Configuration du Windows supervisé dans un Domaine (Active Directory) pour le pack windows-by-WinRM__shinken

Sommaire

Contexte

Cette page a pour but de décrire la mise en place des autorisations minimales nécessaire pour un Windows (Serveur ou PC) **appartenant à un domaine** (*Active Directory*)**.**

REMARQUE : Pour un Windows qui **n'appartiennent PAS à un domaine**, mais à un groupe de travail (*Work Group*) , voir la page Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken

Pré-requis

Il est nécessaire pour les hôtes supervisés d'avoir d'installé **au moins une des langues suivantes**, pour le bon fonctionnement de la sonde :

- Français (**fr-FR**)
- Anglais (**en-US**)

La commande suivante permet d'afficher les langues installées sur votre machine :

```
Get-InstalledLanguage
```

Un résultat similaire à celui-la sera obtenu :

> La commande est disponible uniquement avec le Module LanguagePackManagement.
>
> - Si la commande n'est pas installée,
> - vérifié depuis l'interface graphique : **Paramètres > Heure et langue > Langue > Langue d'affichage de Windows.**

```
Language Language Packs  Language Features
-------- --------------  -----------------
en-US    LpCab, LXP      BasicTyping, Handwriting, Speech, TextToSpeech, OCR
fr-FR    LpCab, LXP      BasicTyping, Handwriting, Speech, TextToSpeech, OCR
```

Alors, si vos Windows à superviser **ont au moins une des langues nécessaires, passer au chapitre suivante**.

Sinon, voici quelques outils pour installer de nouvelles langues :

Ici, la langue configurée n'a **pas d'impact sur la traduction et l'affichage** des résultats générés par la sonde, mais a un **impact sur le bon fonctionnement**.

Pour les Windows ci-dessous, il est possible d'exécuter la commande suivante afin d'installer une langue :

- Windows 11
- Windows 10
- Windows Server 2025

```
# Installer la langue en Anglais
Install-Language -Language en-US -ExcludeFeatures

# Installer la langue en Francais
Install-Language -Language fr-FR -ExcludeFeatures
```

Pour les autres versions de Windows Server, d'autres solutions existent :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Une façon de déployer un nouveau langage sur ses machines supervisées est d'utiliser Windows *Feature On Demand* (FoD) afin d'installer un pack de langue.
Il est possible de télécharger et d'installer le pack de langue avec la commande suivante (*non disponible sur Windows Server 2012 R2*):

```
DISM.exe /Online /add-capability /CapabilityName:Language.Basic~~~en-US~0.0.1.0
```

Pour les installations hors-ligne, il est possible de demander à son support Microsoft le pack de langue livré dans un fichier *.iso* ou *.cab.* Il faudra ensuite le déployer et l'installer avec l'outil *DISM.EXE*. Plus d'informations ici : https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/features-on-demand-v2--capabilities?view=windows-11.

Configuration de WinRM pour domaine (Active Directory)

L'entièreté de la configuration de vos machines Windows se fera depuis une seule machine, votre contrôleur de domaine.

Autant que possible, la configuration sera définie avec des GPO (*Global Policy Object*) et sera déployée automatiquement à l'ensemble des machines ciblées.

Les **GPOs** sont des objets logiques sur lesquels on attache des règles de configurations.

- Les **GPOs** sont appliqués à des serveurs ou utilisateurs.
- Ils ont l'avantage de se déployer facilement et d'être désactivable.

> ⚠ Toutes les étapes suivantes doivent être appliquées depuis votre **contrôleur de domaine**, avec un **compte** aillant des **droits d'Administrateur de domaine**.

Configuration de l'Active Directory

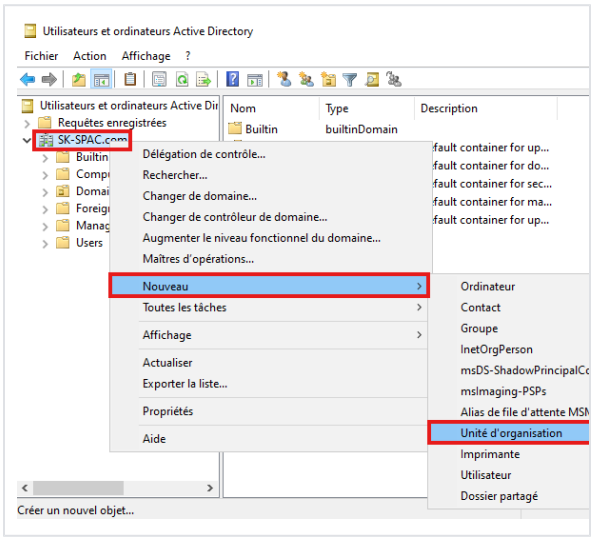
La première étape est d'organiser votre **Active Directory** avec des **UOs** (*Unité d'organisation*) pour shinken.

- Ces **UOs** vont regrouper les éléments de votre **Active Directory** (utilisateurs, serveurs et contrôleurs de domaine) afin d'appliquer les configurations de supervisions.
- Ouvrir "**Utilisateurs et ordinateurs Active directory**" (*dsa.msc*).

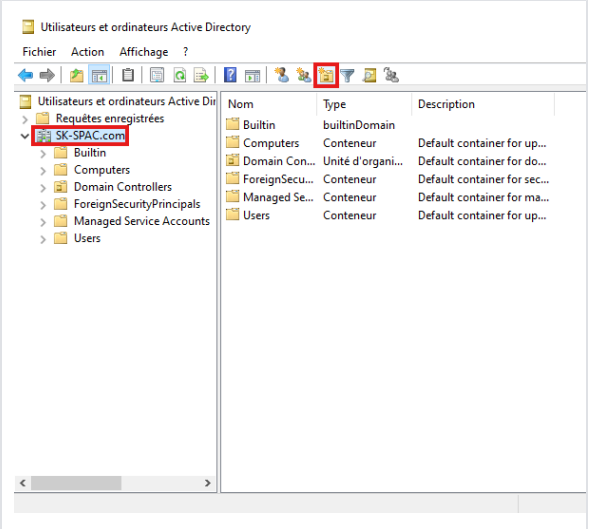
Organiser ses machines par UO

Organiser ses serveurs et postes de travail par UO

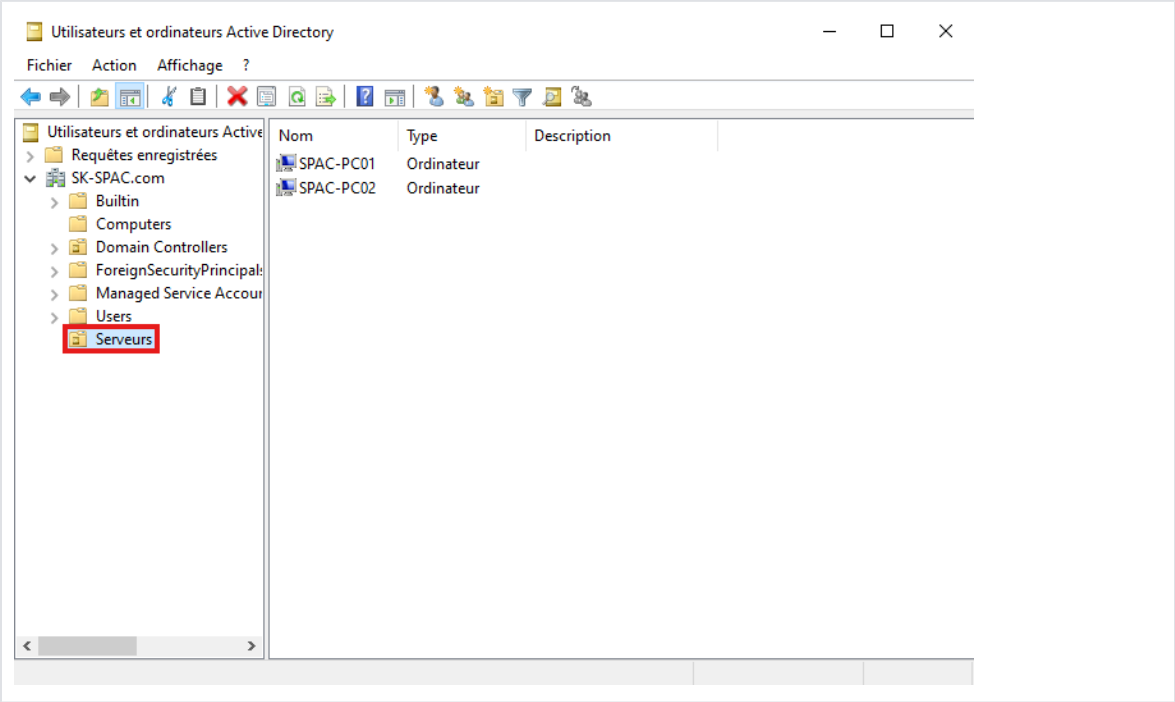
- Cliquer sur son domaine.
- Repérer dans quels dossiers sont les ordinateurs à superviser.
- Si tous les serveurs sont dans le dossier "**Computers**", il est nécessaire de les déplacer dans un nouveau dossier **UO**.
    - Le dossier "**Computers**", présent par défaut, ne permet pas d'appliquer des **GPOs** ou de créer de sous-dossiers.
    - Clic-Droit sur le nom de domaine, Sélectionner "**Nouveau**" > "**Unité d'organisation**" et lui donner un nom tel que "**Serveurs**".



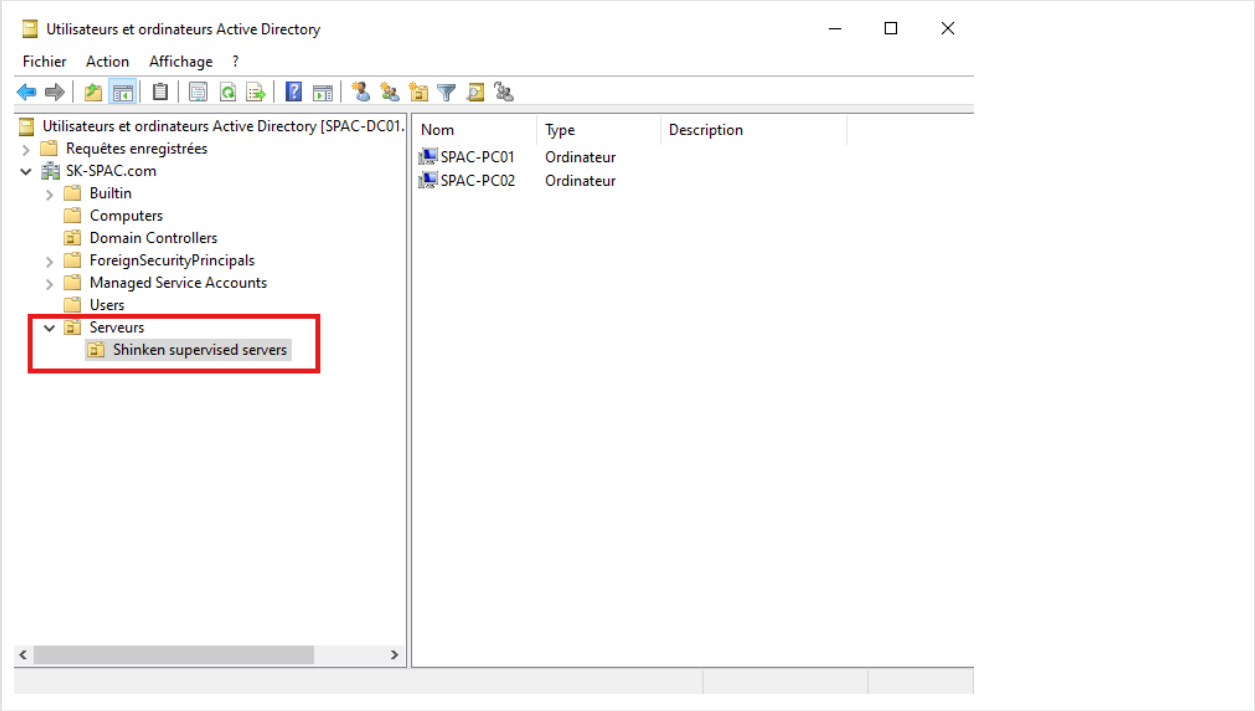
Il est également possible de créer une UO avec le boutton **Dossier** dans la barre d'outils.



- Une fois créée, l'UO se présentera de cette façon :



- Pour chacun des **UOs** où sont vos **serveurs à superviser** (*Ici, il n'y a qu'une seule UO où sont les serveurs, c'est "Serveurs"*), créer un **UO** et nommer le, par exemple "**Shinken supervised server**".
- Déplacer les serveurs à superviser dans la nouvelle **UO**.

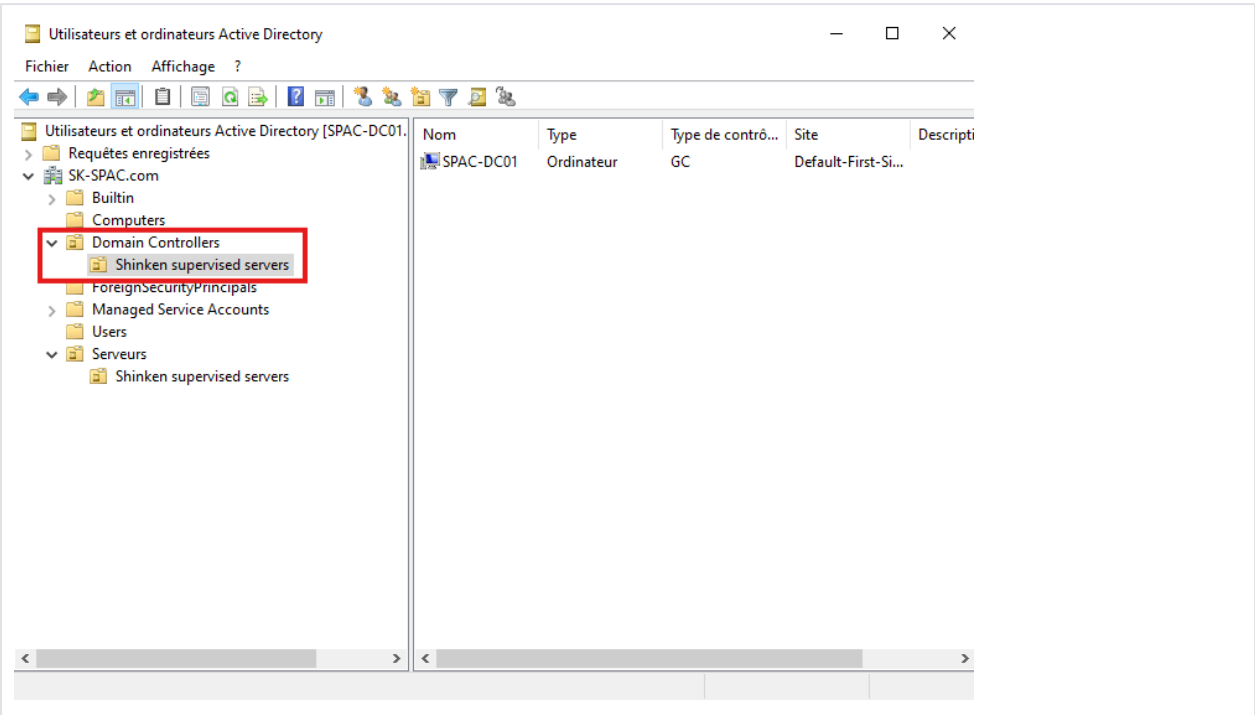


Organiser ses contrôleurs de domaine par UO

Il est également possible de superviser ses contrôleurs de domaine.

Pour cela, il faut tout comme les autres serveurs, tout d'abord les ranger dans une **UO** :

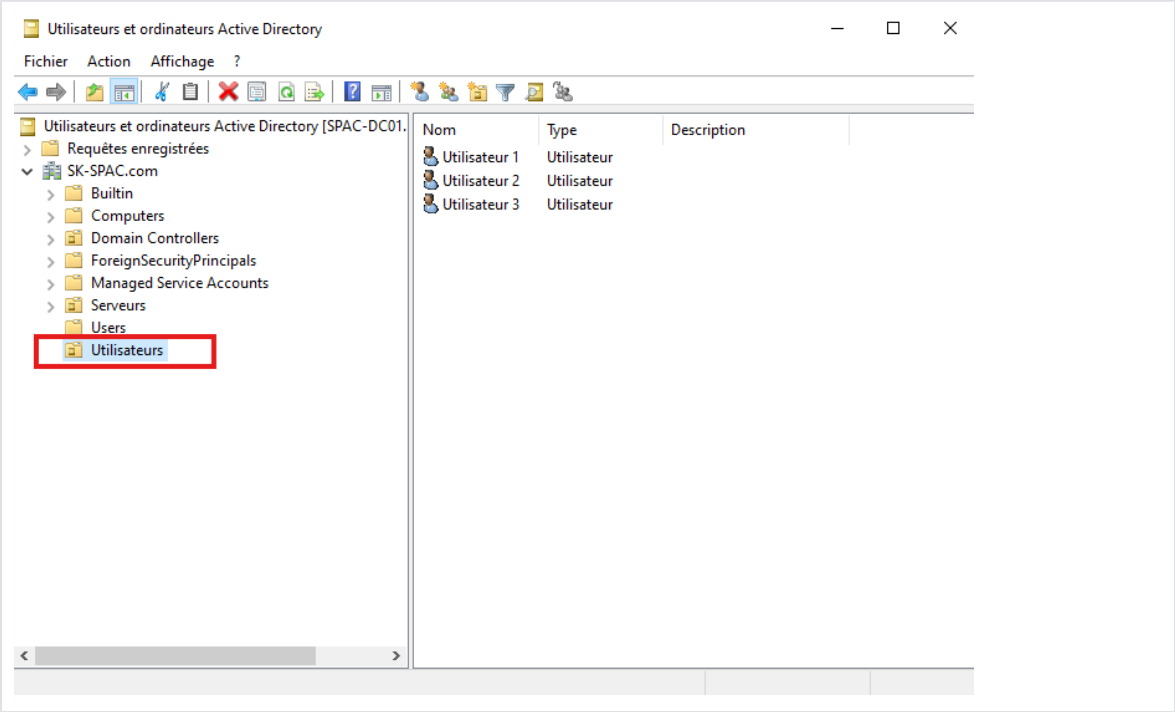
- Dans le dossier "**Domain Controllers**", Clic-Droit, Sélectionner "**Nouveau**" > "**Unité d'organisation**" et nommer le par exemple "**Shinken supervised server**".
- Déplacer les contrôleurs de domaine dans la nouvelle **UO**.



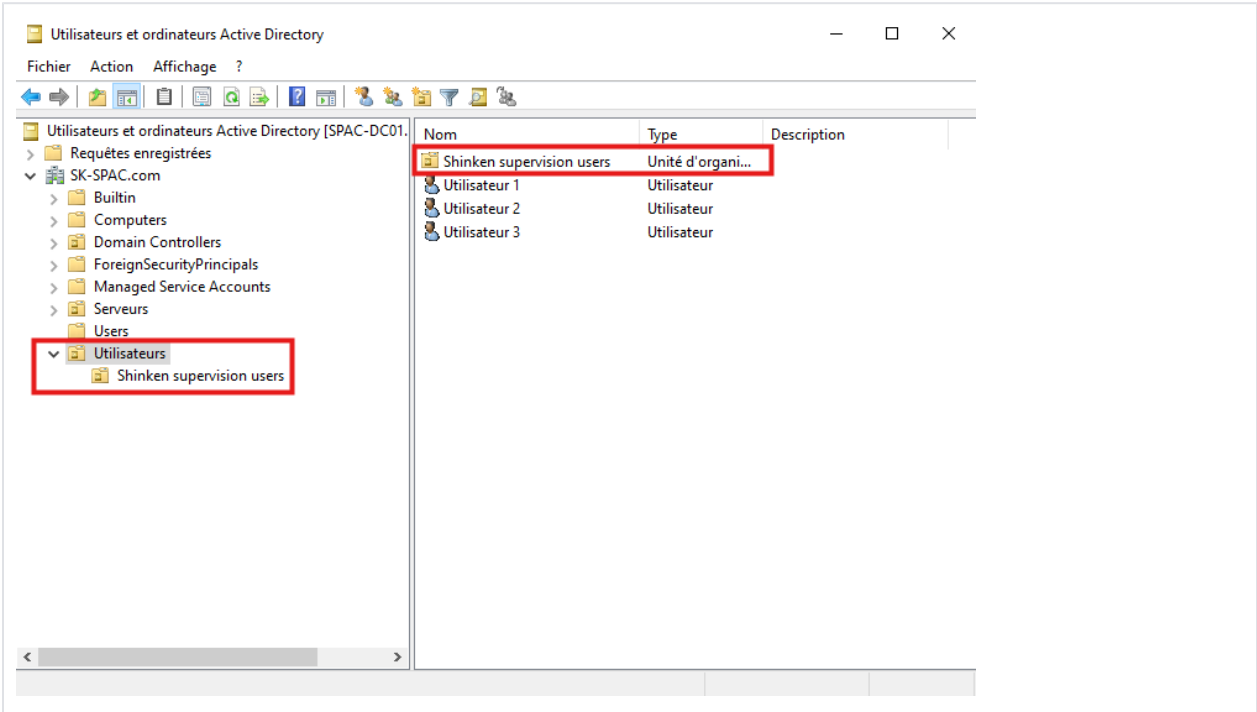
Créer ses utilisateurs de supervision Shinken

Créer une UO pour les utilisateurs

- Cliquer sur son domaine.
- Repérer dans quels dossiers sont les utilisateurs.
- Si tous les utilisateurs sont dans le dossier "**Users**", il est nécessaire de créer un nouveau dossier **UO**.
    - Le dossier "**Users**", présent par défaut, ne permet pas d'appliquer des **GPOs** ou de créer de sous-dossiers.
    - Clic-Droit sur le nom de domaine, Sélectionner "**Nouveau**" > "**Unité d'organisation**" et lui donner un nom tel que "**Utilisateurs**" :

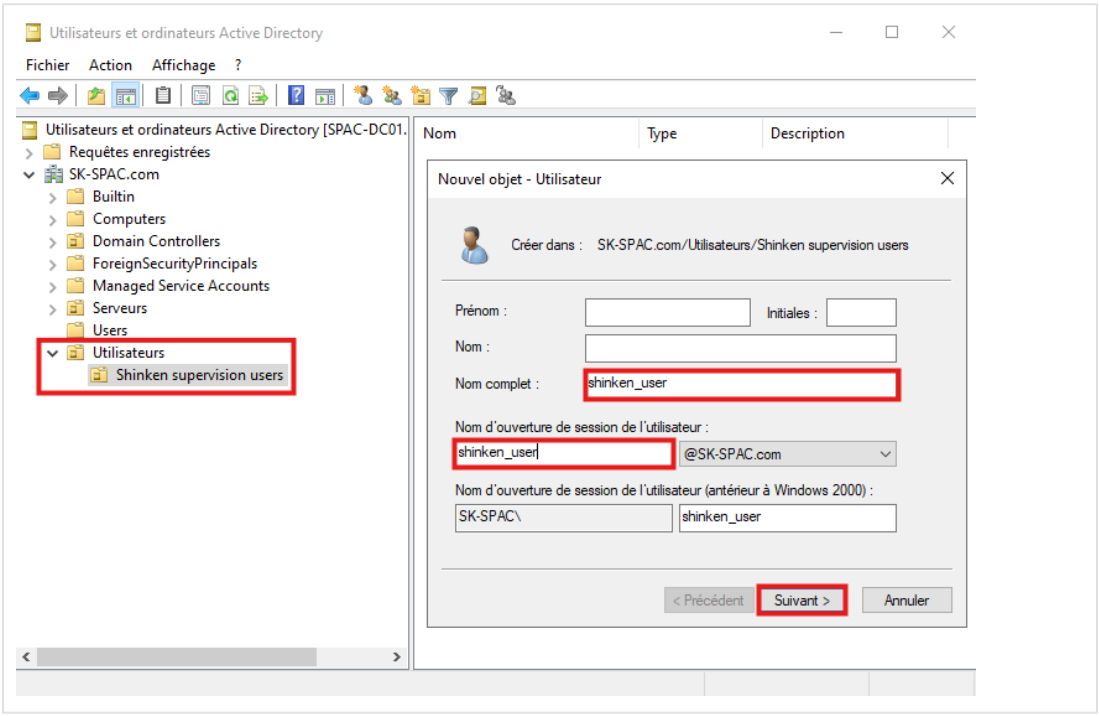


- Dans cette **UO** où sont tous les utilisateurs, créer un **UO** où seront les utilisateurs et groupes de supervision shinken, nommer là par exemple "**Shinken supervision users**".

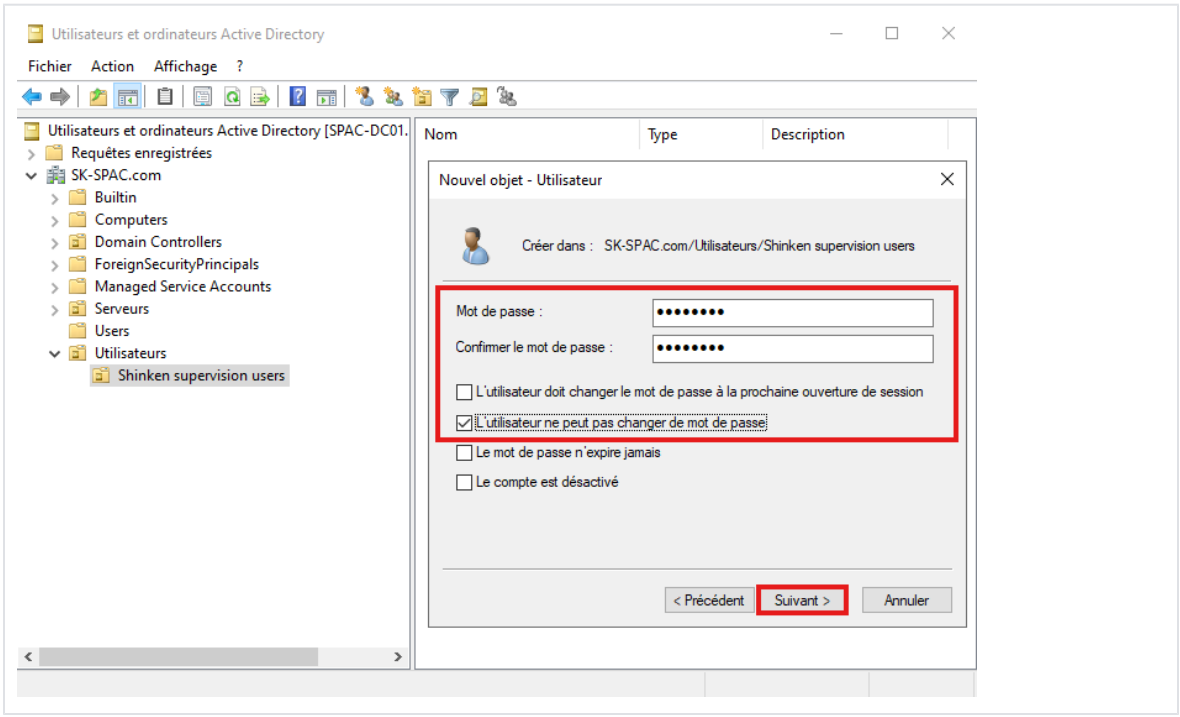


Créer un ou plusieurs utilisateurs de supervision

- Dans la nouvelle **UO** (*ex : Shinken supervision users* **)** pour utilisateurs Shinken de supervision,
  - Clic-Droit, Sélectionner "**Nouveau**" > "**Utilisateur**"
  - Remplir :
    - "Nom complet" (*ex shinken_user*) ;
    - "Nom d'ouverture de session de l'utilisateur" (*ex shinken_user*) ;



- Sur la page suivante :
  - Remplir le mot de passe ;
  - Décocher "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session" ;
  - Cocher "L'utilisateur ne peut pas changer de mot de passe" ;



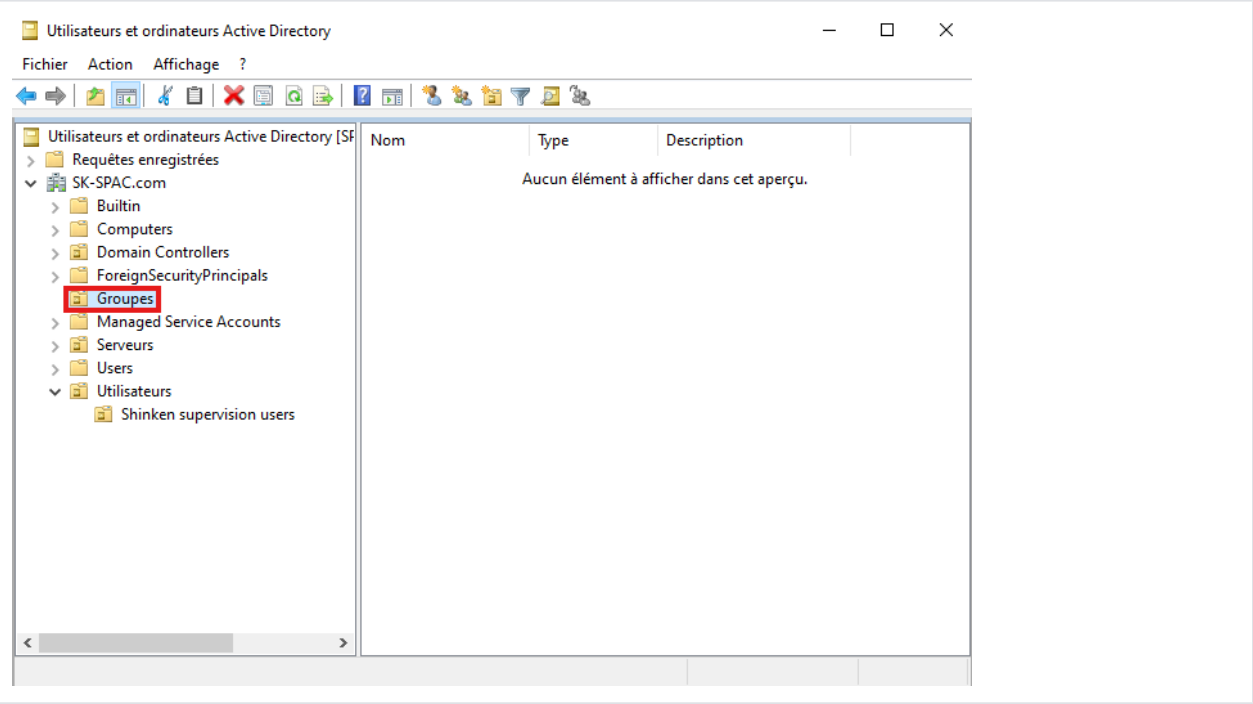
- Finaliser ensuite la création de l'utilisateur.

Créer un groupe de supervision

> La création d'un groupe de supervision permet d'appliquer tous les droits nécessaires à la supervision à un seul endroit.
>
> Par la suite, il est possible de lier un ou plusieurs utilisateurs à ce groupe. Dans le futur, cela permet de révoquer des utilisateurs, les supprimer sans se soucier de devoir refaire la configuration.

C'est une bonne pratique de créer une **UO** spécifiquement pour ranger ses groupes d'utilisateurs.

- Par exemple ici une **UO** nommé "**Groupes**".



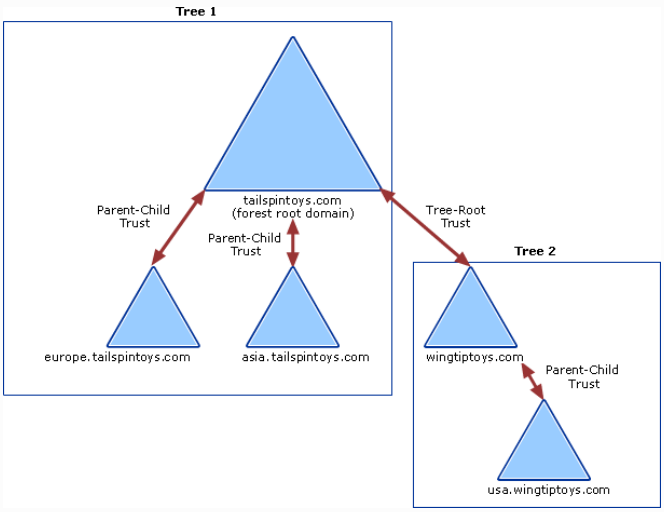
Dans cette nouvelle **UO**, Clic-Droit, Sélectionner "**Nouveau**" > "**Groupe**"

- Remplir le "**Nom de groupe**", par exemple avec "**GRP_SHINKEN**".
- Garder la propriété "**Globale**" cochée :
  - Elle permet de définir la visibilité du nouveau groupe au sein d'un ou plusieurs domaines.
  - "**Domaine locale**" limite l'utilisation du groupe au domaine actuel.
  - "**Globale**" limite l'utilisation du groupe au domaine actuel, et aux autres domaines s'ils sont **approuvés**.

Les **approbations** entre domaines sont des relations de confiance qui permettent de partager certains objets d'un domaine à un autre.

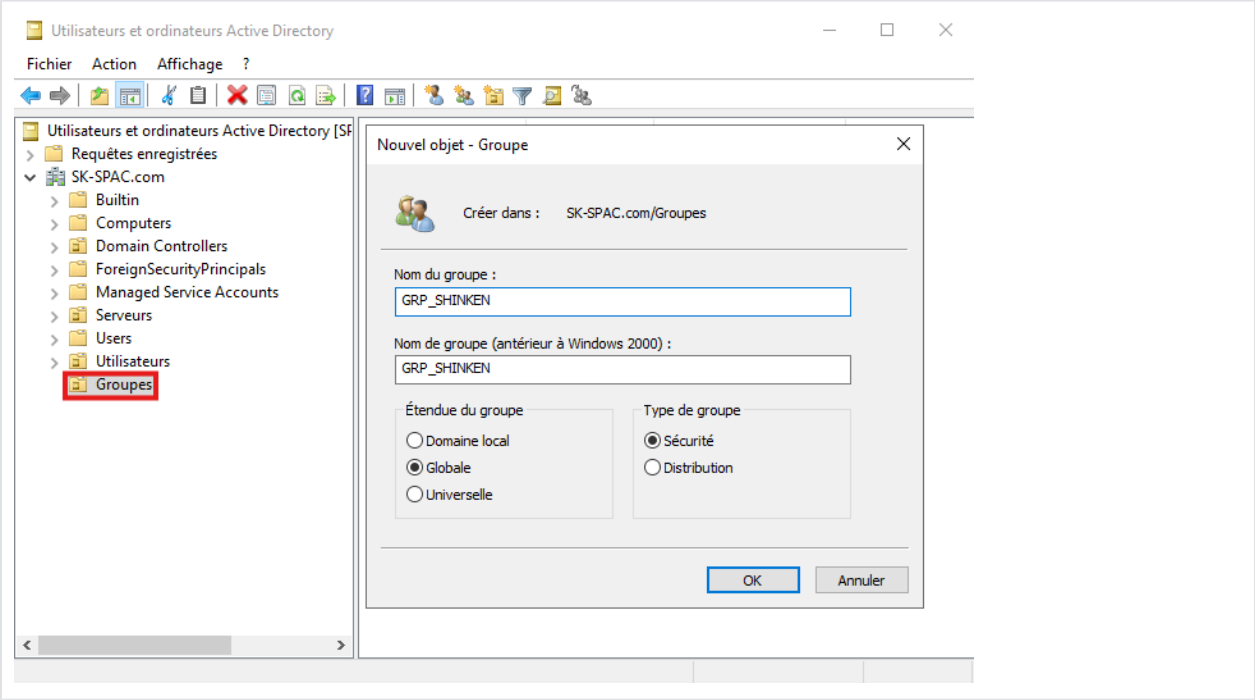
Par défaut, les sous-domaines ont automatiquement une relation de confiance (*approbation*) avec leur domaine parent.

Il est possible de créer des relations de confiances entre domaines de forêts différentes.

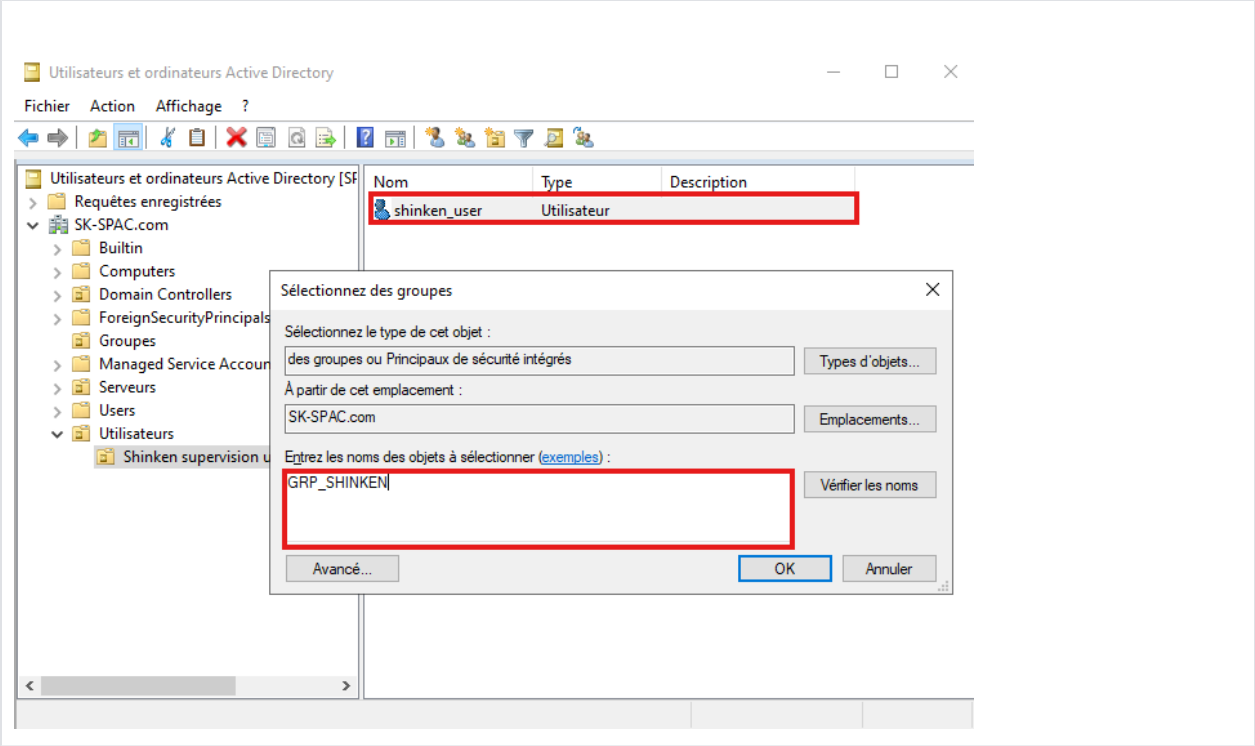


- "**Universelle**" autorise l'utilisation du groupe dans tous les domaines de la forêt.

- Garder la propriété "**Sécurité**" cochée :



- Se déplacer dans l'**UO** où sont le ou les utilisateurs de supervision shinken.
- Ensuite, pour chaque utilisateur de supervision crée, Clic-Droit puis "**Ajouter à un groupe**".
- Remplir le nom du groupe de supervision (*ex : GRP_SHINKEN*).
- Cliquer sur "Vérifier les noms" puis valider :



Configurer des permissions pour le contrôleur de domaine

La configuration du groupe pour le contrôleur de domaine se fait dans le même outil : "**Utilisateurs et ordinateurs Active Directory**" :

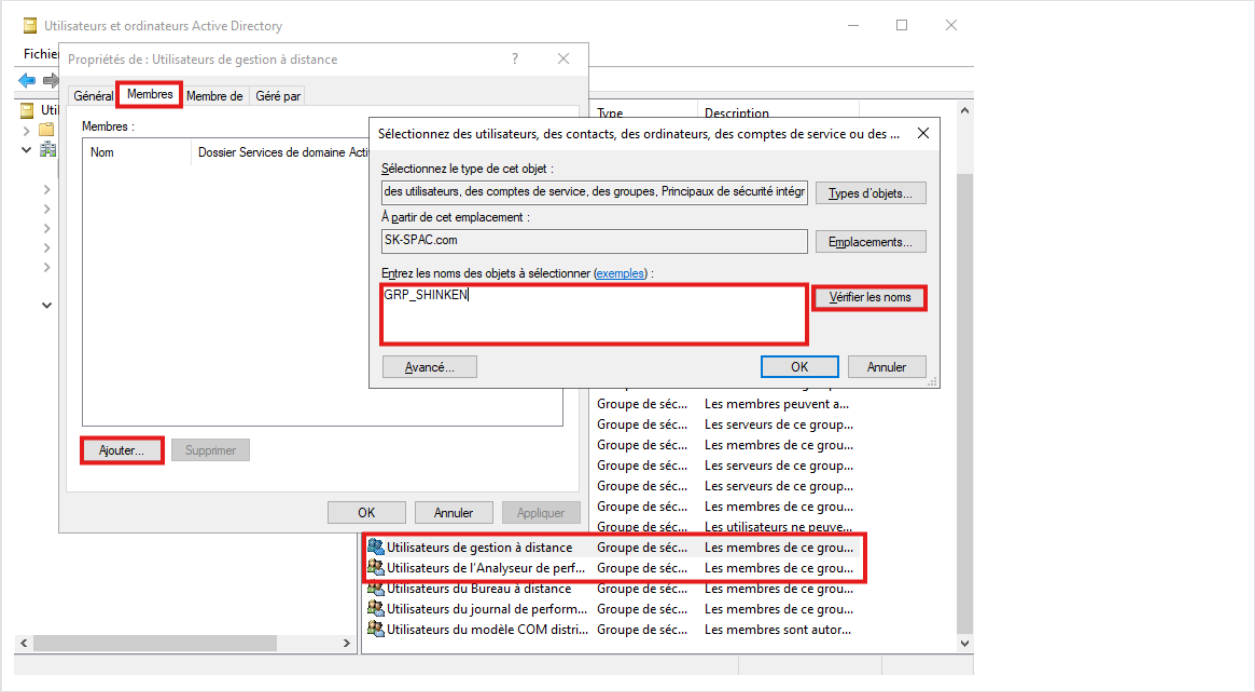
Il faut ajouter le groupe de supervision shinken (*ex : GRP_SHINKEN*) dans les deux groupes suivants :

- `Utilisateur de gestion à distance`
- `Utilisateur de l'Analyseur de performance`

En anglais, les groupes se nomment :

- `Remote Management Users`
- `Performance Monitor Users`

- Dans l'arborescence de votre domaine, sélectionner "**Builtin**".
- Clic-Droit sur le groupe "**Utilisateur de gestion à distance**", puis "**Propriétés**".
- Dans l'onglet "**Membres**", Cliquer sur "**Ajouter...**".
- Remplir le nom du groupe de supervision shinken (*GRP_SHINKEN*) et valider.
- Répéter l'opération pour le groupe "**Utilisateur de l'Analyseur de performance**".



Configuration d'une GPO

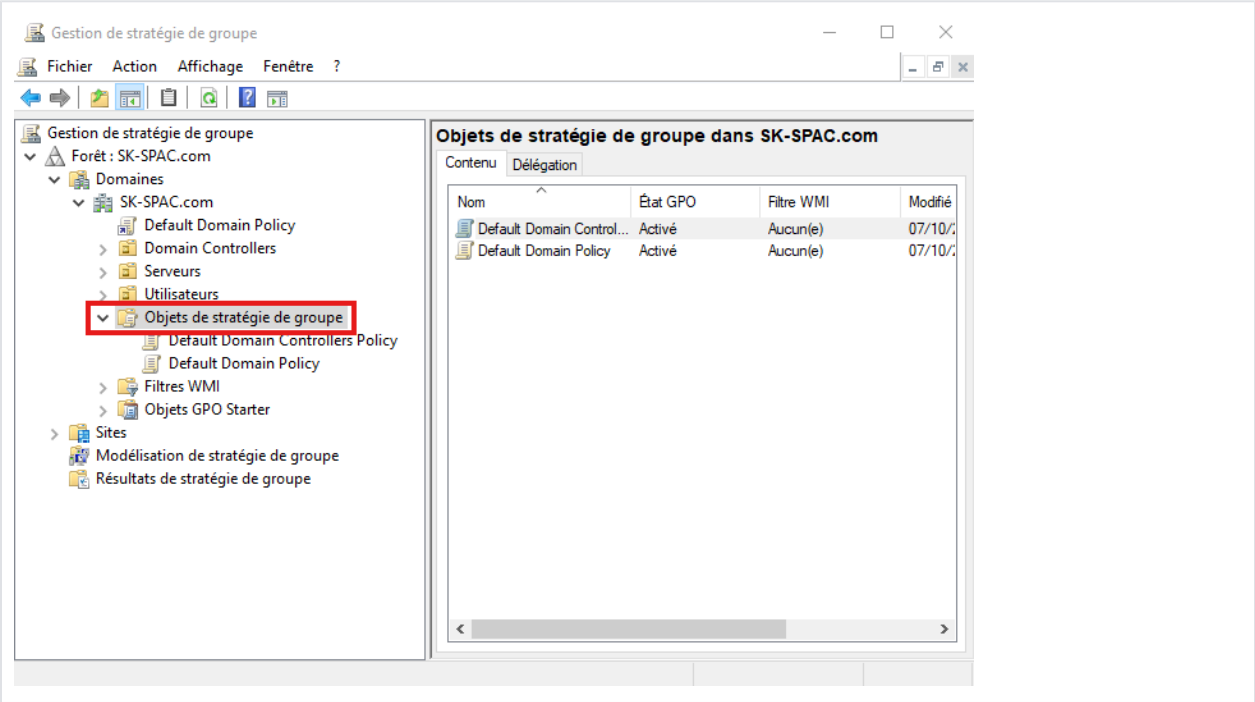
La seconde étape est de créer une GPO (*Global Policy Object*), l'appliquer aux serveurs windows à superviser puis la configuer.

- Ouvrir "**Gestion de stratégie de groupe**" (*gpmc.msc*).

Créer une GPO

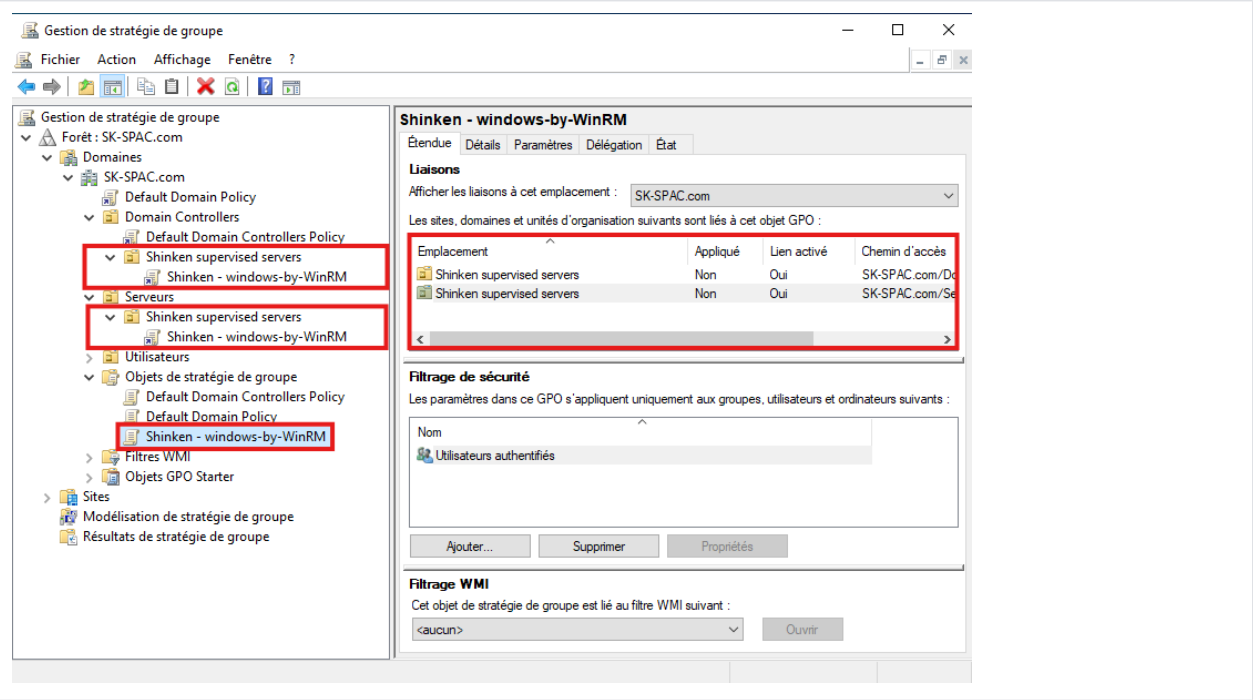
- Dans l'arborescence, Clic-Gauche sur votre "**Forêt: DOMAINE**" > "**Domaines**" > "**DOMAINE**" > "**Objets de stratégie de groupe**"

> "**DOMAINE**" ici sera le nom personnalisé de votre domaine. Dans l'exemple plus bas, le domaine est "SK-SPAC.com"



- Clic-Droit sur "**Objets de stratégie de groupe**" > "**Nouveau**" puis nommer la nouvelle **GPO** avec, par exemple, "**Shinken - windows-by-WinRM**".
- Une fois crée, Glisser-Déposer votre **GPO** dans les **UOs** de vos serveurs à superviser précédemment créés.
  - Dans le UO du Domain Controllers créé (*ex: Shinken supervised servers*) ;
  - Dans le UO des Serveurs créé (*ex: Shinken supervised servers*) ;

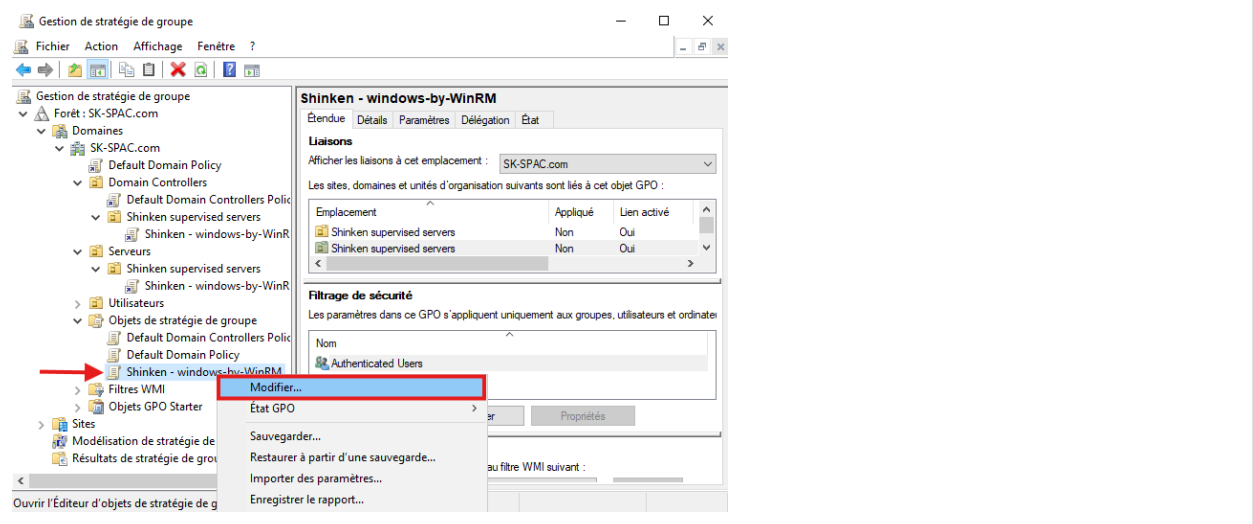
- La liste des liaisons s'affiche à droite de la fenêtre lorsque la **GPO** est sélectionnée.



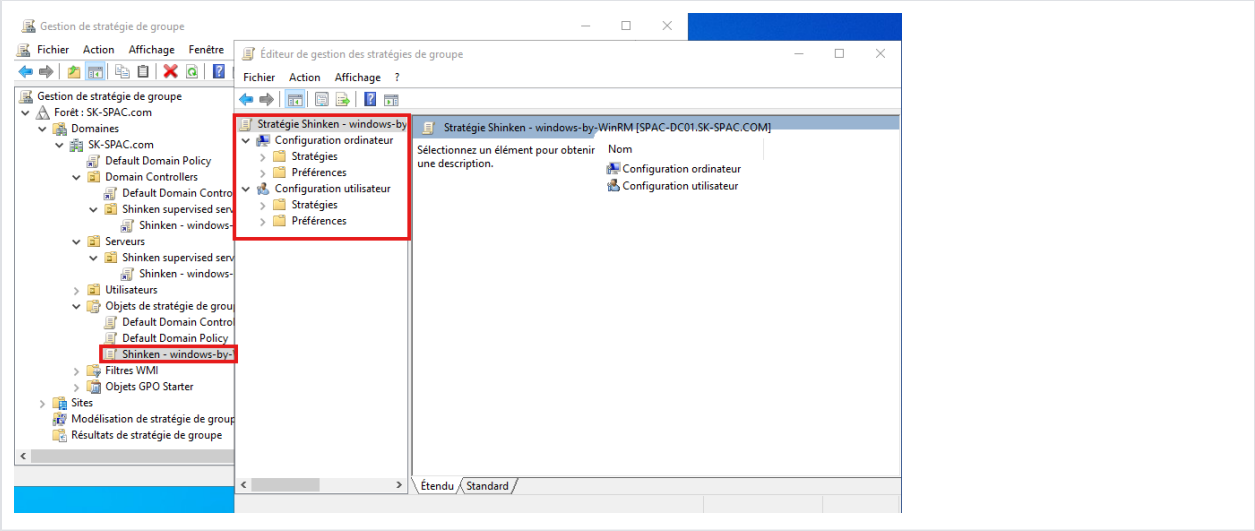
Configuration de la GPO

Une fois créé et lié aux Windows à superviser, il faut configurer la **GPO**, c'est-à-dire lui accrocher des règles qui modifieront la configuration des ordinateurs liés.

- Clic-Droit sur la nouvelle **GPO** (*ex : Shinken - windows-by-WinRM*), puis "Modifier".



- Les règles à appliquer se trouvent dans cette arborescente de configuration.

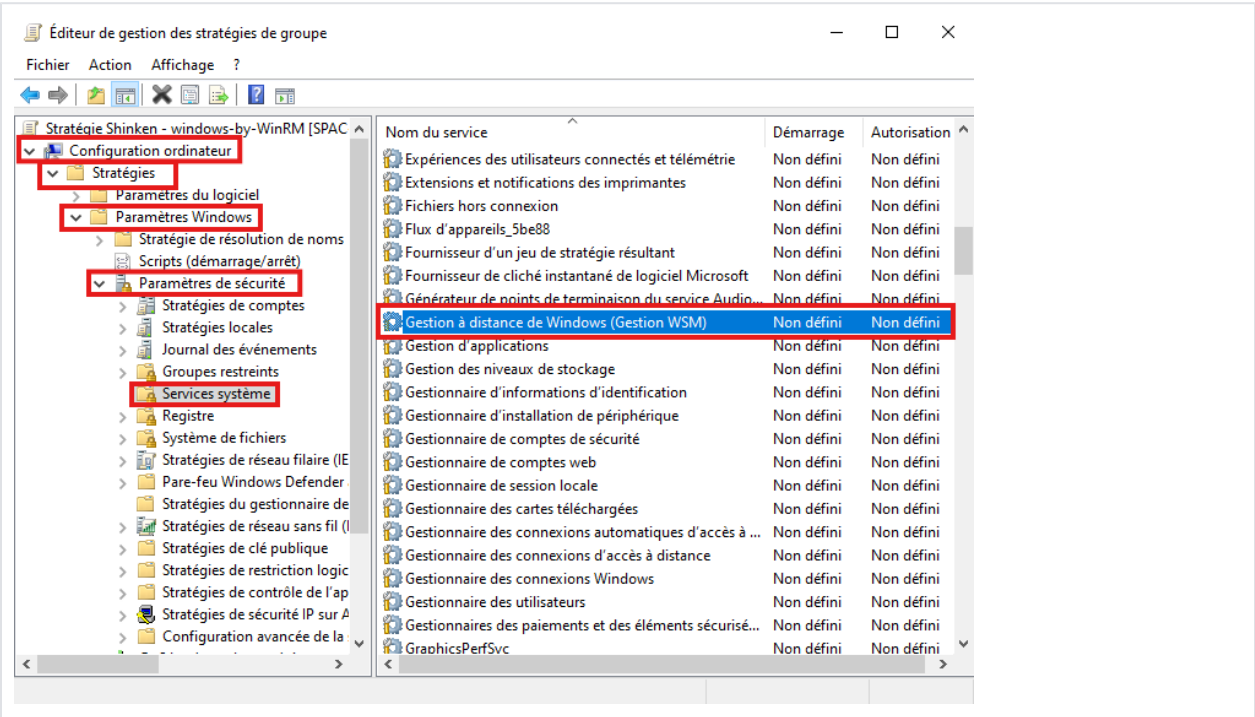


Configuration de WSM

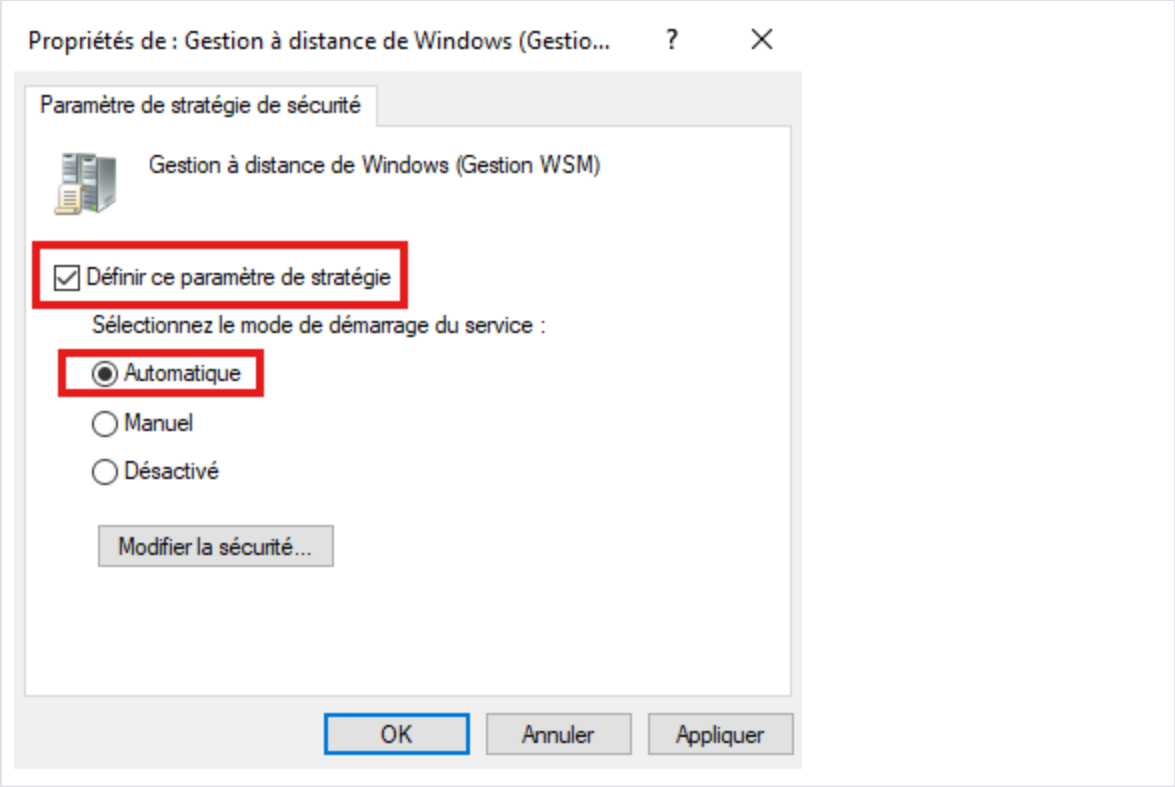
Activation la gestion à distance WSM (*WS-Management*) est essentiel pour la connexion à distance et la collecte d'information pour **WinRM**.

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Services système**" > "**Gestion à distance Windows (Gestion WSM)**"

> En anglais, le service se nomme :
>
> - `Windows Remote Management (WS-Management)`



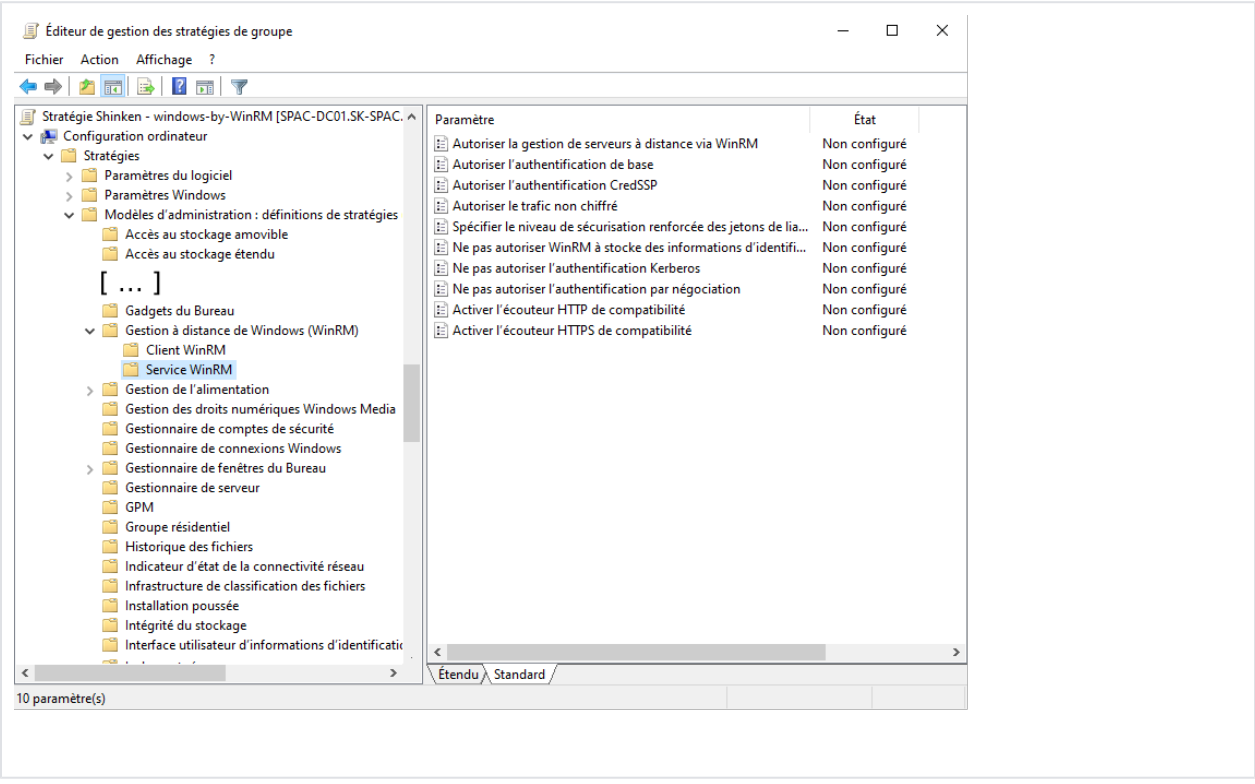
- Double-Clic => Une nouvelle fenêtre s'ouvre.
  - Cocher "**Définir ce paramètre de stratégie**" ;
  - Cocher "**Automatique**" ;



Configuration de WinRM

Il faudra aussi activer le démarrage automatique de **WinRM** et configurer le mode d'authentification.

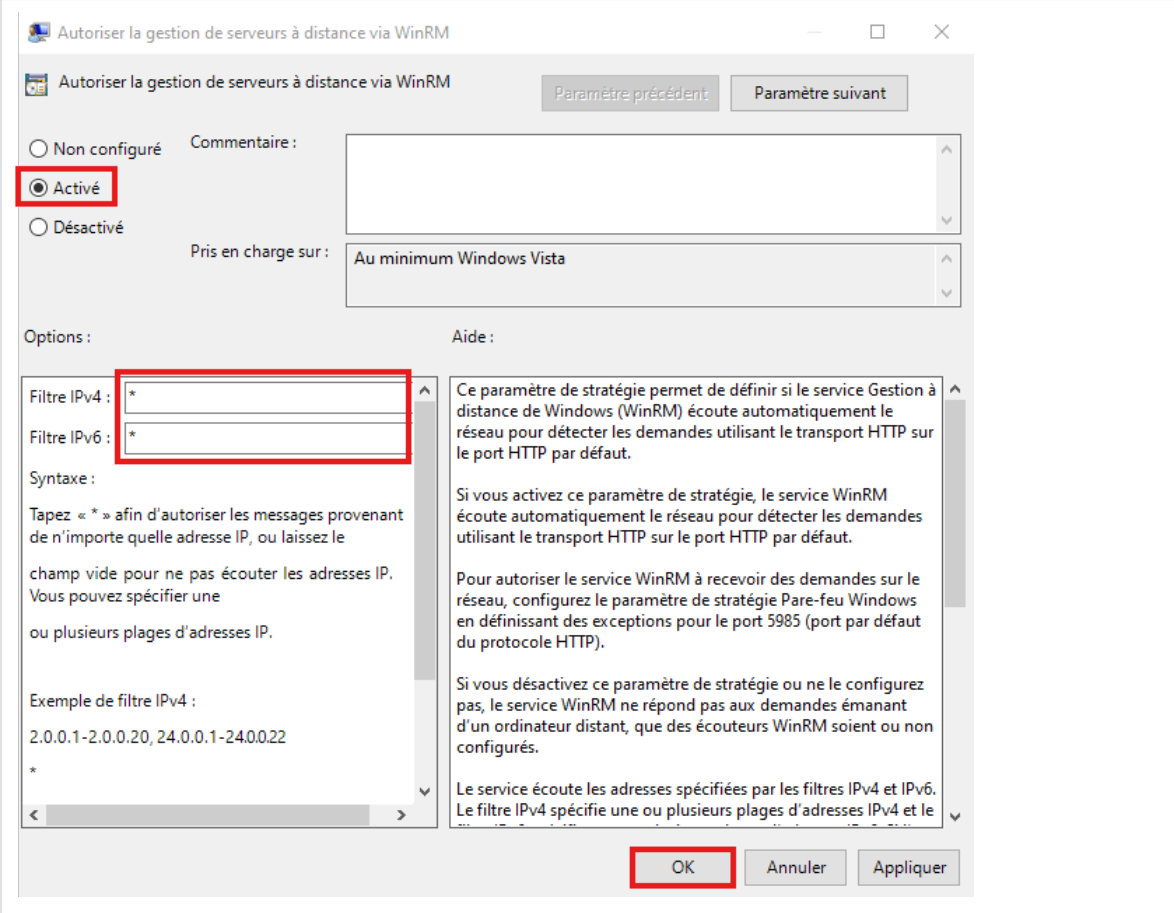
- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Modèle d'administration : définition de stratégies**" > "**Composants Windows**" > "**Gestion à distance Windows (WinRM)**" > "**Service WinRM**"



- Double-Clic sur "**Autoriser la gestion de serveurs à distance via WinRM**", une nouvelle fenêtre s'ouvre :
  - Cocher "Activer" ;
  - Remplir la zone "**Filtre IPv4**" avec : ***** ;
  - Remplir la zone "**Filtre IPv6**" avec : ***** ;

> ⚠ Attention, il est impératif de remplir ces zones de "**Filtres IP**".
>
> Sans cela, le **service WinRM** n'écoutera sur AUCUNE interface réseau et ne **RÉPONDRA PAS**.

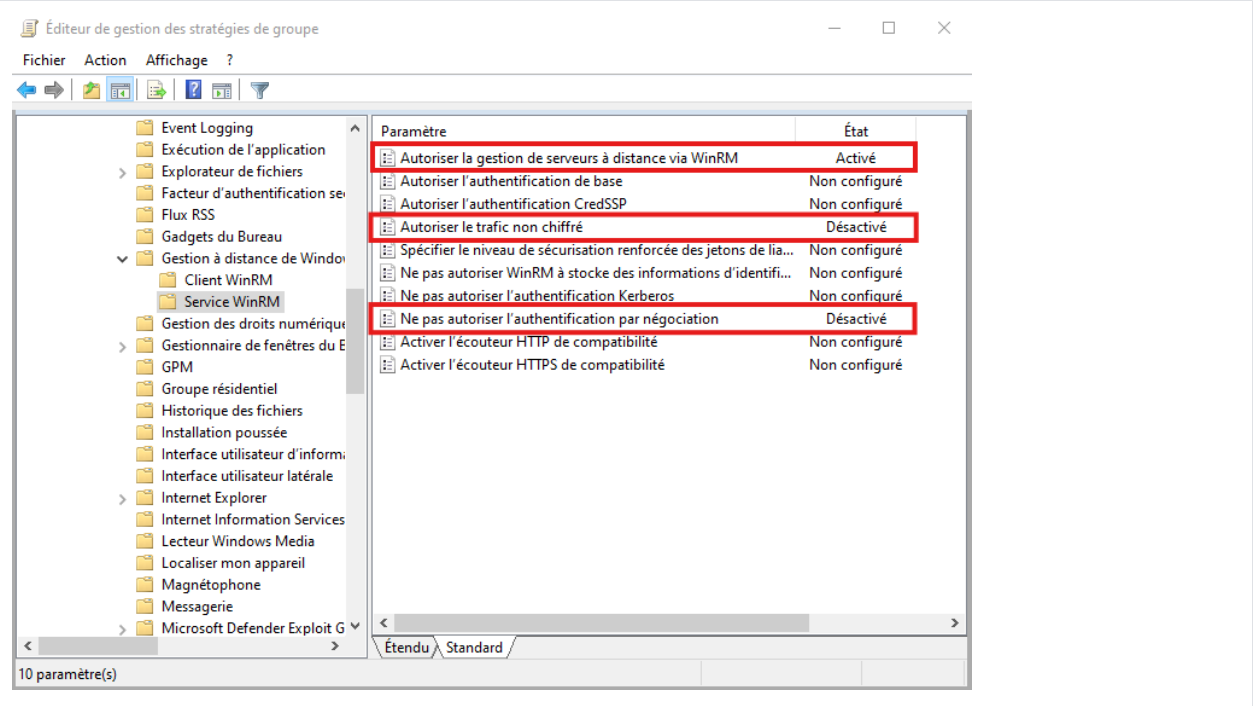
> ⓘ Une fois votre configuration terminée et la sonde fonctionnelle, vous pourrez changer ce masque réseau afin de limiter l'accès à WinRM selon l'IP.
>
> Exemples de filtre : "192.168.1.1-192.168.1.255"

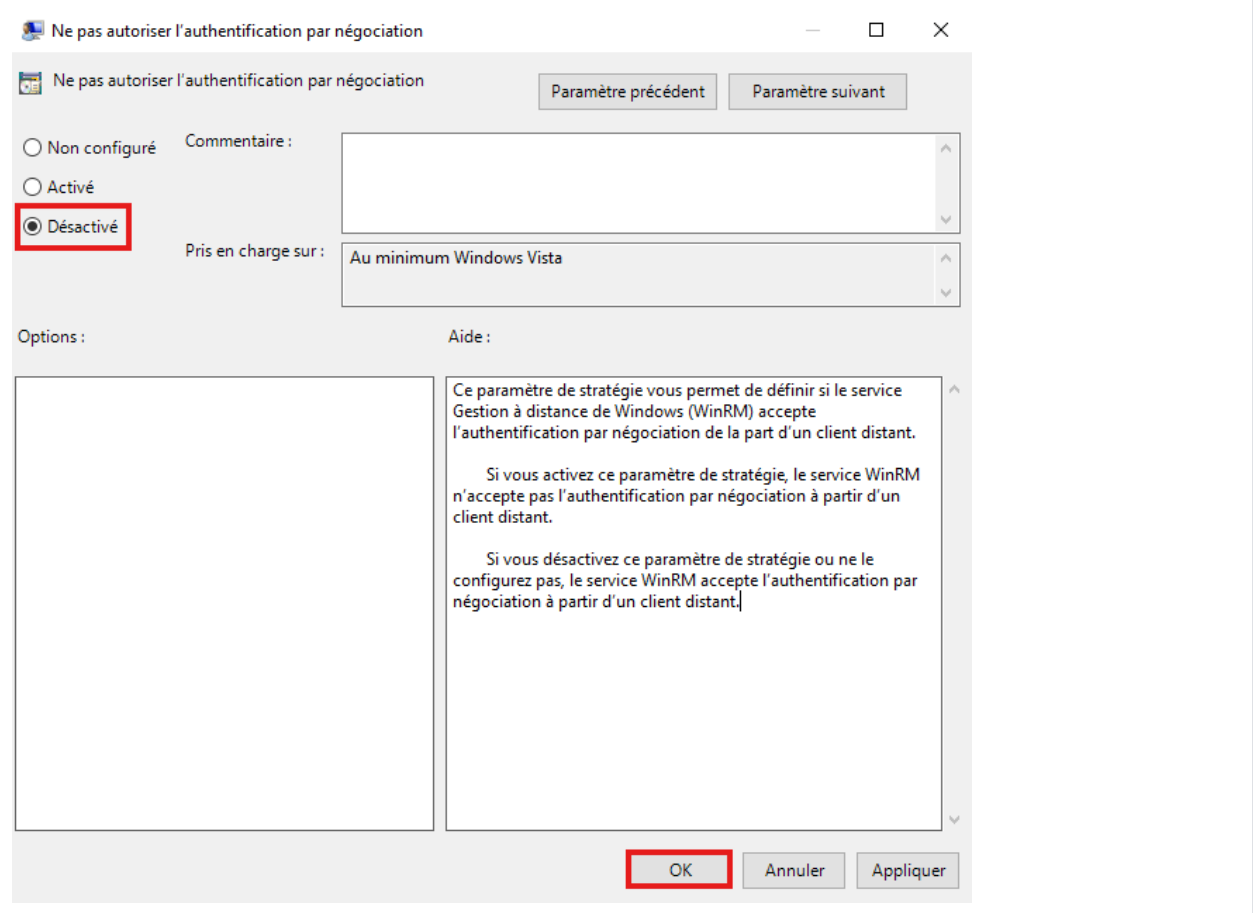


Configurer l'authentification NTLM

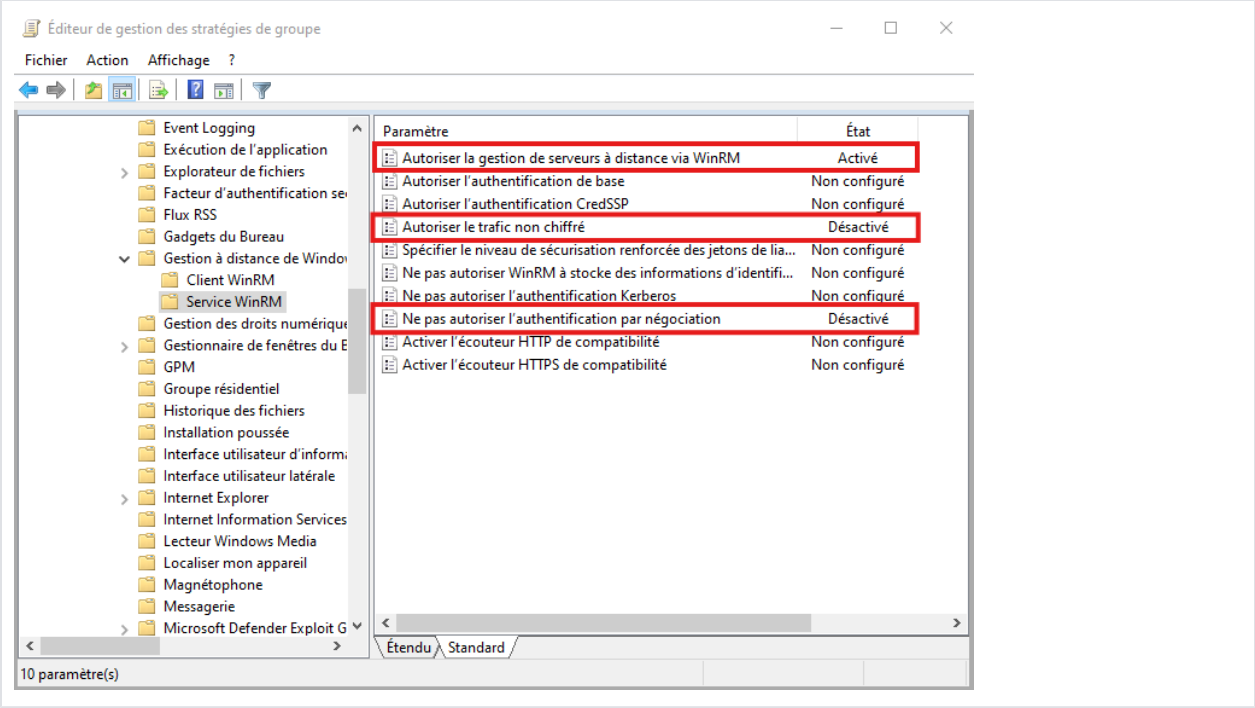
Pour activer l'authentification par NTLM, il faut désactiver l'interdiction l'authentification par négociation.

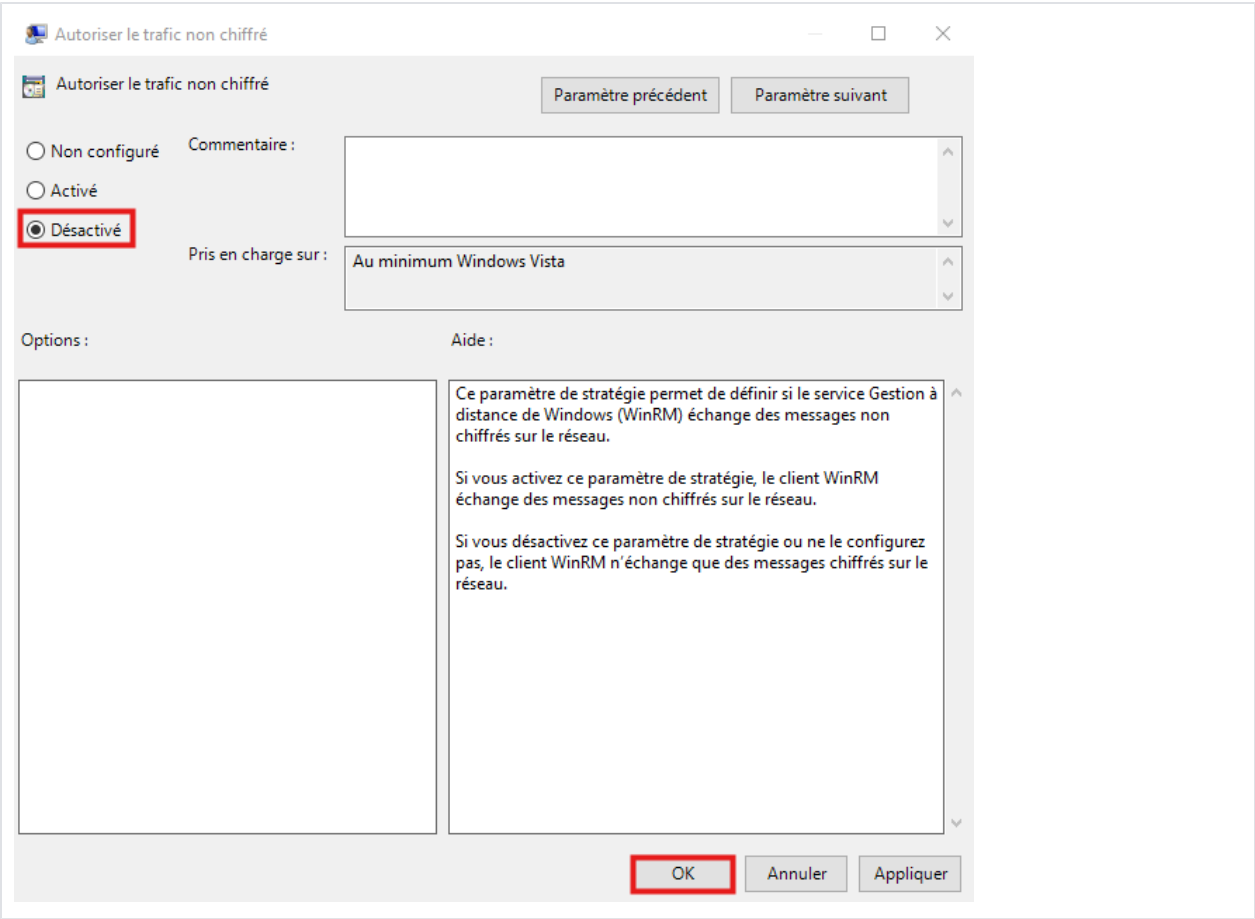
- Double-Clic sur "**Ne pas autoriser l'authentification par négociation**", une nouvelle fenêtre s'ouvre.
- Cocher "**Désactivé**", puis valider.



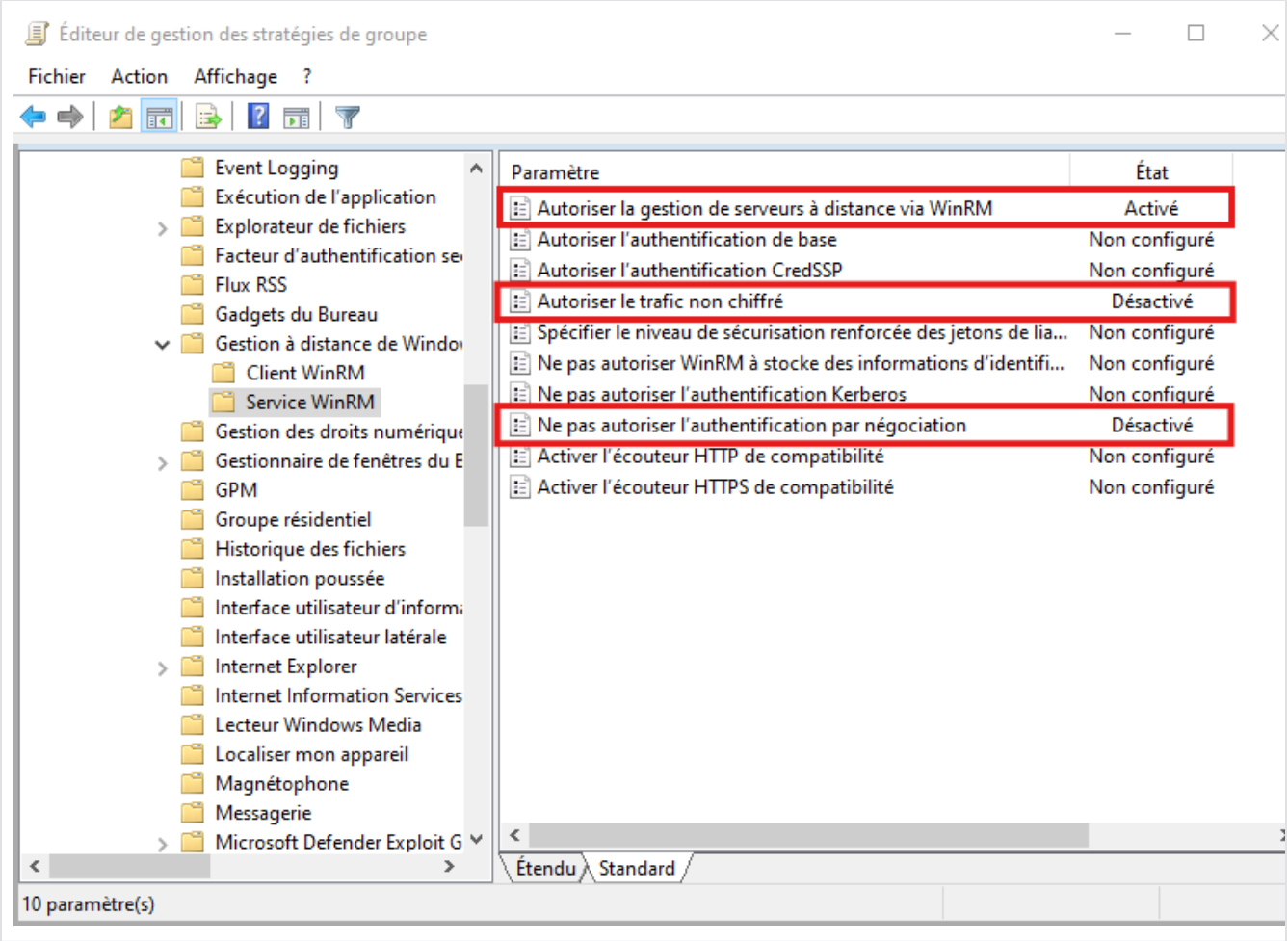


- Double-Clic sur "**Autoriser le trafic non chiffré**", une nouvelle fenêtre s'ouvre.
- Cocher "**Désactivé**", puis valider.





Résumé de la configuration NTLM :



Configurer l'authentification Basic

Il est déconseillé d'utiliser l'authentification **Basic** pour des raisons de sécurités ; cette dernière n'utilise **aucun chiffrement**.
Aucune documentation de configuration ne vous est proposée en raison.

Configuration des groupes locaux

Afin de compléter la configuration d'accès à distance, et l'accès aux ressources (*notamment nécessaire pour le check* ***Uptime by WinRM***),

- il est nécessaire de configurer la GPO pour qu'elle ajoute le groupe de supervision aux **groupes locaux** suivants, présent sur chaque machine :

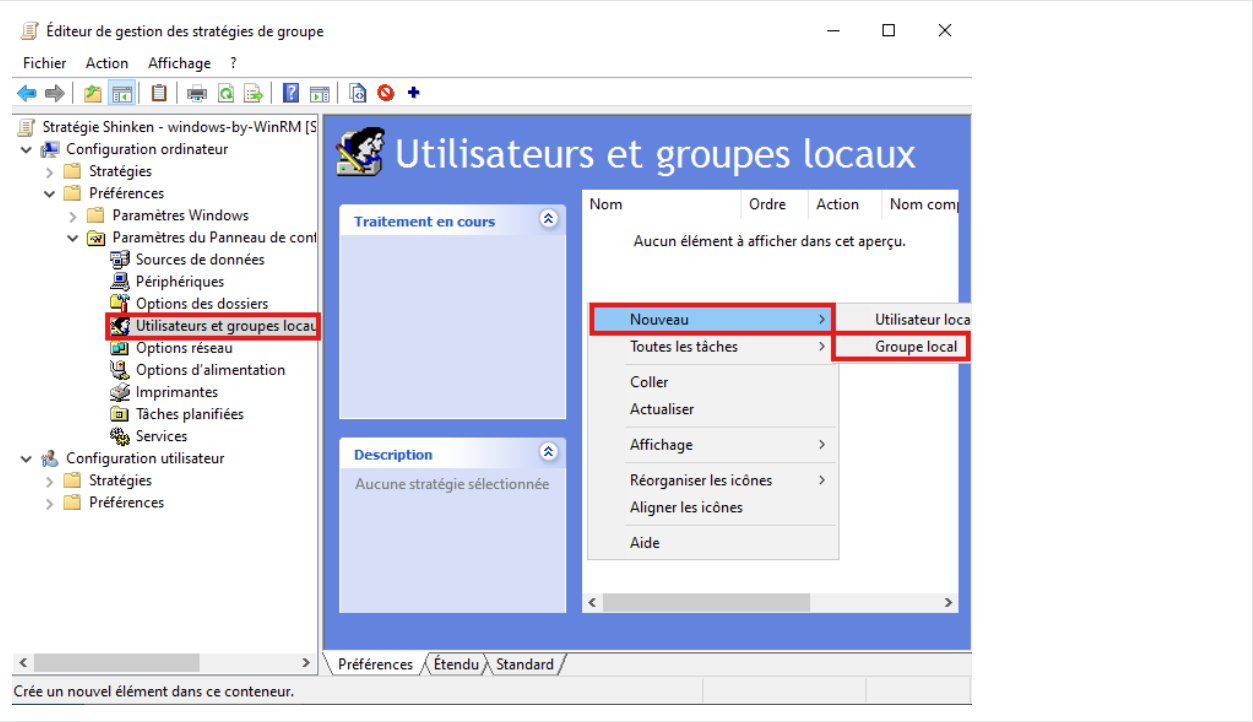
- **Utilisateurs de gestion à distance**
- **Utilisateurs de l'Analyseur de performances**
- **Lecteurs des journaux d'événements**

En anglais, les groupes se nomment :

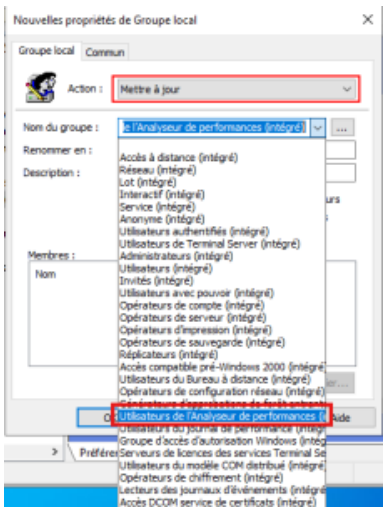
- **Remote Management Users**
- **Performance Monitor Users**
- **Event Log Readers**

Pour cela :

- Dans l'arborescence : "**Configuration ordinateur**" > "**Préférences**" > "**Paramètres du Panneau de configuration**" > "**Utilisateurs et groupes locaux**"
- Clic-Droit, "**Nouveau**" > "**Groupe local**". Une nouvelle fenêtre s'ouvre.

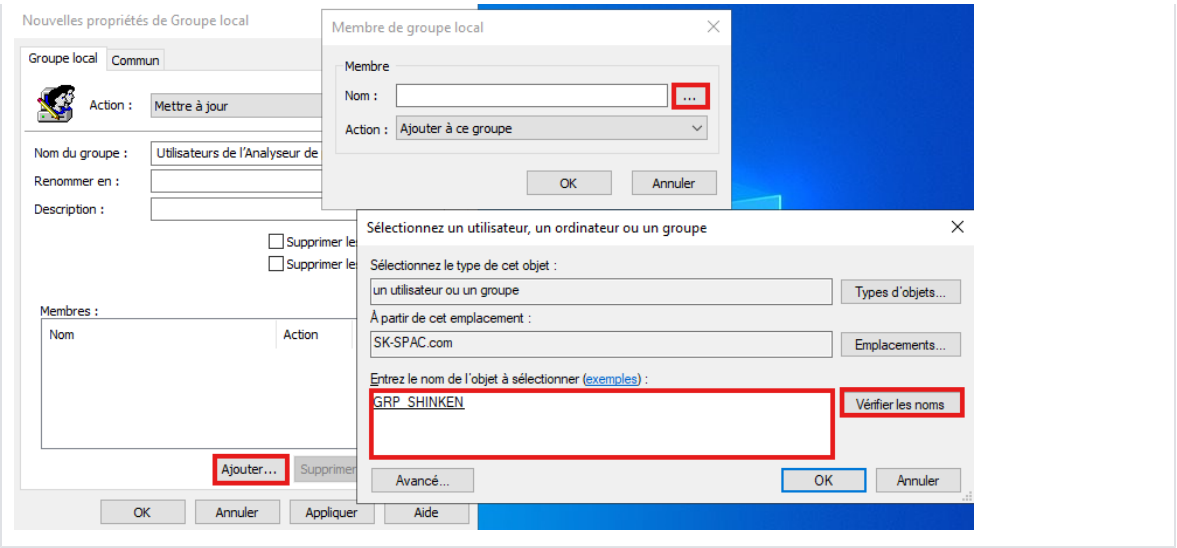


  - Sélectionner "**Mettre à jour**" pour la propriété "**Action**",
  - Cliquer dans la zone "Nom du groupe", et sélectionner "**Utilisateurs de l'Analyseur de performance (intégré)**" dans la liste.



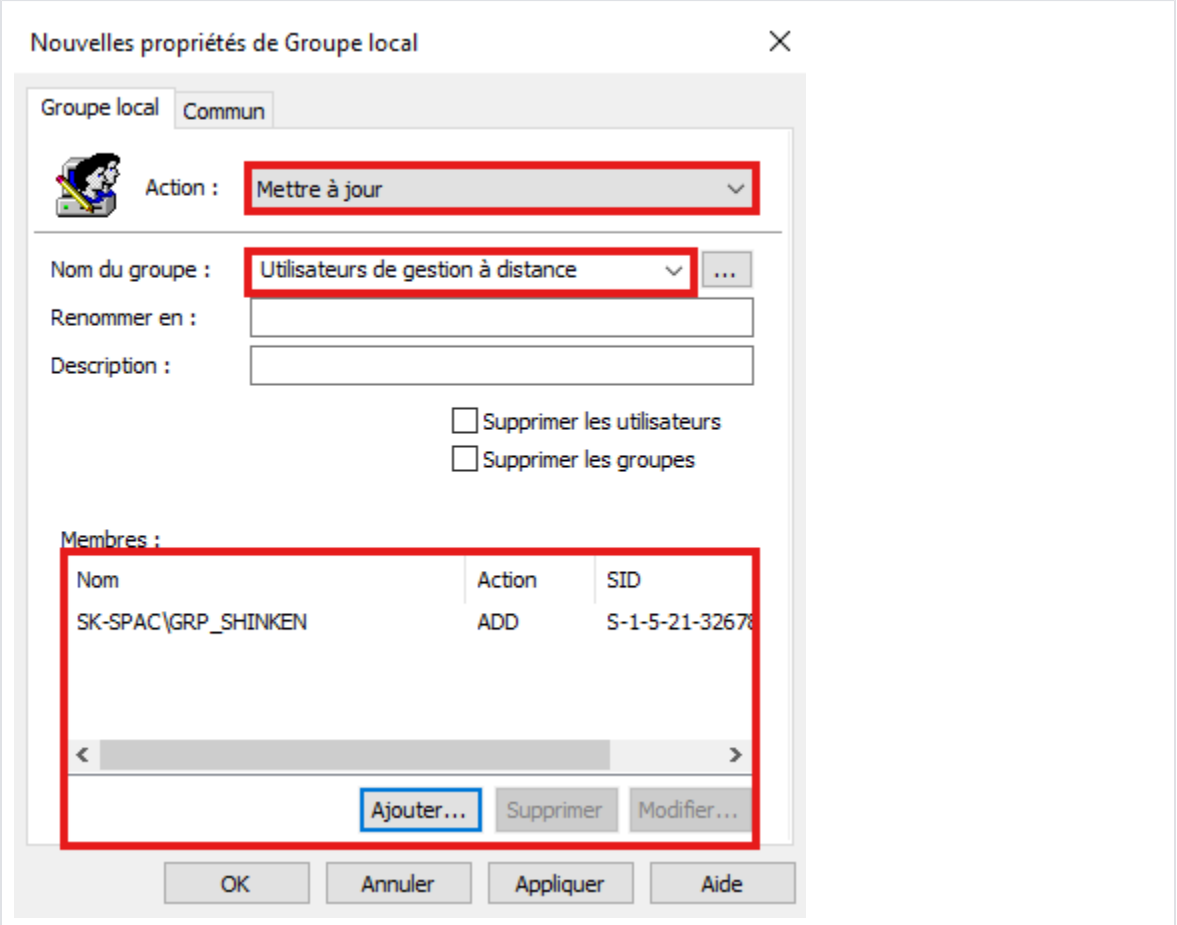
> Attention, il faut sélectionner, le groupe depuis la liste.
> Remplir le nom du groupe à la main ne fonctionnera pas.

  - Cliquer sur "**Ajouter**", puis dans la nouvelle fenêtre la case "**...**" après la zone "**Nom**"
  - Remplir le nom du groupe de supervision puis valider.

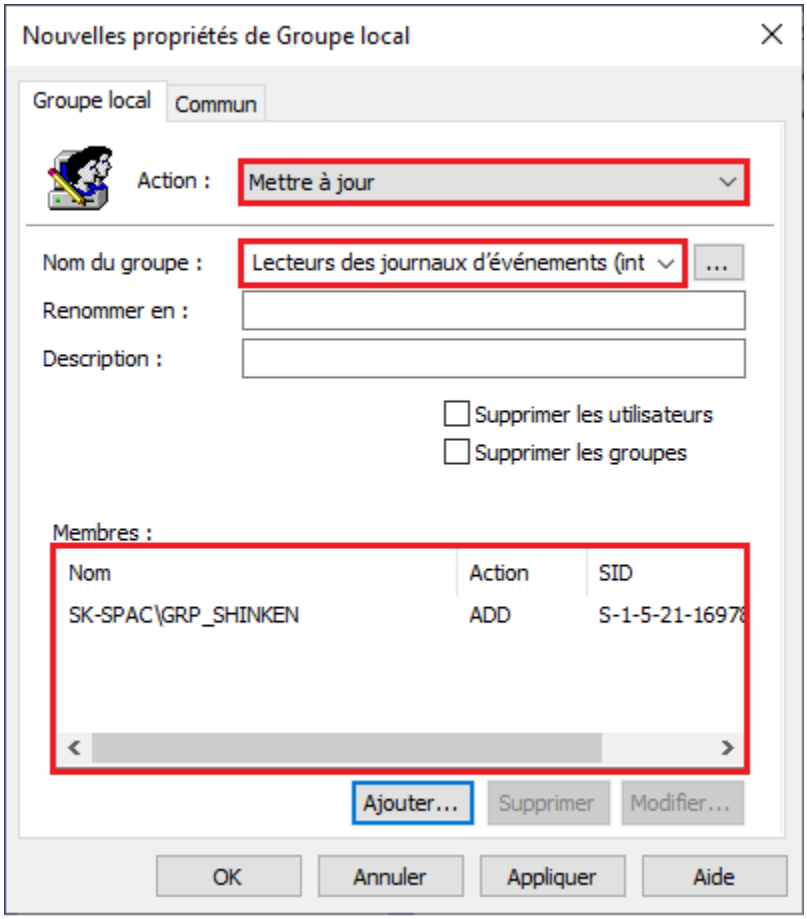


- Répéter l'opération pour le groupe "**Utilisateurs de gestion à distance"**

> "**Utilisateurs de gestion à distance"** ne figure pas dans la liste des groupes "intégrés". Il est nécessaire de l'ajouter à la main.
>
> Si parmi vos serveurs Windows à superviser, certains sont en configurés **Français** tandis que d'autres en **Anglais**, alors **r épéter l'opération deux fois** pour la version francaise et anglaise :
>
> - **Utilisateur de gestion à distance**
> - **Remote Management Users**



- Répéter l'opération pour le groupe "**Lecteurs des journaux d'événements (intégré)"**

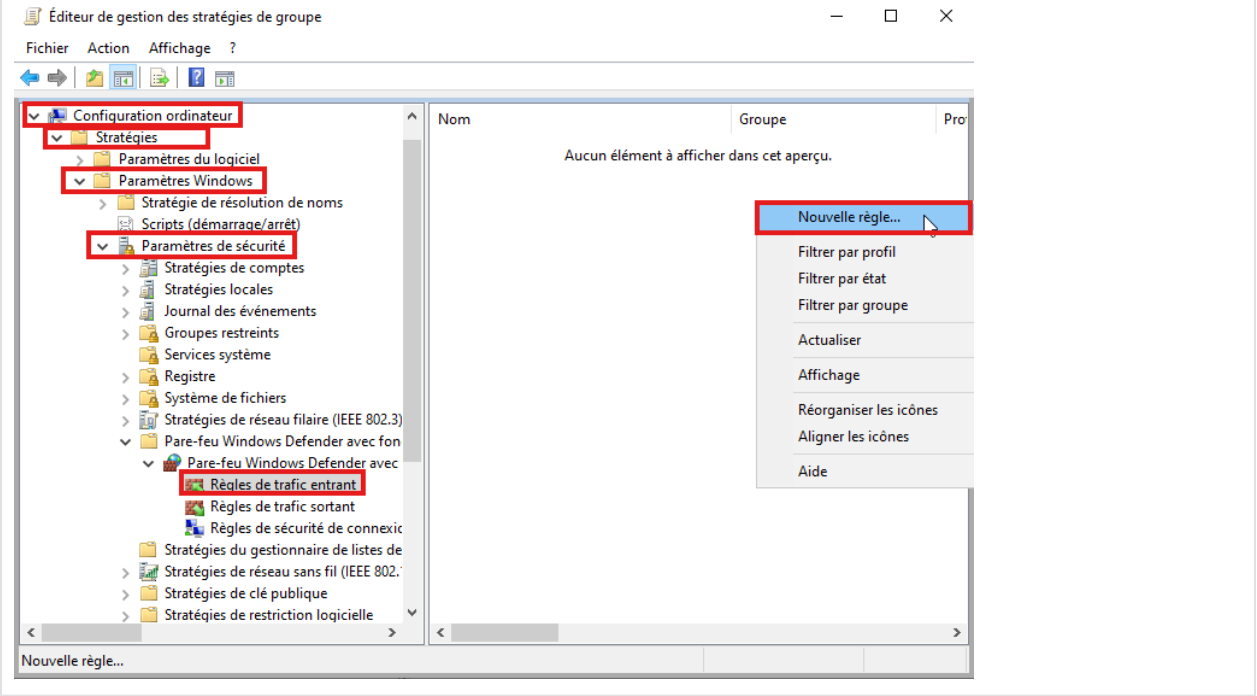


> ⚠ Vérifier que le groupe shinken ajouté (*ici GRP_SHINKEN*)a bien un **SID** correspondant (*ici S-1-5-21-3267...*).
> S'il n'en a pas, le groupe n'est alors pas détecté. Pour corriger cela, répéter les étapes précédentes, et s'assurer d'ajouter le groupe via "**Ajouter**" puis le bouton "**...**".

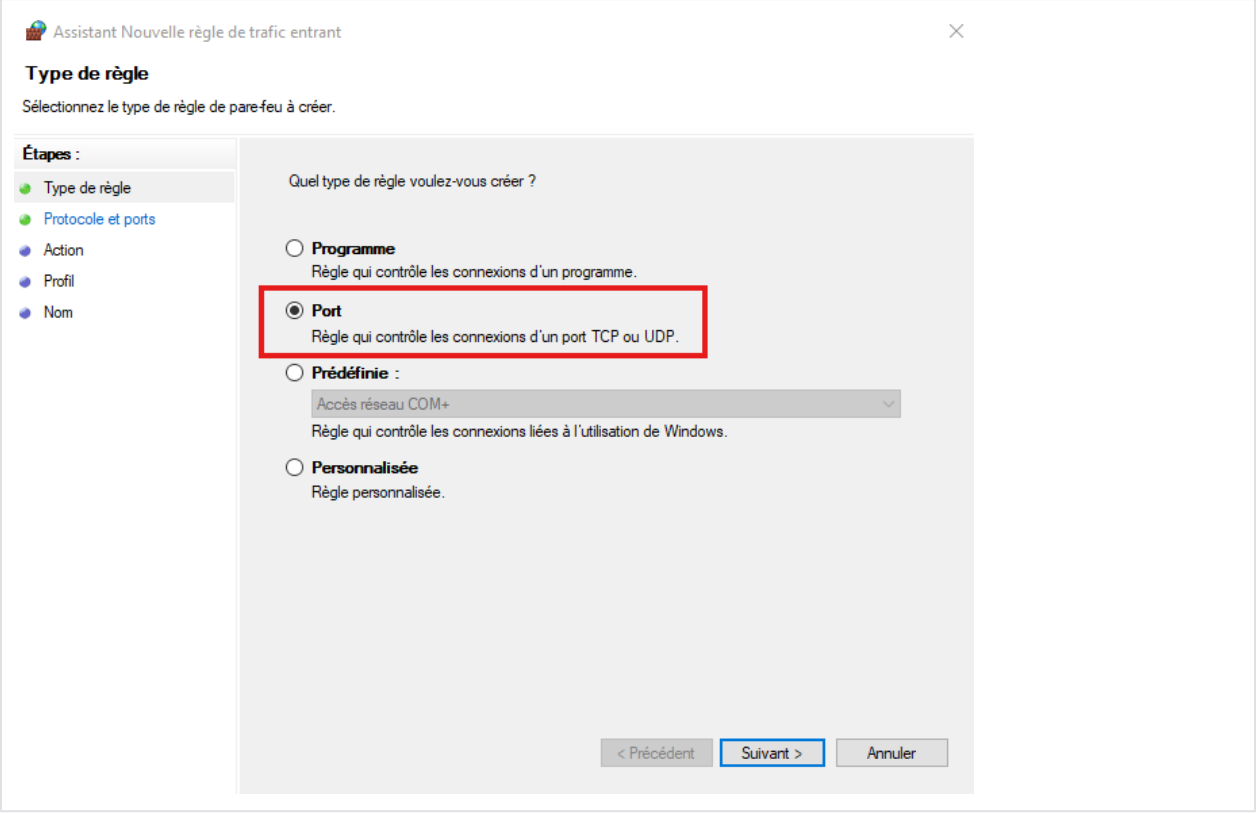
Configuration du Pare-Feu

Dans cette section, il faudra ajouter au Pare-Feu une règle pour autoriser le trafic **WinRM**.

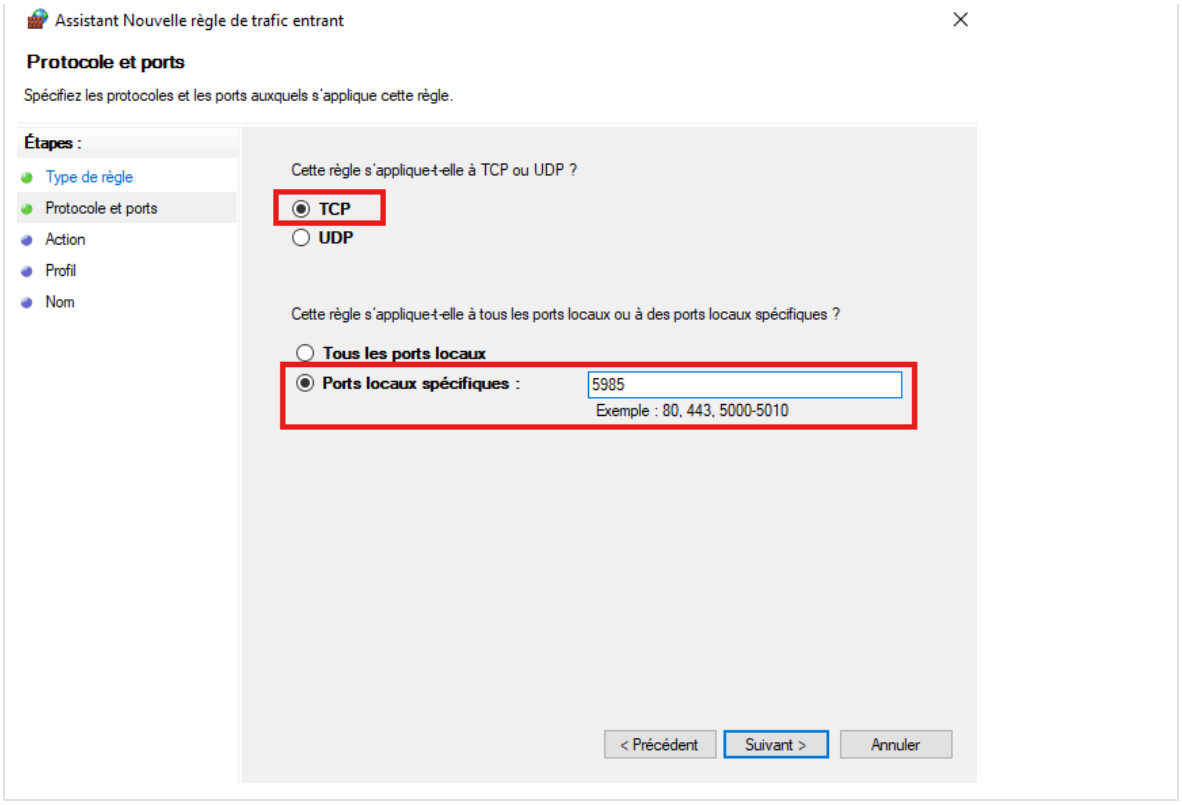
- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Pare-feu Windows Defender avec fonctions avancées de sécurité**" > "**Règles de trafic entrant**"
- Clic-Droit, "Nouvelle Règle", une nouvelle fenêtre s'ouvre :



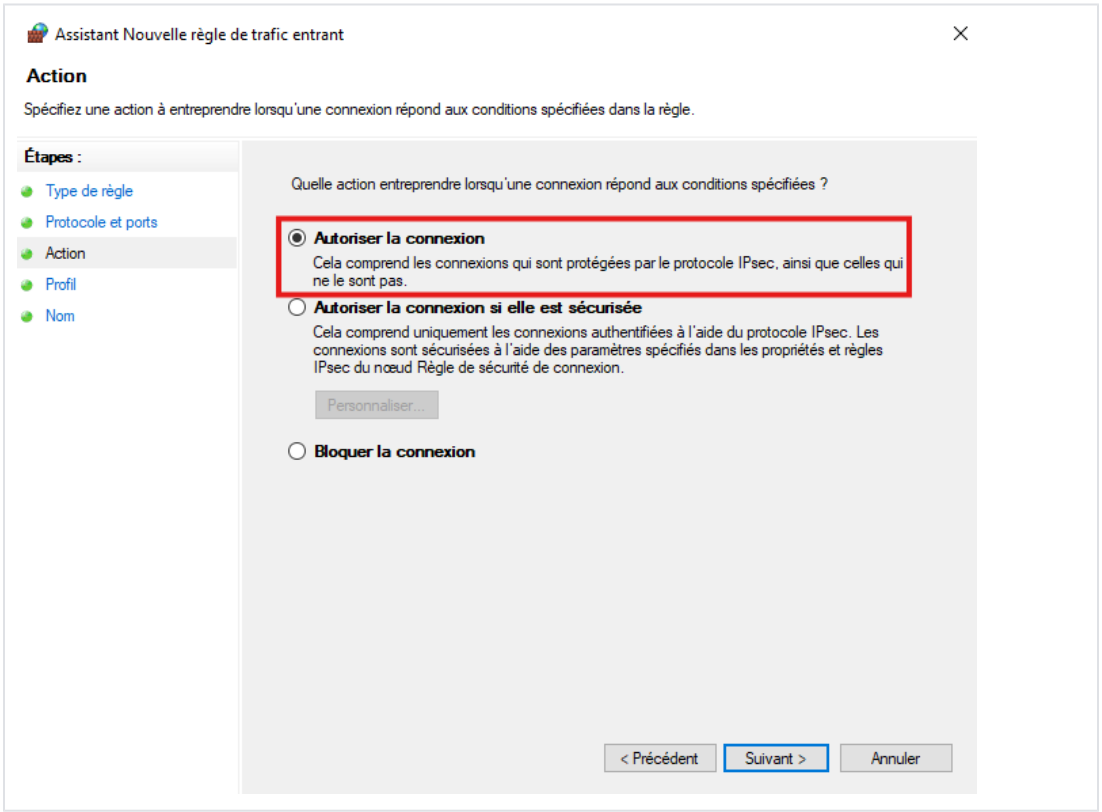
- Cocher "**Port**"



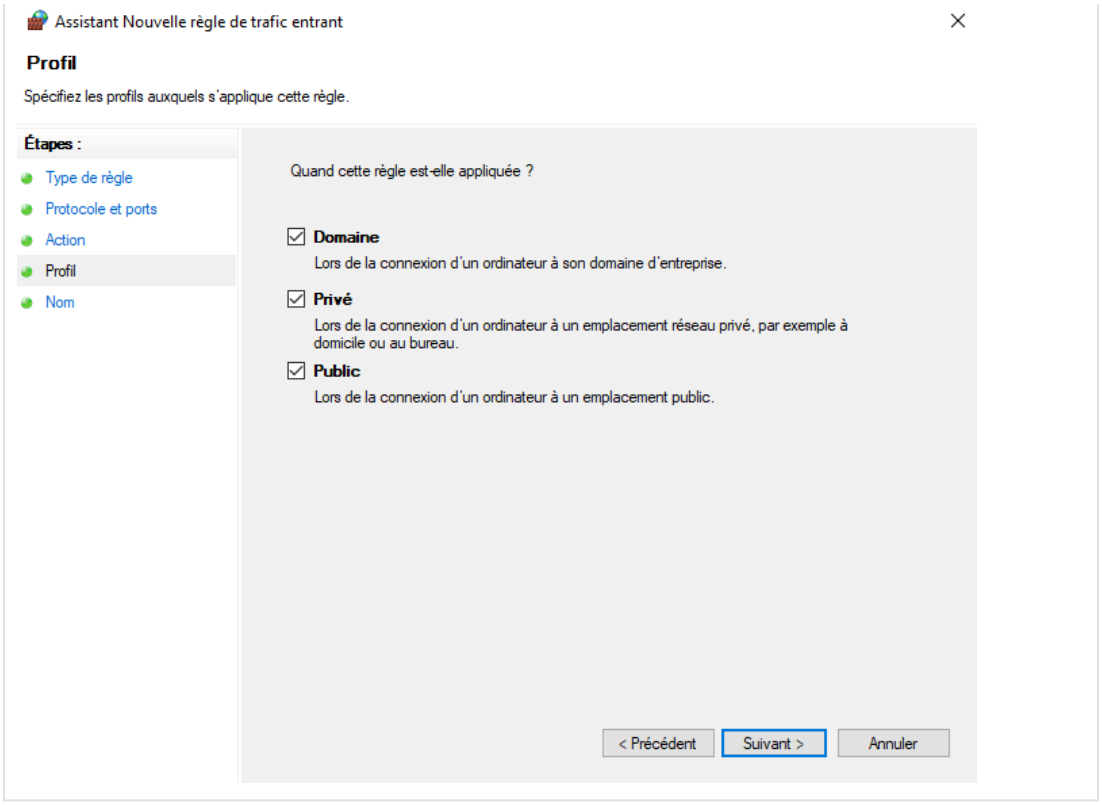
- Sur la page suivante :
  - Cocher "**TCP**" ;
  - Cocher "**Ports locaux spécifiques**", et remplissez "**5985**" ;



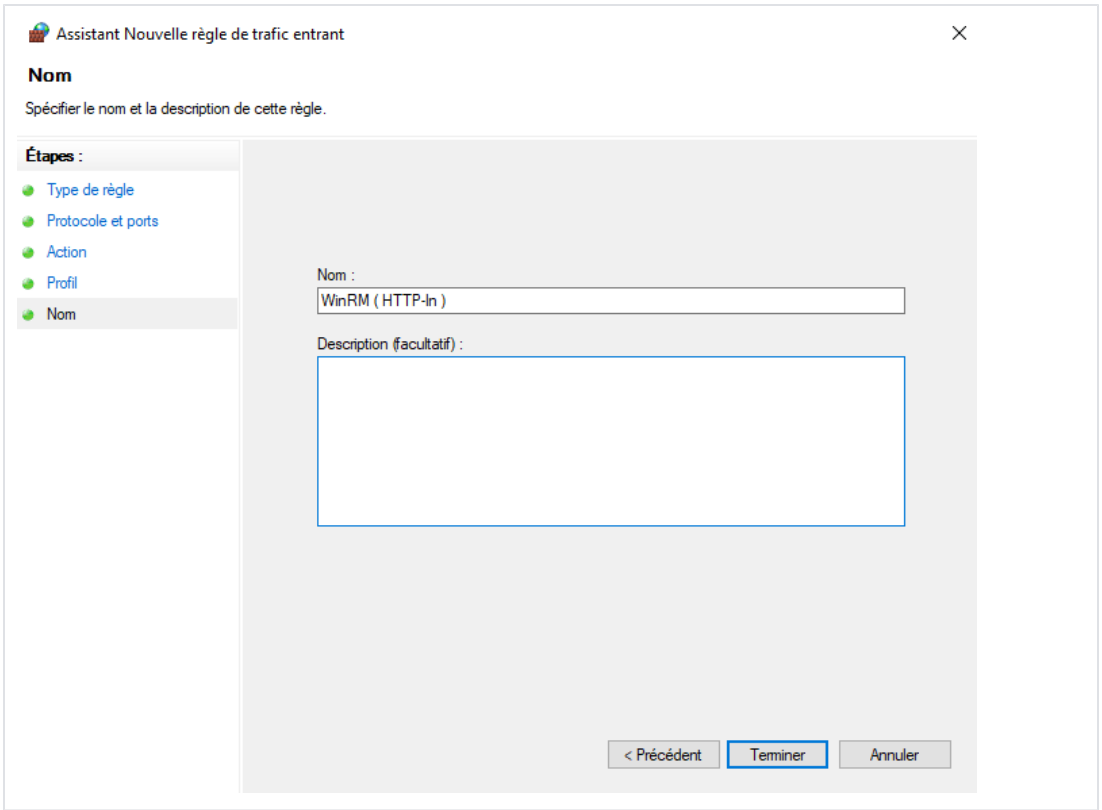
- Sur la page suivante :
  - Cocher "**Autoriser la connexion**"



- Sur la page suivante :
  - Sélectionner les types d'interfaces réseau à exposer.



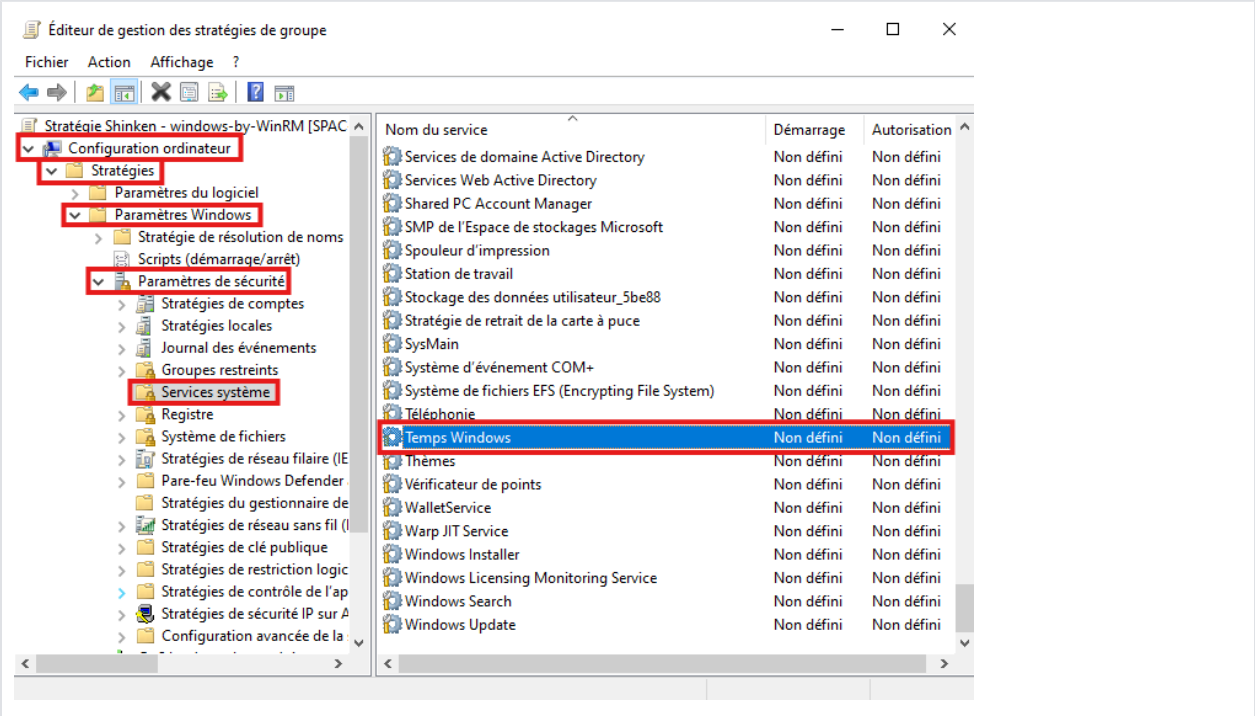
- Sur la page suivante :
  - Nommer la règle avec, par exemple, "**WinRM (HTTP-In)**"



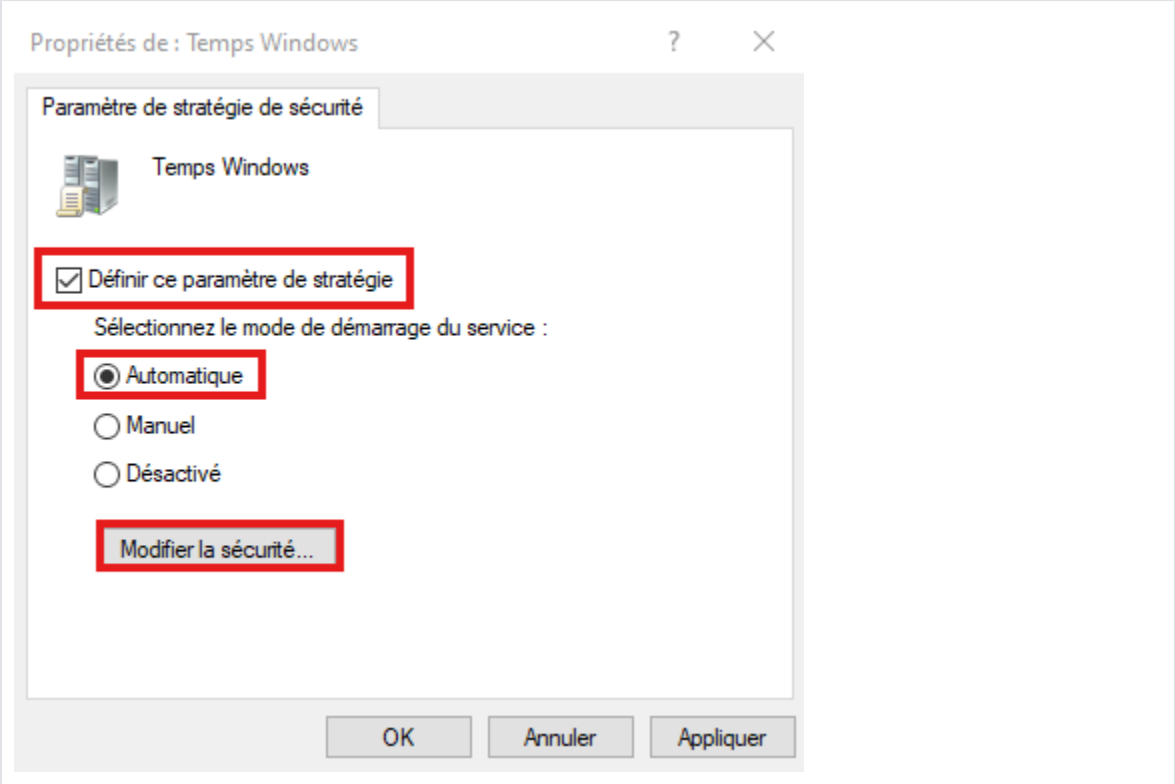
Configuration de Windows Time (synchronisation de l'heure des serveurs)

Nécessaire au fonctionnement du check "**Ntp Sync by WinRM**", si le temps de votre machine est géré par Windows Time (*W32Time*), il est nécessaire de donner les permissions suivantes :

- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Paramètres de sécurité**" > "**Services système**" > "**Temps Windows**"

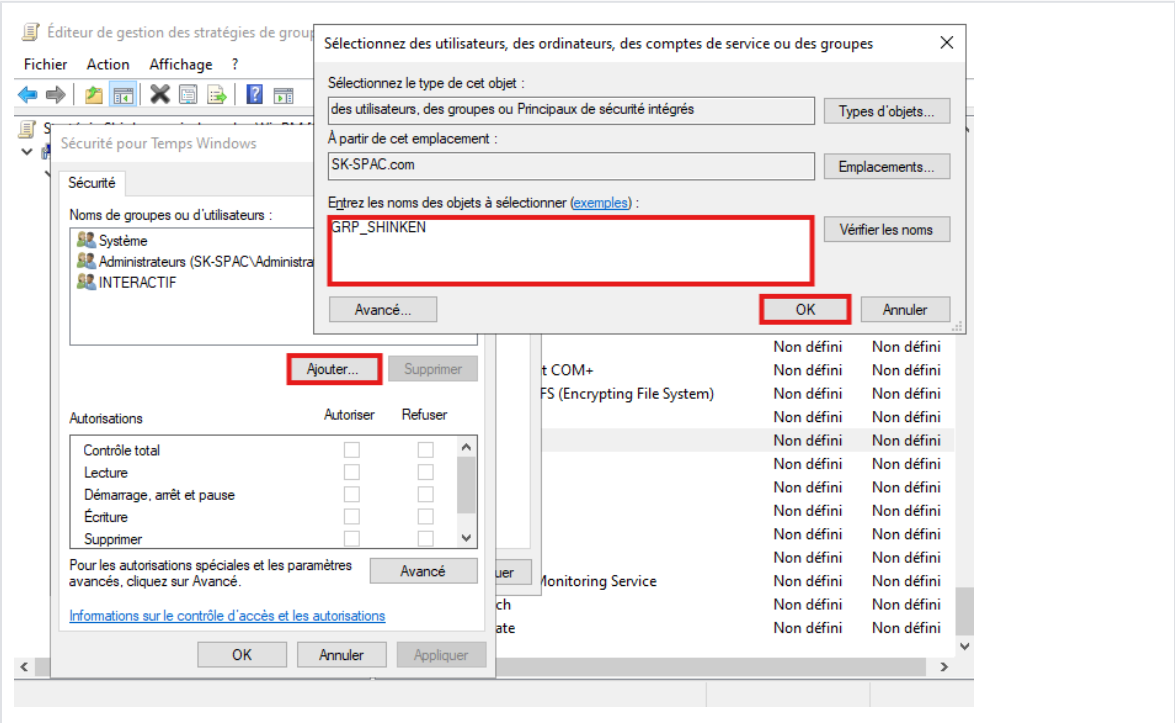


- Double-Clic, Une nouvelle fenêtre s'ouvre.
  - Cocher "**Définir ce paramètre de stratégie**"
  - Cocher "**Automatique**"

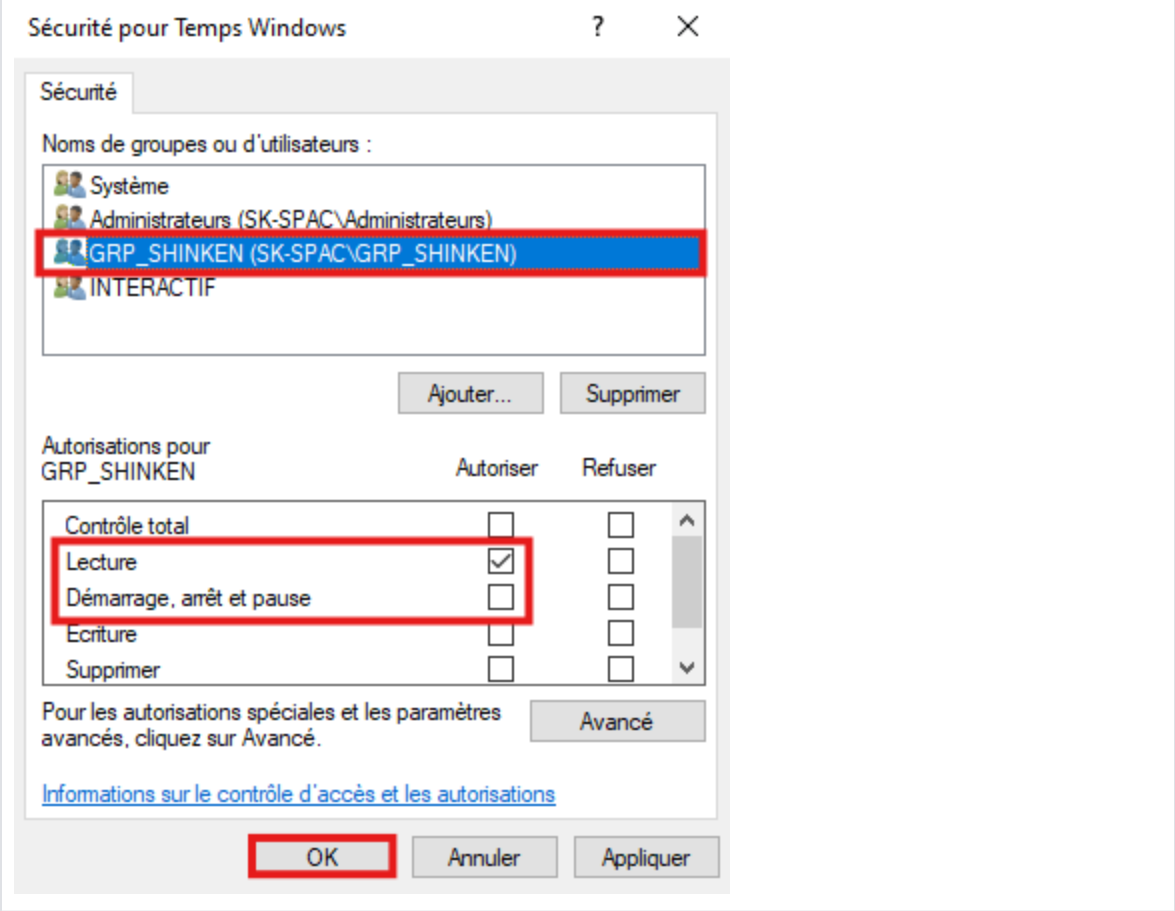


- Cliquer ensuite sur "**Modifier la sécurité...**", une nouvelle fenêtre s'ouvre.

- Cliquer sur ajouter
- Remplir le nom du groupe de supervision shinken (*GRP_SHINKEN*)
- Vérifier le nom et confirmer.



- Une fois le groupe ajouté, le sélectionner :
  - Cocher "**Autoriser**" / "**Lecture**"
  - Décocher "**Autoriser**" / "**Démarrage, arrêt et pause**"



Configuration de Script par GPO

En résumé, la dernière étape de la configuration est d'accrocher **les scripts** livrés dans le dossier **supervised-host/domain** du pack à une nouvelle **GPO** qui va les déployer.

Vous allez devoir choisir la méthode dont les scripts vont se déclencher :

- **Méthode 1** : Déclenchement un démarrage de la machine.

  ⚠ Le script s'exécutera sur une machine lorsque cette dernière redémarrera.

  C'est la méthode la plus simple et rapide pour configurer son parc Windows.
  Elle a le désavantage de nécessiter un redémarrage de chaque machine, et donc potentiellement la mise hors service pendant un court instant de vos serveurs.

- **Méthode 2** : Déclenchement à la connexion d'un compte Administrateur.

  ⚠ Le script s'exécutera sur une machine lorsqu'un compte administrateur configuré se connectera à cette dernière.

  C'est une bonne méthode complémentaire à la première.
  Elle permet de lancer le script pour les serveurs qui ne peuvent pas être mis hors tension.

ⓘ Vous pouvez choisir une seule méthode, ou bien les combiner selon votre besoin.

Téléchargement des scripts

Avant toute chose, **télécharger les trois scripts** sur votre **contrôleur de domaine**.

Permissions WinRM

Autorisation aux objets WMI/CIM

Télécharger le script ICI

AddSecurityPrincipalonDefaultWinRMSDDL.ps1

Télécharger le script ICI

Set-WMINameSpaceSecurity.ps1

Permissions EventLog Security

Télécharger le script ICI

Set-EventLogSecurity.ps1

Permissions des Services

Télécharger le script ICI

Set-ServicesPermission.ps1

Méthode 1 : Script au démarrage de la machine

Dans cette méthode, il faudra

- créer une nouvelle GPO,
- l'attacher aux serveurs Windows à superviser,
- configurer la GPO pour y accrocher les scripts.

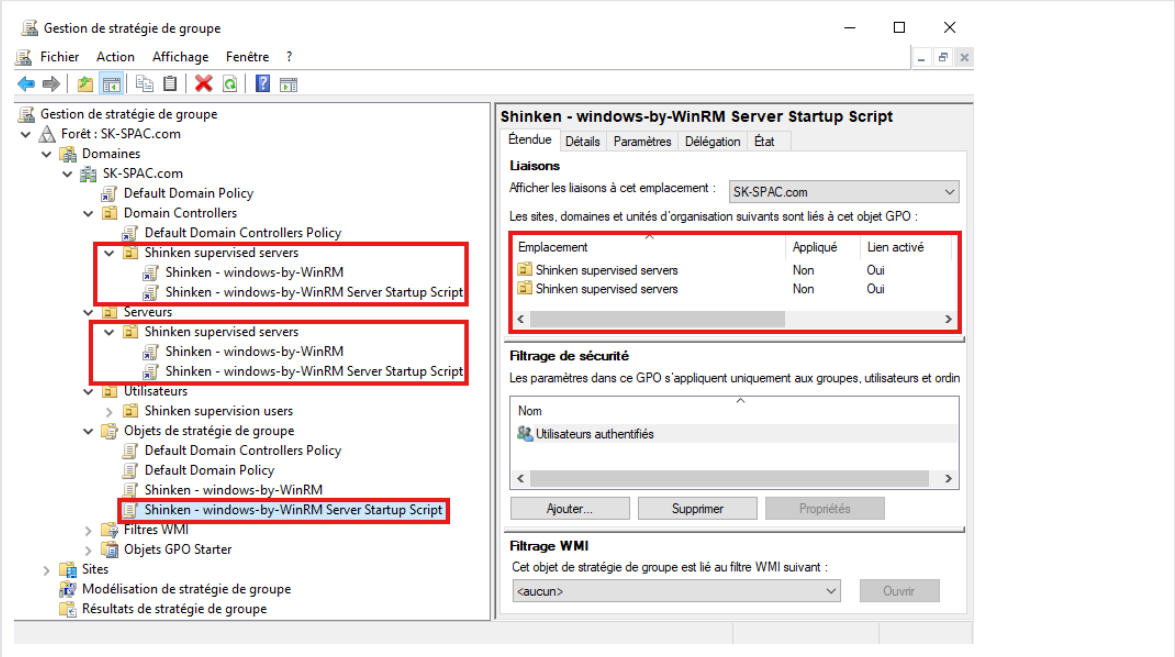
Ensuite, ces serveurs Windows seront configurés au prochain redémarrage.

Créer une GPO

- Ouvrir "**Gestion de stratégie de groupe**" (*gpmc.msc*)

> Il est conseillé de créer une nouvelle GPO, différente de la précédente.
> Celle-ci pourra être désactivé lorsque l'entièreté de votre parc Windows à superviser sera configuré.

- Dans l'arborescence, Clic-Gauche sur votre "**Forêt: DOMAINE**" > "**Domaines**" > "**DOMAINE**" > "**Objets de stratégie de groupe**" ;
- Clic-Droit sur "**Objets de stratégie de groupe**" > "**Nouveau**" puis nommer la nouvelle **GPO** avec, par exemple, "**Shinken - windows-by-WinRM Server Startup Script**" ;
- Une fois crée, Cliquer-Glisser votre **GPO** dans les **UOs** de vos serveurs à superviser précédemment créés, aux mêmes endroits où est liée la précédente **GPO** :
  - La liste des liaisons s'affiche à droite de la fenêtre lorsque la **GPO** est sélectionnée :

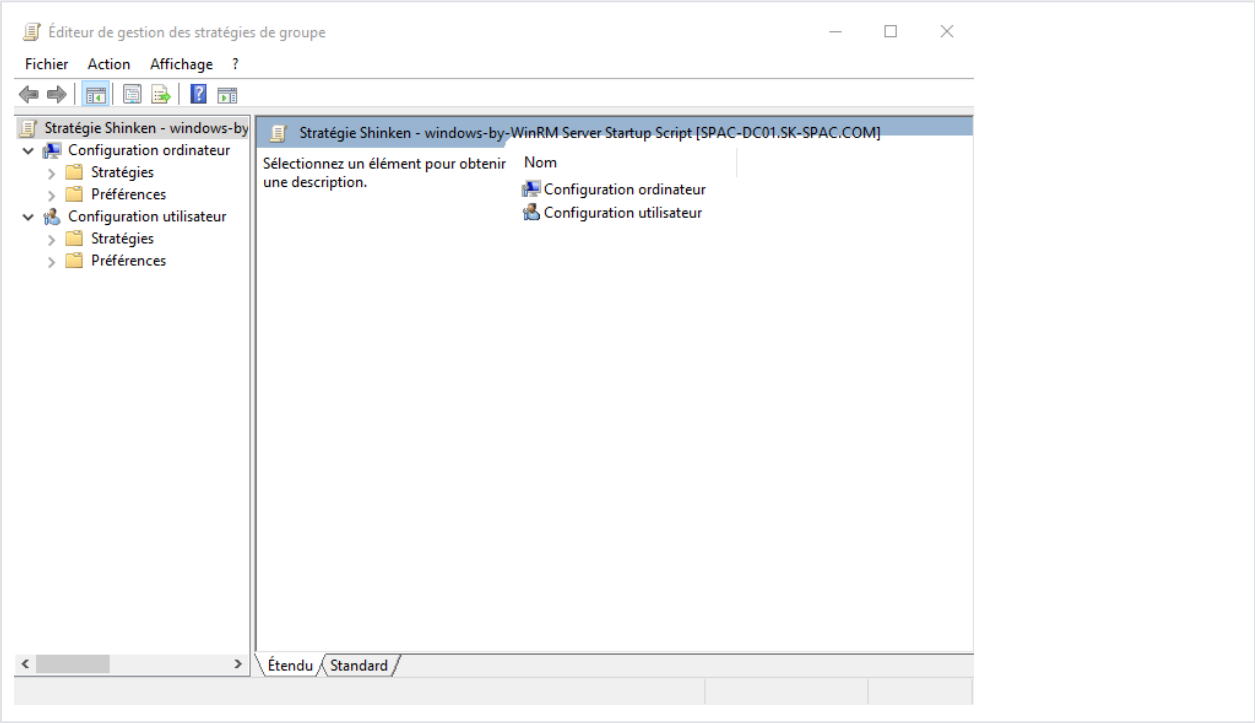


Configuration de la GPO : Accrocher les scripts

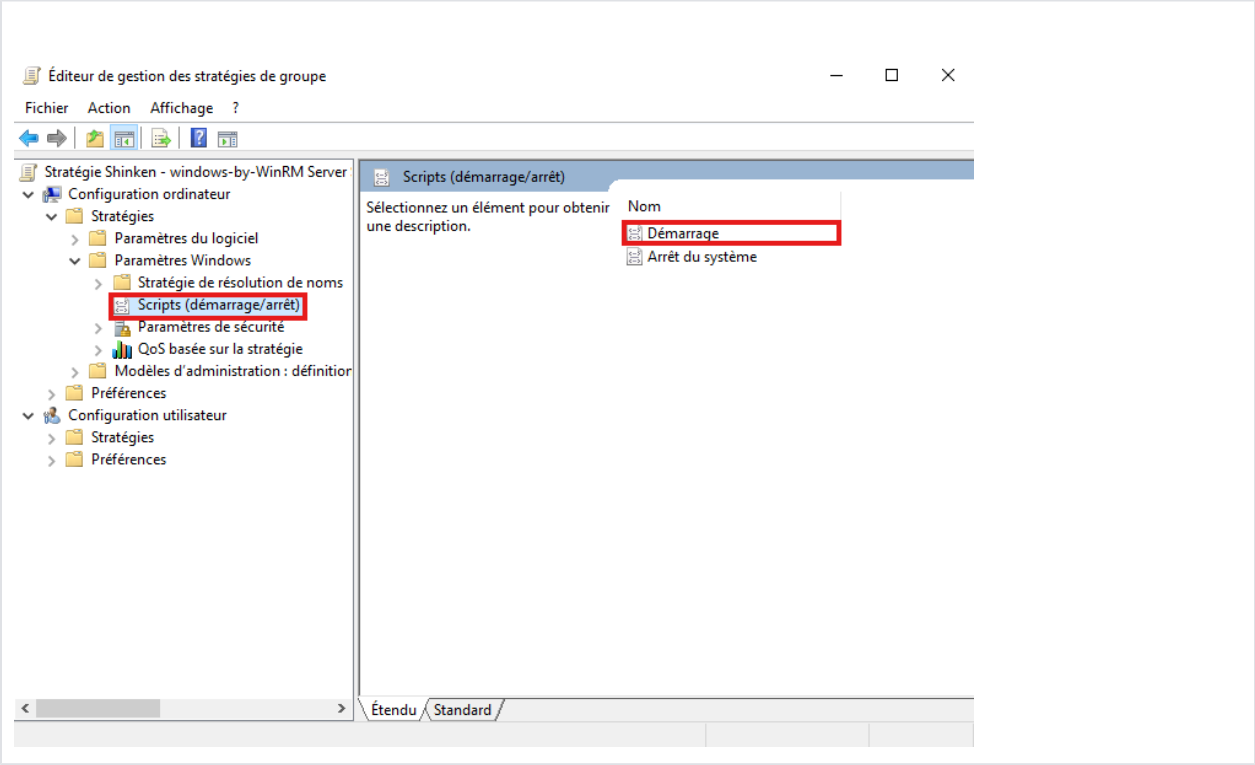
Une fois créé et lié aux Windows à superviser, il faut configurer la **GPO**.

- Clic-Droit sur la nouvelle **GPO**, puis "Modifier" ;

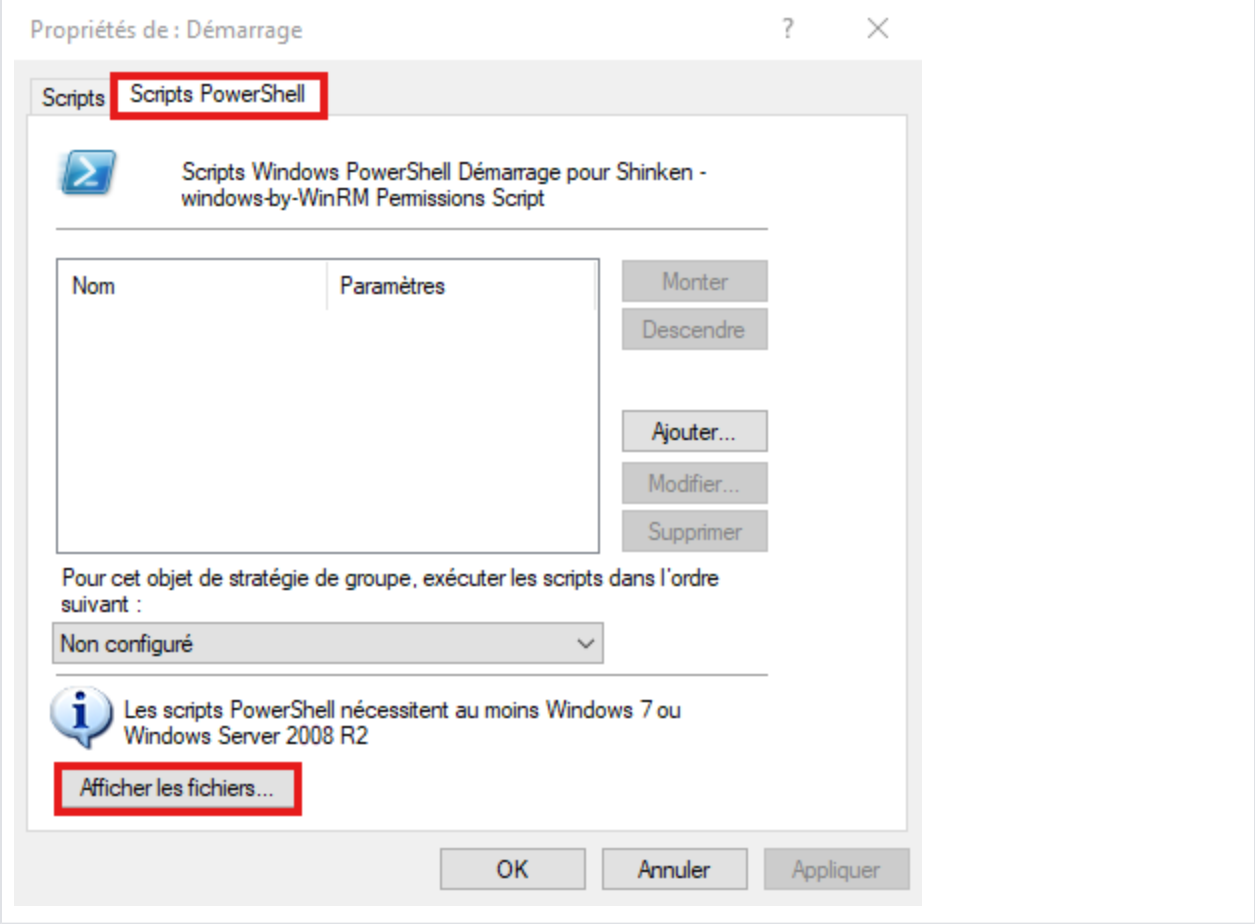
- Les règles à appliquer se trouvent dans cette arborescente de configuration.



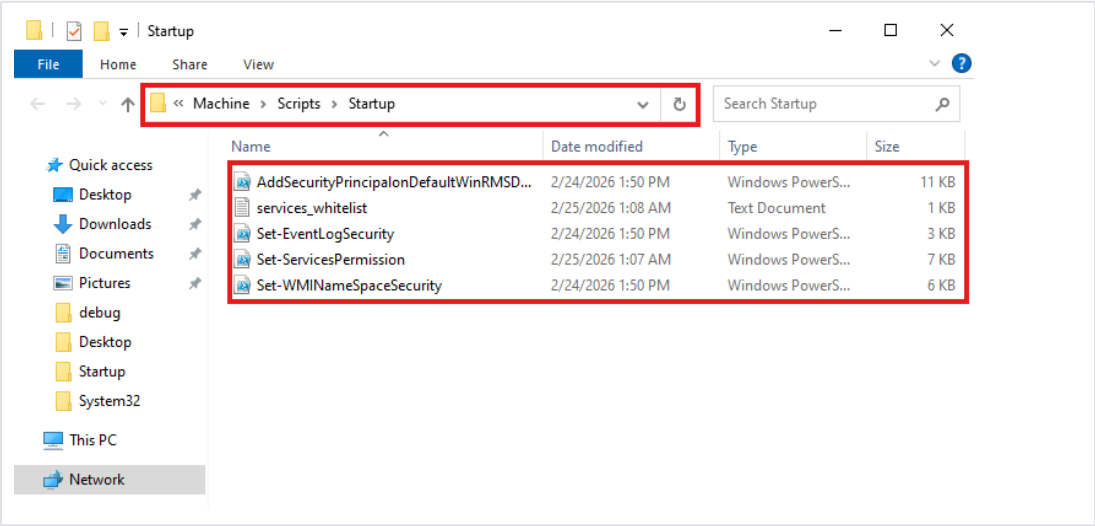
- Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Paramètres Windows**" > "**Scripts (démarrage/arrêt)**"
- Double-Clic sur "Démarrage", une nouvelle fenêtre s'ouvre :



- Dans la nouvelle fenêtre, aller dans l'onglet "**Scripts PowerShell**"
- Clic sur "**Afficher les fichiers...**".



- Une nouvelle fenêtre s'ouvre.
  - Dans ce dossier (*... > Machine > Scripts > Startup*), **déposer les scripts** téléchargés précédemment.



- Fermer le dossier.

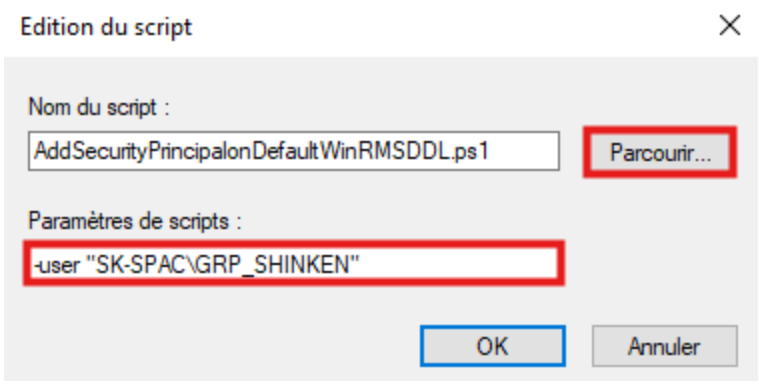
- Toujours dans l'onglet "**Scripts PowerShell**", cliquer sur "Ajouter"
  - Une nouvelle fenêtre s'ouvre pour ajouter un script.
  - Cliquer sur parcourir et ajouter le 1er script : "**AddSecurityPrincipalonDefaultWinRMSDDL.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
  - Dans la zone "Paramètre de scripts", remplissez :

```
-user "MON_DOMAINE\GRP_SHINKEN"
```

Ici, remplacez "MON_DOMAINE" par le nom **NetBios** de votre domaine.

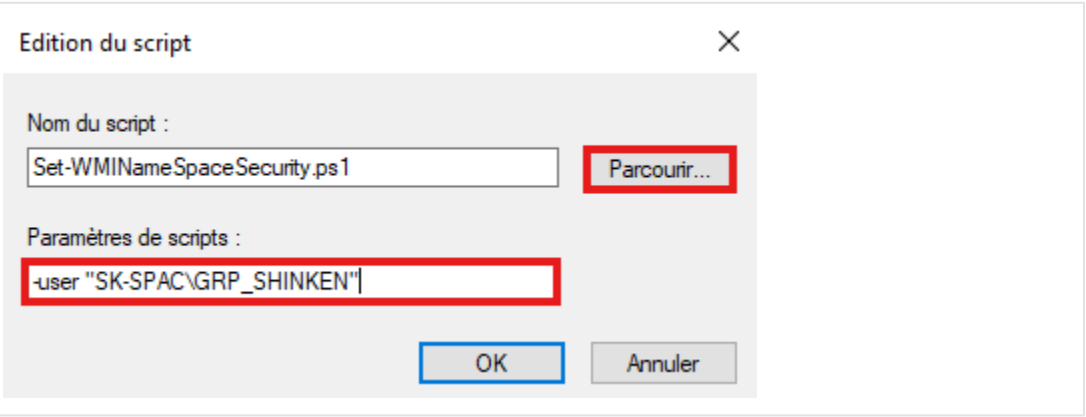
Le nom **NetBios** de votre domaine s'obtient avec la commande suivante, exécuté dans un **PowerShell** :

```
(Get-ADDomain).NetBIOSName
```



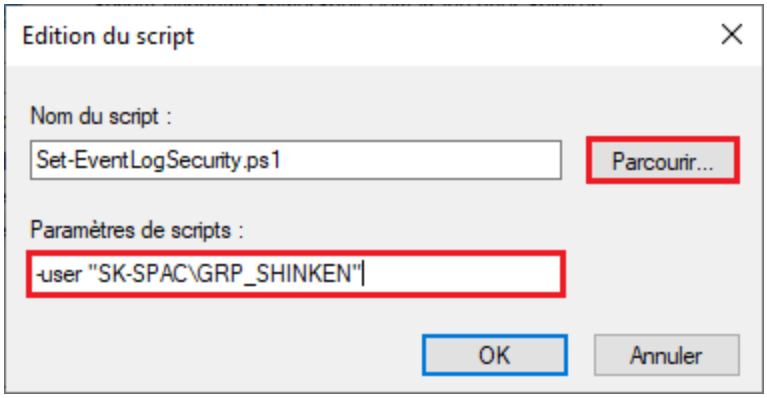
- Répéter l'opération avec le 2 script : "**Set-WMINameSpaceSecurity.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*).
  - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN"
```



- Répéter l'opération avec le 3 script : "**Set-EventLogSecurity.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*).
  - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN"
```

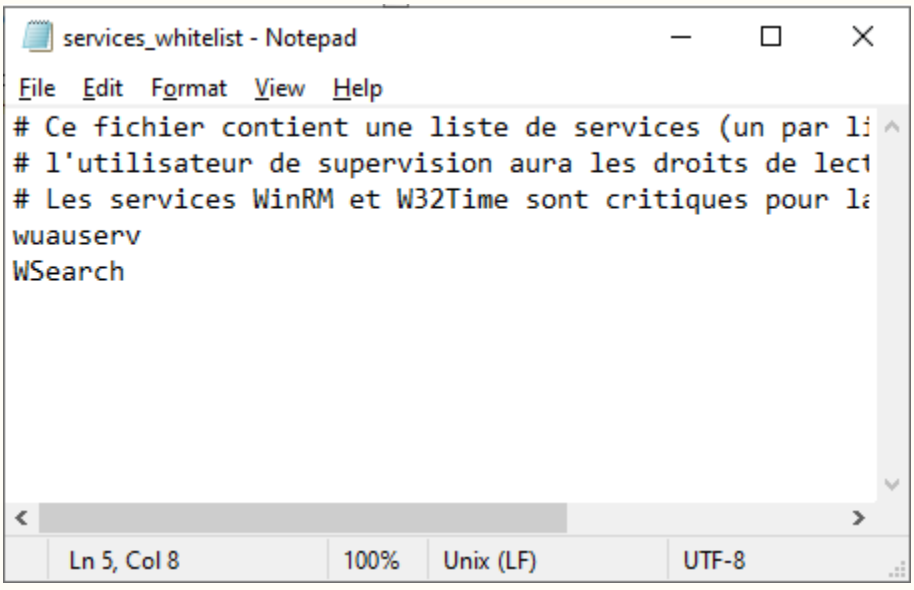


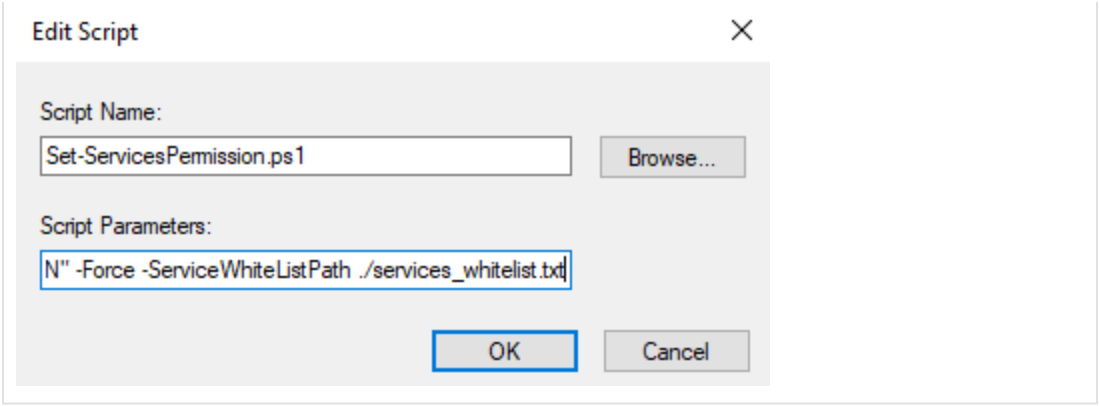
- Répéter l'opération avec le 4 script : "**Set-ServicesPermissions.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*).
  - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN" -Force -ServiceWhiteListPath ./services_whitelist.txt
```

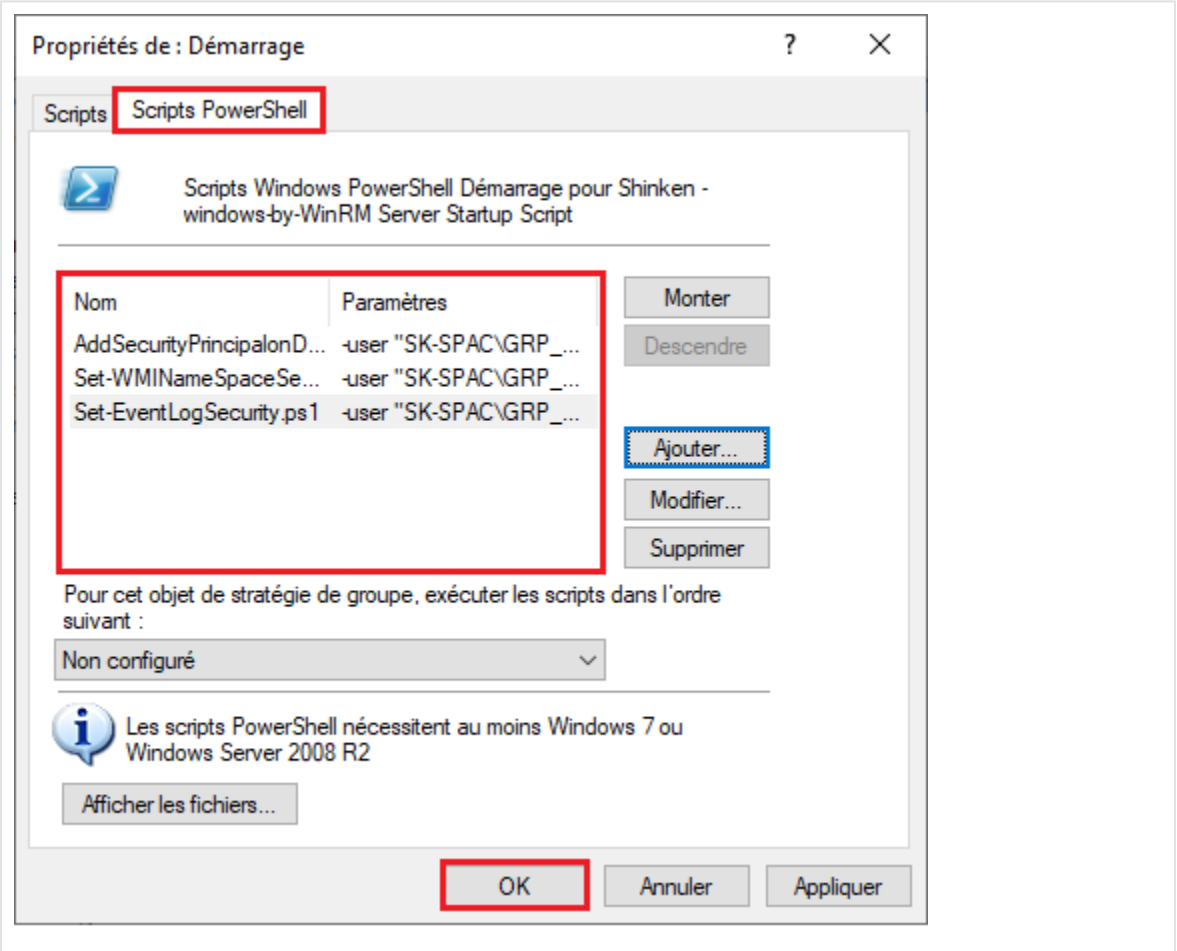
⚠ Cette étape de configuration permet le bon fonctionnement du check Service KEY State by WinRM.
Le fichier texte 'services_whitelist.txt' comprend une liste ligne par ligne de noms de services à superviser.
Pour chaque nouveau service à mettre à superviser, **mettre à jour cette liste**.

Une configuration d'avantage paramétrable est expliqué ici : Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken





- La configuration finale des scripts ressemblera à ca :



- Les scripts s'exécutent à chaque démarrage des machines configurées.
  - Afin de ne pas consommer de ressources inutilement, le script est fait pour ne s'exécuter en entier qu'une fois.
  - Les prochaines exécutions des scripts s'arrêteront prématurément.

> ⚠ Il est possible de rajouter l'argument "**-Force**" dans les paramètres des deux scripts pour les exécuter à chaque fois.
> Cela peut être utile si les premières exécutions ont échoué et que de nouvelles doivent être lancés.

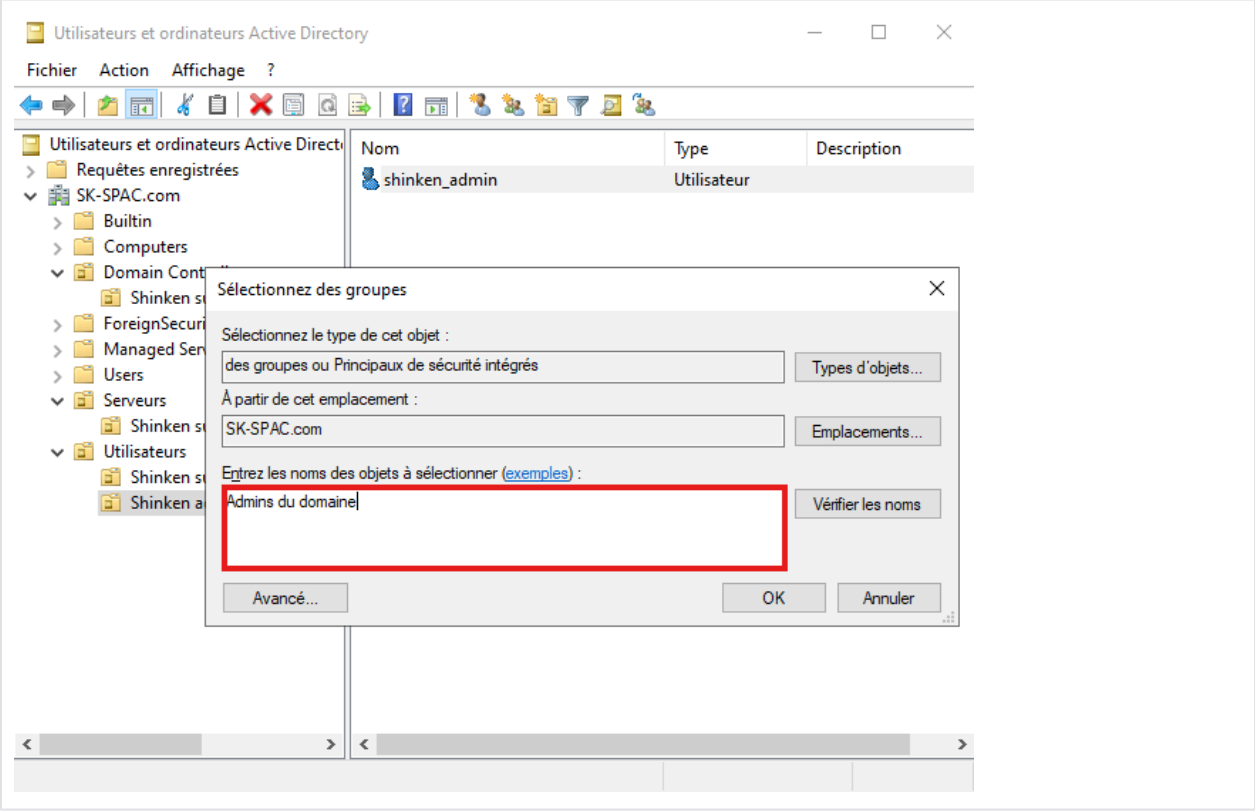
Méthode 2 : Script à la connexion d'un compte Administrateur

Dans cette méthode,

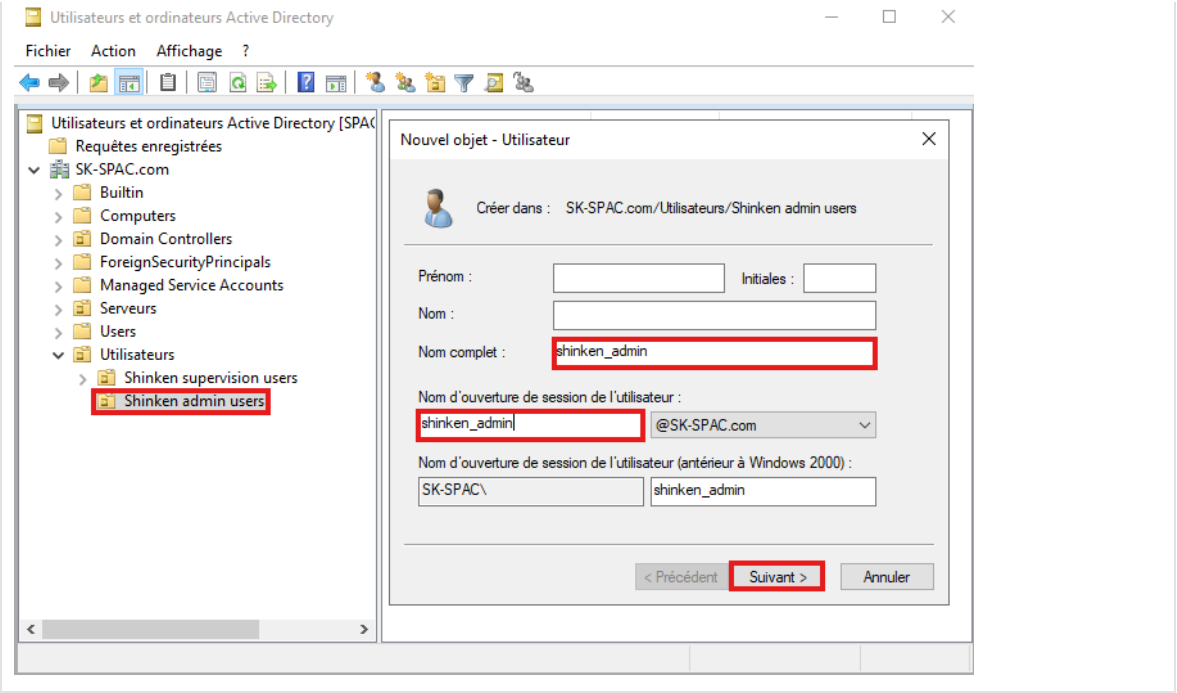
- il faudra
  - créer un nouvel administrateur de domaine (*ou utiliser un existant*) ,
  - puis créer une nouvelle GPO et l'attacher à cet administrateur,
  - configurer la GPO pour y accrocher les scripts.
- Ensuite, chaque serveur sur lequel se connectera l'administrateur sera configuré.

Créer un administrateur de domaine

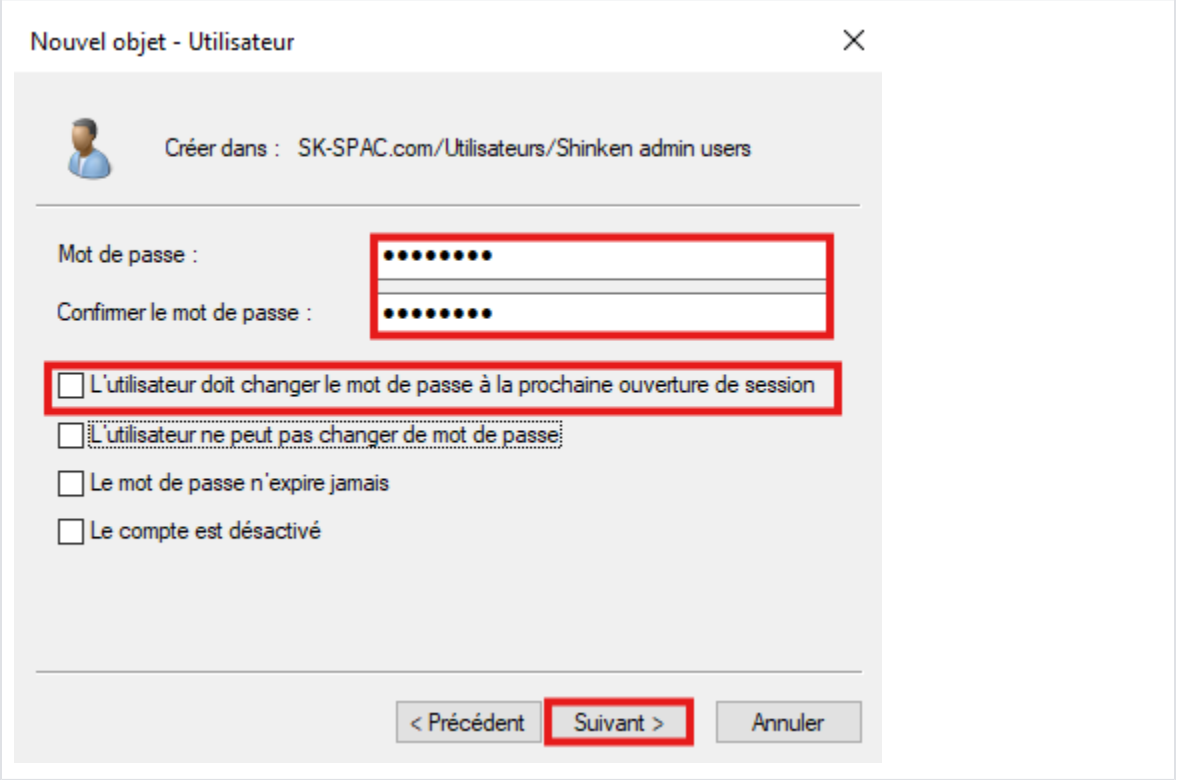
- Ouvrir "**Utilisateurs et ordinateurs Active directory**" (*dsa.msc*),
- Cliquer sur son domaine,
- Repérer dans quel **UO** sont les utilisateurs,
- Créer une nouvelle **UO** et l'appeler par exemple "**Shinken admin users**" :



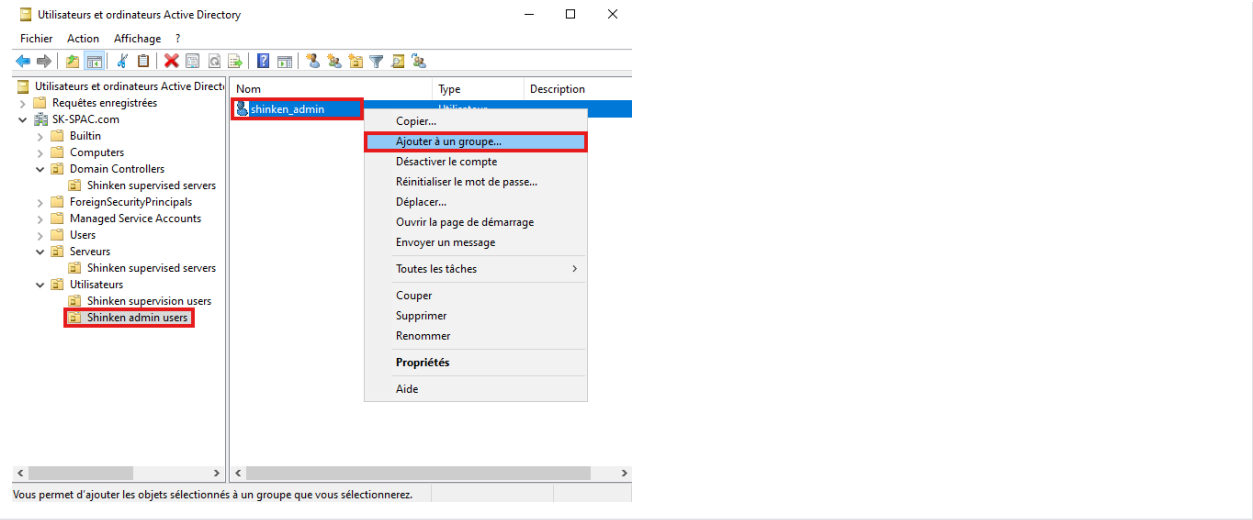
- Dans cette nouvelle **UO**, Clic-Droit, Sélectionner "**Nouveau**" > "**Utilisateur**"
- Remplir :
  - "Nom complet"
  - "Nom d'ouverture de session de l'utilisateur"



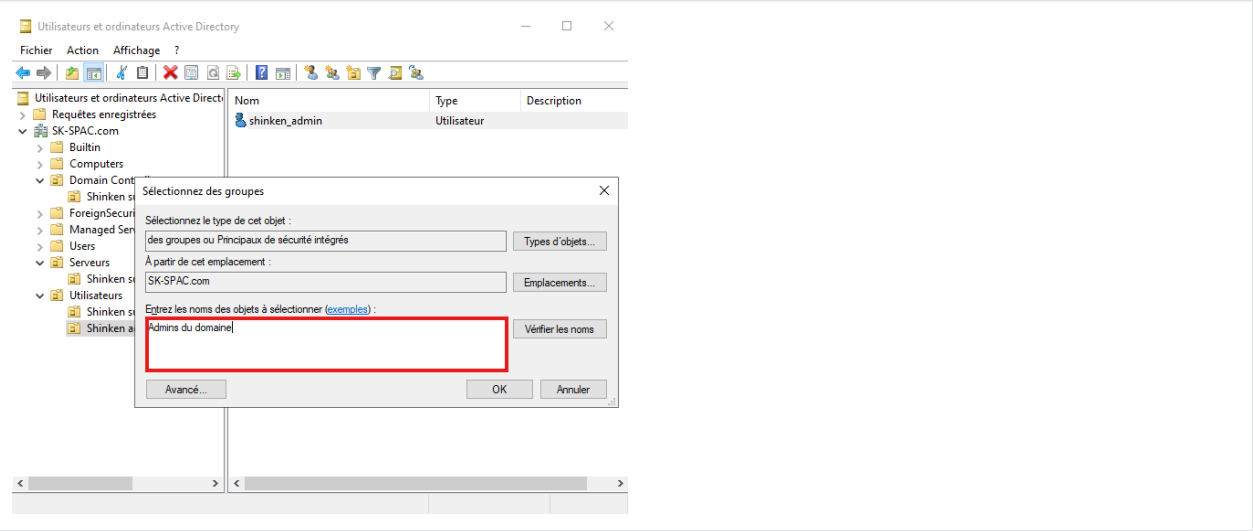
- Sur la page suivante :
  - Remplir le mot de passe .
  - Décocher "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session" :



- Finaliser ensuite la création de l'utilisateur.
- Ensuite, Clic-Droit sur l'utilisateur puis "**Ajouter à un groupe**"



- Remplir le nom "**Admins du domaine**"



- Cliquer sur "**Vérifier les noms**" puis valider.

L'administrateur de domaine est désormais configuré.

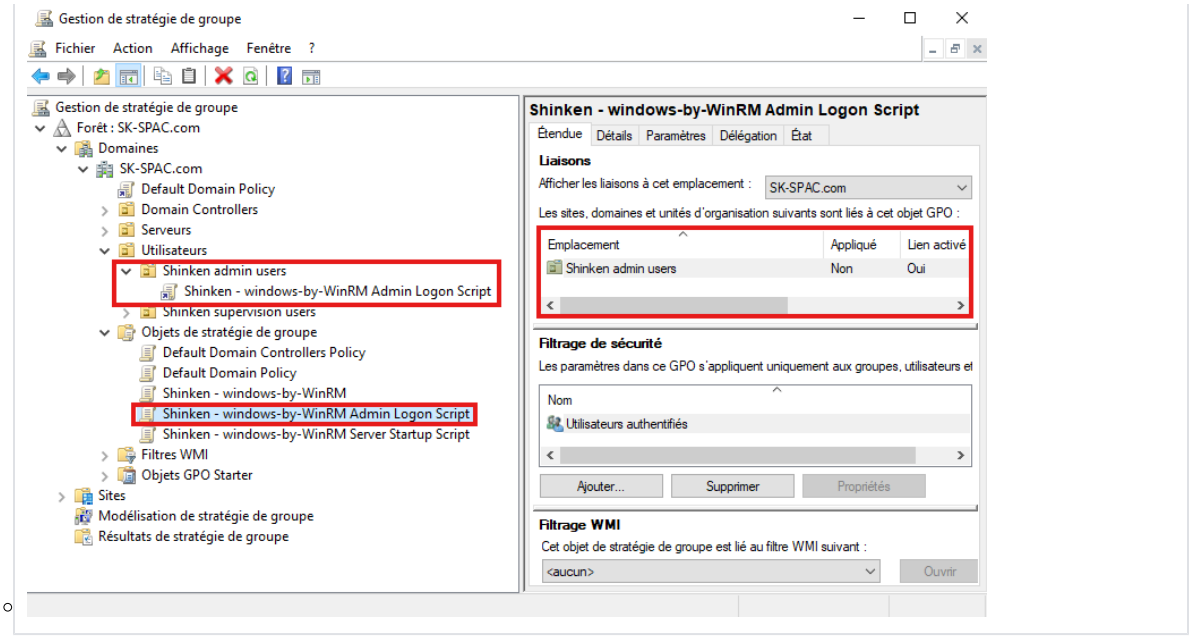
> ⚠ Cet utilisateur administrateur ne doit pas être utilisé pour la connexion des sondes shinken, mais pour se connecter sur les Windows afin de les configurer.

Créer une GPO

- Ouvrir "**Gestion de stratégie de groupe**" (*gpmc.msc*)

> ⓘ Il est conseillé de créer une nouvelle GPO, différente de la précédente.
>
> Celle-ci pourra être désactivé lorsque l'entièreté de votre parc Windows à superviser sera configuré.

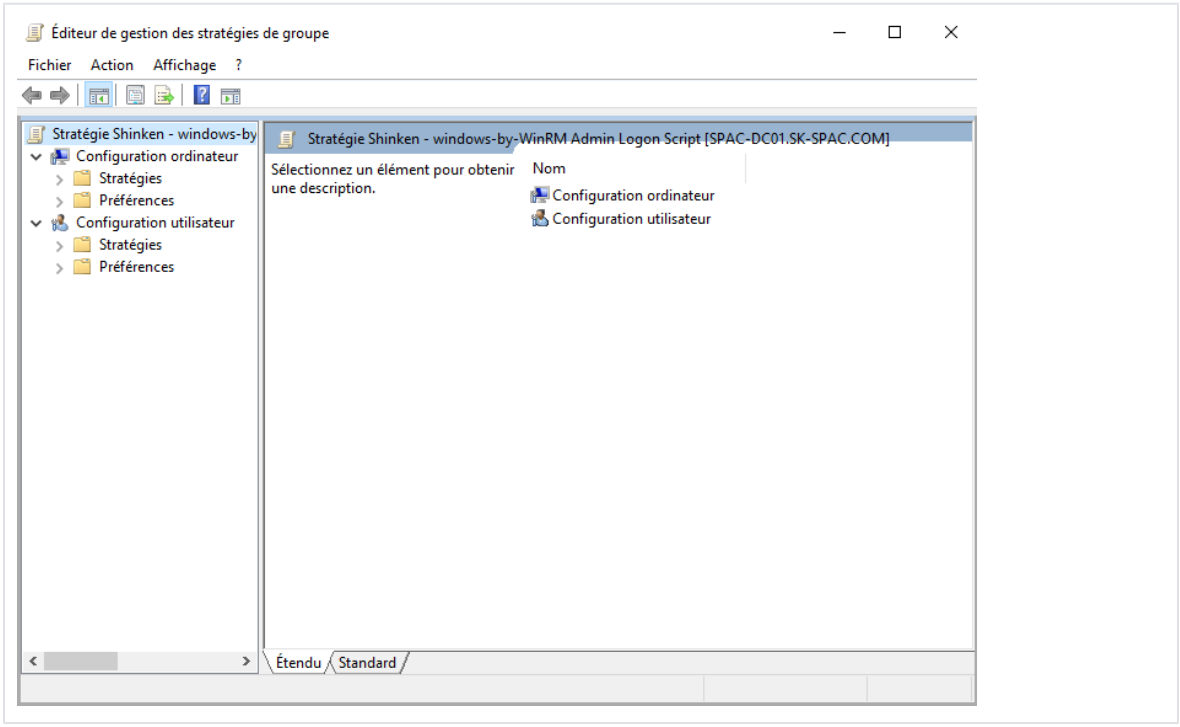
- Dans l'arborescence, Clic-Gauche sur votre "**Forêt: DOMAINE**" > "**Domaines**" > "**DOMAINE**" > "**Objets de stratégie de groupe**"
- Clic-Droit sur "**Objets de stratégie de groupe**" > "**Nouveau**" puis nommer la nouvelle **GPO** avec, par exemple, "**Shinken - windows-by-WinRM Admin Logon Script**"
- Une fois crée, Cliquer-Glisser votre **GPO** dans l'**UO** créé où se trouve le nouvel administrateur.
    - La liste des liaisons s'affiche à droite de la fenêtre lorsque la **GPO** est sélectionnée.



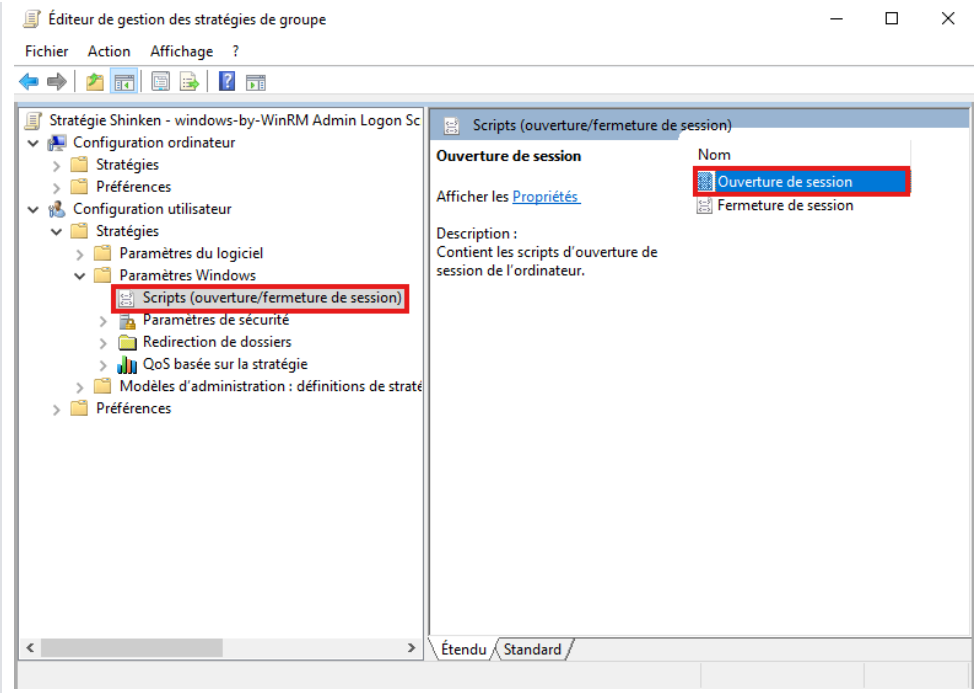
Configuration de la GPO : Accrocher les scripts

Une fois créé et lié à l'administrateur, il faut configurer la **GPO**.

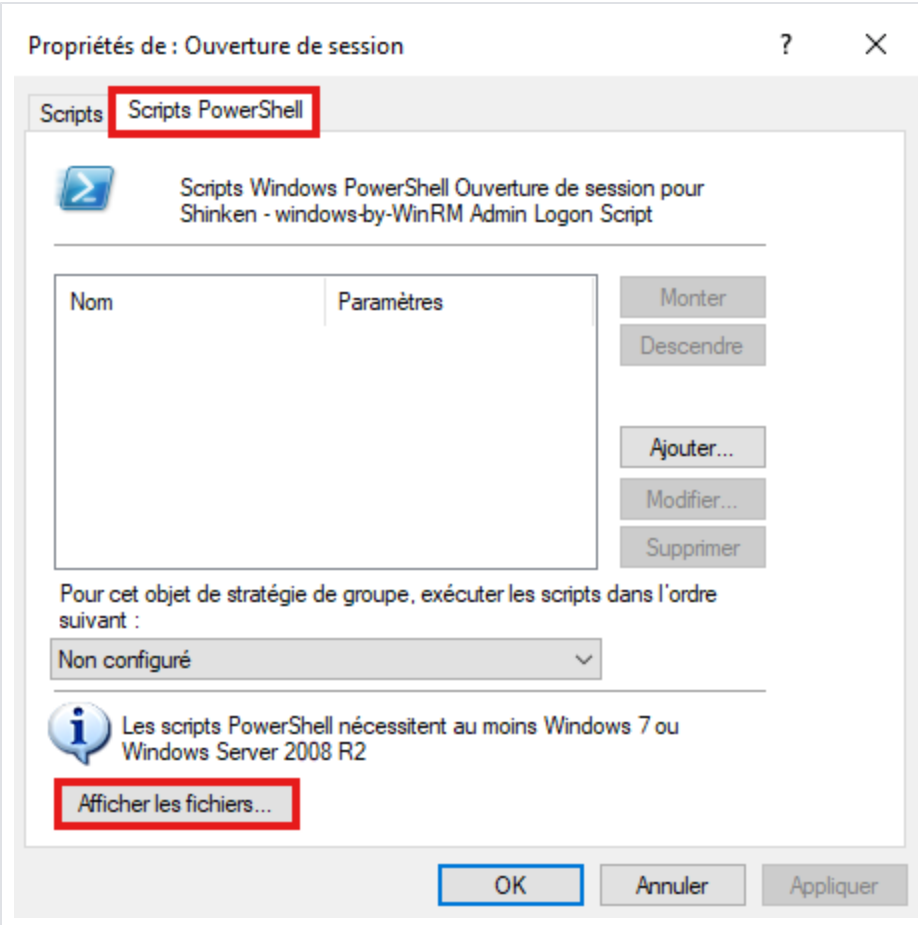
- Clic-Droit sur la nouvelle **GPO**, puis "Modifier"
- Les règles à appliquer se trouvent dans cette arborescente de configuration.



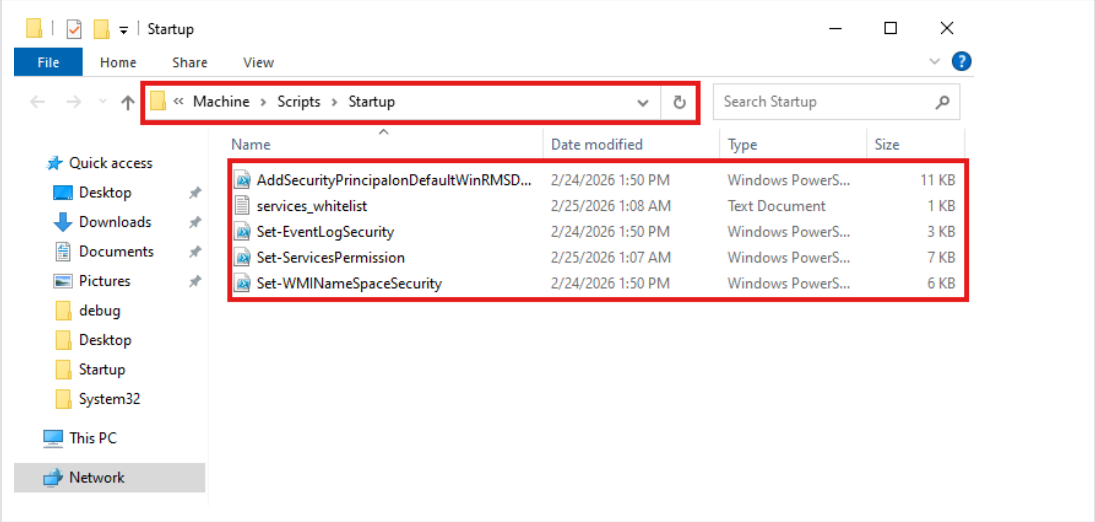
- Dans l'arborescence : "**Configuration utilisateur** > "**Stratégies**" > "**Paramètres Windows**" > "**Scripts (ouverture/fermeture de session)**"
- Double-Clic sur "Ouverture de session", une nouvelle fenêtre s'ouvre



- Dans la nouvelle fenêtre, aller dans l'onglet "**Scripts PowerShell**"
- Clic sur "**Afficher les fichiers...**" :



- Une nouvelle fenêtre s'ouvre. Dans ce dossier (*... > User> Scripts > Logon*), **déposer les scripts** téléchargés précédemment.

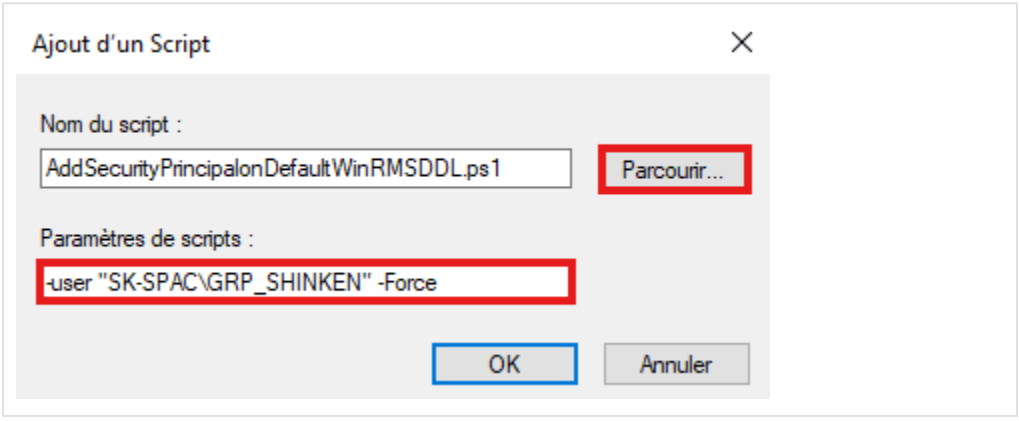


- Fermer le dossier.

- Toujours dans l'onglet "**Scripts PowerShell**", cliquer sur "Ajouter" :
  - Une nouvelle fenêtre s'ouvre pour ajouter un script.
    - Cliquer sur parcourir et ajouter le 1er script : "**AddSecurityPrincipalonDefaultWinRMSDDL.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
    - Dans la zone "Paramètre de scripts", remplissez :

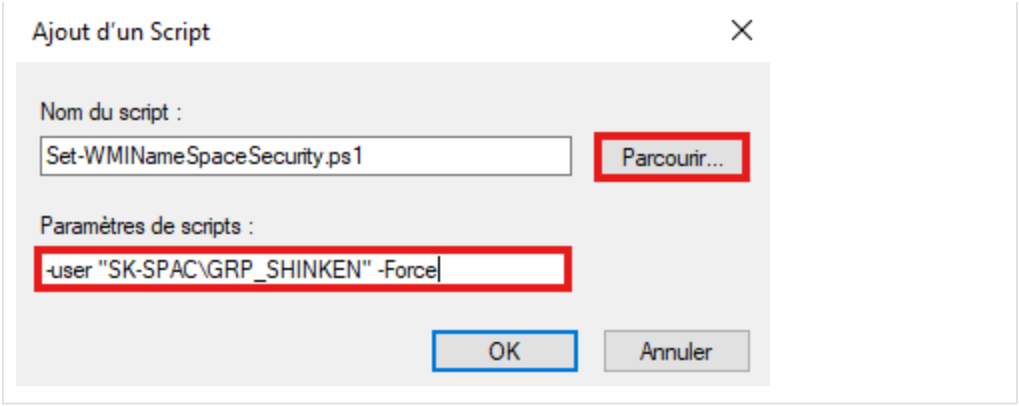
```
-user "MON_DOMAINE\GRP_SHINKEN" -Force
```

> Ici, remplacez "MON_DOMAINE" par le nom **NetBios** de votre domaine.
>
> Le nom **NetBios** de votre domaine s'obtient avec la commande suivante, exécuté dans un **PowerShell** :
>
> ```
> (Get-ADDomain).NetBIOSName
> ```



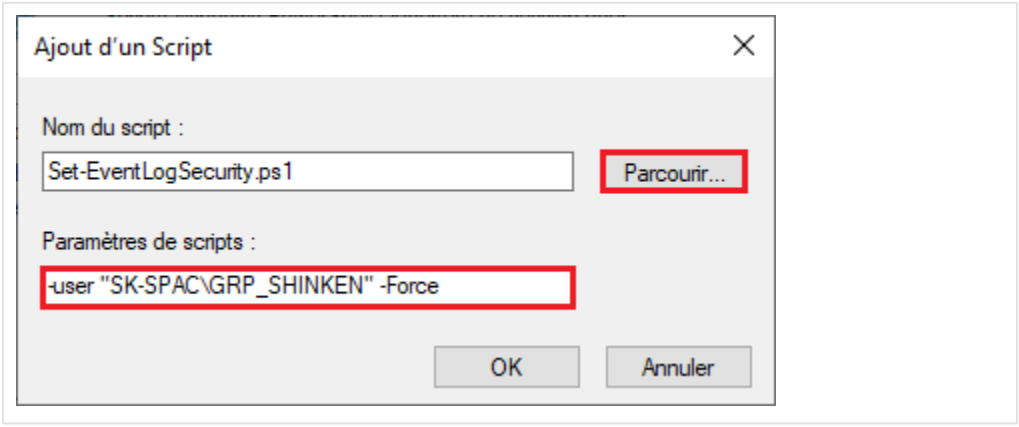
  - Répéter l'opération avec le 2 script : "**Set-WMINameSpaceSecurity.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
    - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN" -Force
```



- Répéter l'opération avec le 3 script : "**Set-EventLogSecurity.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
  - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN" -Force
```

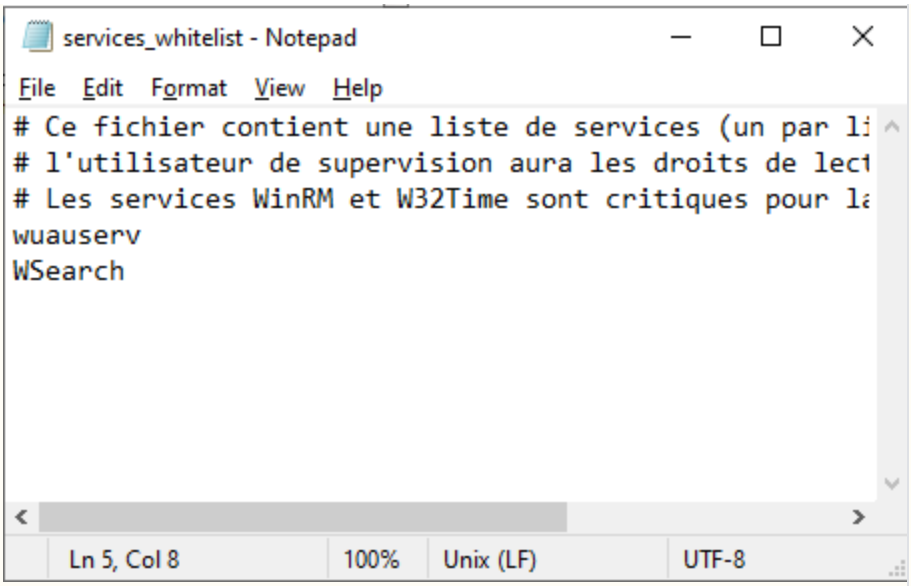


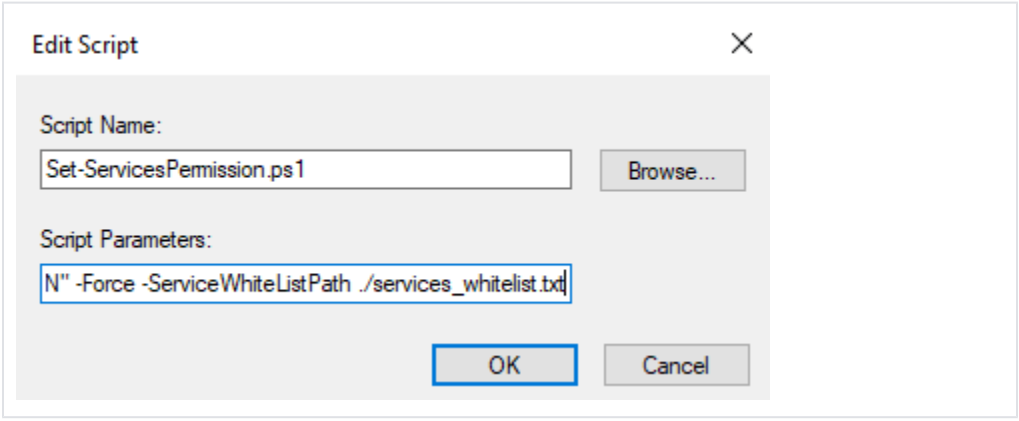
- Répéter l'opération avec le 4 script : "**Set-ServicesPermissions.ps1**", dans le dossier présélectionné (*... > Machine > Scripts > Startup*)
  - Dans la zone "Paramètre de scripts", remplissez les mêmes paramètres :

```
-user "MON_DOMAINE\GRP_SHINKEN" -Force -ServiceWhiteListPath ./services_whitelist.
txt
```

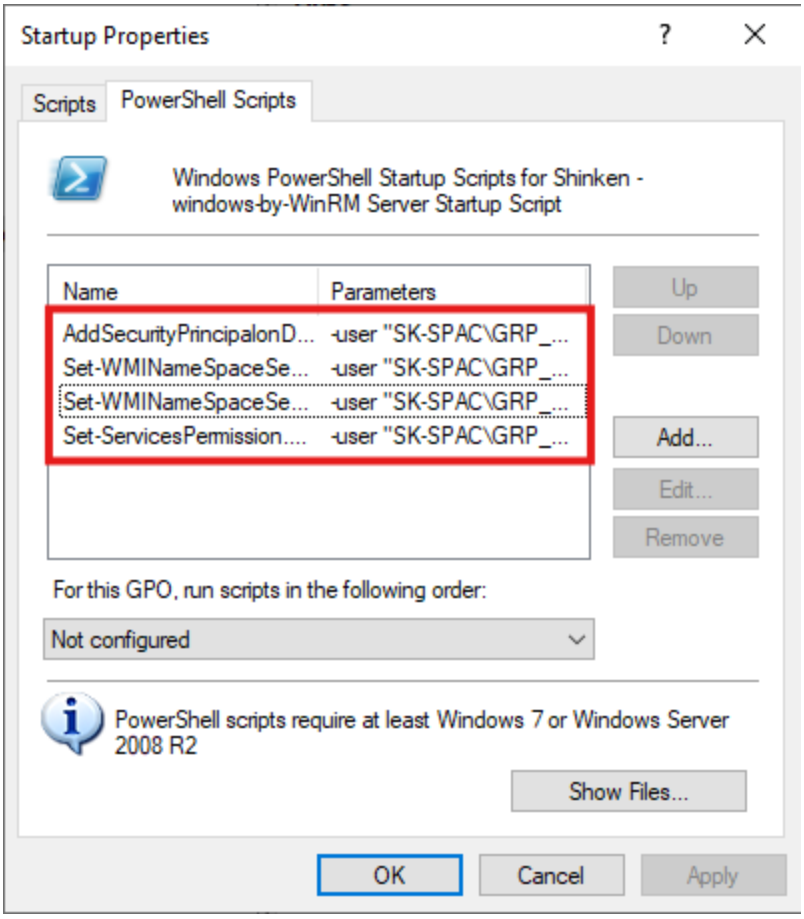
Cette étape de configuration permet le bon fonctionnement du check Service KEY State by WinRM.
Le fichier texte 'services_whitelist.txt' comprend une liste ligne par ligne de noms de services à superviser.
Pour chaque nouveau service à mettre à superviser, **mettre à jour cette liste**.

Une configuration d'avantage paramétrable est expliqué ici : Configuration du Windows supervisé pour le pack windows-by-WinRM__shinken



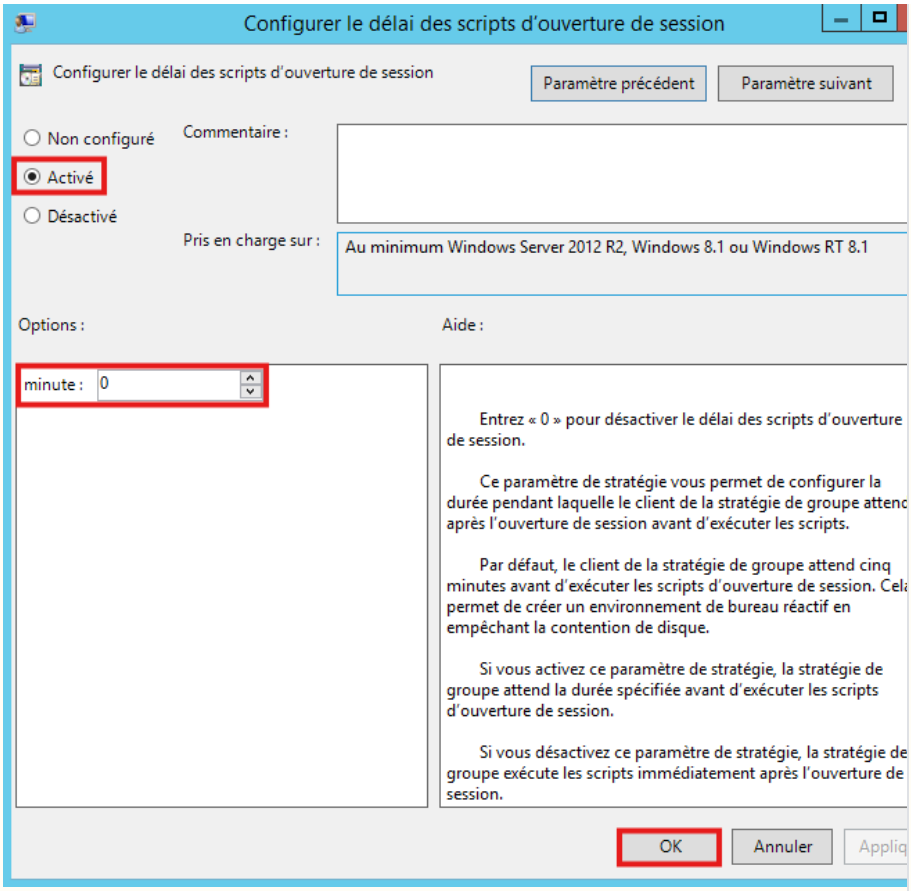


- La configuration finale des scripts ressemblera à ça :



- Les scripts s'exécutent à chaque fois que l'utilisateur Administrateur shinken configuré se connecte à une machine.

> ⚠ Attention, sur les machines **Windows Serveur 2012R2**, par défaut, les scripts accrochés à l'ouverture/fermeture de session ont un **délai d'attente de 5 minutes** après l'ouverture de la session avant de s'exécuter.
>
> Vous pouvez alors attendre ces 5 minutes ou bien changer la configuration de ce délai en modifiant la GPO :
>
> - Dans l'arborescence : "**Configuration ordinateur**" > "**Stratégies**" > "**Modèle d'administration : définition de stratégies**" > "**Système**" > "**Stratégie de groupe**" > "**Configurer le délai des scripts d'ouverture de session**"
>   - Cocher "**Activer**"
>   - Remplir "**0**" dans le champ "**minute**"



Appliquer la configuration

Une fois les étapes précédentes effectuées, il faut **appliquer la configuration**.

Par défaut, **Windows** applique la configuration des **GPO** :

- Après un redémarrage de la machine.
- Après 90 minutes à 120 minutes (*Application automatique des GPO*).
- Après avoir exécuté sur une machine la commande :

```
gpupdate.exe /Force
```

Avec cette commande, les GPOs ne seront uniquement mis à jour et appliqués sur la machine qui lance cette commande.

Ensuite, les scripts de configuration se déclencheront selon la configuration que vous avez choisie d'appliquer. Il faudra alors :

- Redémarrer les serveurs Windows ;
- Ou se connecter à distance avec le compte Administrateur Shinken ;

La configuration de votre domaine (*Active Directory*) Windows **est terminée** et il est prêt à être supervisé.

L'étape suivante est de choisir, d'accrocher et de paramétrer les modèles d'hôtes fournis dans le pack (*Voir la page Modèles d'hôtes du pack windows-by-WinRM__shinken*).