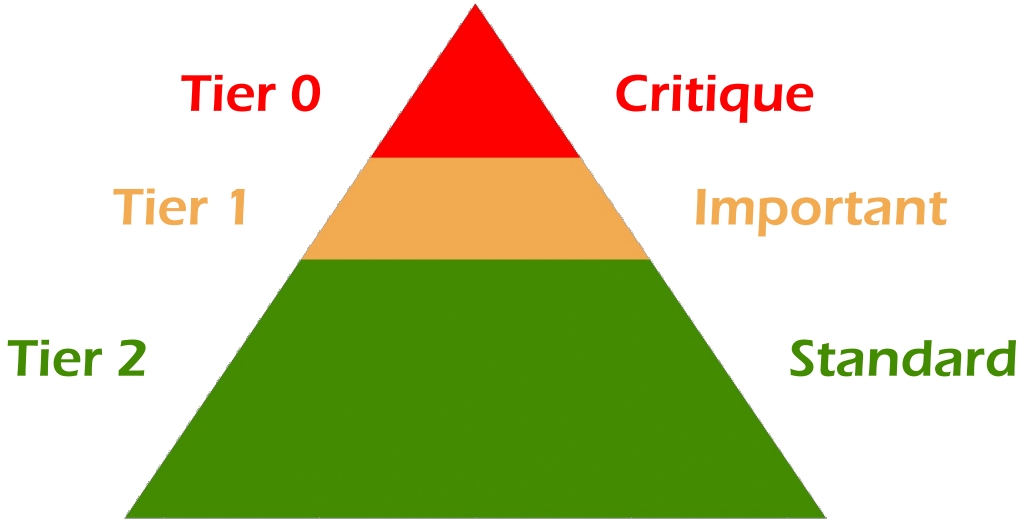
(environnement Active Directory)

Version 1.1 - 2025

Principe de l'architecture en Tier

Classifier les ressources en niveaux (Tiers) :

- Chaque niveau (tier) représente un niveau de criticité



Le nombre de niveaux (tiers) n'est pas limité et doit être adapté au contexte

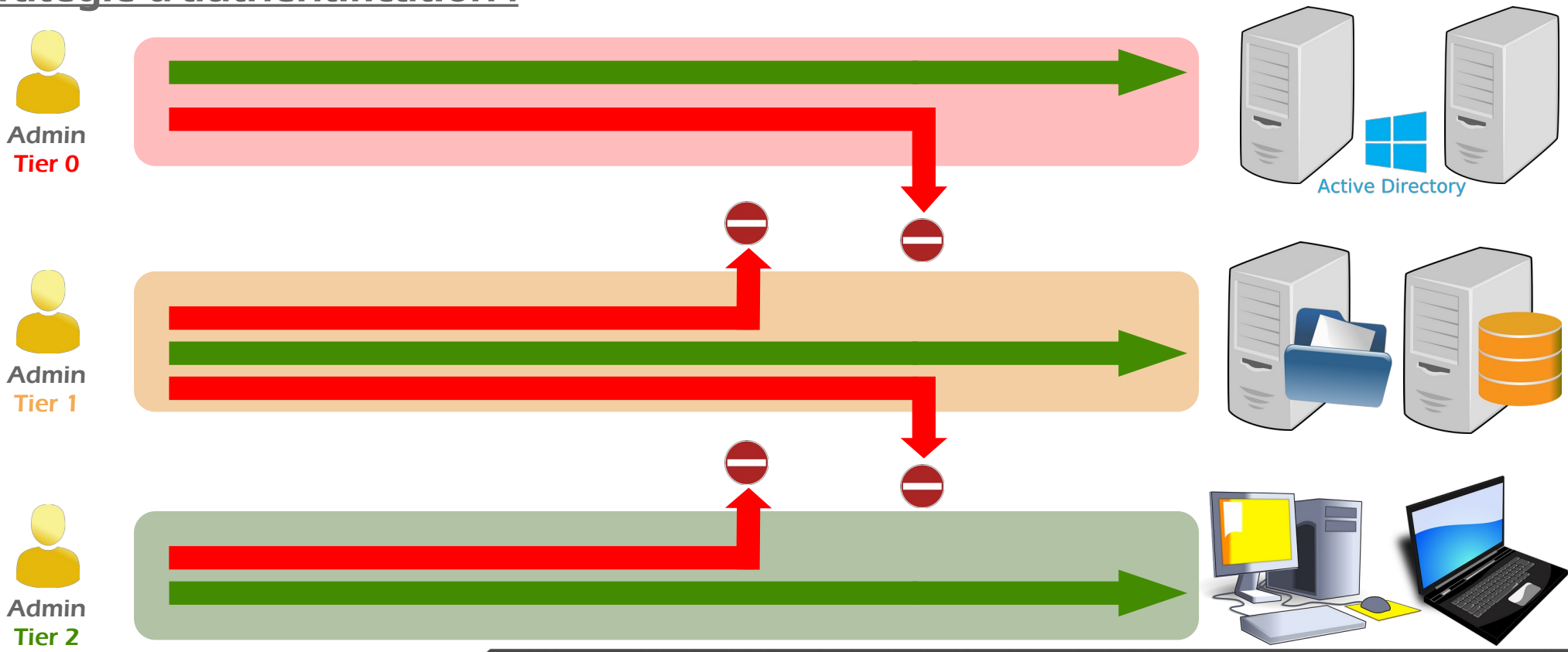
Principe de l'architecture en Tier

Segmenter les accès :

- Les ressources (machines) d'un niveau ne doivent être administrées que par des comptes d'administration dédiés à ce niveau
- Les actifs les plus sensibles (contrôleurs de domaine, PKI, postes d'administration...) ne doivent être accessible que par des comptes d'administration dédiés à ce niveau, appelé Tier 0
- À l'inverse, des comptes d'administration du Tier 0 ne doivent pas pouvoir ouvrir de sessions locales sur une machine d'un Tier inférieur

Principe de l'architecture en Tier

Stratégie d'authentification :



Principe de l'architecture en Tier

Stratégie d'authentification :

- Un administrateur système en charge de l'administration des différents Tiers, aura donc autant de comptes d'administration qu'il y a de Tiers
- Sans oublier son compte utilisateur pour les tâches du quotidien (surf web, accès à la messagerie, outils collaboratifs...)
- Une stratégie pas toujours facile à faire adopter

Les risques dont on veut se protéger

Compromission d'une machine = compromission possible du compte utilisateur connecté :

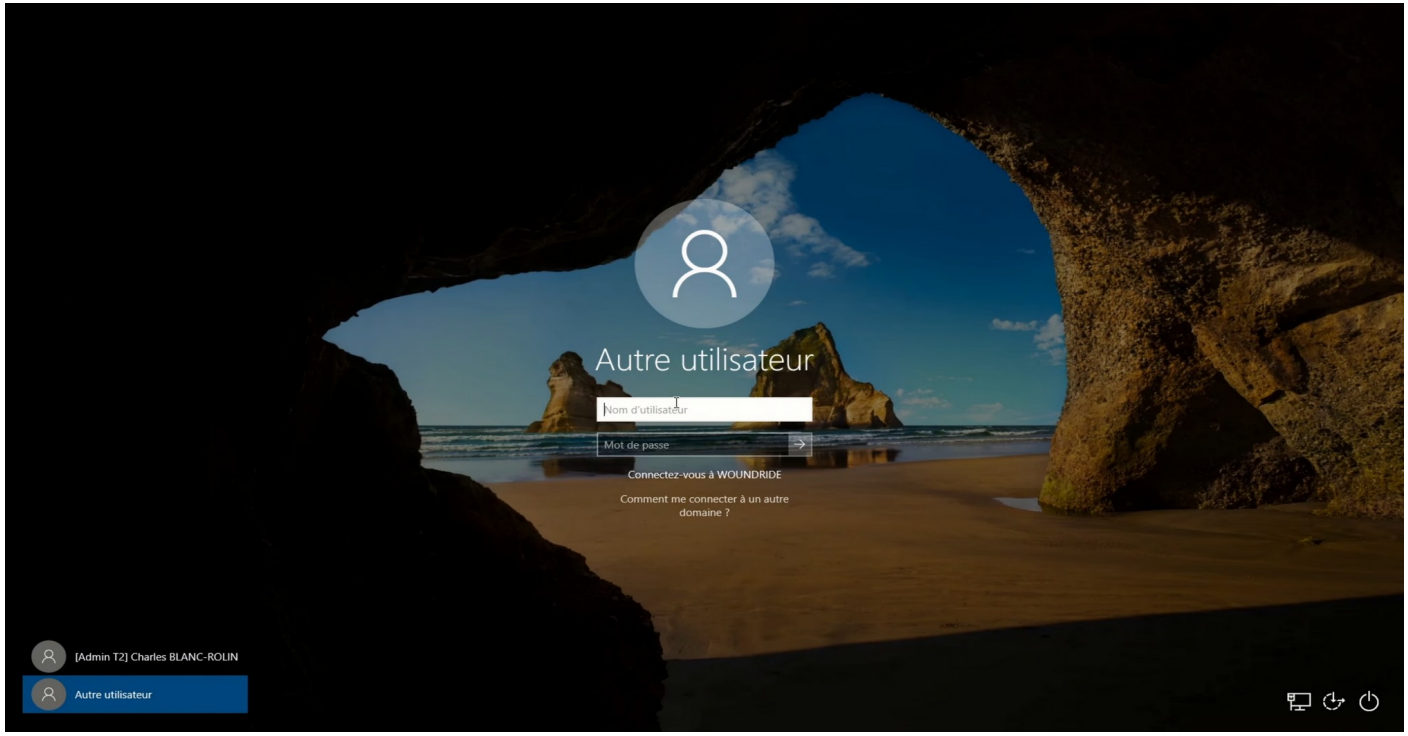
- Scénario : l'utilisateur exécute du code malveillant (fichier reçu en pièce jointe d'un courriel, lien malveillant...) sur une machine permettant à l'attaquant d'obtenir un accès

- Avec des privilèges élevés (administrateur local), l'attaquant pourra extraire les données d'authentification (identifiant(s) + mot(s) de passe ou condensat(s)) du processus LSASS exécuté en mémoire

- Si un compte administrateur du domaine a ouvert une session sur la machine : JACKPOT pour l'attaquant !

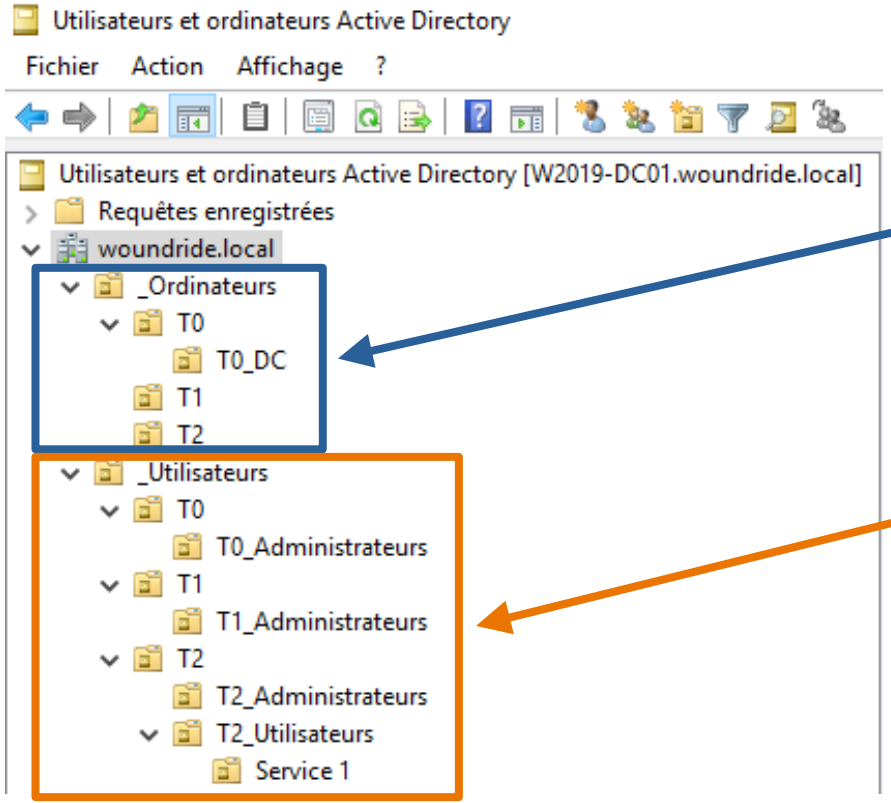
Exemple de compromission d'un compte admin du T2

Tier 2



Mise en place de l'architecture en Tier

Création de l'arborescence (Unités d'organisation) :

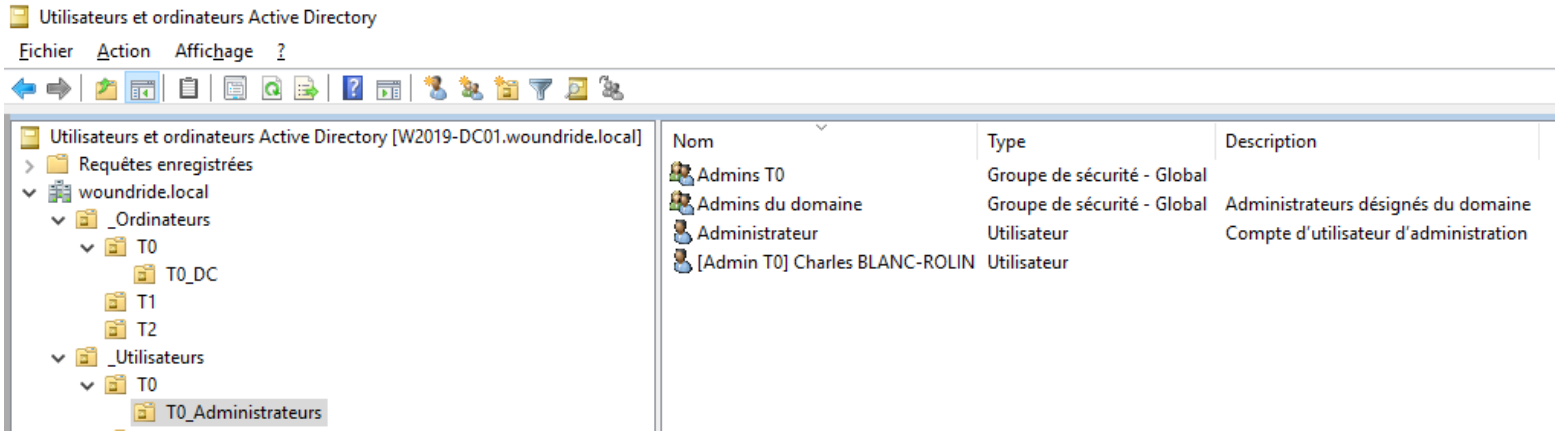


Arborescence pour stocker les objets de type « comptes d'ordinateurs » avec les différents niveaux (Tier 0, Tier 1 et Tier 2)

Arborescence pour stocker les objets de type « comptes utilisateurs » avec les différents niveaux (Tier 0, Tier 1 et Tier 2)

Mise en place de l'architecture en Tier

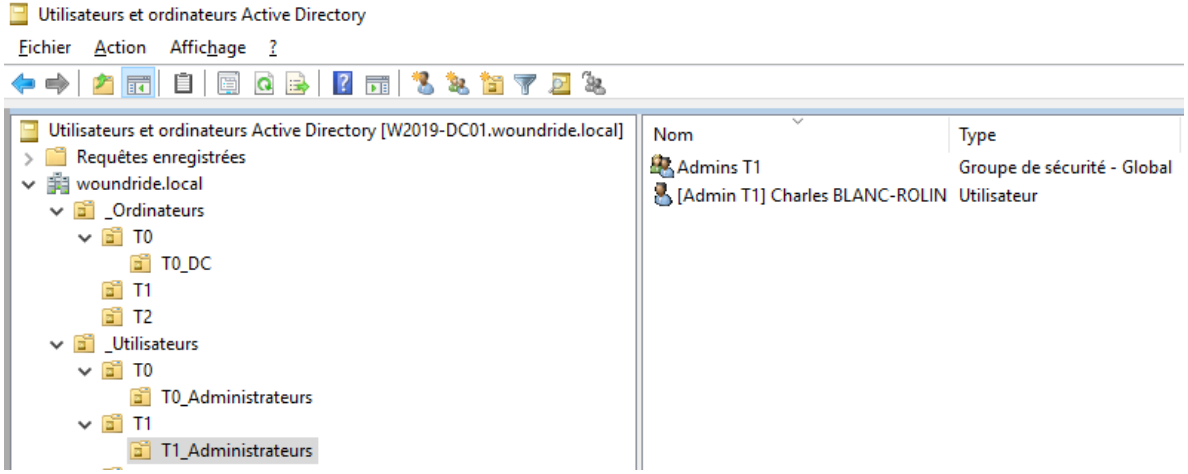
Rangement / création des comptes d'administrateurs (Tier 0) :



- On retrouve ici les administrateurs avec les privilèges les plus élevés (administrateurs du domaine)
- Ces comptes ne doivent en aucun cas pouvoir se connecter à des serveurs ou ordinateurs d'un niveau inférieur aux contrôleurs de domaine (DC)
- Pour faciliter la gestion des privilèges, on peut créer un groupe « Admin T0 » auquel seront rattachés les comptes utilisateurs d'administration du Tier 0 (Admins du domaine)

Mise en place de l'architecture en Tier

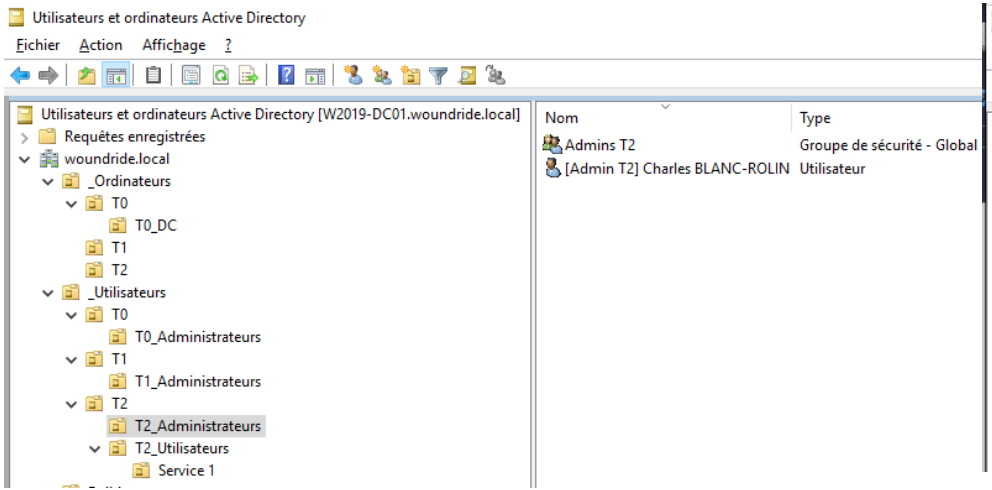
Rangement / création des comptes d'administrateurs (Tier 1) :

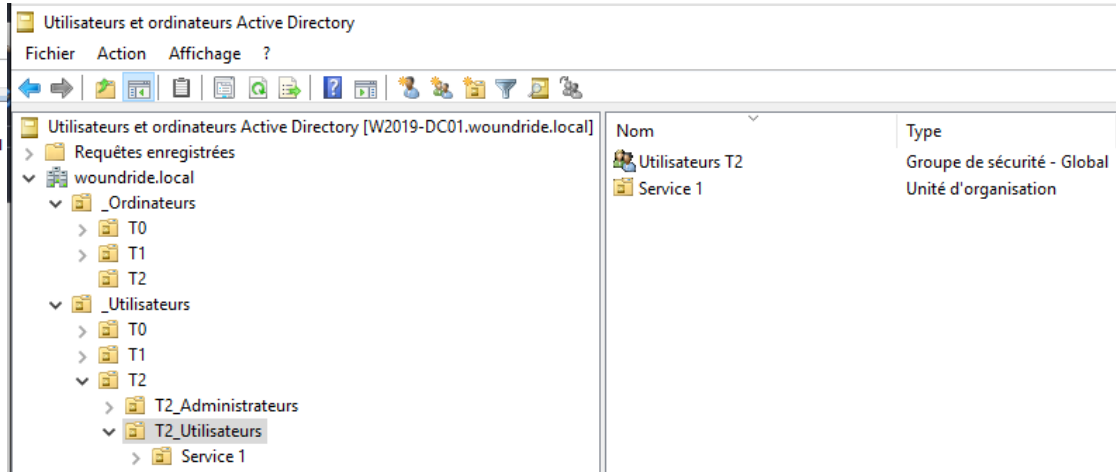


- On retrouve ici les administrateurs des serveurs du Tier 1
- Ces comptes doivent pouvoir se connecter uniquement aux serveurs du Tier 1
- Pour faciliter la gestion des privilèges, on peut créer un groupe « Admin T1 » auquel seront rattachés les comptes utilisateurs d'administration du Tier 1

Mise en place de l'architecture en Tier

Rangement / création des comptes d'administrateurs et d'utilisateurs du Tier 2 :

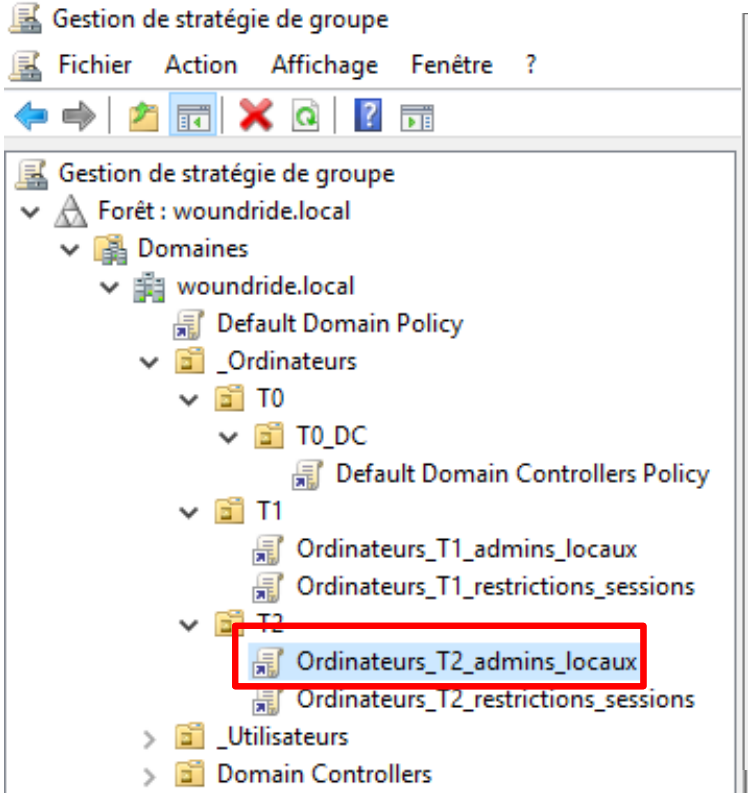


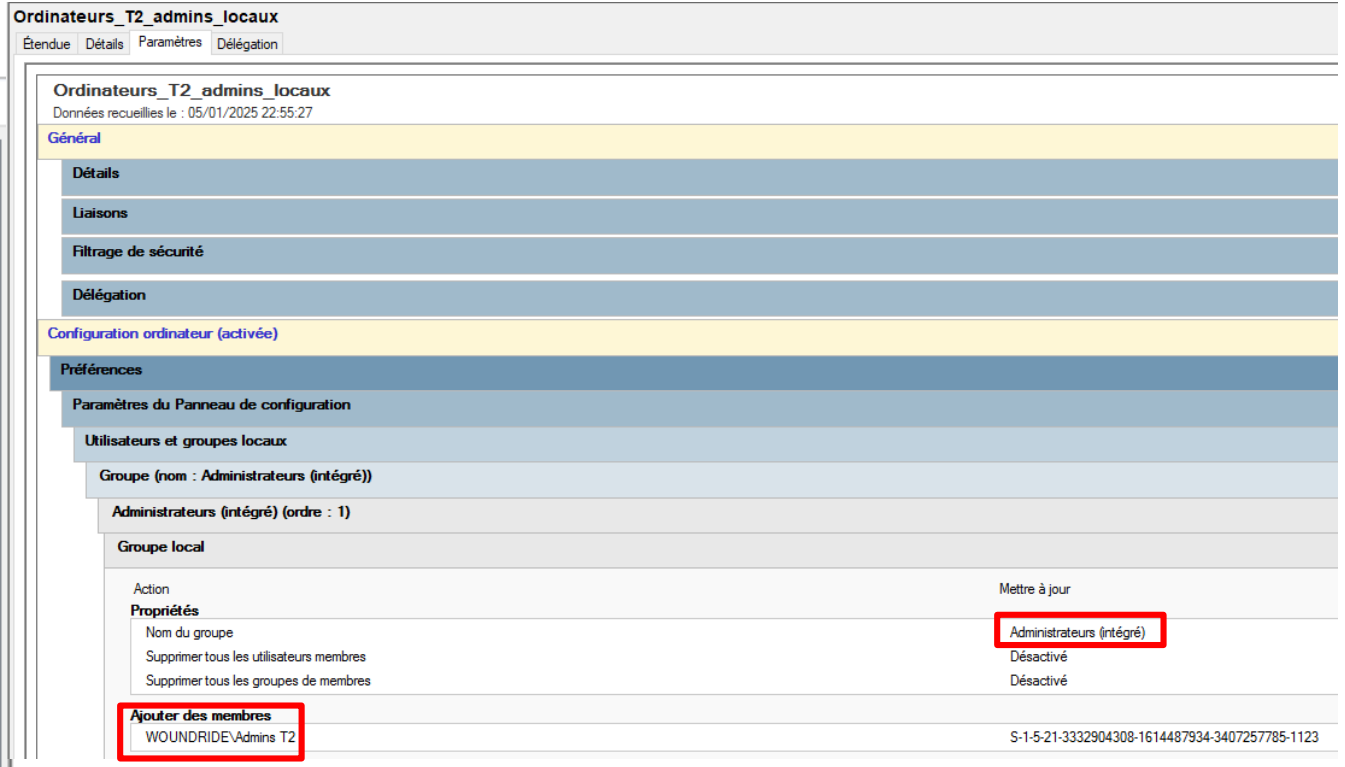


- On retrouve ici les administrateurs des postes utilisateurs du Tier 2, mais aussi les comptes utilisateurs exempts de privilèges sur les machines
- Ces comptes doivent pouvoir se connecter uniquement aux postes utilisateurs du Tier 2
- Pour faciliter la gestion des privilèges, on peut créer un groupe « Admin T2 » auquel seront rattachés les comptes utilisateurs d'administration du Tier 2

Mise en place de l'architecture en Tier

Attribution des privilèges d'administration sur les machines des T1 et T2 :

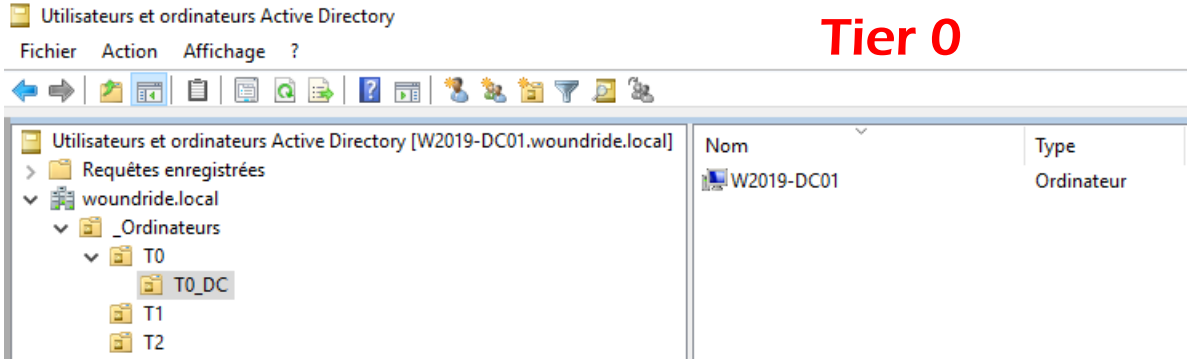




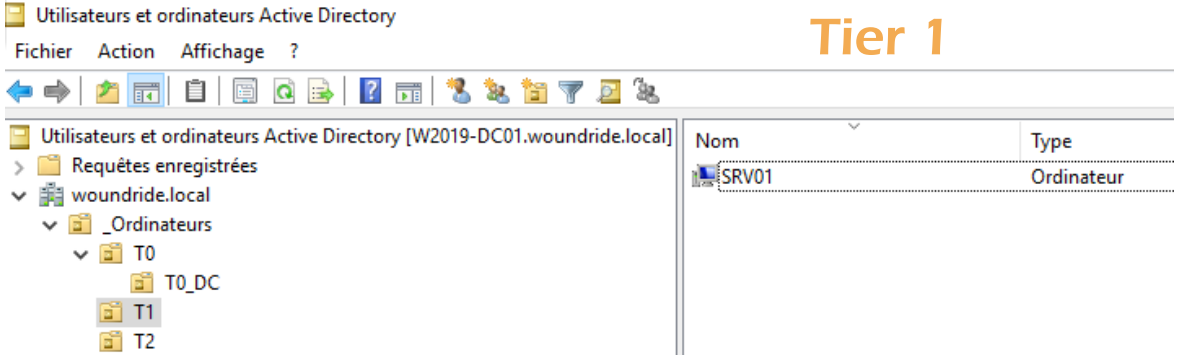
Mise en place de l'architecture en Tier

Rangement des comptes d'ordinateurs :

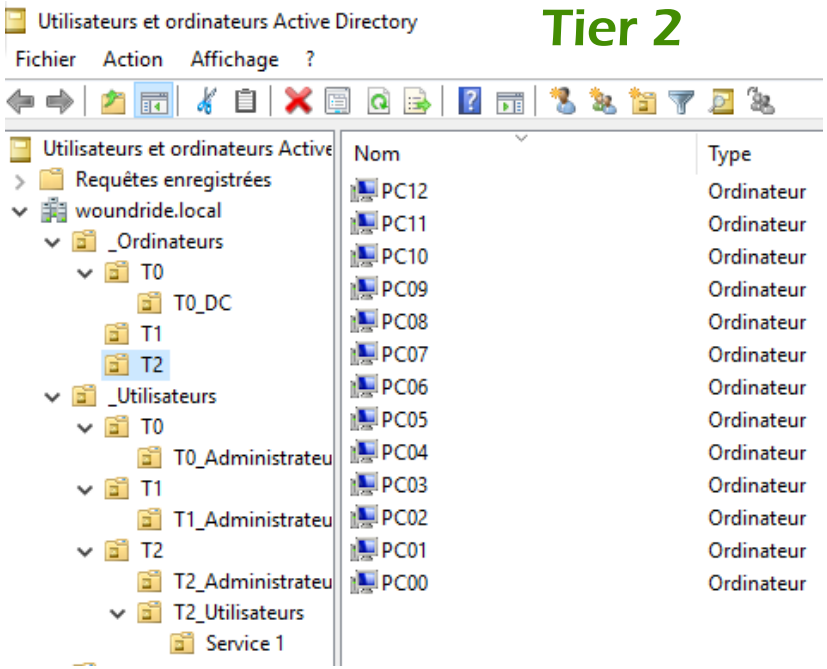
Tier 0



Tier 1



Tier 2



Restrictions d'accès aux machines

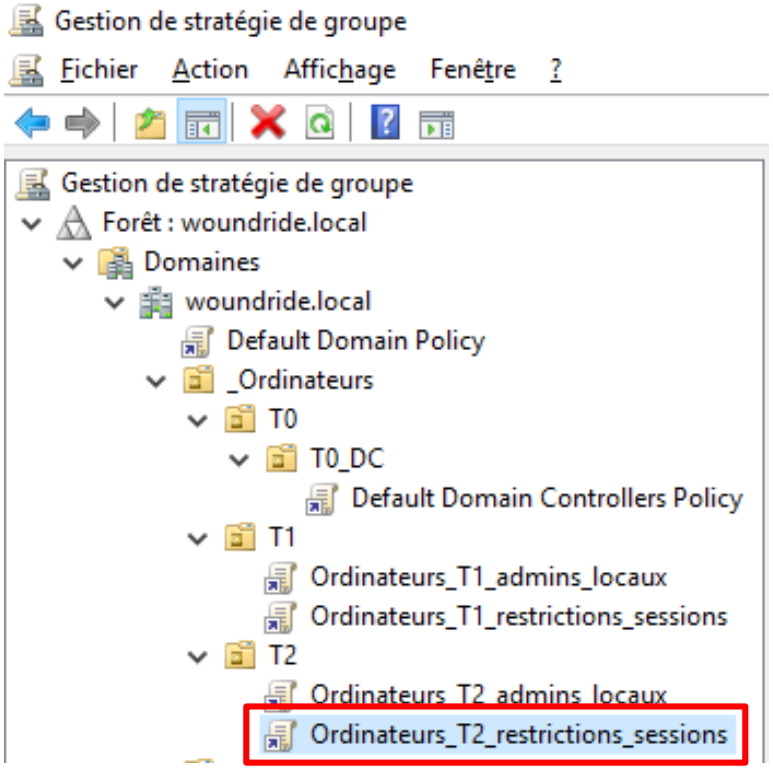
Deux méthodes :

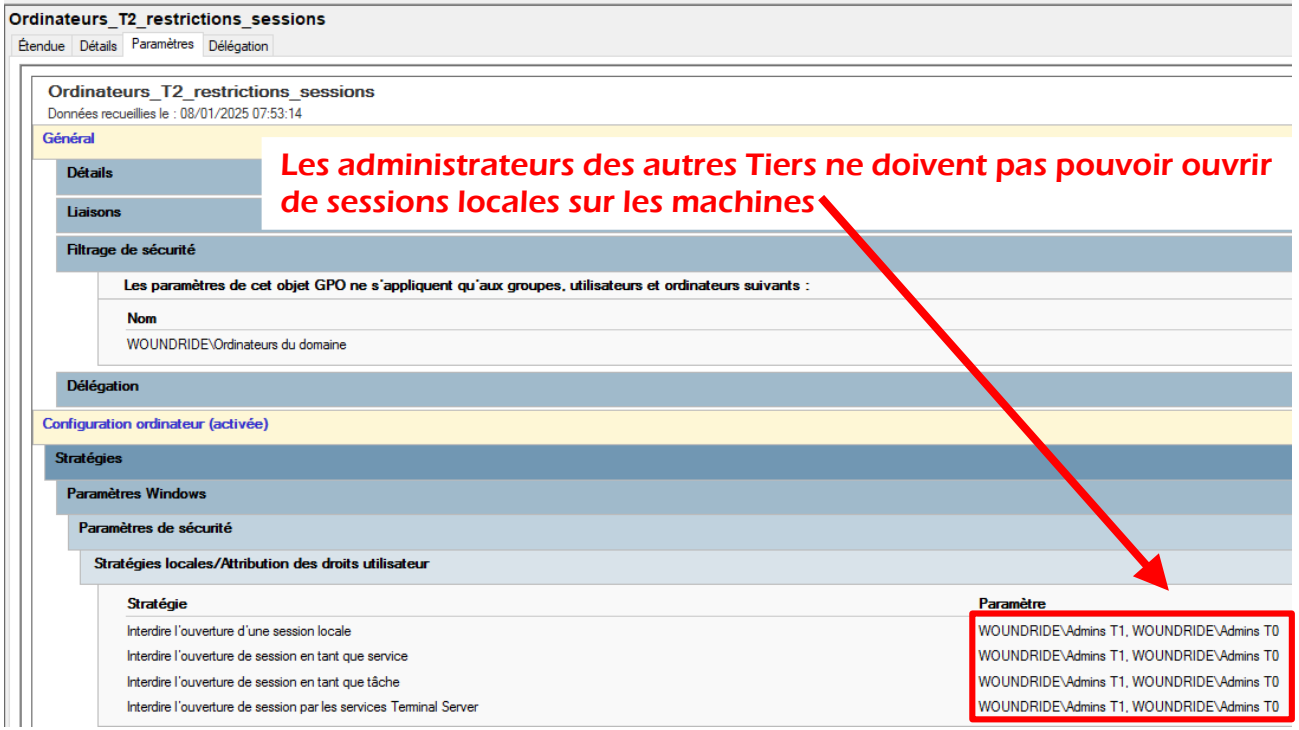
- Définir des **GPO** interdisant l'ouverture de sessions sur les ordinateurs d'un Tier :
  - Efficacité (mais n'empêche pas les connexions RDP depuis un autre Tier)
  - Facilité de mise en œuvre (application directe aux UO et / ou groupes)
  - Prise en charge des systèmes d'exploitation (très) obsolètes

- Création de **Silos** d'autorisation d'authentification :
  - Prérequis (OS minimum, niveau AD minimum, config Kerberos)
  - Efficacité (mais nécessite plus de rigueur dans l'administration et n'empêche pas les connexions aux utilisateurs hors Silo)
  - Permet une gestion plus fine de l'authentification et permet de restreindre les connexions RPD depuis un autre Tier
  - Mise en œuvre plus lourde (création de 2 politiques par Tier + application à l'objet)
  - Maintien en conditions opérationnelles plus fastidieux (gestion de l'appartenance au Silo)

Méthode 1 : Mise en place de GPO de restrictions d'accès

Restriction d'accès aux machines du T2 :

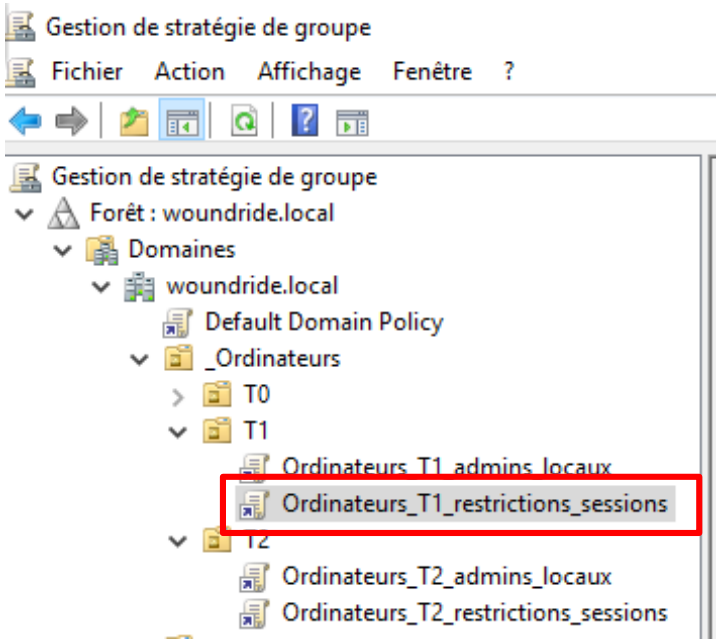


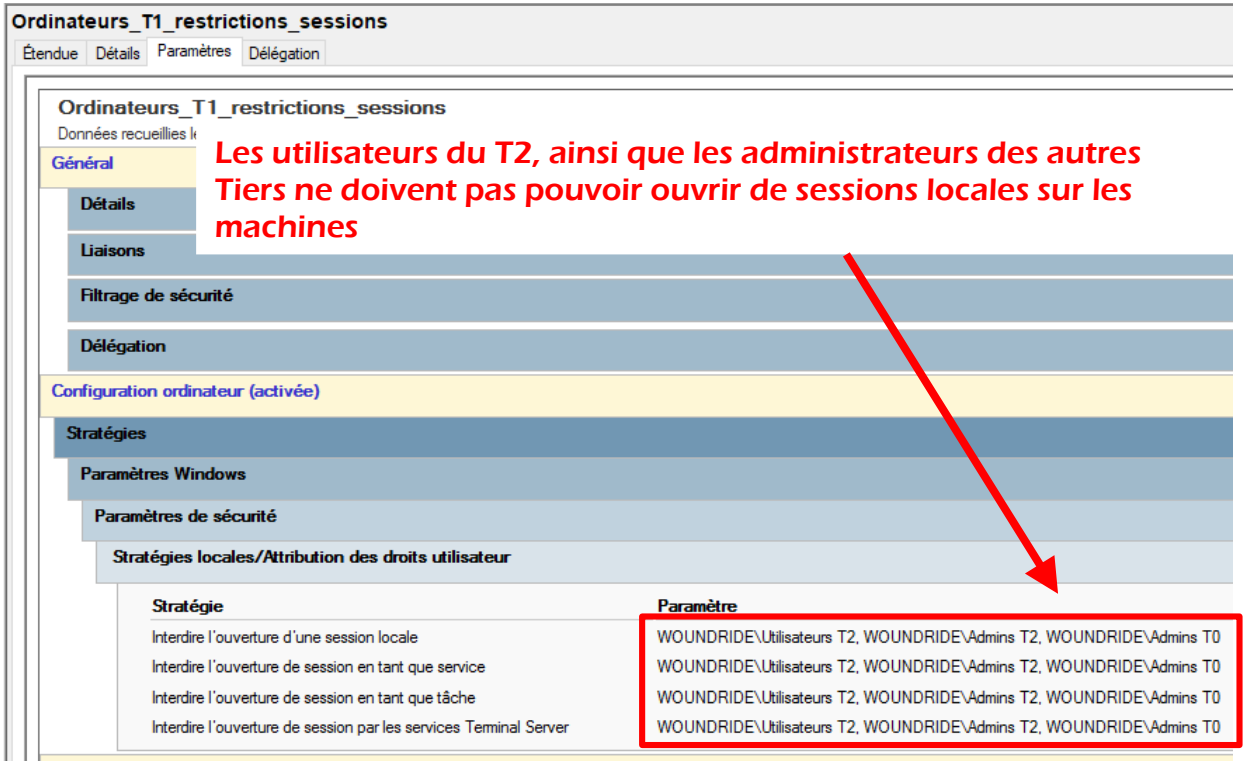


Les administrateurs des autres Tiers ne doivent pas pouvoir ouvrir de sessions locales sur les machines

Méthode 1 : Mise en place de GPO de restrictions d'accès

Restriction d'accès aux machines du T1 :

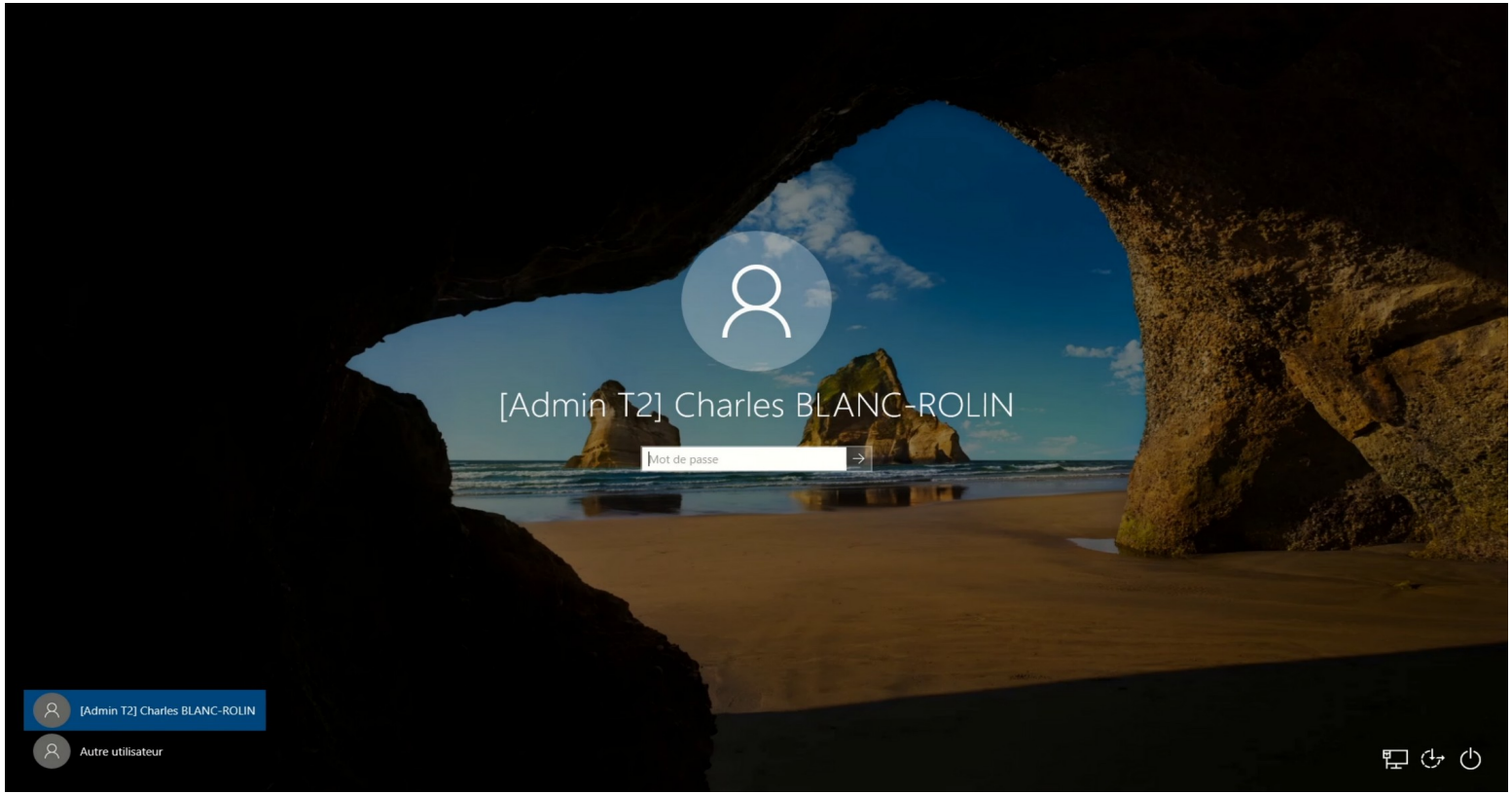




Les utilisateurs du T2, ainsi que les administrateurs des autres Tiers ne doivent pas pouvoir ouvrir de sessions locales sur les machines

Exemple d'accès restreint sur le Tier 2

Tier 2



Les risques résiduels

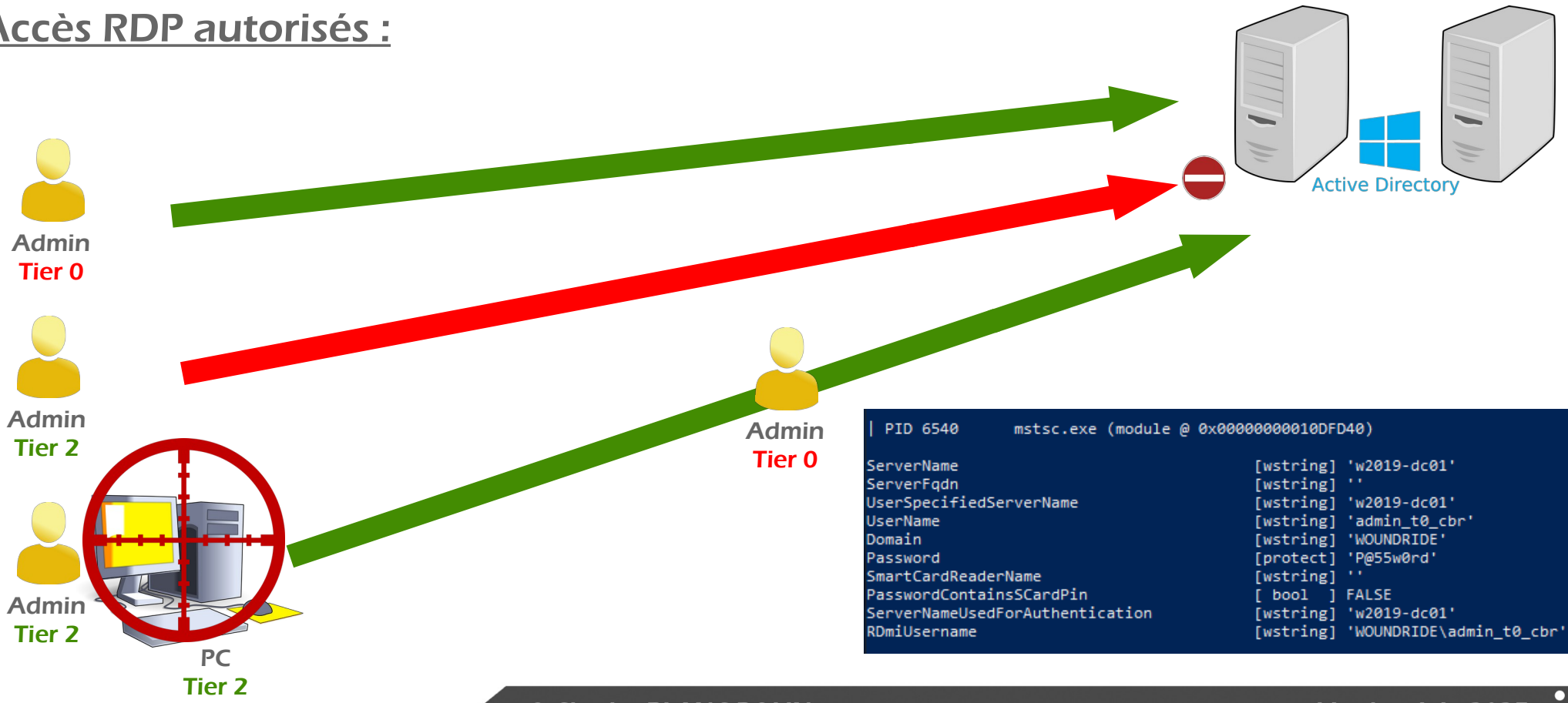
Risques non couverts ici :

- *Un administrateur pourrait par facilité, utiliser le même mot de passe sur l'ensemble de ses comptes (peut être audité lors des revues de comptes par exemple)*

- Si l'accès RDP/TSE est interdit sur une machine du Tier 0 par un administrateur du Tier 2, rien n'empêche un administrateur du Tier 2 de se connecter depuis une machine du Tier 2 en RDP vers une machine du Tier 0, avec un compte du Tier 0. Dans ce cas, si la machine du Tier 2 est compromises, les informations d'authentification de la connexion RDP (identifiant + mot de passe du Tier 0) pourraient être récupérées par l'attaquant

Limites des restrictions VS l'utilisation de RDP

Accès RDP autorisés :

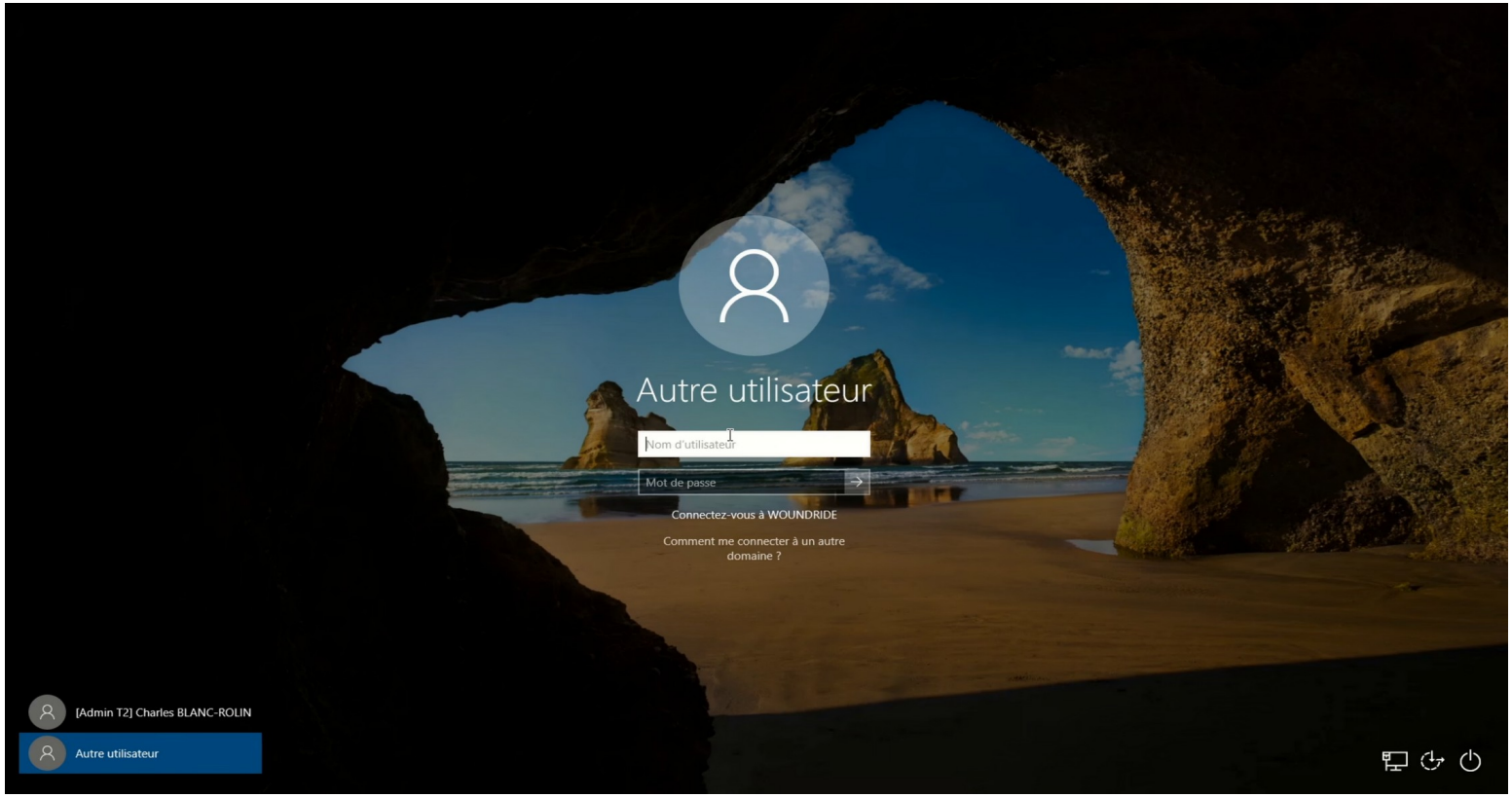



```
| PID 6540      mstsc.exe (module @ 0x00000000010DFD40)

ServerName                              [wstring] 'w2019-dc01'
ServerFqdn                              [wstring] ''
UserSpecifiedServerName                 [wstring] 'w2019-dc01'
UserName                                [wstring] 'admin_t0_cbr'
Domain                                  [wstring] 'WOUNDRIDE'
Password                                [protect] 'P@55w0rd'
SmartCardReaderName                     [wstring] ''
PasswordContainsSCardPin                [ bool  ] FALSE
ServerNameUsedForAuthentication         [wstring] 'w2019-dc01'
RDmiUsername                            [wstring] 'WOUNDRIDE\admin_t0_cbr'
```

Récupération d'infos d'authentification via RDP

Tier 2



Les solutions pour pallier les risques

Il existe plusieurs solutions pour palier les risques liés à l'administration à distance des Tiers sensibles via RDP :

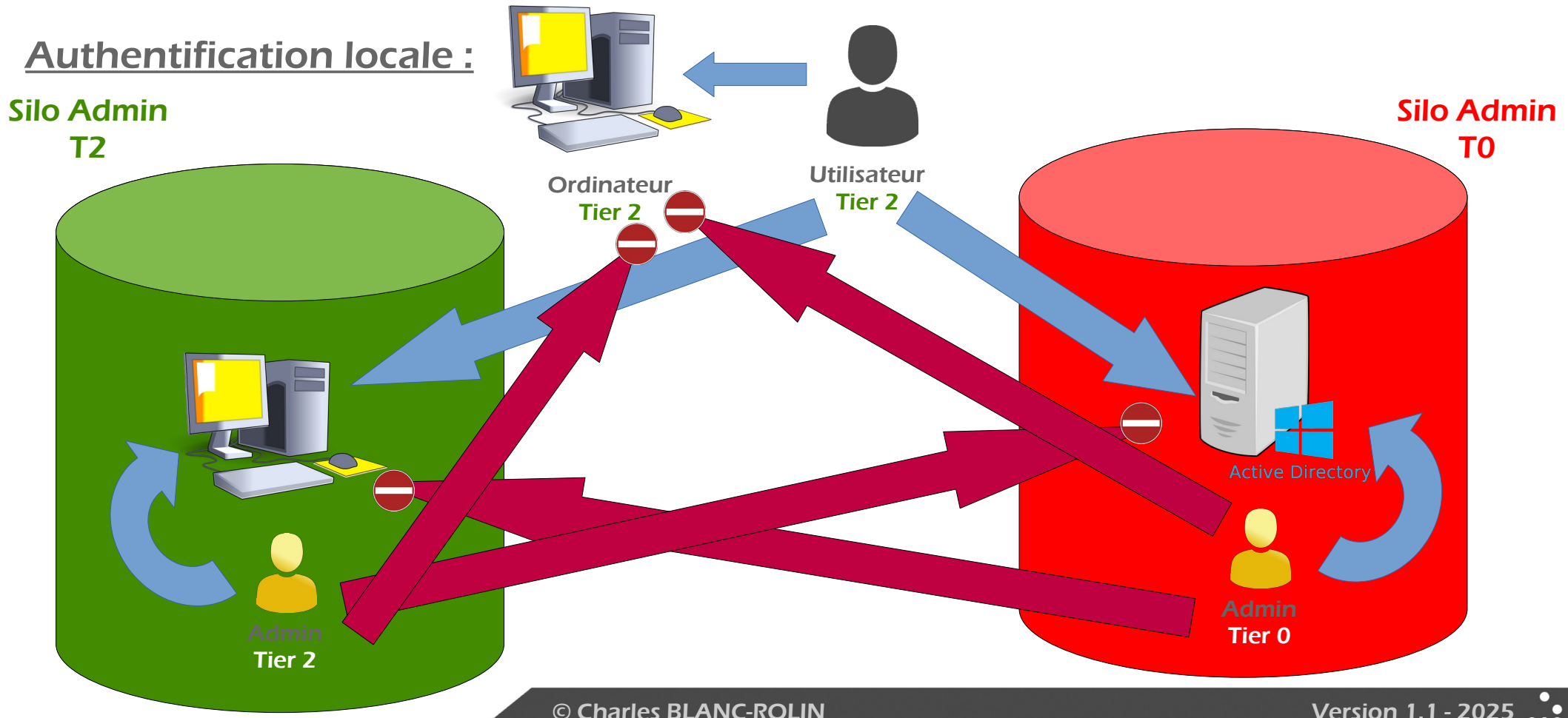
- **Créer des Silos d'authentification (méthode 2)**
- Mettre en place une segmentation et un filtrage des réseaux, créer à minima 1 VLAN par Tier et limiter les flux au strict nécessaire (recommandé dans tous les cas)
- N'autoriser l'utilisation du protocole RDP qu'au sein d'un même Tier (filtrage des flux) => Nécessite pour un administrateur de disposer d'un poste pour chaque Tier qu'il doit administrer (efficace, mais fastidieux et onéreux)
- Utiliser une solution d'administration à distance tierce (mais fortement déconseillé par l'ANSSI d'installer un produit tiers sur les contrôleurs de domaine)
- Administrer les machines (virtuelles) via la console de l'hyperviseur (mode dégradé)
- Utiliser un bastion d'administration permettant une rupture protocolaire (recommandé dans tous les cas)

Méthode 2 : Mise en place de Silos d'authentification

Les prérequis :

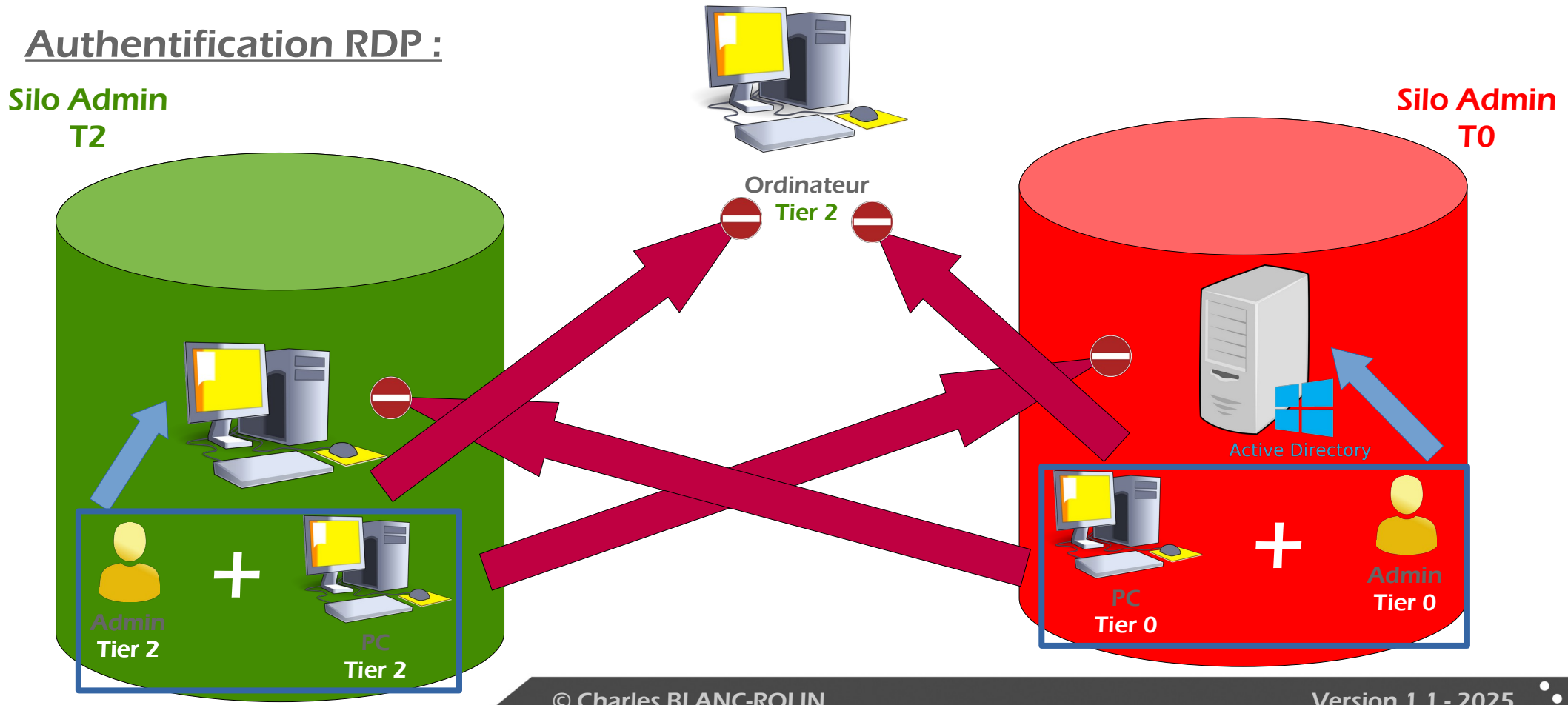
- Avoir un niveau de domaine supérieur ou égal à 2012R2
- Activer la prise en charge du contrôle d'accès dynamique et du blindage Kerberos sur les contrôleurs de domaine
- Activer la prise en charge des revendications et du blindage Kerberos sur les postes clients, ce qui nécessite d'avoir des serveurs membres minimums en 2012 et des postes clients minimums en Windows 8
- Attention : si des ordinateurs avec des systèmes d'exploitation non supportés sont présents dans le silo, les utilisateurs du silo ne pourront pas se connecter sur ces machines, quand bien même elles feraient partie du silo
- A noter également : un compte d'ordinateur et un compte utilisateur ne peuvent appartenir qu'à un seul et unique Silo

Méthode 2 : Mise en place de Silos d'authentification



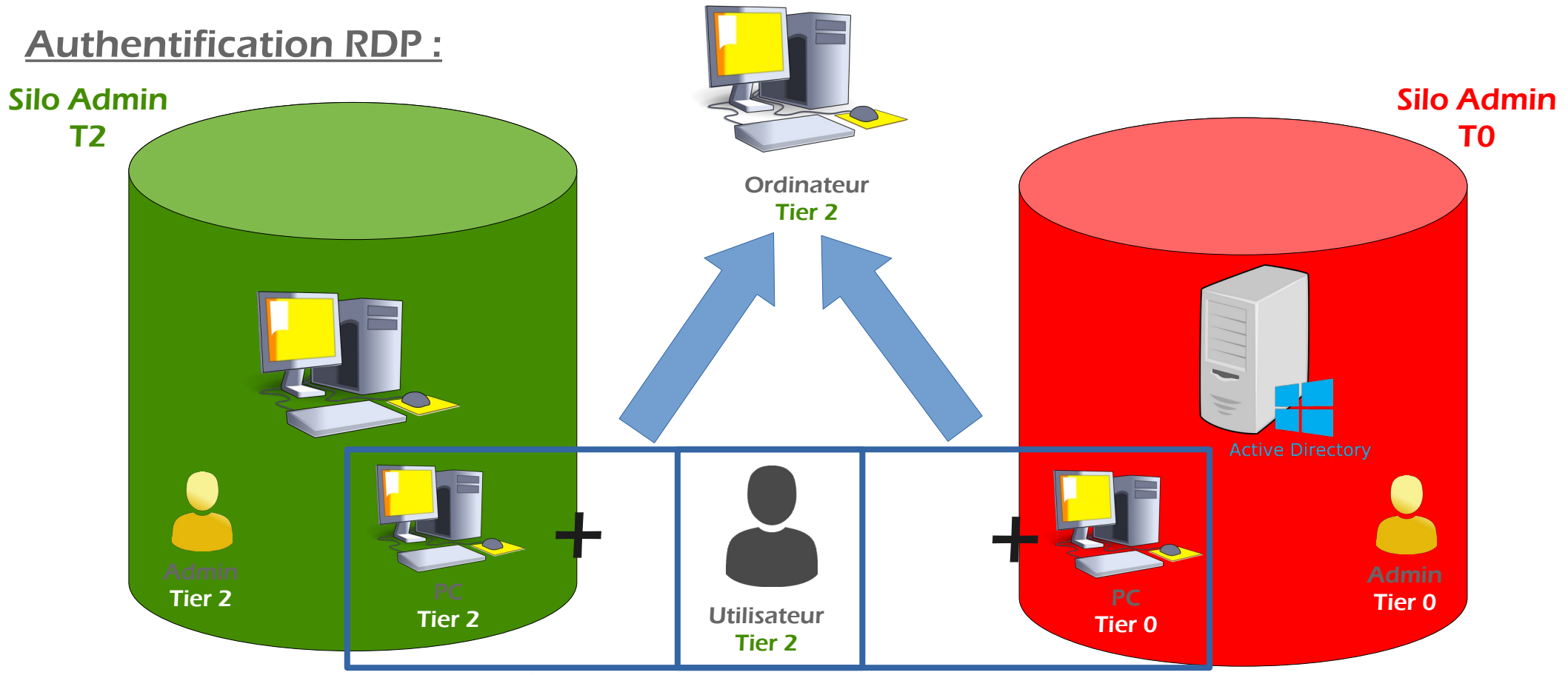
Méthode 2 : Mise en place de Silos d'authentification

Authentification RDP :



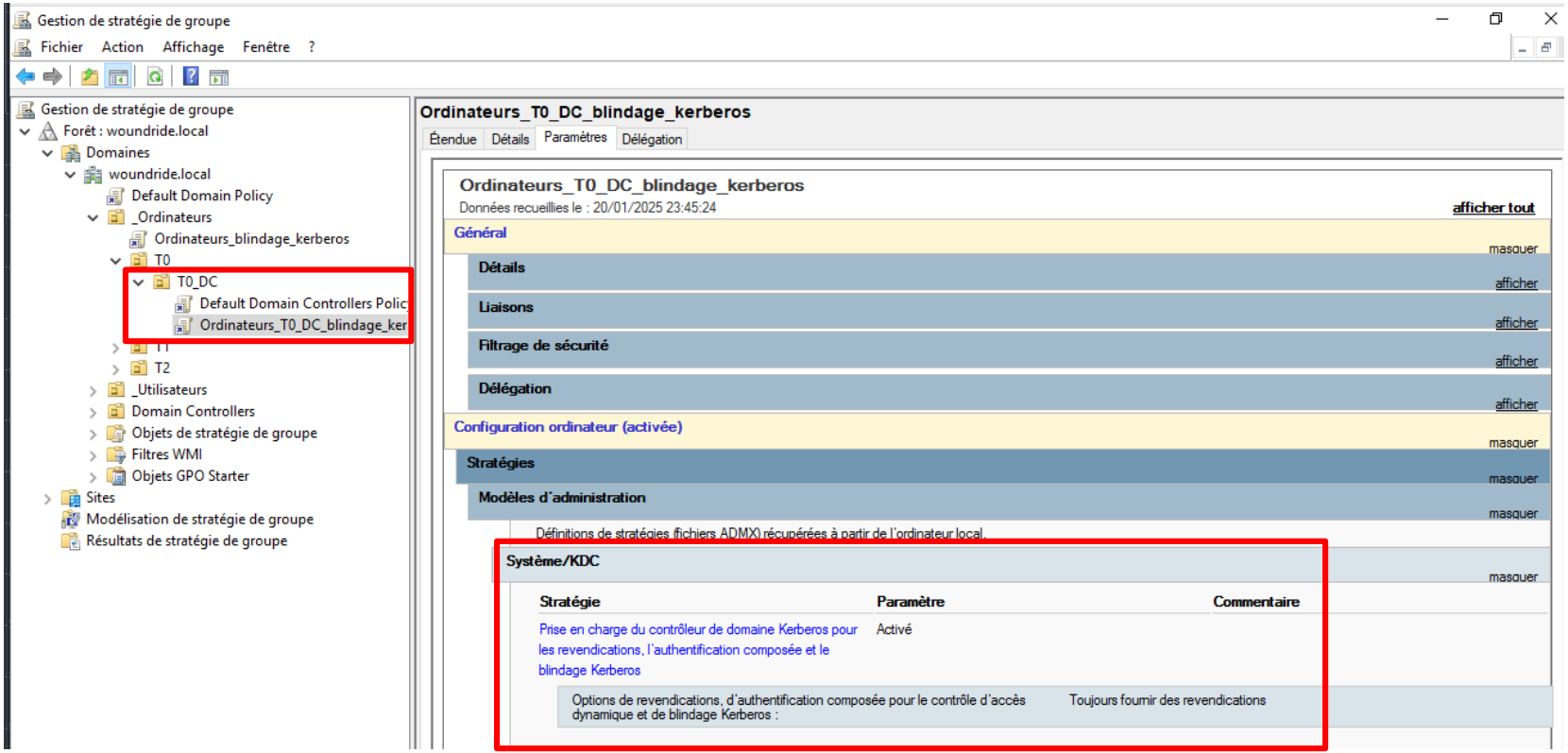
Méthode 2 : Mise en place de Silos d'authentification

Authentification RDP :



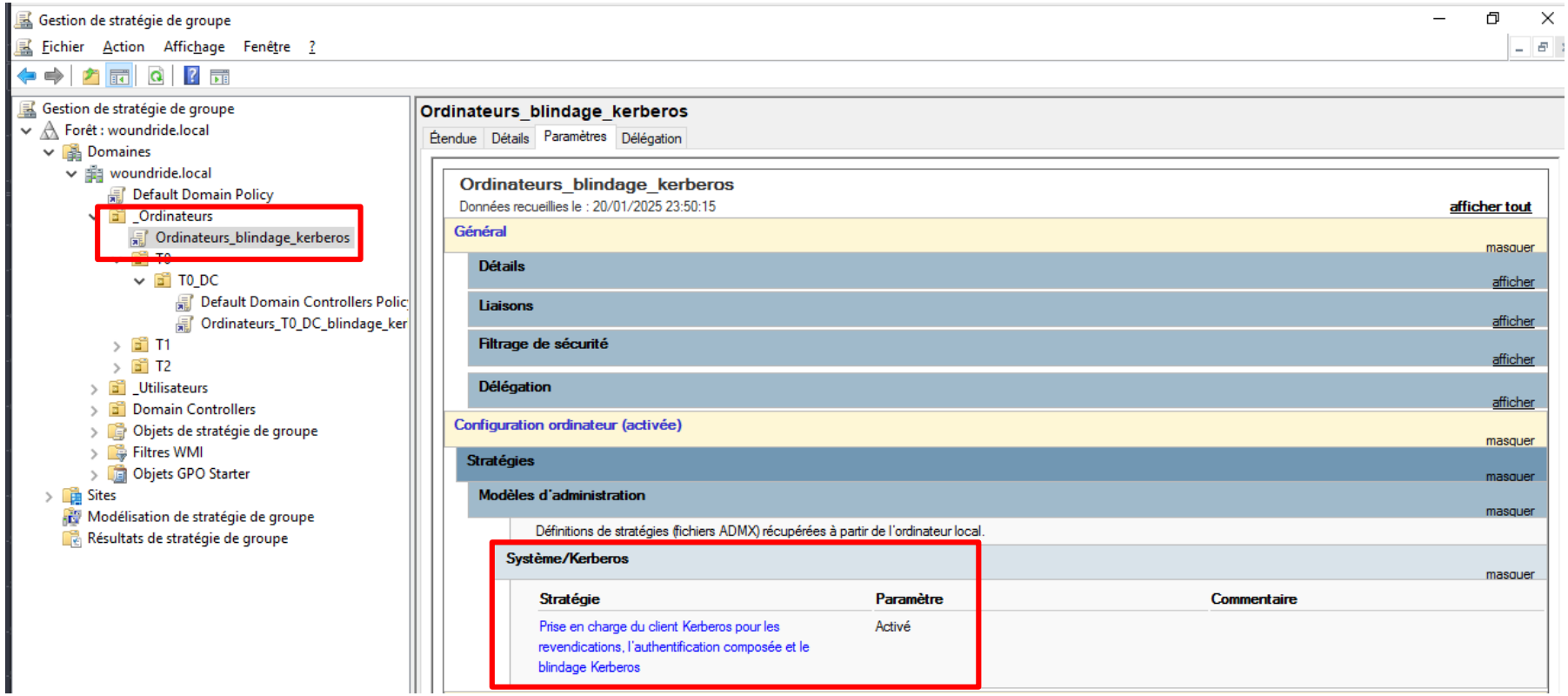
Méthode 2 : Mise en place de Silos d'authentification

Création de la GPO d'activation du blindage Kerberos sur les DC :



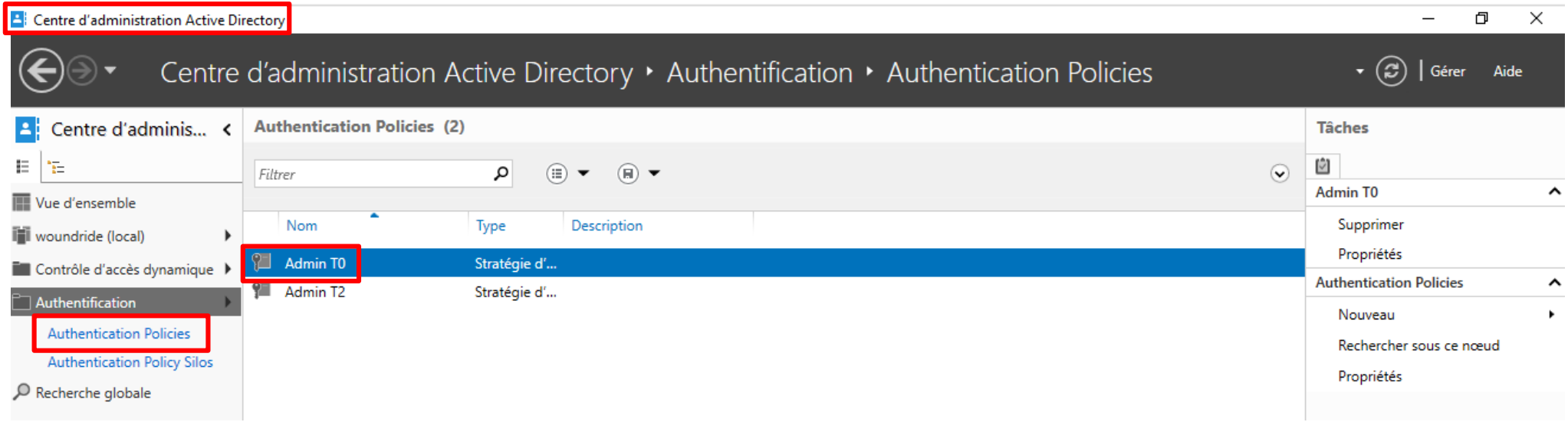
Méthode 2 : Mise en place de Silos d'authentification

Création de la GPO d'activation du blindage Kerberos sur les postes :



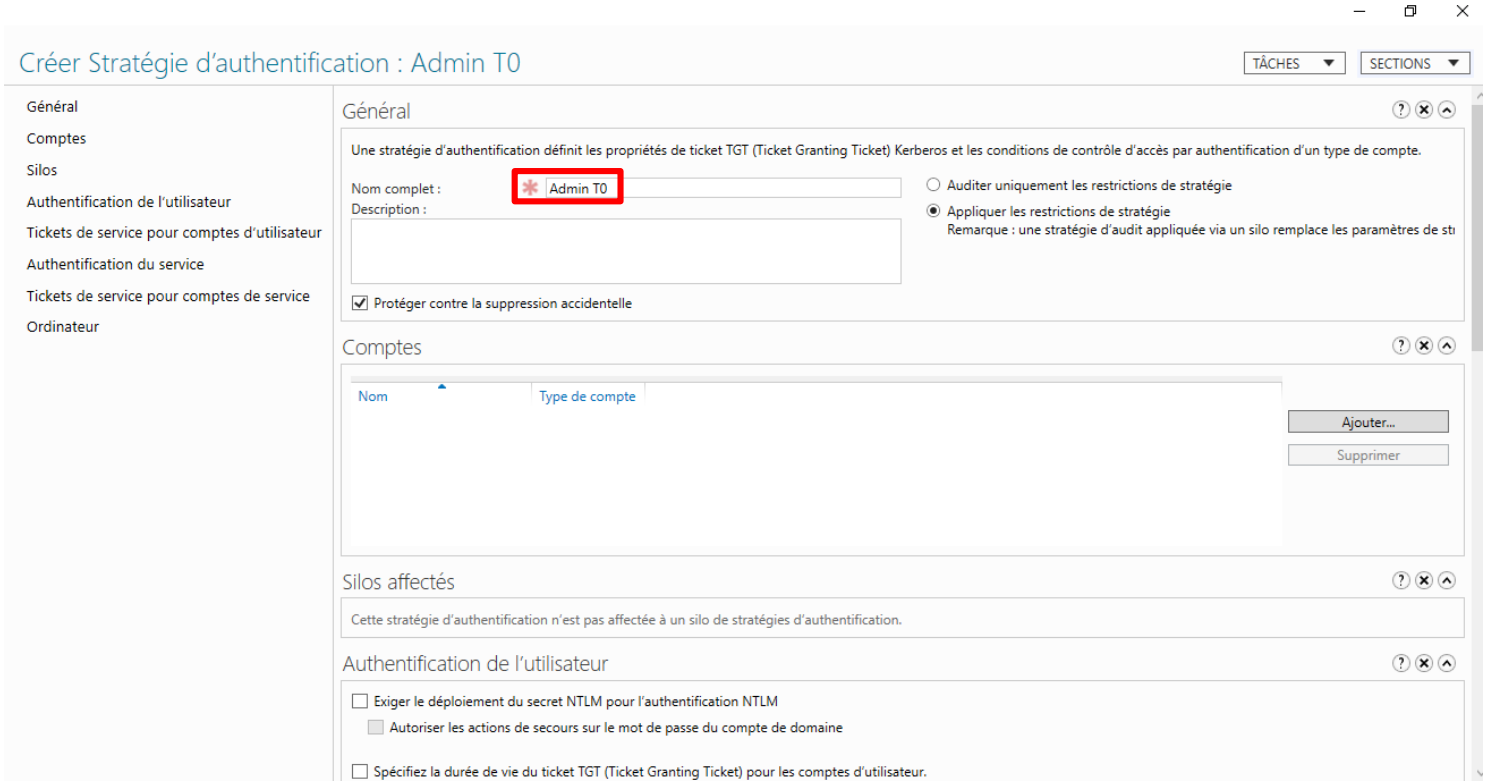
Méthode 2 : Mise en place de Silos d'authentification

Création de la politique d'authentification Admin T0 :



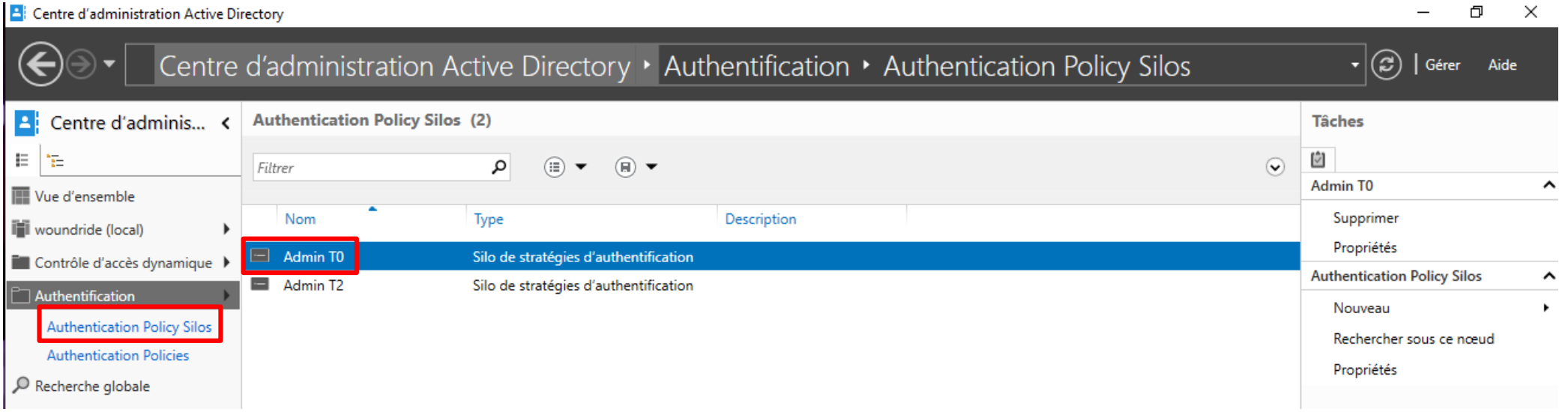
Méthode 2 : Mise en place de Silos d'authentification

Création de la politique d'authentification Admin T0 :



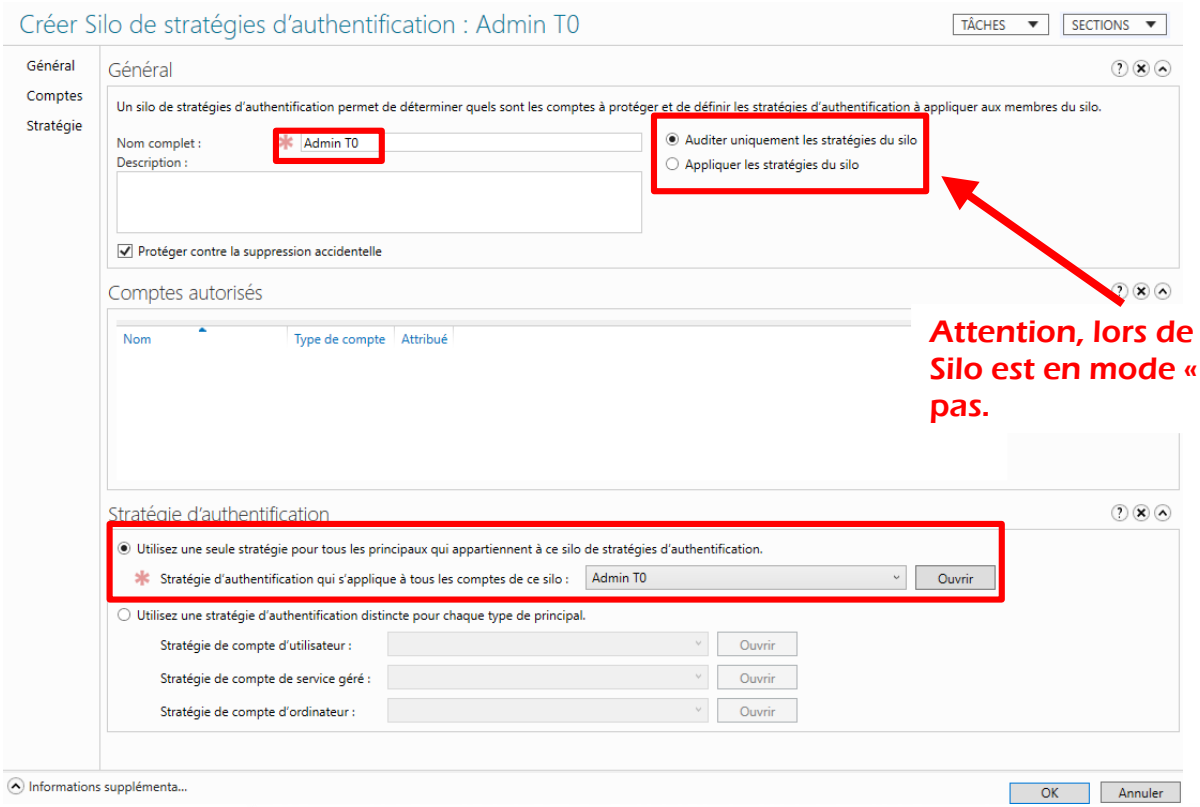
Méthode 2 : Mise en place de Silos d'authentification

Création du Silo Admin T0 et application de la politique d'authentification :



Méthode 2 : Mise en place de Silos d'authentification

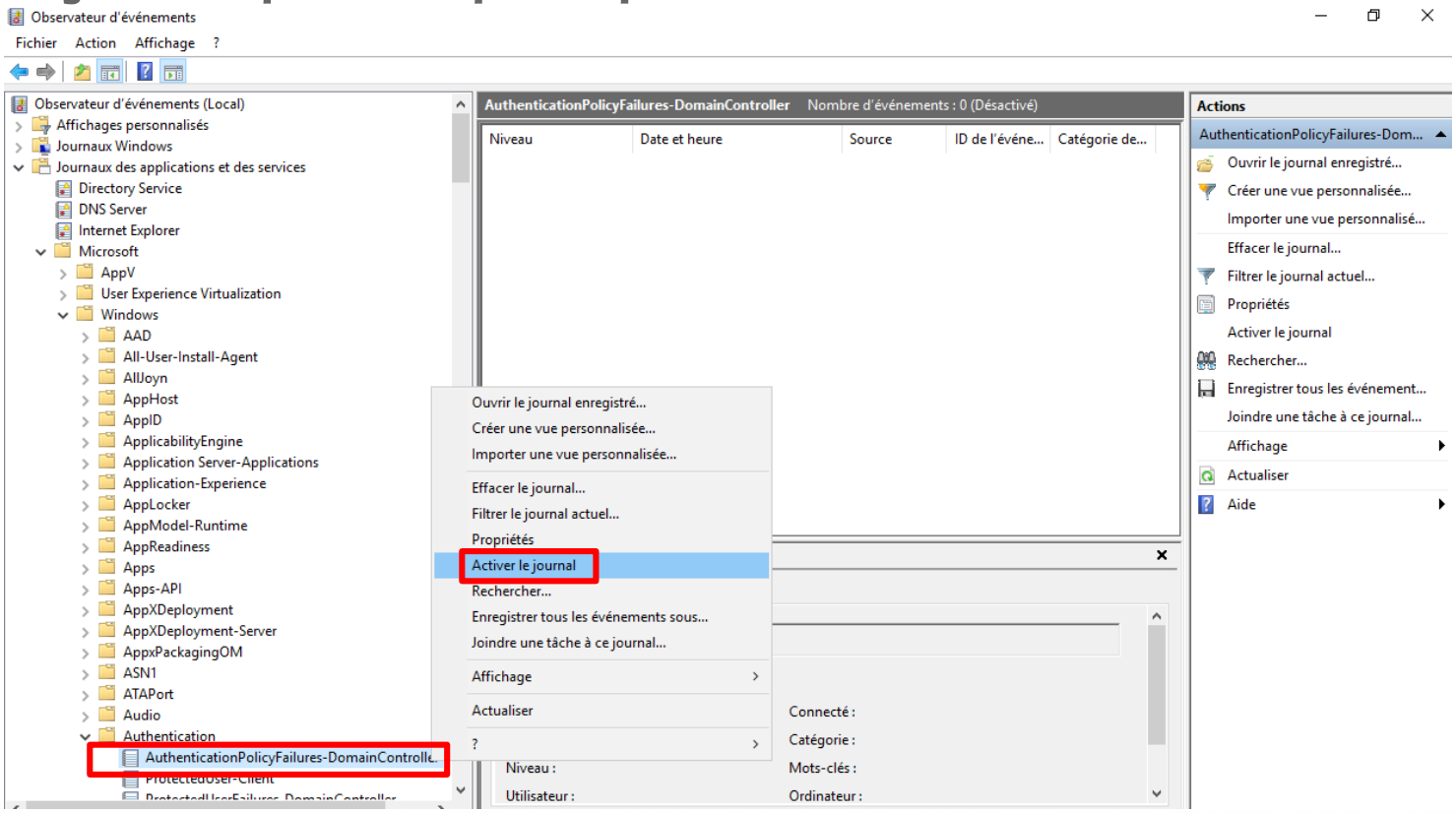
Création du Silo Admin T0 et application de la politique d'authentification :



Attention, lors de sa création, la stratégie du Silo est en mode « audit » et ne s'applique pas.

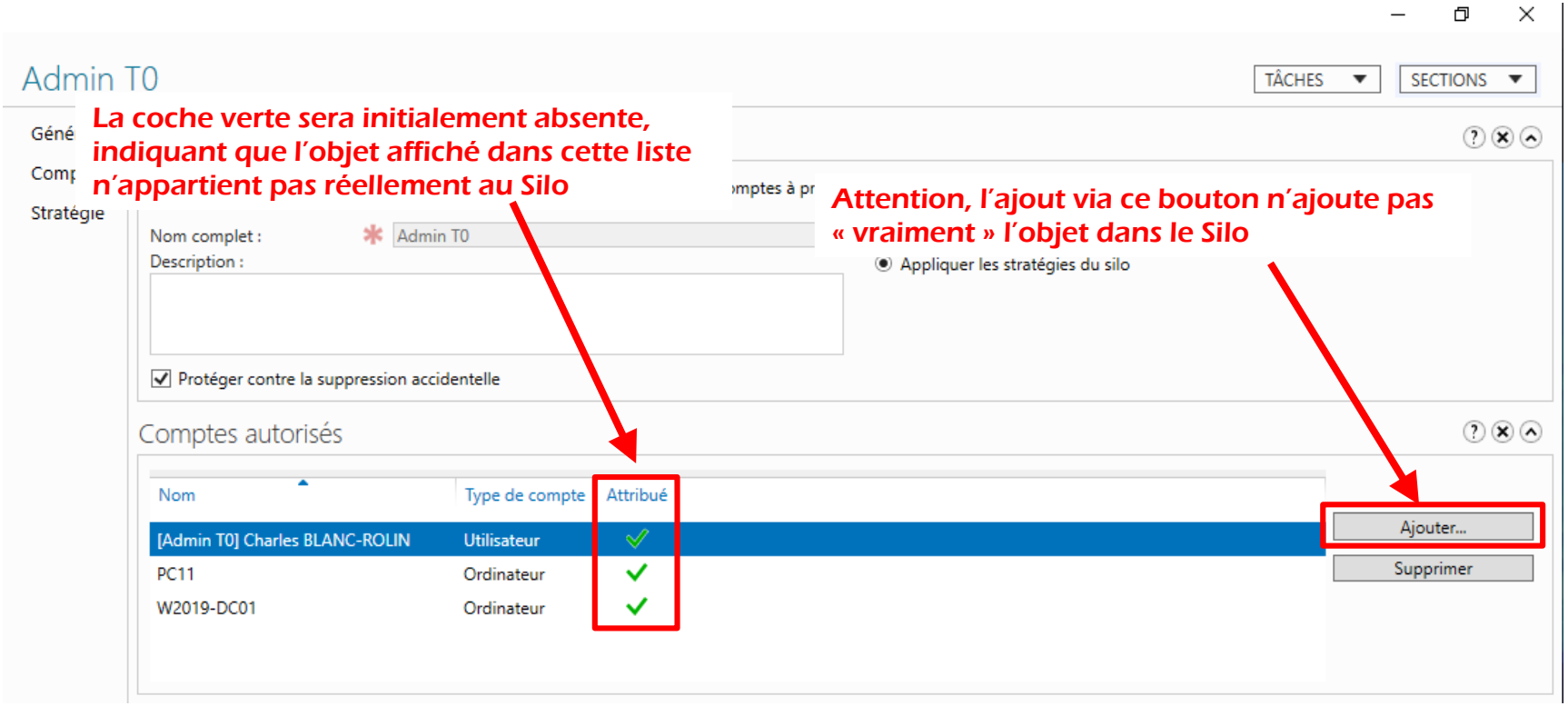
Méthode 2 : Mise en place de Silos d'authentification

Activation du journal pour les politiques d'authentification :



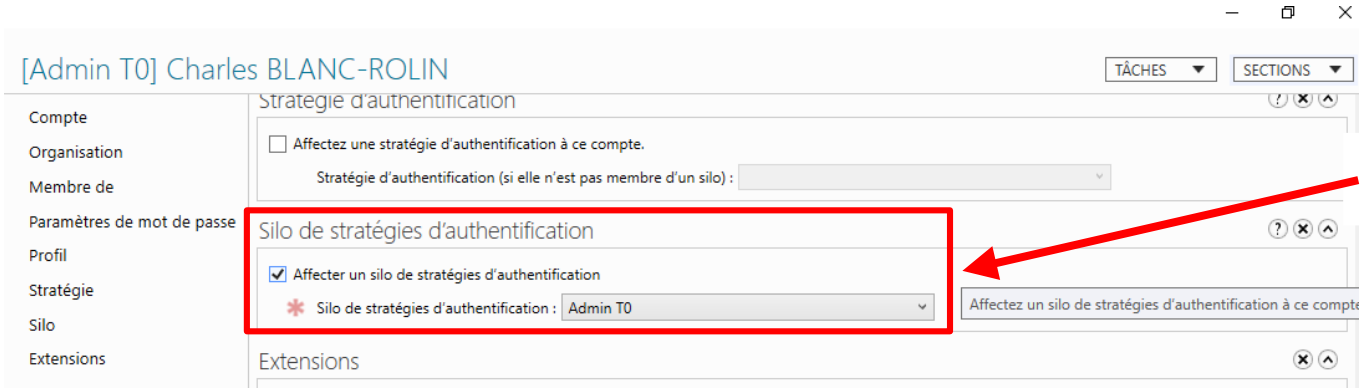
Méthode 2 : Mise en place de Silos d'authentification

Ajout des comptes (utilisateurs + ordinateurs) dans le Silo Admin T0 :

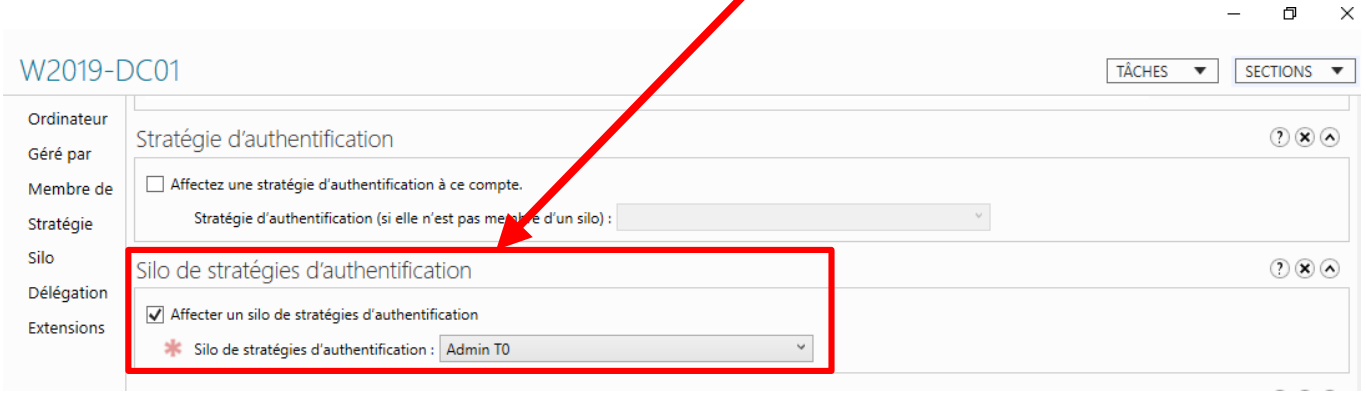


Méthode 2 : Mise en place de Silos d'authentification

Ajout des comptes (utilisateurs + ordinateurs) dans le Silo Admin T0 :

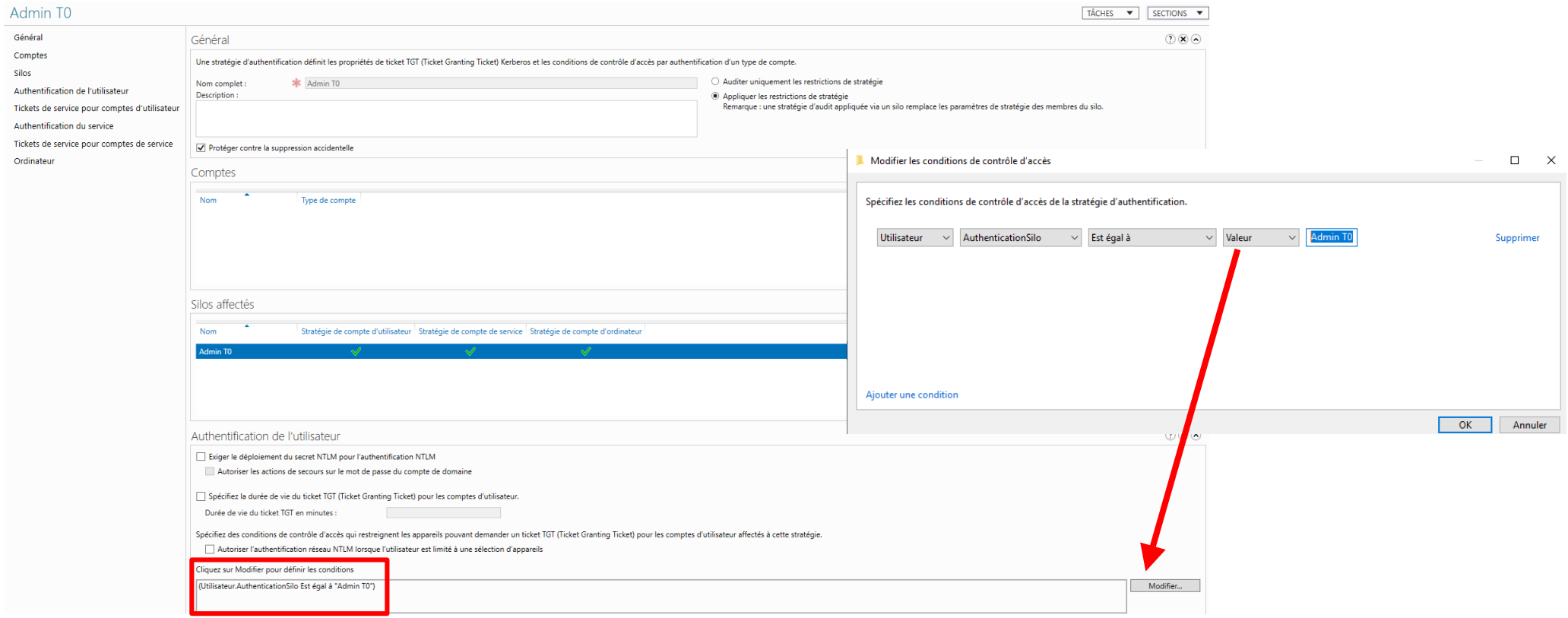


Le Silo devra être configuré sur chaque objet

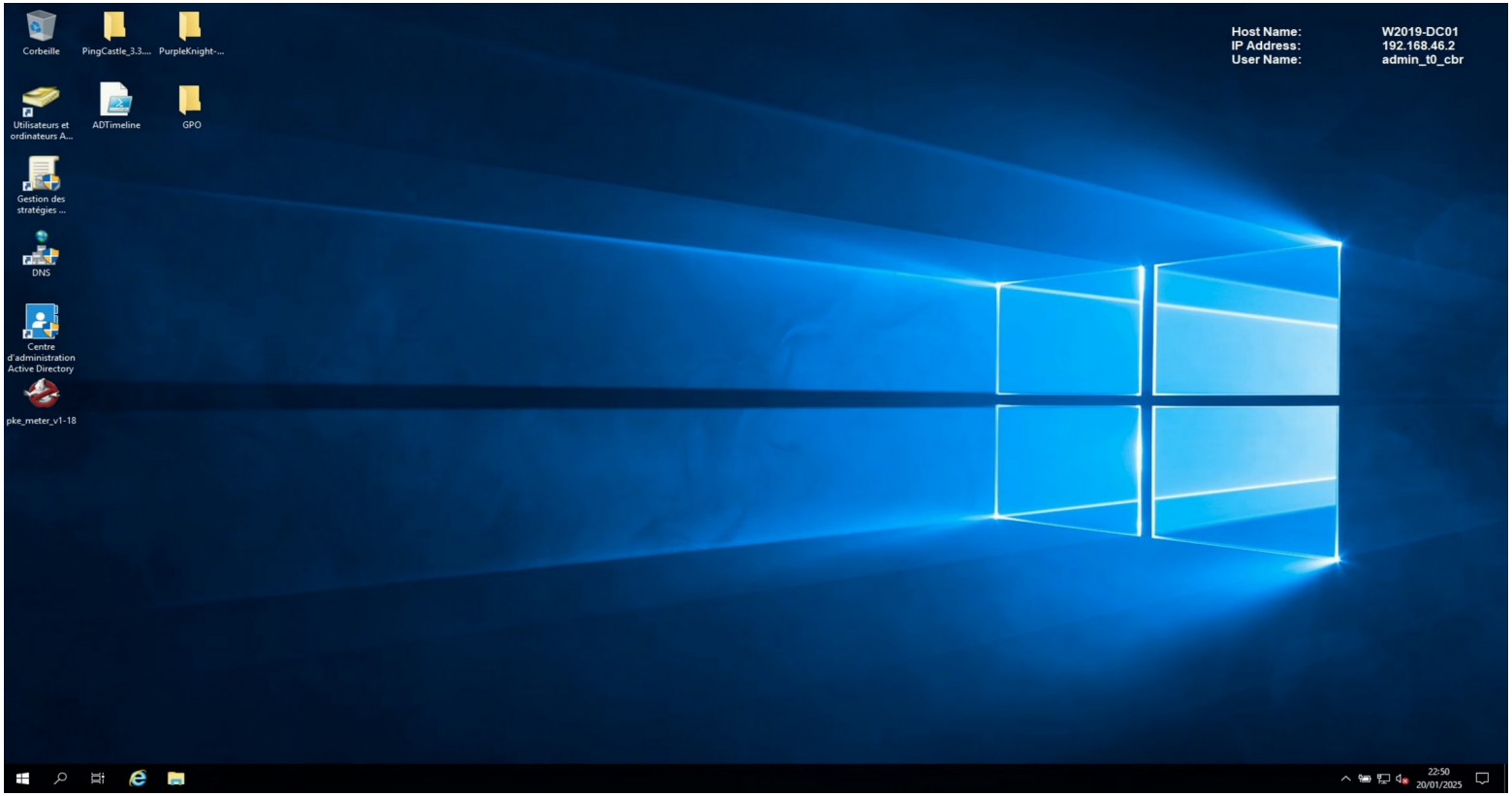


Méthode 2 : Mise en place de Silos d'authentification

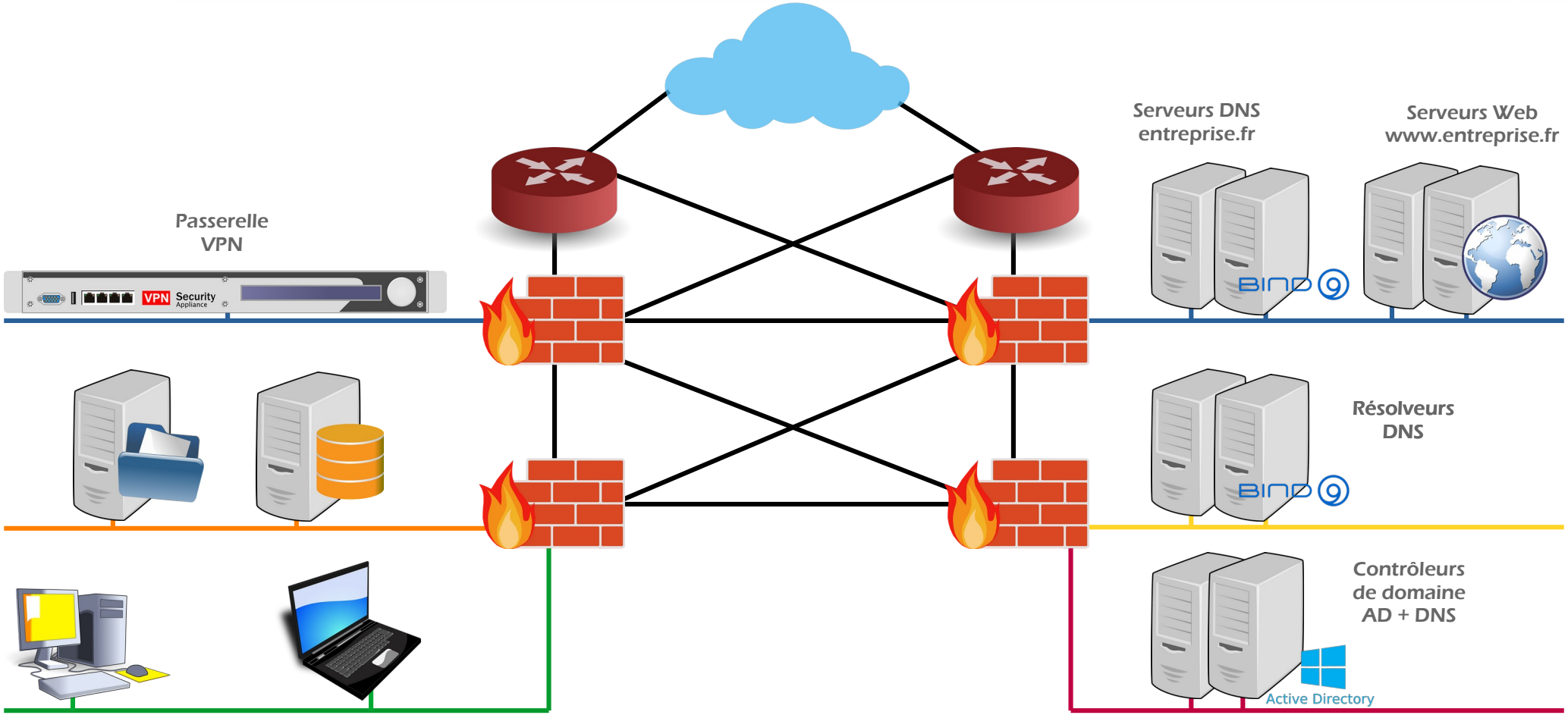
Définition des conditions d'authentification pour la politique Admin T0 :



Démonstration de l'authentification en Silo



Positionnement des contrôleurs de domaine dans un SI



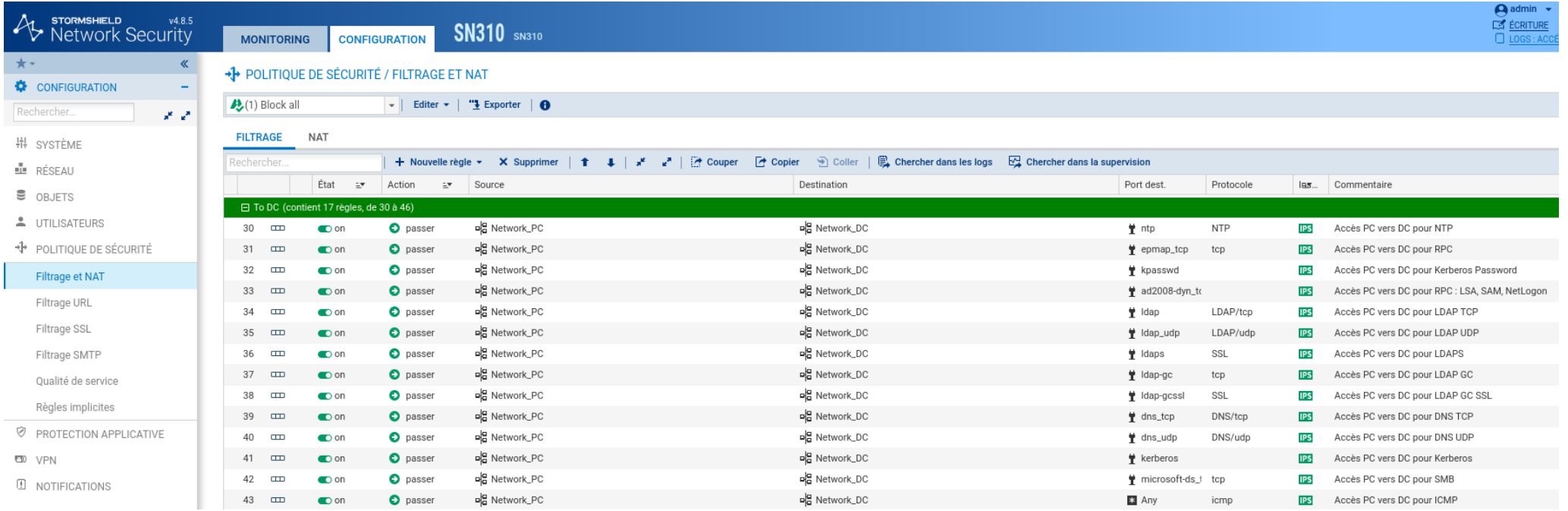
Les flux réseau nécessaires au fonctionnement de l'AD

Flux réseau nécessaires entre un poste du T2 et un contrôleur de domaine du T0 pour le fonctionnement de l'annuaire Active Diractory

Port(s) client(s)	Port serveur	Service
49152-65535/UDP	123/UDP	W32Time
49152-65535/TCP	135/TCP	Mappeur de point de terminaison RPC
49152-65535/TCP	464/TCP/UDP	Modification de mot de passe Kerberos
49152-65535/TCP	49152-65535/TCP	RPC pour LSA, SAM, NetLogon (*)
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152-65535/TCP	636/TCP	LDAP SSL
49152-65535/TCP	3268/TCP	LDAP GC
49152-65535/TCP	3269/TCP	LDAP GC SSL
53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
49152-65535/TCP	49152-65535/TCP	FRS RPC (*)
49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
49152-65535/TCP/UDP	445/TCP	SMB (**)
49152-65535/TCP	49152-65535/TCP	DFSR RPC (*)

Les flux réseau nécessaires au fonctionnement de l'AD

Règles de flux réseau nécessaires entre un poste du T2 et un contrôleur de domaine du T0 pour le fonctionnement de l'annuaire Active Directory



Ressources et outils utilisés

- Flux pare-feu AD (Microsoft)
  https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/active-directory/config-firewall-for-ad-domains-and-trusts

- L'administration en silo – SSTIC (Aurélien Bordes) :
  https://www.sstic.org/2017/presentation/administration_en_silo/

- Guide ANSSI – Administration sécurisée de l'AD
  https://cyber.gouv.fr/publications/recommandations-pour-ladministration-securisee-des-si-reposant-sur-ad

- Mimikatz (Benjamin Delpy / @gentilkiwi) :
  https://github.com/gentilkiwi/mimikatz