



Administration sécurisée et Tiering (environnement Active Directory)

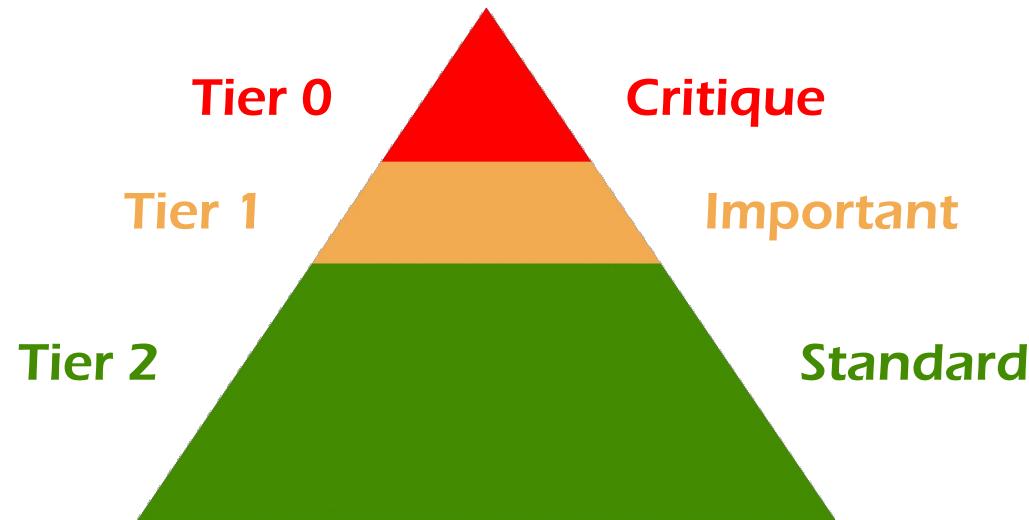




Principe de l'architecture en Tier

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**

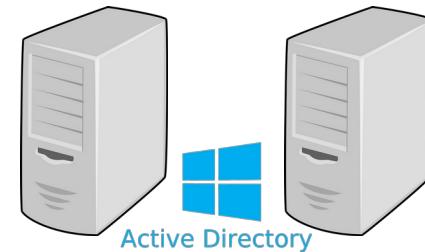




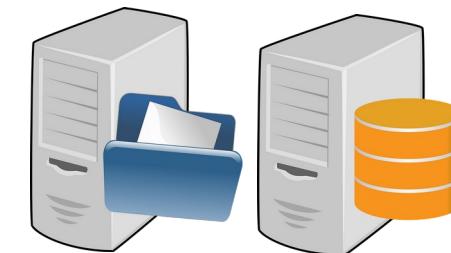
Principe de l'architecture en Tier

Stratégie d'authentification :

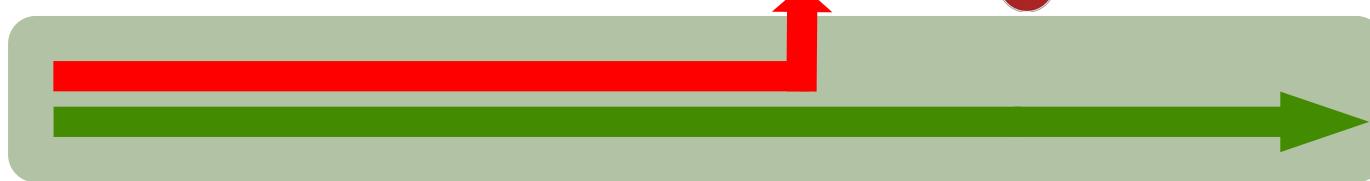
Admin
Tier 0



Admin
Tier 1



Admin
Tier 2





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 :

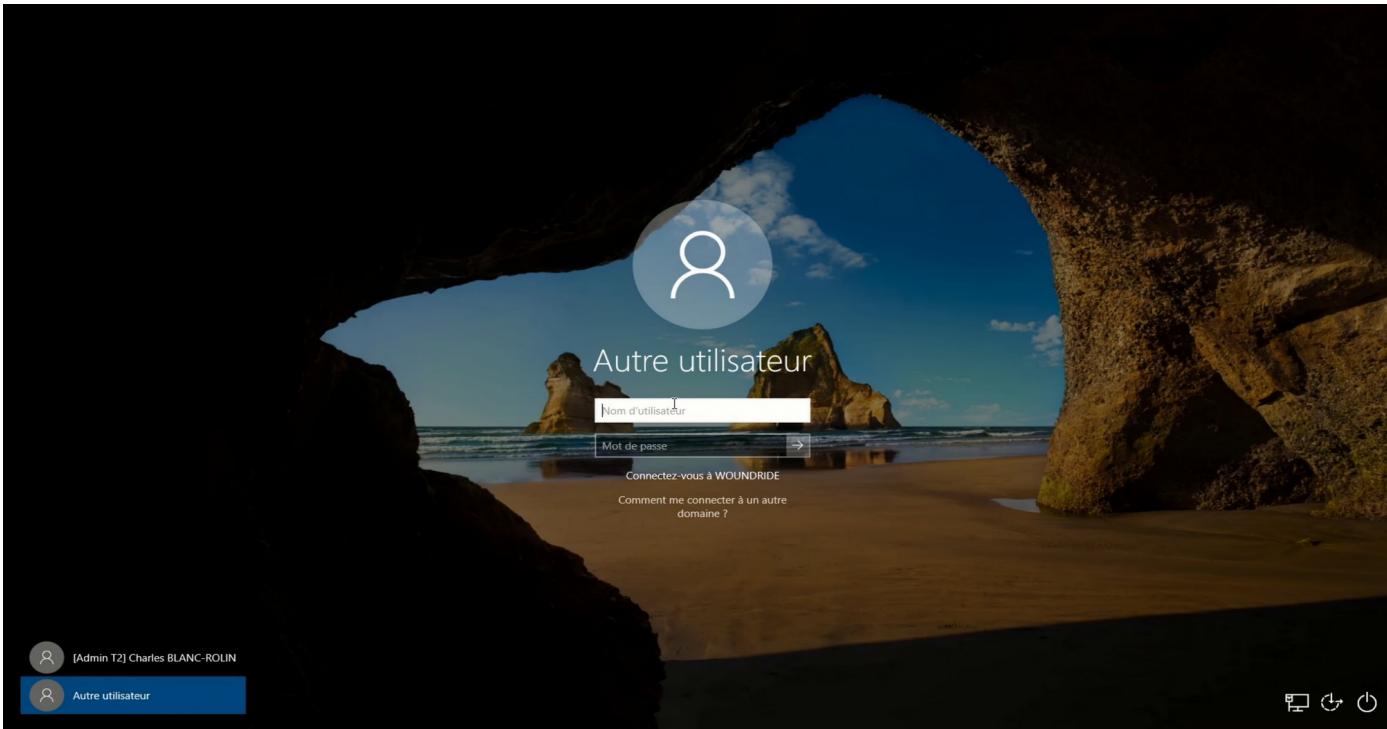
- Scénario : l'utilisateur exécute du code malveillant (fichier reçu en pièce jointe d'un courriel, lien malveillant...) sur une machine permettant à l'attaquant d'obtenir un accès
- Avec des privilèges élevés (administrateur local), l'attaquant pourra extraire les données d'authentification (identifiant(s) + 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) :

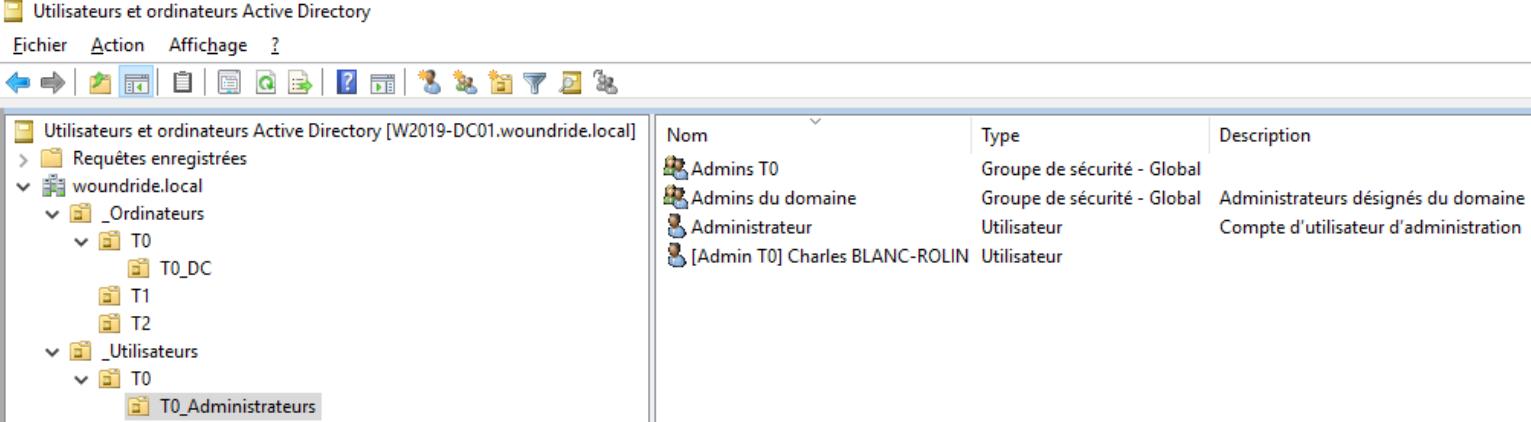
The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' management console. The left pane displays the structure of the 'woundride.local' domain, with 'Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]' as the root. Under 'woundride.local', there are two main OUs: '_Ordinateurs' and '_Utilisateurs'. The '_Ordinateurs' OU contains three sub-OUs: 'T0', 'T0_DC', 'T1', and 'T2'. The '_Utilisateurs' OU contains four sub-OUs: 'T0', 'T0_Administrateurs', 'T1', 'T1_Administrateurs', 'T2', 'T2_Administrateurs', 'T2_Utilisateurs', and 'Service 1'. A blue box highlights the 'T0', 'T0_DC', and 'T1' sub-OUs under '_Ordinateurs'. An orange box highlights the 'T0', 'T0_Administrateurs', 'T1', 'T1_Administrateurs', 'T2', 'T2_Administrateurs', 'T2_Utilisateurs', and 'Service 1' sub-OUs under '_Utilisateurs'. A blue arrow points from the text 'Arborescence pour stocker les objets de type « comptes d'ordinateurs » avec les différents niveaux (Tier 0, Tier 1 et Tier 2)' to the blue box. An orange arrow points from the text 'Arborescence pour stocker les objets de type « comptes utilisateurs » avec les différents niveaux (Tier 0, Tier 1 et Tier 2)' to the orange box.

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) :



Nom	Type	Description
Admins T0	Groupe de sécurité - Global	
Admins du domaine	Groupe de sécurité - Global	Administrateurs désignés du domaine
Administrateur	Utilisateur	Compte d'utilisateur d'administration
[Admin T0] Charles BLANC-ROLIN	Utilisateur	

- 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

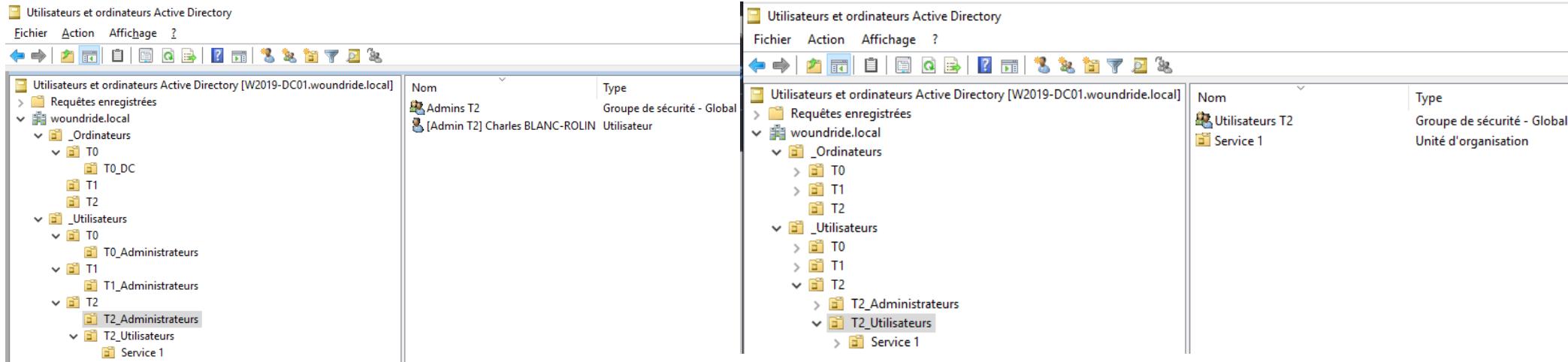
Rangement / création des comptes d'administrateurs (Tier 1) :

Nom	Type
Admins T1	Groupe de sécurité - Global
[Admin T1] Charles BLANC-ROLIN	Utilisateur

- 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 priviléges, 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 :



The screenshot displays two instances of the Active Directory Users and Computers (ADC) management console. The left instance shows the 'Utilisateurs et ordinateurs Active Directory' view for the domain 'W2019-DC01.woundride.local'. The right instance shows the same view for the same domain, but with a different account structure. Both instances have the 'Utilisateurs' tab selected.

Left ADC Instance (woundride.local structure):

- Root node: Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]
- Requêtes enregistrées
- woundride.local
 - _Ordinateurs
 - T0
 - T0_DC
 - T1
 - T2
 - T0_Utilisateurs
 - T0_Administrateurs
 - T1
 - T1_Administrateurs
 - T2
 - T2_Administrateurs
 - T2_Utilisateurs

Right ADC Instance (woundride.local structure):

 - Root node: Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]
 - Requêtes enregistrées
 - woundride.local
 - _Ordinateurs
 - T0
 - T1
 - T2
 - _Utilisateurs
 - T0
 - T0_Administrateurs
 - T1
 - T1_Administrateurs
 - T2
 - T2_Administrateurs
 - T2_Utilisateurs
 - Service 1

Nom	Type
Admins T2	Groupe de sécurité - Global
[Admin T2] Charles BLANC-ROLIN	Utilisateur

Nom	Type
Utilisateurs T2	Groupe de sécurité - Global
Service 1	Unité d'organisation

- On retrouve ici les administrateurs des postes utilisateurs du Tier 2, mais aussi les comptes utilisateurs exempts de priviléges sur les machines
- Ces comptes doivent pouvoir se connecter uniquement aux postes utilisateurs du Tier 2
- Pour faciliter la gestion des priviléges, 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 :

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Gestion de stratégie de groupe

Forêt : woundride.local

Domaines

- woundride.local
 - Default Domain Policy
 - _Ordinateurs
 - T0
 - T0_DC
 - Default Domain Controllers Policy
 - T1
 - Ordinateurs_T1_admins_locaux
 - Ordinateurs_T1_restrictions_sessions
 - T2
 - Ordinateurs_T2_admins_locaux
 - Ordinateurs_T2_restrictions_sessions
 - _Utilisateurs
 - Domain Controllers

Ordinateurs_T2_admins_locaux

Étendue Détails Paramètres Délégation

Ordinateurs_T2_admins_locaux
Données recueillies le : 05/01/2025 22:55:27

Général

Détails

Liaisons

Filtrage de sécurité

Délégation

Configuration ordinateur (activée)

Préférences

Paramètres du Panneau de configuration

Utilisateurs et groupes locaux

Groupe (nom : Administrateurs (intégré))

Administrateurs (intégré) (ordre : 1)

Groupe local

Action

Propriétés

Nom du groupe

Supprimer tous les utilisateurs membres

Supprimer tous les groupes de membres

Mettre à jour

Administrateurs (intégré)

Désactivé

Désactivé

Ajouter des membres

WOUNDRIDE\Admins T2

S-1-5-21-3332904308-1614487934-3407257785-1123

Mise en place de l'architecture en Tier

Rangement des comptes d'ordinateurs :

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?



Tier 0

Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]	
>	Requêtes enregistrées
>	woundride.local
>	_Ordinateurs
>	T0
>	T0_DC
>	T1
>	T2

Nom	Type
W2019-DC01	Ordinateur

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?



Tier 1

Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]	
>	Requêtes enregistrées
>	woundride.local
>	_Ordinateurs
>	T0
>	T0_DC
>	T1
>	T2

Nom	Type
SRV01	Ordinateur

Tier 2

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory [W2019-DC01.woundride.local]	
>	Requêtes enregistrées
>	woundride.local
>	_Ordinateurs
>	T0
>	T0_DC
>	T1
>	T2
>	_Utilisateurs
>	T0
>	T0_Administrateur
>	T1
>	T1_Administrateur
>	T2
>	T2_Administrateur
>	T2_Utilisateurs
>	Service 1



Restrictions d'accès aux machines

Deux méthodes :

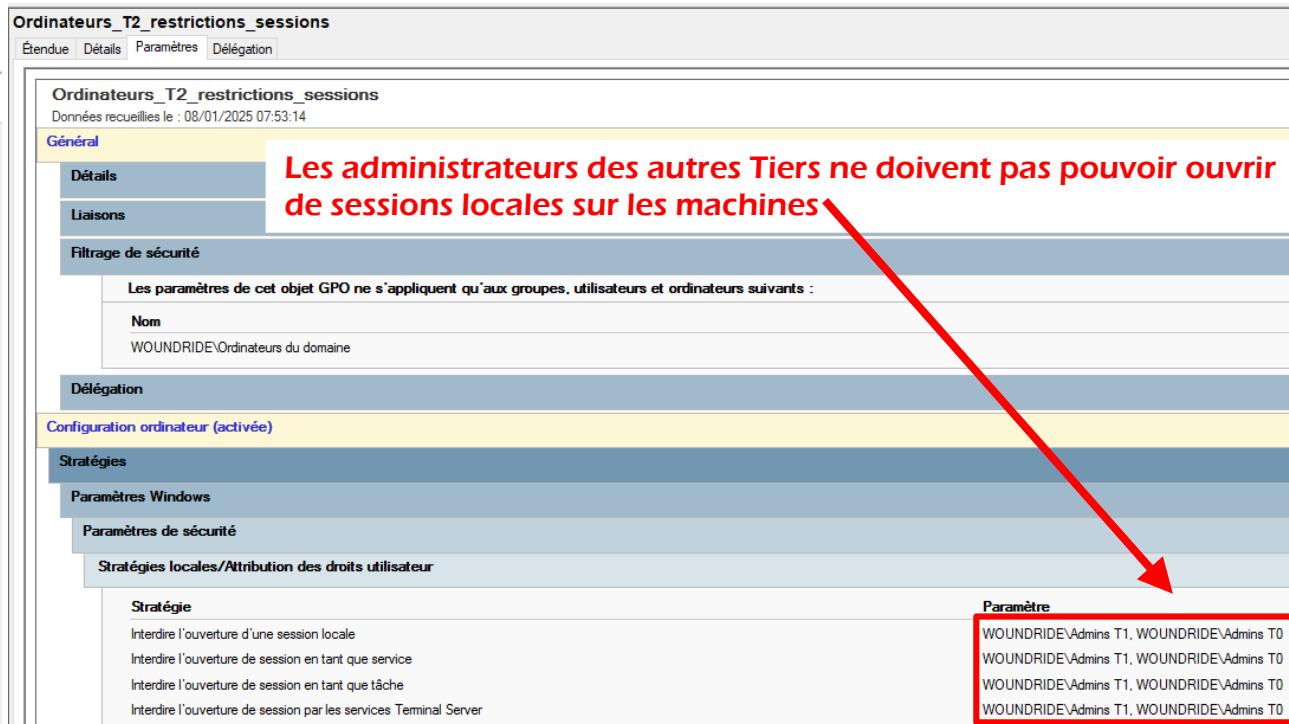
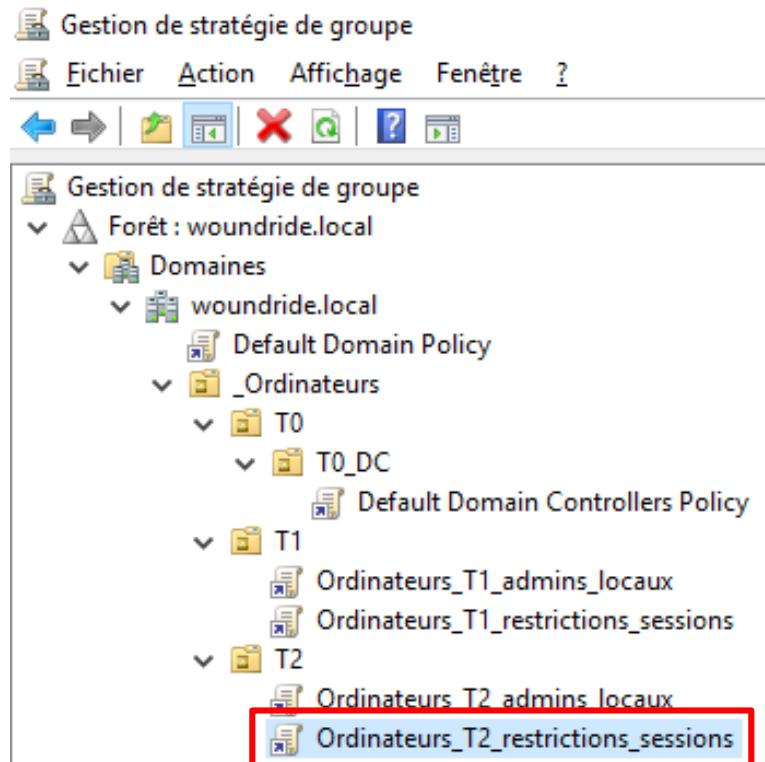
- Définir des **GPO** **interdisant** l'ouverture de sessions sur les ordinateurs d'un Tier :
 - Efficacité (mais n'empêche pas les connexions RDP depuis un autre Tier)
 - Facilité de mise en œuvre (application directe aux UO et / ou groupes)
 - Prise en charge des systèmes d'exploitation (très) obsolètes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





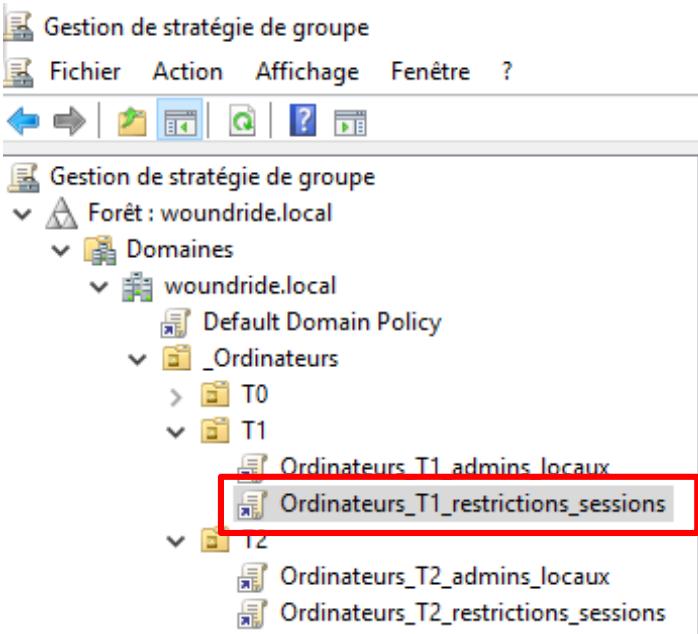
Méthode 1 : Mise en place de GPO de restrictions d'accès

Restriction d'accès aux machines du T2 :



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

Restriction d'accès aux machines du T1 :



Ordinateurs_T1_restrictions_sessions

Étendue Détails Paramètres Délégation

Ordinateurs_T1_restrictions_sessions

Données recueillies :
Général

Détails

Liaisons

Filtrage de sécurité

Délégation

Configuration ordinateur (activée)

Stratégies

Paramètres Windows

Paramètres de sécurité

Stratégies locales/Attribution des droits utilisateur

Stratégie

Paramètre

Interdire l'ouverture d'une session locale

WOUNDRIDE\Utilisateurs T2, WOUNDRIDE\Admins T2, WOUNDRIDE\Admins T0

Interdire l'ouverture de session en tant que service

WOUNDRIDE\Utilisateurs T2, WOUNDRIDE\Admins T2, WOUNDRIDE\Admins T0

Interdire l'ouverture de session en tant que tâche

WOUNDRIDE\Utilisateurs T2, WOUNDRIDE\Admins T2, WOUNDRIDE\Admins T0

Interdire l'ouverture de session par les services Terminal Server

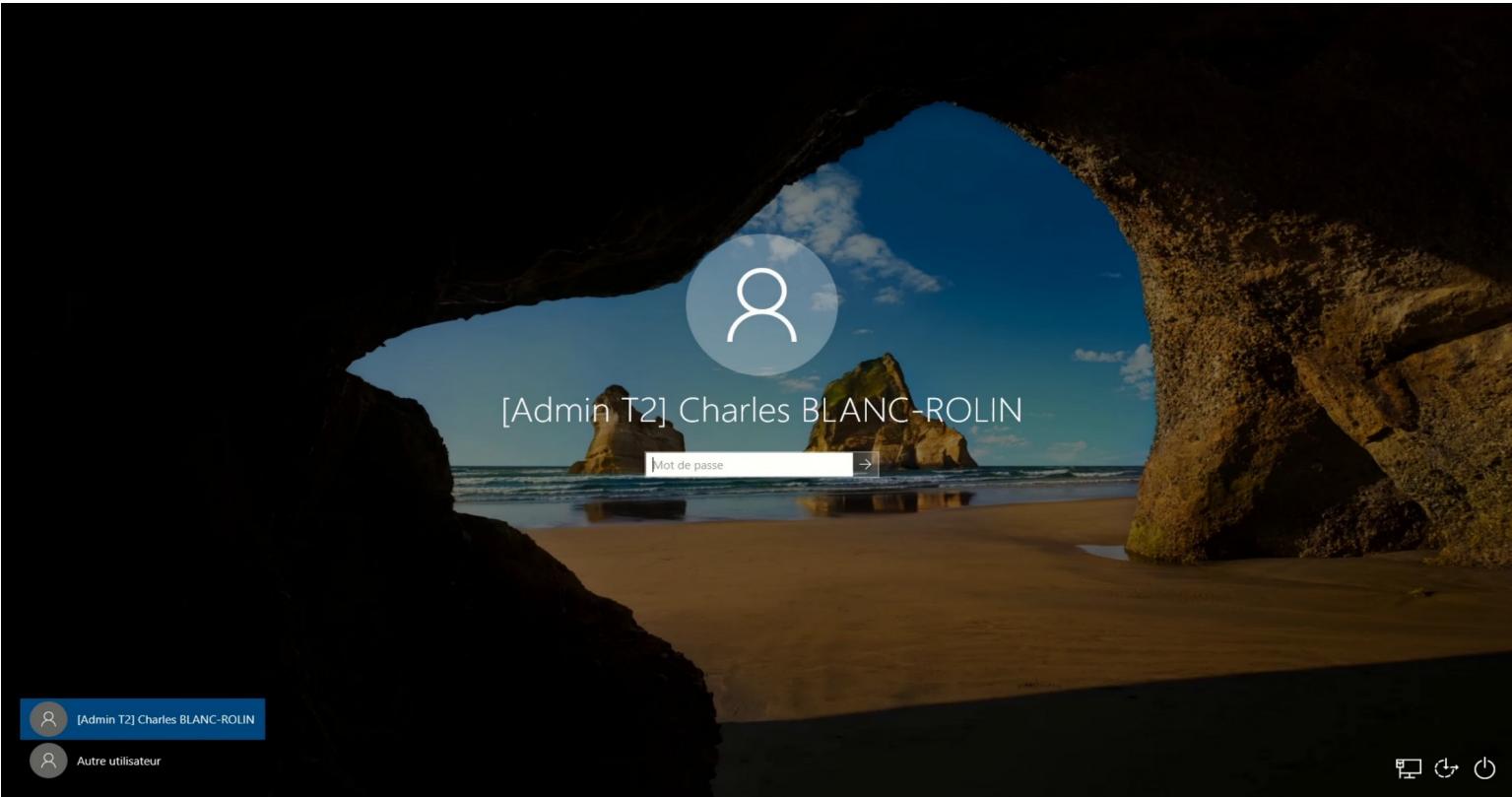
WOUNDRIDE\Utilisateurs T2, WOUNDRIDE\Admins T2, WOUNDRIDE\Admins T0

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

WOUNDRIDE\Utilisateurs T2, WOUNDRIDE\Admins T2, WOUNDRIDE\Admins T0

Exemple d'accès restreint sur le Tier 2

Tier 2





Les risques résiduels

Risques non couverts ici :

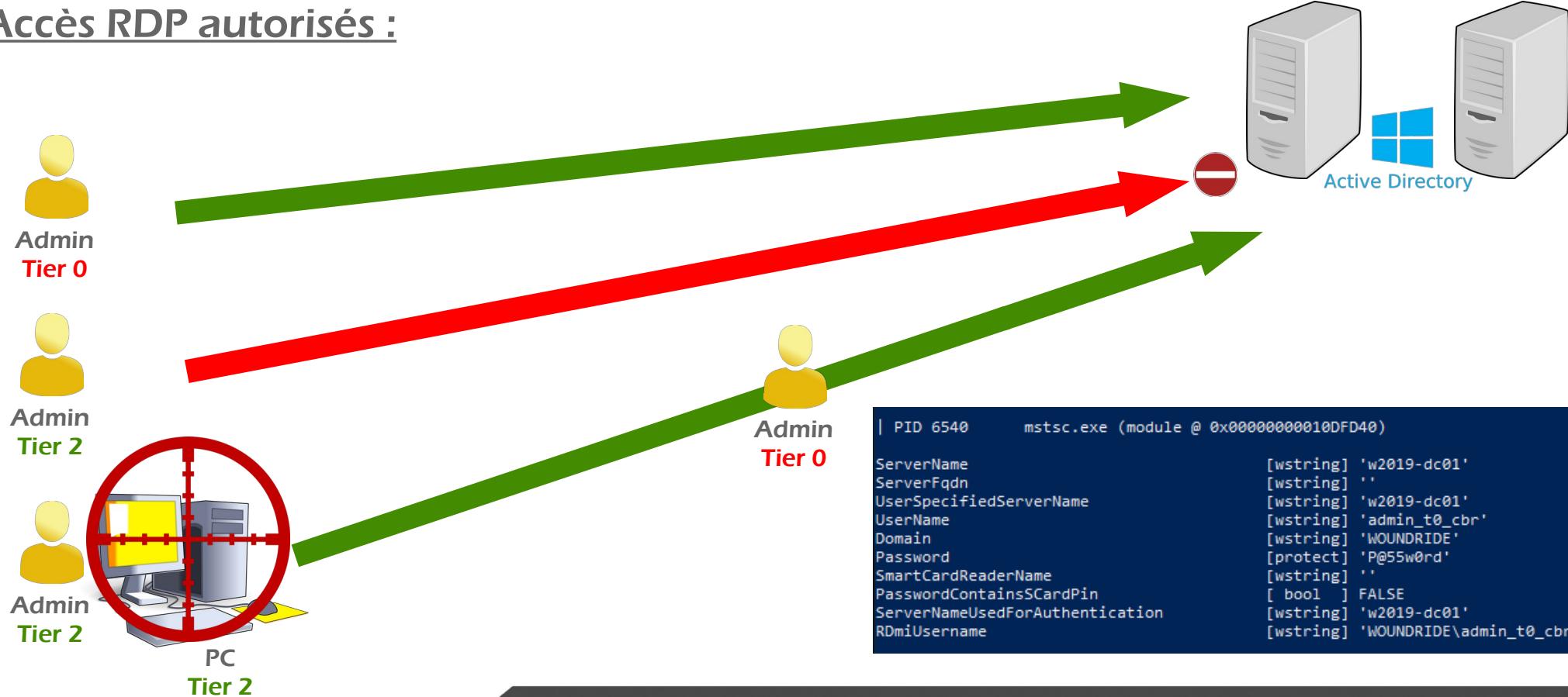
- *Un administrateur pourrait par facilité, utiliser le même mot de passe sur l'ensemble de ses comptes (peut être audité lors des revues de comptes par exemple)*
- *Si l'accès RDP/TSE est interdit sur une machine du Tier 0 par un administrateur du Tier 2, rien n'empêche un administrateur du Tier 2 de 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*





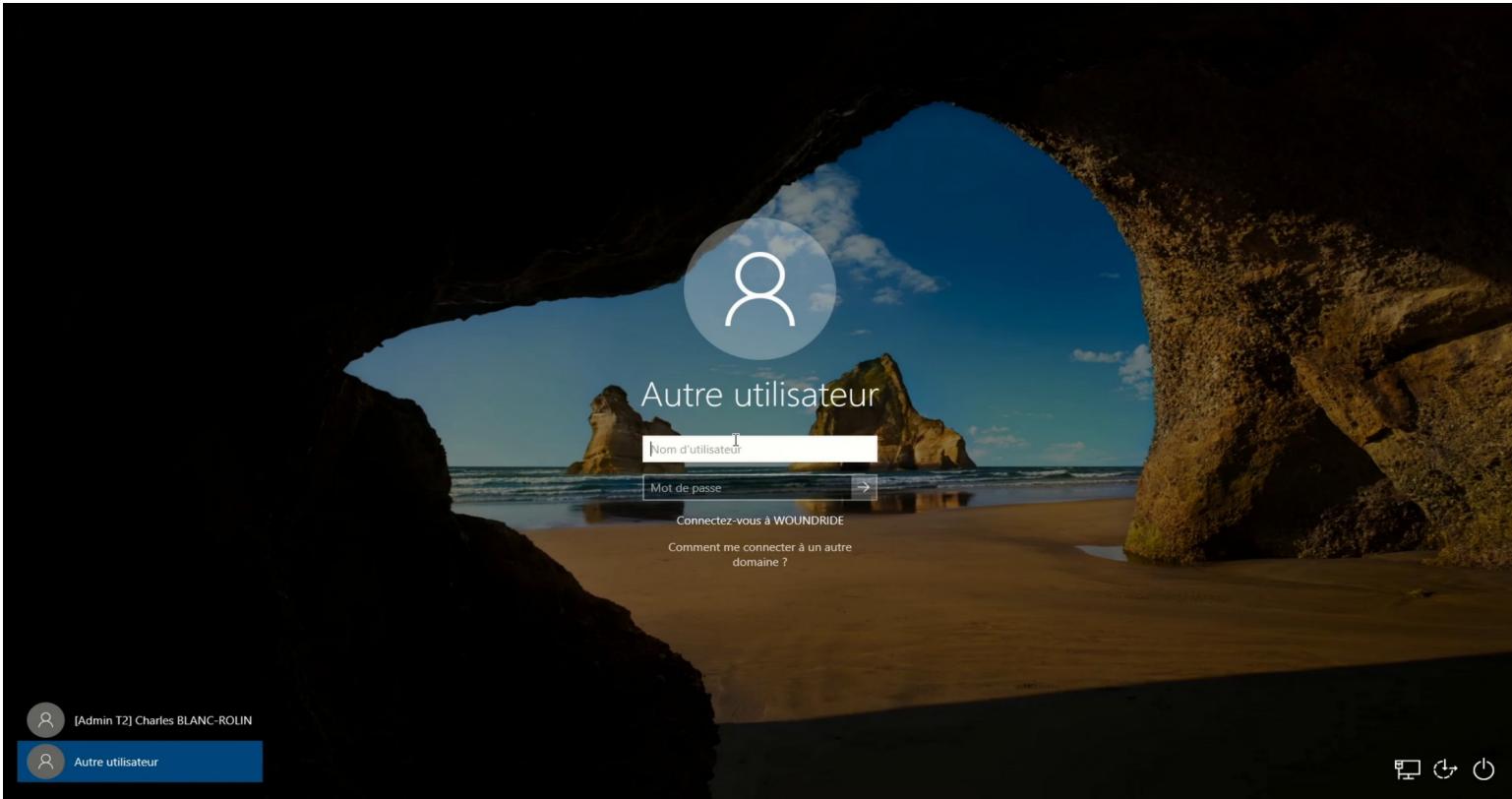
Limites des restrictions VS l'utilisation de RDP

Accès RDP autorisés :



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 :

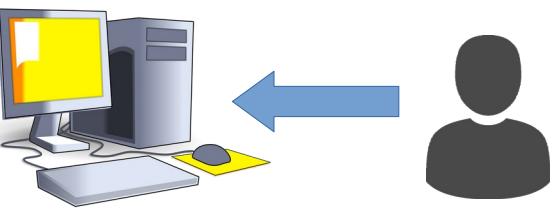
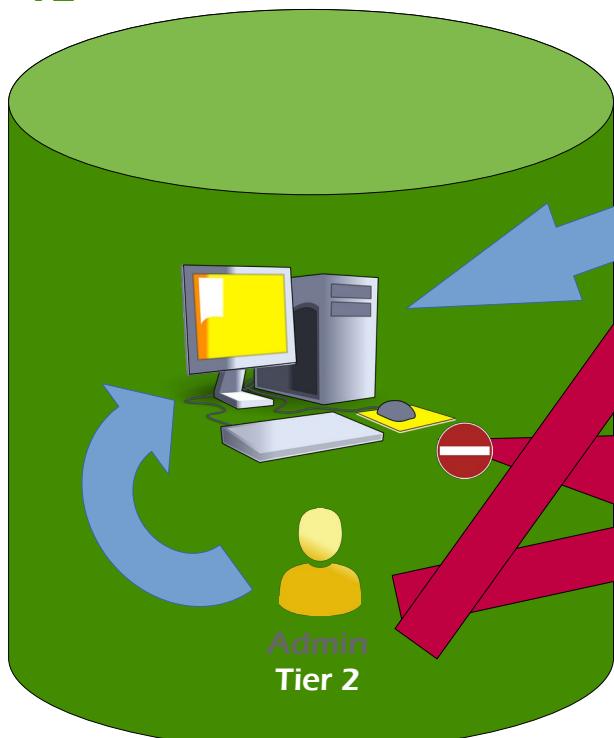
- **Avoir un niveau de domaine supérieur ou égal à 2012R2**
- **Activer la prise en charge du contrôle d'accès dynamique et du blindage Kerberos sur les contrôleurs de domaine**
- **Activer la prise en charge des revendications et du blindage Kerberos sur les postes clients, ce qui nécessite d'avoir 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**



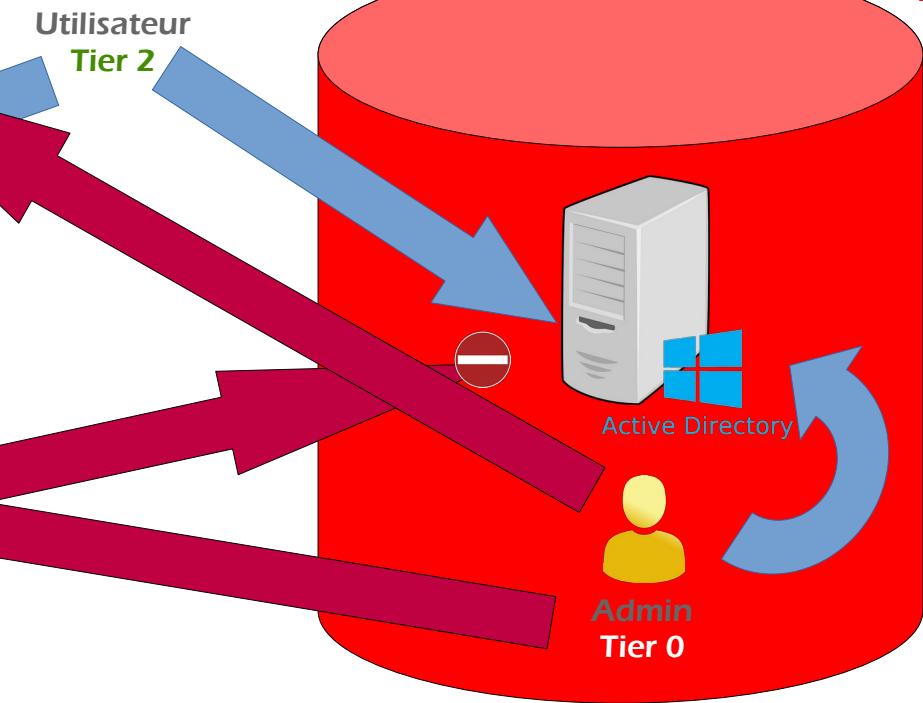
Méthode 2 : Mise en place de Silos d'authentification

Authentification locale :

Silo Admin
T2



Silo Admin
T0

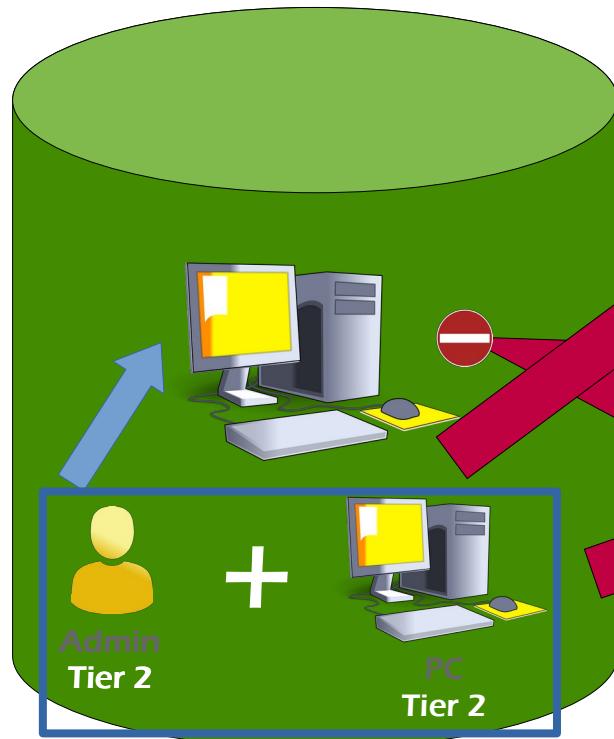


Méthode 2 : Mise en place de Silos d'authentification

Authentification RDP :

Silo Admin

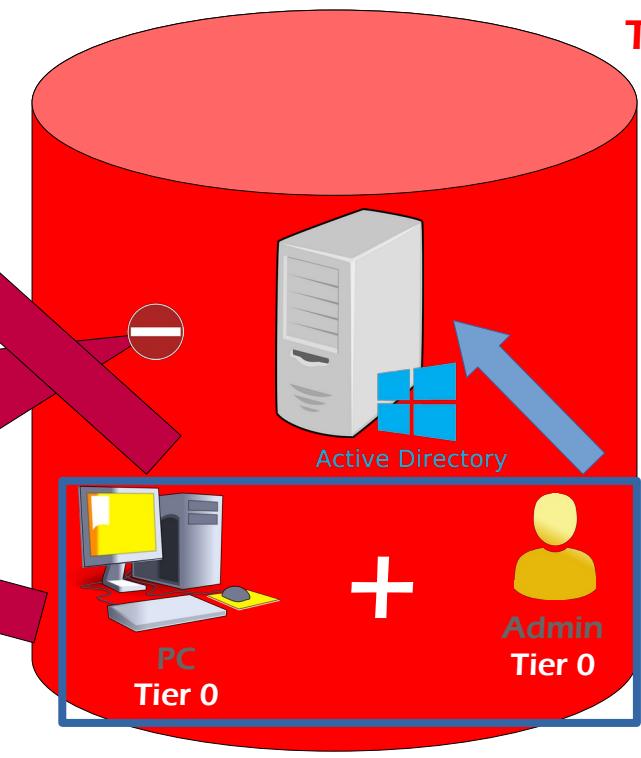
T2



Ordinateur
Tier 2

Silo Admin

T0



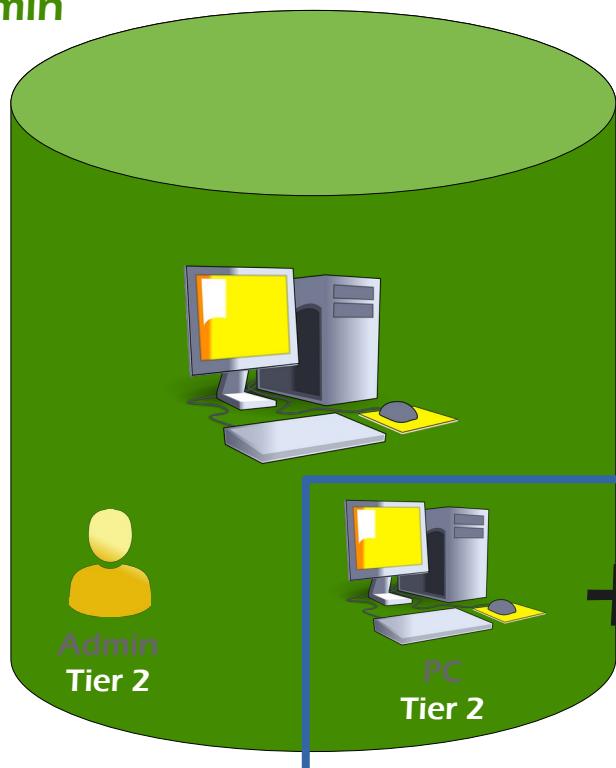
Active Directory

Méthode 2 : Mise en place de Silos d'authentification

Authentification RDP :

Silo Admin

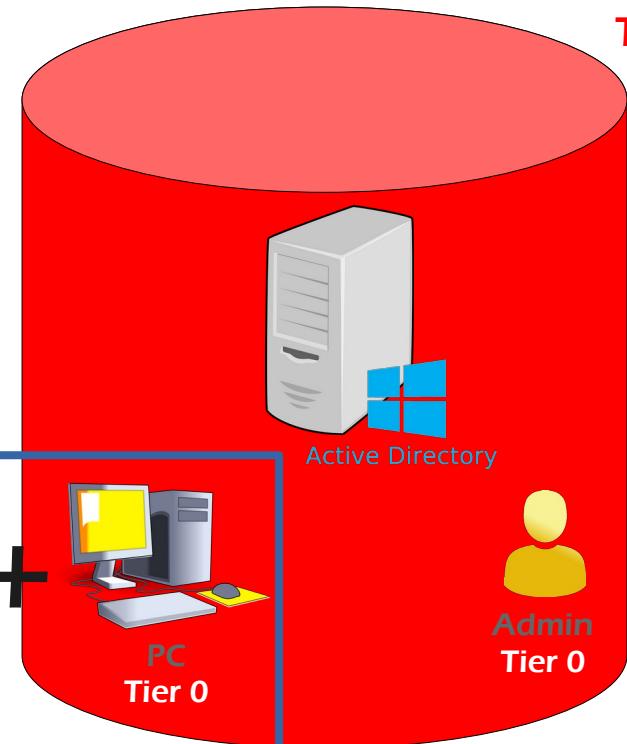
T2



Ordinateur
Tier 2

Silo Admin

T0



Active Directory

Méthode 2 : Mise en place de Silos d'authentification

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

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, the 'Gestion de stratégie de groupe' navigation pane is visible, showing the forest 'woundride.local' and its domains, including 'woundride.local' and 'T0'. The 'T0' domain is expanded, showing 'T0_DC' which is further expanded to show 'Default Domain Controllers Policy' and 'Ordinateurs_T0_DC_blidage_kerberos'. The 'Ordinateurs_T0_DC_blidage_kerberos' GPO is highlighted with a red box. On the right, the 'Ordinateurs_T0_DC_blidage_kerberos' properties window is open, showing the 'Général' tab. The 'Configuration ordinateur (activée)' section is expanded, showing the 'Système/KDC' table. This table has a single row with the following data:

Stratégie	Paramètre	Commentaire
Prise en charge du contrôleur de domaine Kerberos pour les revendications, l'authentification composée et le blindage Kerberos	Activé	

Below the table, a note states: 'Options de revendications, d'authentification composée pour le contrôle d'accès Toujours fournir des revendications dynamique et de blindage Kerberos :'

Méthode 2 : Mise en place de Silos d'authentification

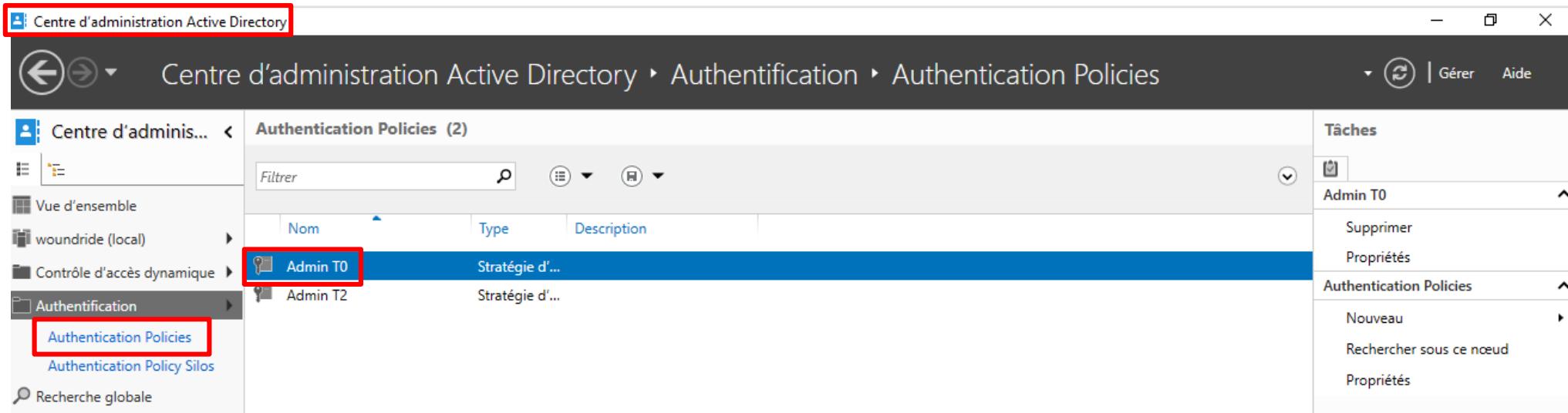
Création de la GPO d'activation du blindage Kerberos sur les postes :

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, the 'Forêt : woundride.local' tree is displayed, with 'Domaines' expanded to show 'woundride.local' and its sub-objects: 'Default Domain Policy', '_Ordinateurs', 'T0', 'T1', 'T2', '_Utilisateurs', 'Domain Controllers', 'Objets de stratégie de groupe', 'Filtres WMI', and 'Objets GPO Starter'. The 'Ordinateurs' folder is highlighted with a red box. On the right, the 'Ordinateurs_blindage_kerberos' GPO details are shown. The 'Général' tab is selected, displaying the 'Configuration ordinateur (activée)' section. The 'Stratégies' section shows a table for 'Système/Kerberos' with one row: 'Stratégie' (Prise en charge du client Kerberos pour les revendications, l'authentification composée et le blindage Kerberos) and 'Paramètre' (Activé). The entire 'Système/Kerberos' table is highlighted with a red box.

Stratégie	Paramètre	Commentaire
Prise en charge du client Kerberos pour les revendications, l'authentification composée et le blindage Kerberos	Activé	

Méthode 2 : Mise en place de Silos d'authentification

Création de la politique d'authentification Admin T0 :



Centre d'administration Active Directory

Centre d'administration Active Directory › Authentification › Authentication Policies

Centre d'adminis... < Authentication Policies (2)

Vue d'ensemble

woundrider (local)

Contrôle d'accès dynamique

Authentification >

Authentication Policies

Authentication Policy Silos

Recherche globale

Filter

Nom	Type	Description
Admin T0	Stratégie d'...	
Admin T2	Stratégie d'...	

Tâches

Admin T0

Supprimer

Propriétés

Authentication Policies

Nouveau

Rechercher sous ce nœud

Propriétés



Méthode 2 : Mise en place de Silos d'authentification

Création de la politique d'authentification Admin T0 :

Créer Stratégie d'authentification : Admin T0

Général

Comptes

Silos

Authentification de l'utilisateur

Tickets de service pour comptes d'utilisateur

Authentification du service

Tickets de service pour comptes de service

Ordinateur

Général

Une stratégie d'authentification définit les propriétés de ticket TGT (Ticket Granting Ticket) Kerberos et les conditions de contrôle d'accès par authentification d'un type de compte.

Nom complet : **Admin T0**

Description :

Protéger contre la suppression accidentelle

Auditer uniquement les restrictions de stratégie

Appliquer les restrictions de stratégie

Remarque : une stratégie d'audit appliquée via un silo remplace les paramètres de stratégie.

Comptes

Nom	Type de compte

Ajouter...

Supprimer

Silos affectés

Cette stratégie d'authentification n'est pas affectée à un silo de stratégies d'authentification.

Authentification de l'utilisateur

Exiger le déploiement du secret NTLM pour l'authentification NTLM

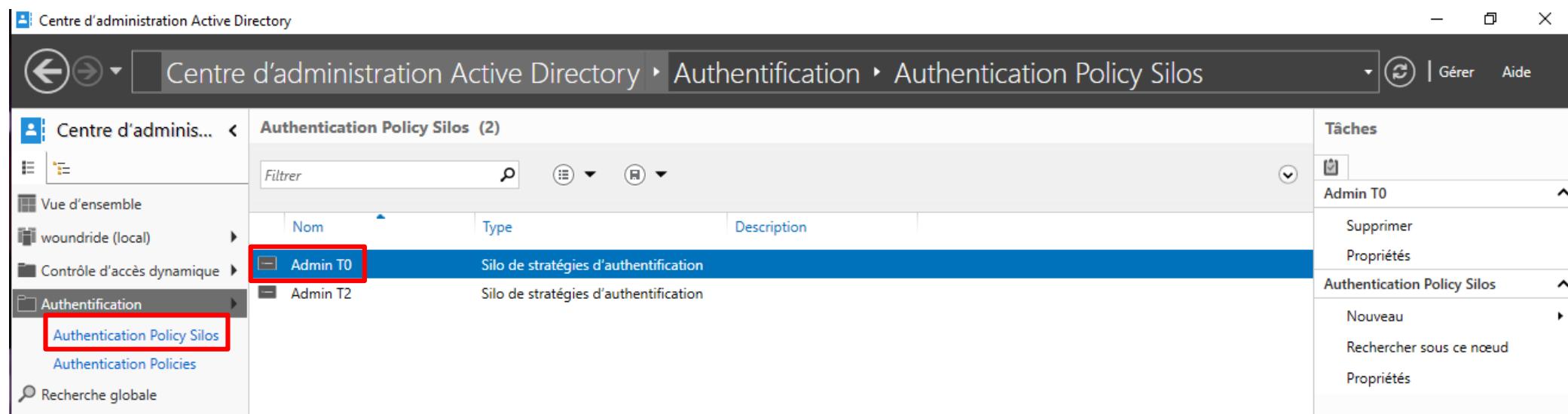
Autoriser les actions de secours sur le mot de passe du compte de domaine

Spécifiez la durée de vie du ticket TGT (Ticket Granting Ticket) pour les comptes d'utilisateur.



Méthode 2 : Mise en place de Silos d'authentification

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



The screenshot shows the 'Centre d'administration Active Directory' interface. The left navigation pane is open, showing 'Centre d'administration Active Directory', 'Vue d'ensemble', 'woundrider (local)', 'Contrôle d'accès dynamique', 'Authentication' (selected), and 'Recherche globale'. Under 'Authentication', 'Authentication Policy Silos' is selected and highlighted with a red box. The main pane displays 'Authentication Policy Silos (2)'. A table lists two entries: 'Admin T0' (selected and highlighted with a red box) and 'Admin T2'. The 'Admin T0' row shows 'Silo de stratégies d'authentification' in the 'Type' column. The right pane shows a 'Tâches' (Tasks) list with 'Admin T0' selected, and options like 'Supprimer' (Delete) and 'Propriétés' (Properties). A context menu for 'Authentication Policy Silos' is also visible, with options like 'Nouveau' (New) and 'Rechercher sous ce nœud' (Search under this node).

Nom	Type	Description
Admin T0	Silo de stratégies d'authentification	
Admin T2	Silo de stratégies d'authentification	



Méthode 2 : Mise en place de Silos d'authentification

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

Créer Silo de stratégies d'authentification : Admin T0

Général

Un silo de stratégies d'authentification permet de déterminer quels sont les comptes à protéger et de définir les stratégies d'authentification à appliquer aux membres du silo.

Nom complet : *

Description :

Auditer uniquement les stratégies du silo

Appliquer les stratégies du silo

Protéger contre la suppression accidentelle

Comptes autorisés

Nom	Type de compte	Attribué

Stratégie d'authentification

Utilisez une seule stratégie pour tous les principaux qui appartiennent à ce silo de stratégies d'authentification.

* Stratégie d'authentification qui s'applique à tous les comptes de ce silo : Ouvrir

Utilisez une stratégie d'authentification distincte pour chaque type de principal.

Stratégie de compte d'utilisateur : Ouvrir

Stratégie de compte de service géré : Ouvrir

Stratégie de compte d'ordinateur : Ouvrir

Informations supplémentaires...

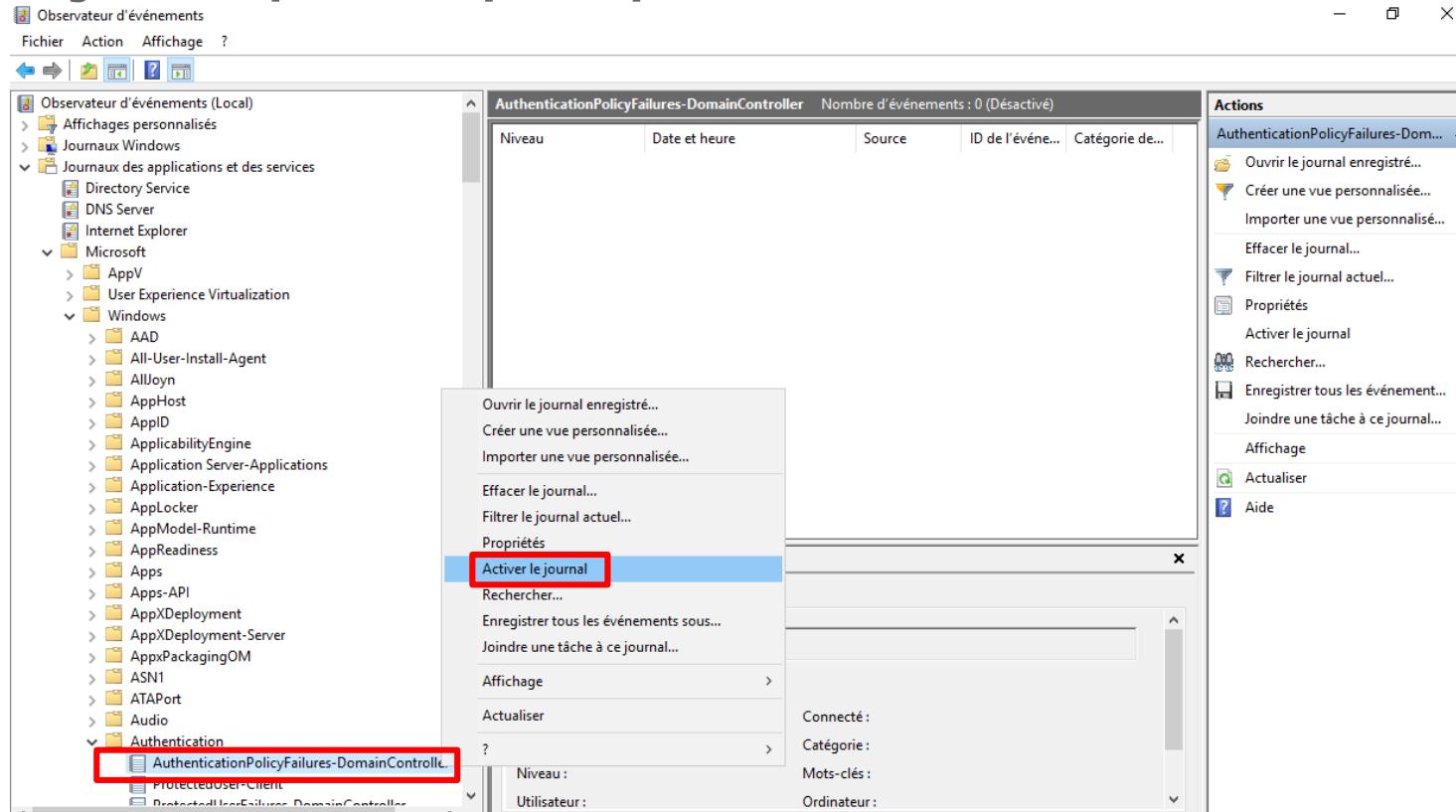
OK Annuler

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 :

Admin T0

Général

Comptes

Stratégie

La coche verte sera initialement absente, indiquant que l'objet affiché dans cette liste n'appartient pas réellement au Silo

Nom complet : * Admin T0

Description :

Protéger contre la suppression accidentelle

Comptes autorisés

Nom	Type de compte	Attribué
[Admin T0] Charles BLANC-ROLIN	Utilisateur	✓
PC11	Ordinateur	✓
W2019-DC01	Ordinateur	✓

TÂCHES

SECTION

Impôts à pr.

Attention, l'ajout via ce bouton n'ajoute pas « vraiment » l'objet dans le Silo

Appliquer les stratégies du silo

Ajouter...

Supprimer

Détails





Méthode 2 : Mise en place de Silos d'authentification

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

The screenshot shows two windows of the Active Directory User and Computer Management console. The top window is for a user account named [Admin T0] Charles BLANC-ROLIN. The bottom window is for a computer object named W2019-DC01.

User Account Configuration (Top Window):

- Left pane (Navigation):** Compte, Organisation, Membre de, Paramètres de mot de passe, Profil, Stratégie, Silo, Extensions.
- Right pane (Main View):**
 - Stratégie d'authentification:** A checkbox labeled "Affectez une stratégie d'authentification à ce compte." is empty. A dropdown menu labeled "Stratégie d'authentification (si elle n'est pas membre d'un silo)" is shown.
 - Silo de stratégies d'authentification:** A checkbox labeled "Affecter un silo de stratégies d'authentification" is checked. A dropdown menu labeled "Silo de stratégies d'authentification" is open, showing "Admin T0".
 - Buttons:** TÂCHES, SECTION, Help, Close.

Text Annotation: "Le Silo devra être configuré sur chaque objet" (The Silo must be configured on each object) is written in red text on the right side of the top window.

Computer Object Configuration (Bottom Window):

- Left pane (Navigation):** Ordinateur, Géré par, Membre de, Stratégie, Silo, Délégation, Extensions.
- Right pane (Main View):**
 - Stratégie d'authentification:** A checkbox labeled "Affectez une stratégie d'authentification à ce compte." is empty. A dropdown menu labeled "Stratégie d'authentification (si elle n'est pas membre d'un silo)" is shown.
 - Silo de stratégies d'authentification:** A checkbox labeled "Affecter un silo de stratégies d'authentification" is checked. A dropdown menu labeled "Silo de stratégies d'authentification" is open, showing "Admin T0".
 - Buttons:** TÂCHES, SECTION, Help, Close.

Text Annotation: A red arrow points from the text "Le Silo devra être configuré sur chaque objet" in the top window to the "Silo de stratégies d'authentification" section of the bottom window.





Méthode 2 : Mise en place de Silos d'authentification

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

Admin T0

Général
Comptes
Silos
Authentification de l'utilisateur
Tickets de service pour comptes d'utilisateur
Authentification du service
Tickets de service pour comptes de service
Ordinateur

Général

Une stratégie d'authentification définit les propriétés de ticket TGT (Ticket Granting Ticket) Kerberos et les conditions de contrôle d'accès par authentification d'un type de compte.

Nom complet : Description :
 Auditer uniquement les restrictions de stratégie
 Appliquer les restrictions de stratégie
Remarque : une stratégie d'audit appliquée via un silo remplace les paramètres de stratégie des membres du silo.

Protéger contre la suppression accidentelle

Comptes

Nom	Type de compte

Silos affectés

Nom	Stratégie de compte d'utilisateur	Stratégie de compte de service	Stratégie de compte d'ordinateur
Admin T0	✓	✓	✓

Authentification de l'utilisateur

Exiger le déploiement du secret NTL pour l'authentification NTL
 Autoriser les actions de secours sur le mot de passe du compte de domaine

Spécifiez la durée de vie du ticket TGT (Ticket Granting Ticket) pour les comptes d'utilisateur.
Durée de vie du ticket TGT en minutes :

Spécifiez des conditions de contrôle d'accès qui restreignent les appareils pouvant demander un ticket TGT (Ticket Granting Ticket) pour les comptes d'utilisateur affectés à cette stratégie.
 Autoriser l'authentification réseau NTL lorsque l'utilisateur est limité à une sélection d'appareils

Cliquez sur Modifier pour définir les conditions

Modifier les conditions de contrôle d'accès

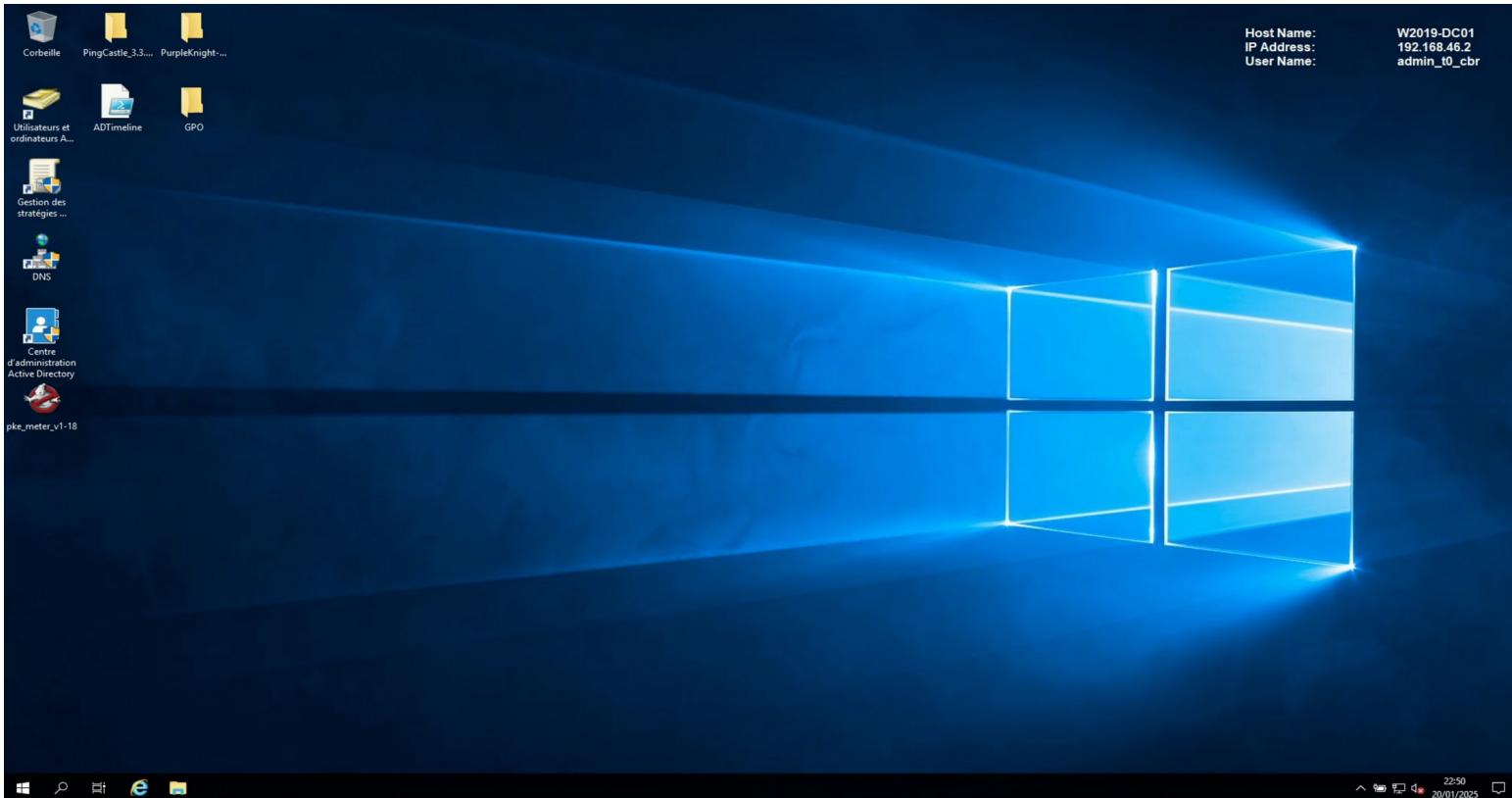
Spécifiez les conditions de contrôle d'accès de la stratégie d'authentification.

Utilisateur AuthenticationSilo Est égal à Valeur Admin T0

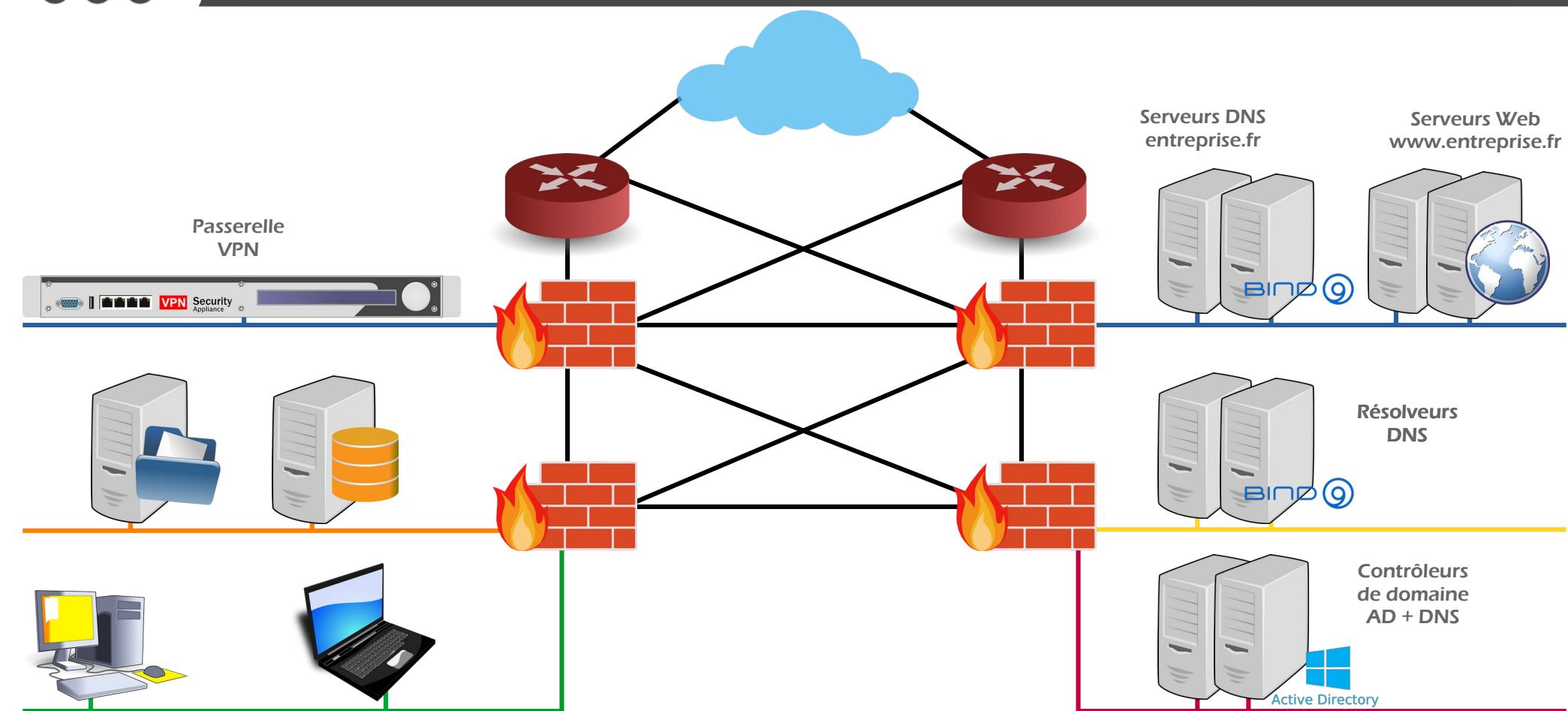
[Ajouter une condition](#)



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 Directory

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

STORMSHIELD v4.8.5

MONITORING CONFIGURATION SN310 SN310 admin ÉCRITURE LOGS : ACCÈS

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

OBJETS

UTILISATEURS

Politique de Sécurité

Filtrage et NAT

Filtrage URL

Filtrage SSL

Filtrage SMTP

Qualité de service

Règles implicites

PROTECTION APPLICATIVE

VPN

NOTIFICATIONS

Filtrage NAT

TO DC (contient 17 règles, de 30 à 46)

Numéro	Etat	Action	Source	Destination	Port dest.	Protocole	Commentaire
30	on	passer	Network_PC	Network_DC	ntp	NTP	Accès PC vers DC pour NTP
31	on	passer	Network_PC	Network_DC	epmap_tcp	tcp	Accès PC vers DC pour RPC
32	on	passer	Network_PC	Network_DC	kpasswd		Accès PC vers DC pour Kerberos Password
33	on	passer	Network_PC	Network_DC	ad2008-dn_tr		Accès PC vers DC pour RPC : LSA, SAM, NetLogon
34	on	passer	Network_PC	Network_DC	ldap	LDAP/tcp	Accès PC vers DC pour LDAP TCP
35	on	passer	Network_PC	Network_DC	ldap_udp	LDAP/udp	Accès PC vers DC pour LDAP UDP
36	on	passer	Network_PC	Network_DC	ldaps	SSL	Accès PC vers DC pour LDAPS
37	on	passer	Network_PC	Network_DC	ldap_gc	tcp	Accès PC vers DC pour LDAP GC
38	on	passer	Network_PC	Network_DC	ldap_gcssl	SSL	Accès PC vers DC pour LDAP GC SSL
39	on	passer	Network_PC	Network_DC	dns_tcp	DNS/tcp	Accès PC vers DC pour DNS TCP
40	on	passer	Network_PC	Network_DC	dns_udp	DNS/udp	Accès PC vers DC pour DNS UDP
41	on	passer	Network_PC	Network_DC	kerberos		Accès PC vers DC pour Kerberos
42	on	passer	Network_PC	Network_DC	microsft-ds_i	tcp	Accès PC vers DC pour SMB
43	on	passer	Network_PC	Network_DC	Any	icmp	Accès PC vers DC pour ICMP



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>

