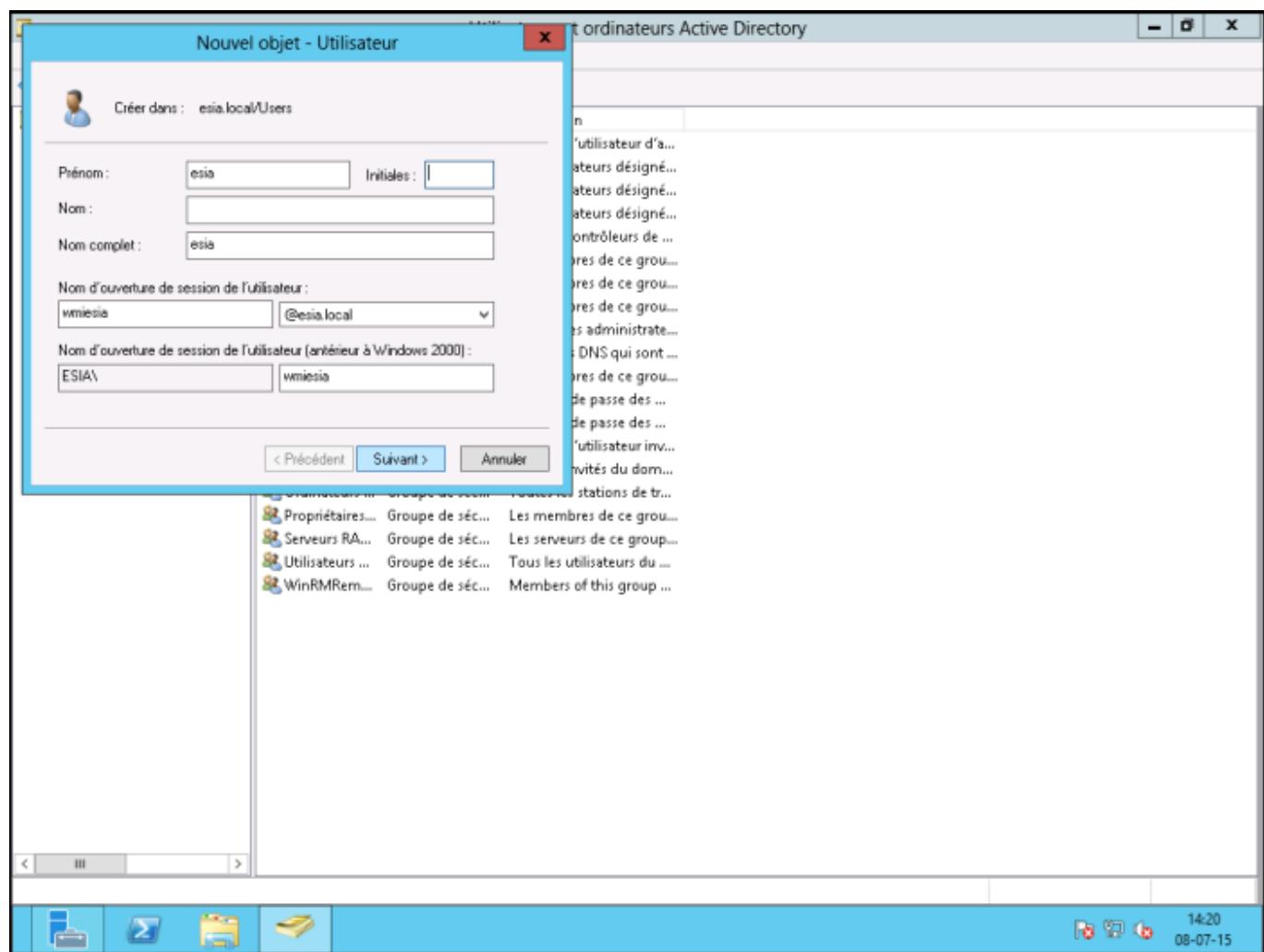


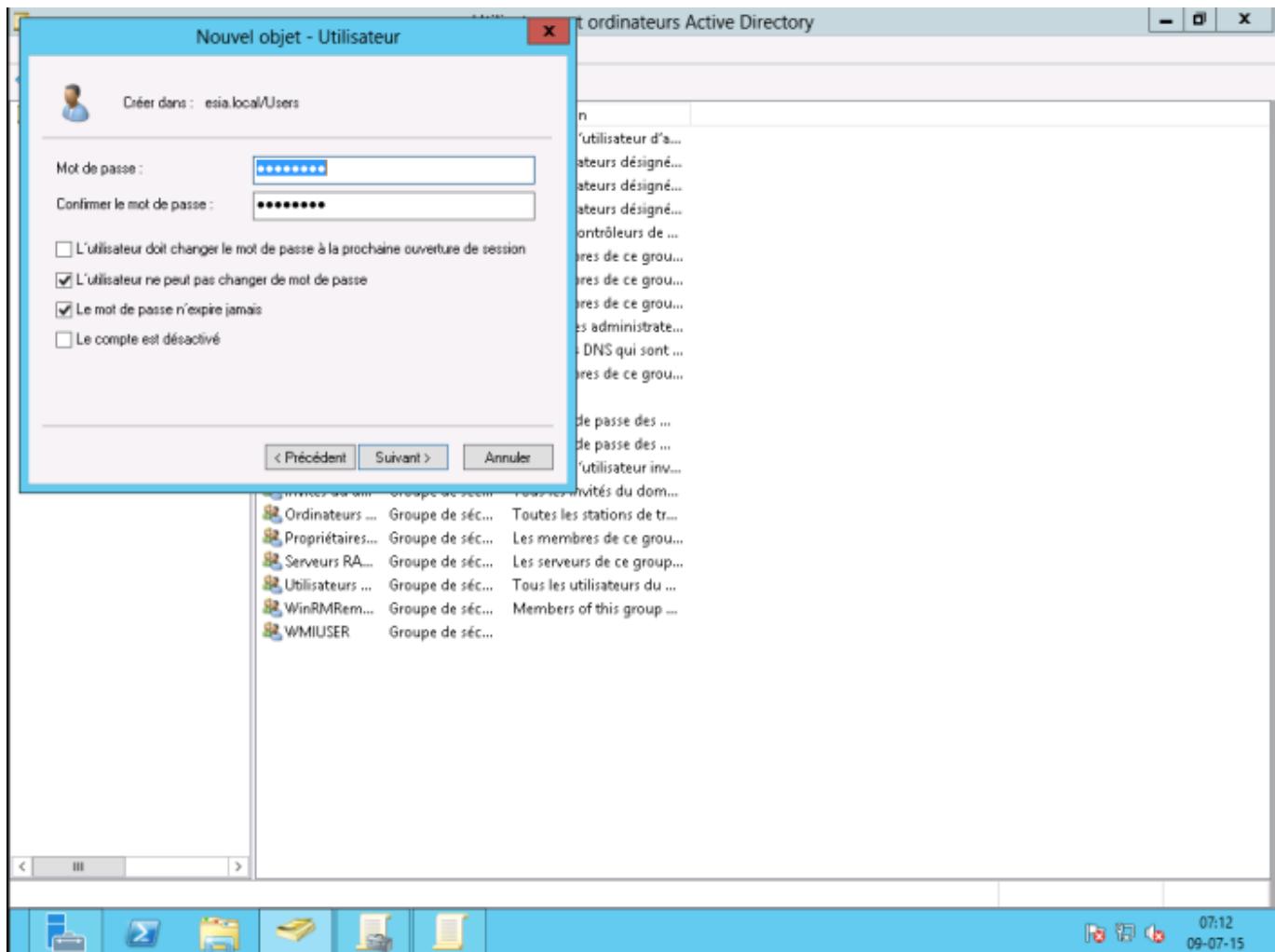
Activer WMI sur Windows Serveur 2012 via GPO

Voici comment activer WMI via les GPO sur un Active Directory

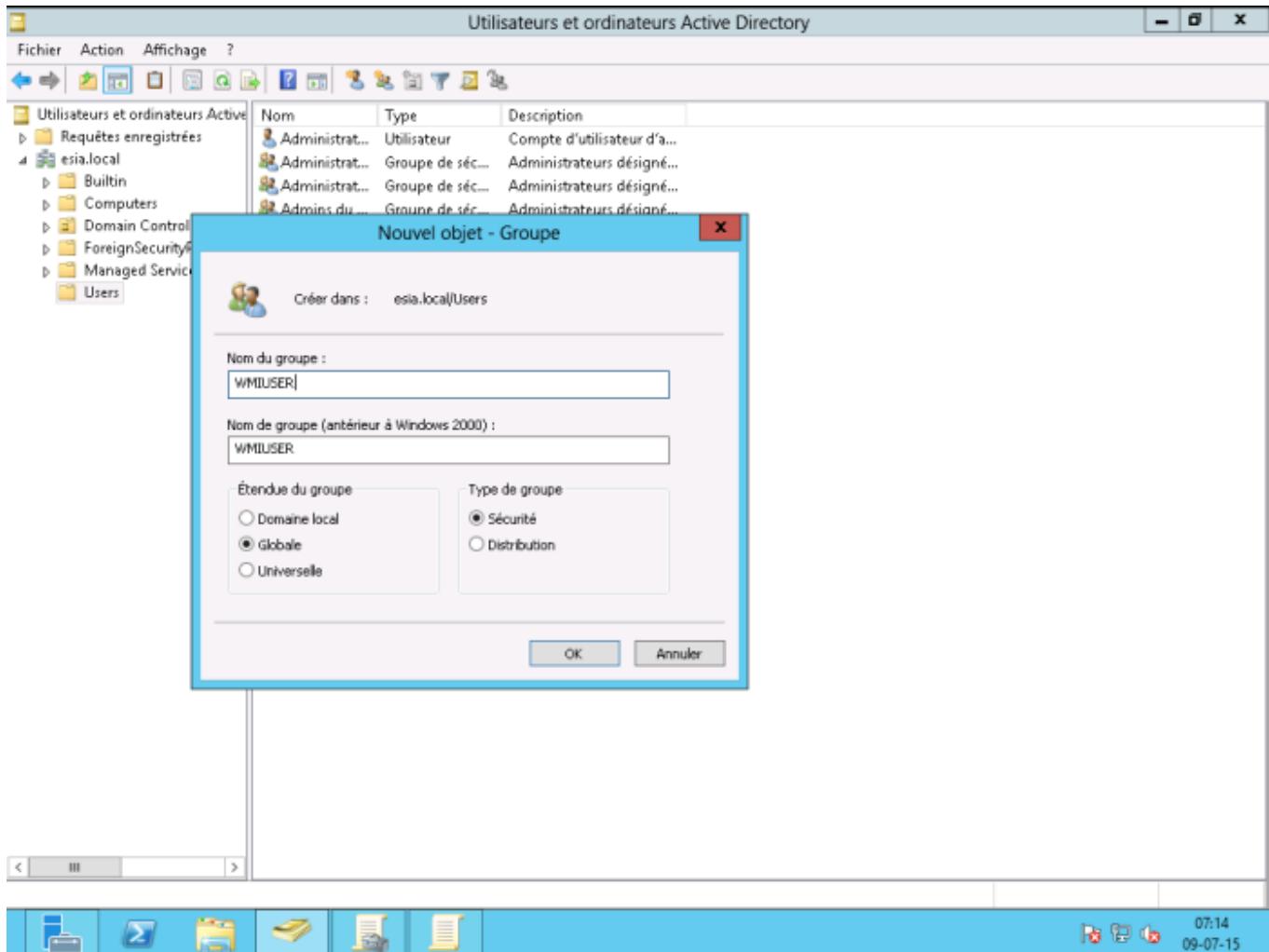
Création de l'utilisateur & du groupe

Créez un utilisateur (ici : « `wmiesia` ») avec comme mot de passe : `Wmic2015` (dans ce tutoriel). N'oubliez pas de sélectionner « le mot de passe n'expire jamais » et « l'utilisateur ne peut pas changer de mot de passe »

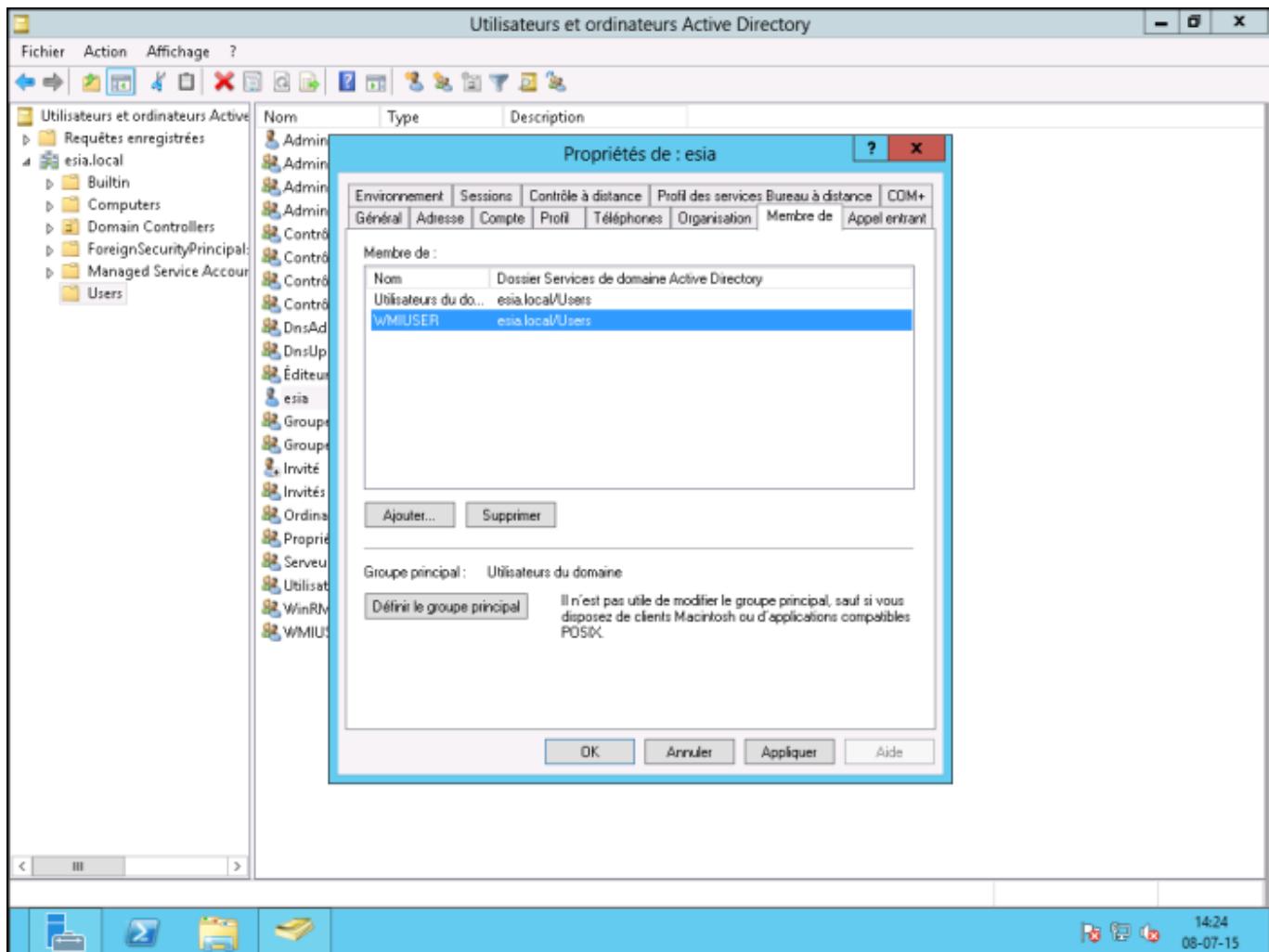




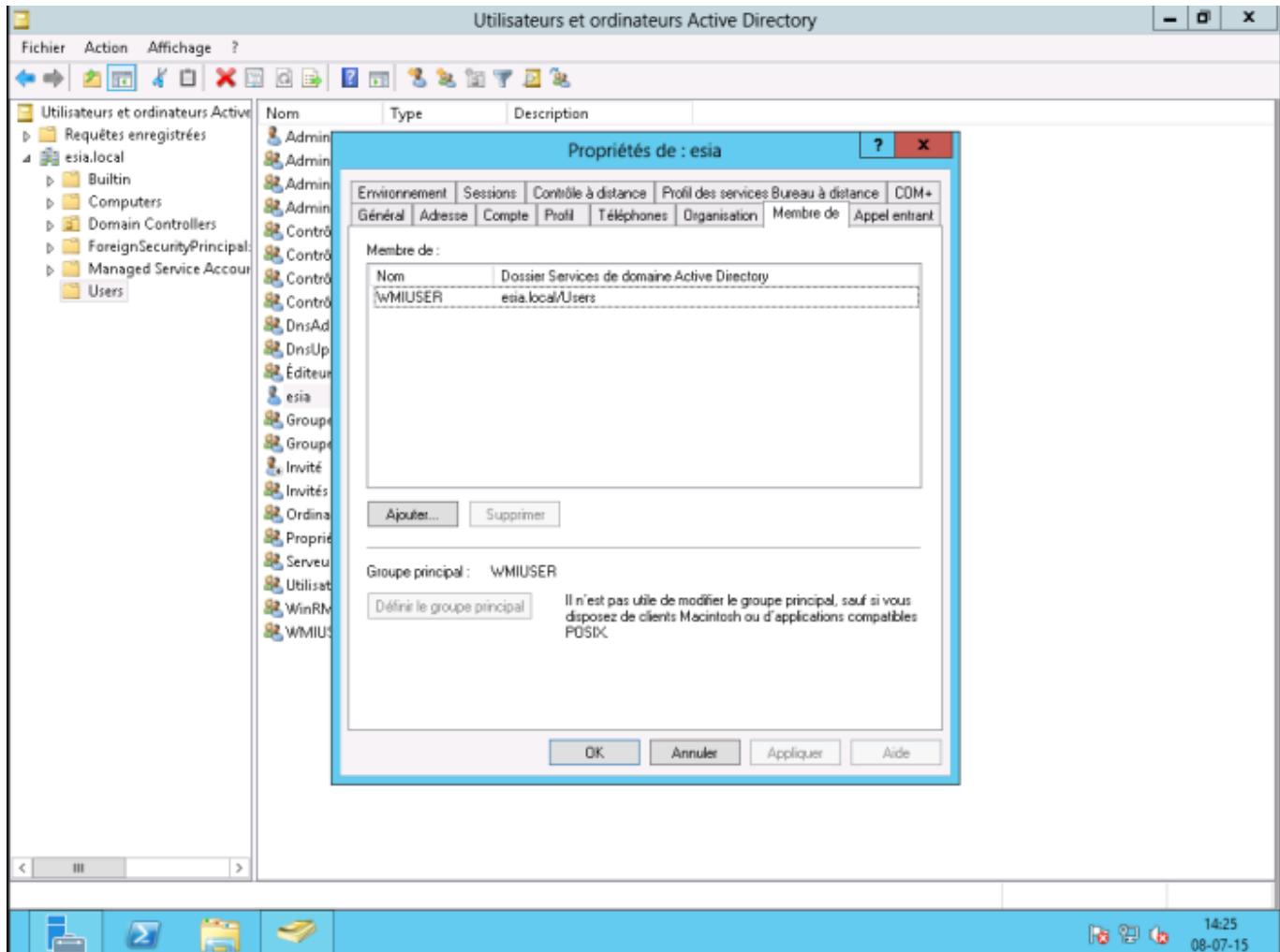
Créer un groupe « WMIUSER » avec un domaine global et comme type de groupe : « sécurité ».



Faites un clic droit sur l'utilisateur Esia et allez dans l'onglet « Membre de » et ajoutez le au groupe WMIUSER. Définissez le groupe WMIUSER comme groupe principal et supprimez-le du groupe « Utilisateur du domaine »



Vous devriez avoir ceci :

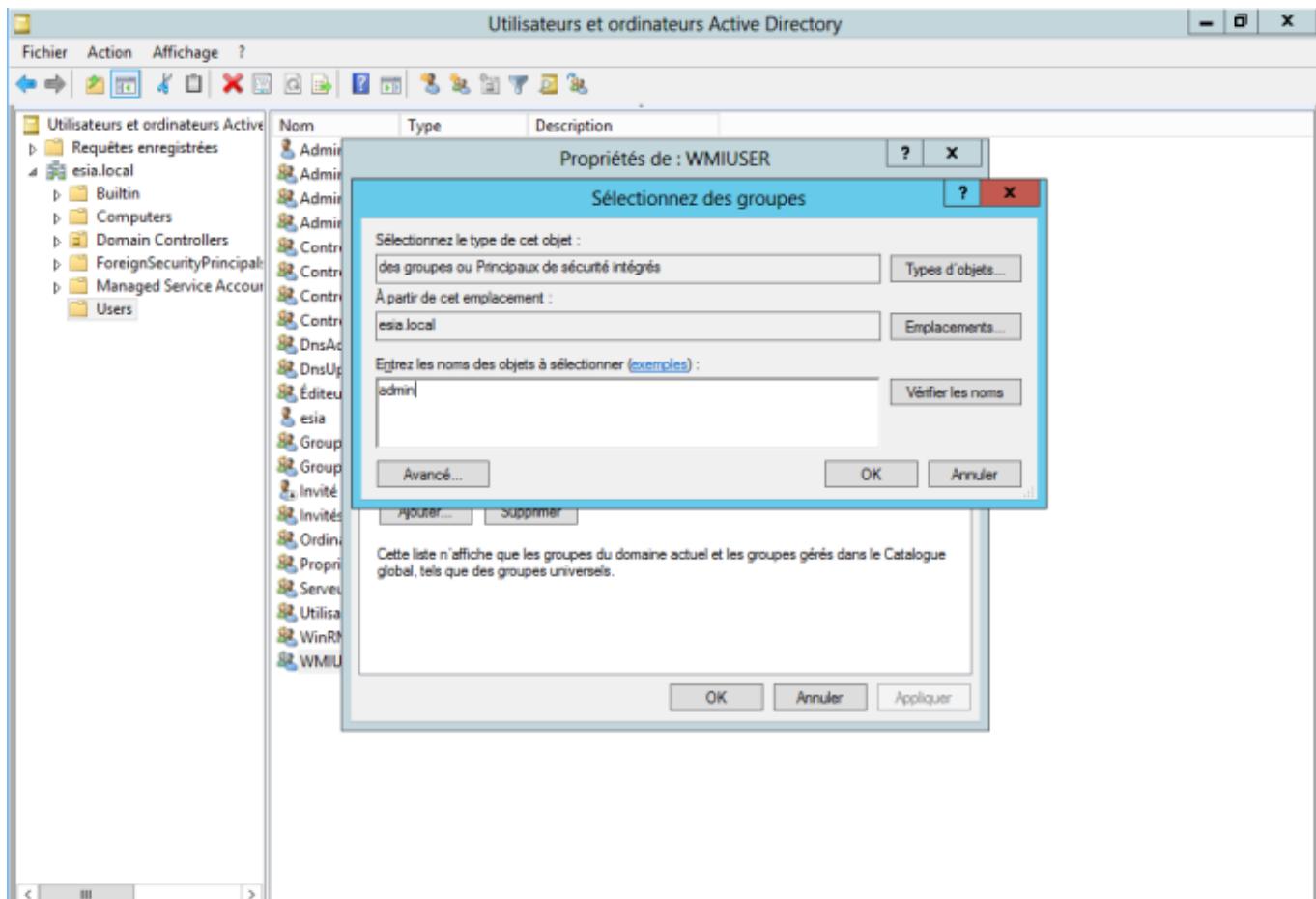


Maintenant 2 solutions s'offrent à vous. Ajoutez le groupe WMIUSER au groupe "**Admins du domaine**", mais ce n'est pas sécurisé ou alors faire une manipulation sur chacune des machines pour autoriser un utilisateur non-administrateur à se connecter.

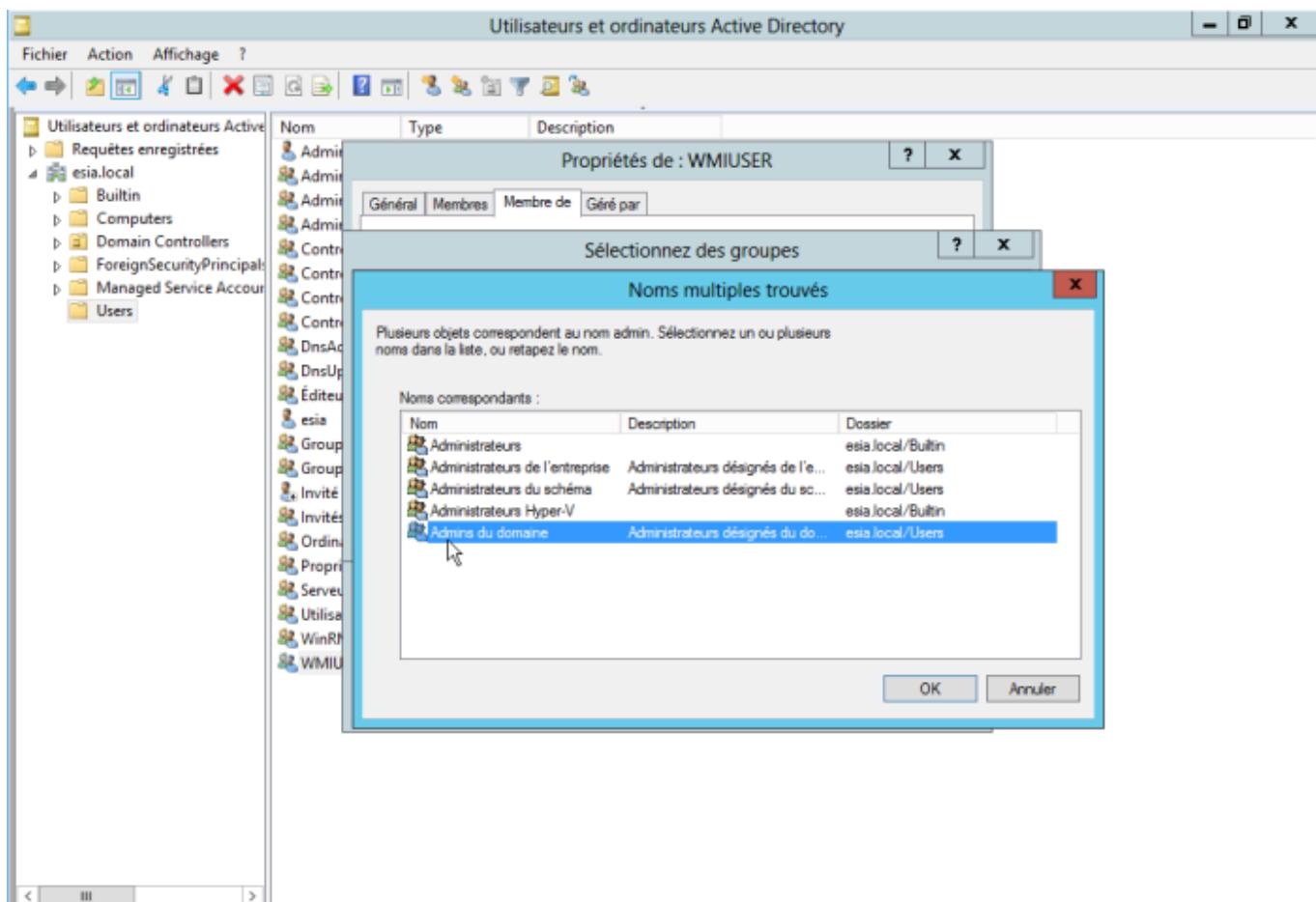
Ajout du groupe WMIUSER en tant qu'administrateur

Pour ajouter le groupe WMIUSER au groupe « Admins du domaine », faites un clic droit sur celui-ci et allez dans « propriété ». Ensuite, allez dans l'onglet « Membre de » et cliquez sur « Ajouter ».

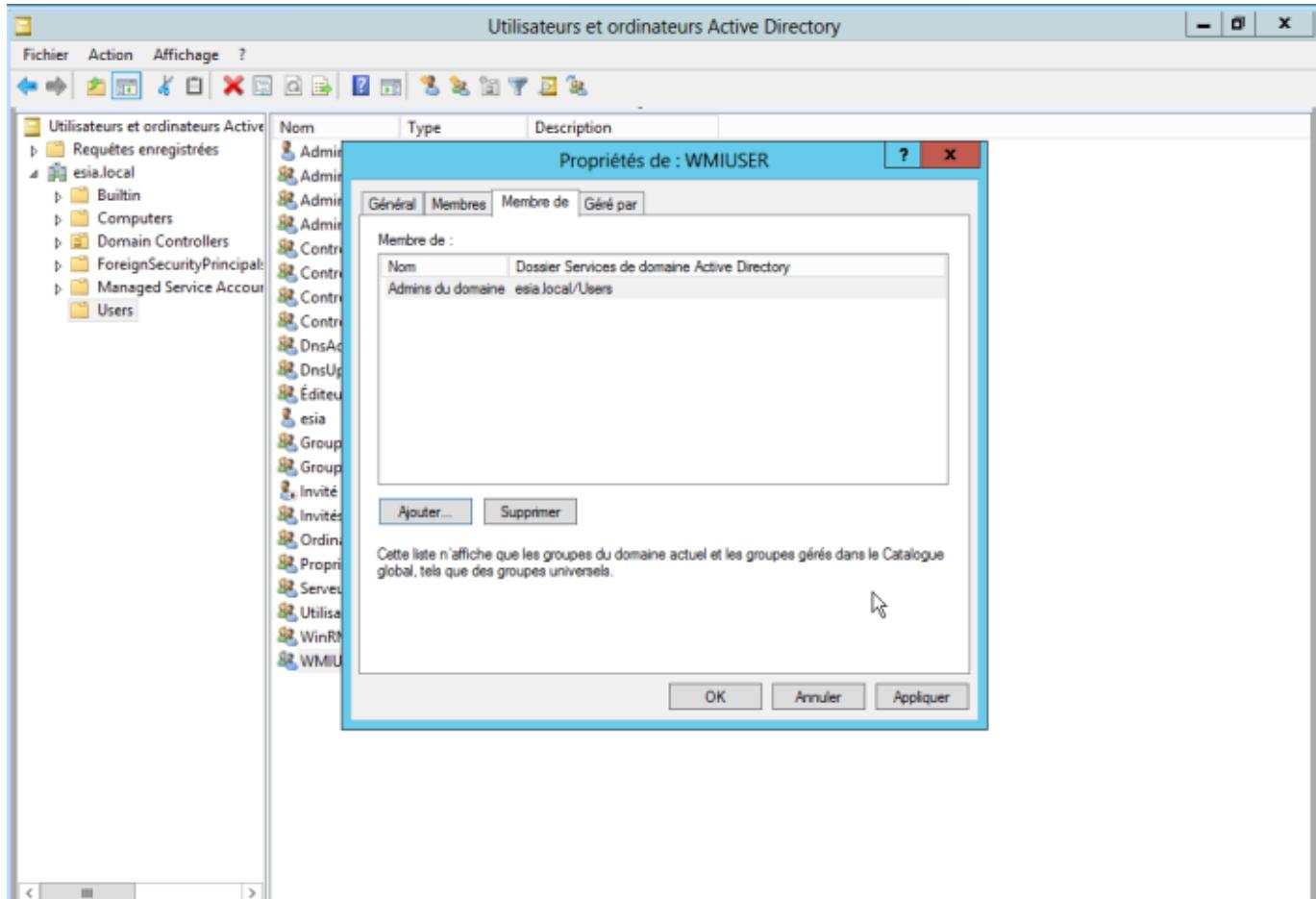
Tapez « admin » puis cliquez sur « Vérifiez les noms »



Sélectionnez, "admin du domaine" et cliquez sur OK.

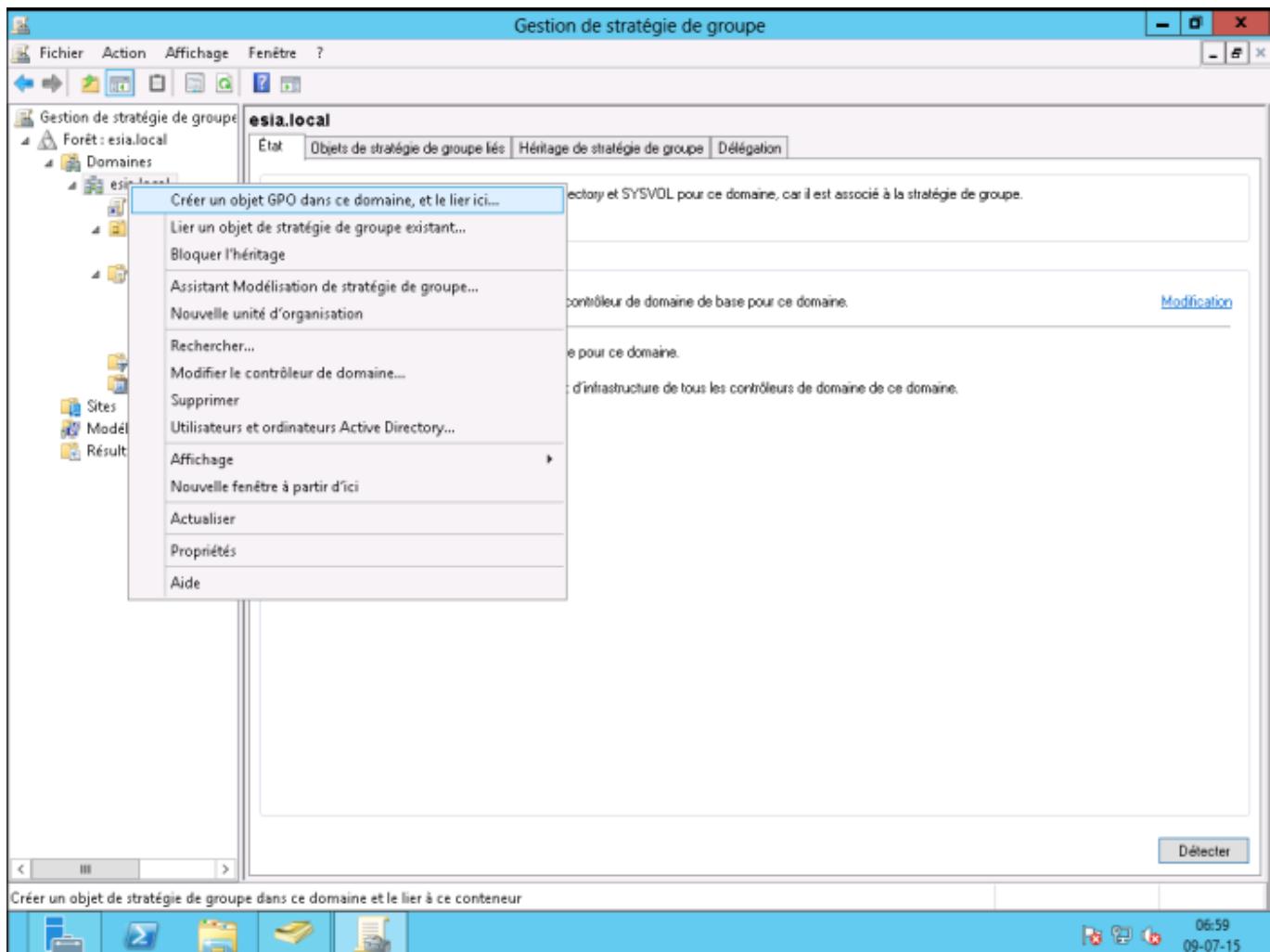


Pour finir, cliquez sur OK.

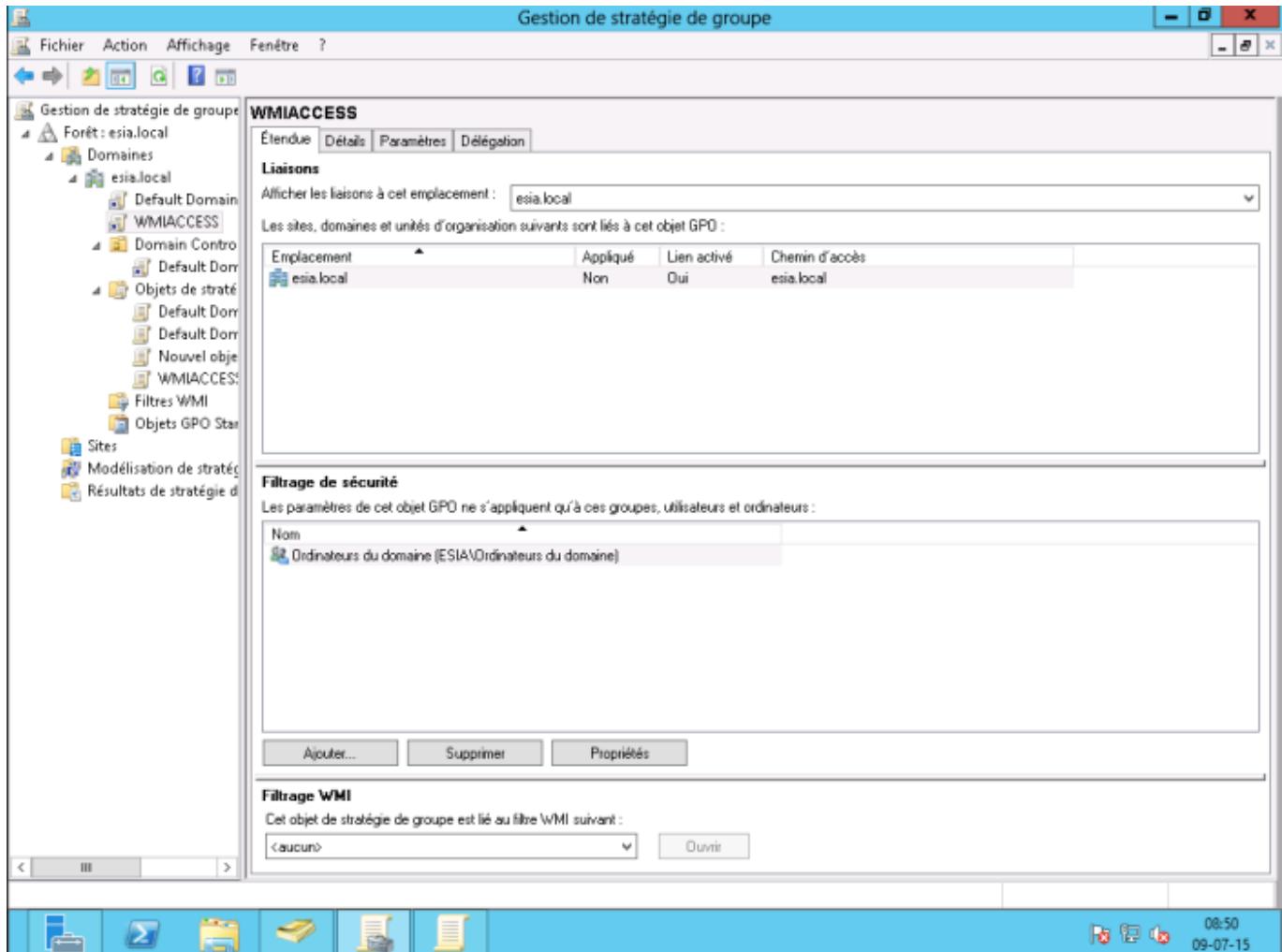


Création de la GPO (Groups Policies Objects)

Ouvrez la “Gestion de stratégie de groupe” de votre Active Directory. Faites un clic droit sur votre domaine et créez une nouvelle GPO (ici : WMIACCESS)



Dans les filtrages de sécurité, supprimez « utilisateurs authentifiés » et ajoutez « ordinateurs du domaine »



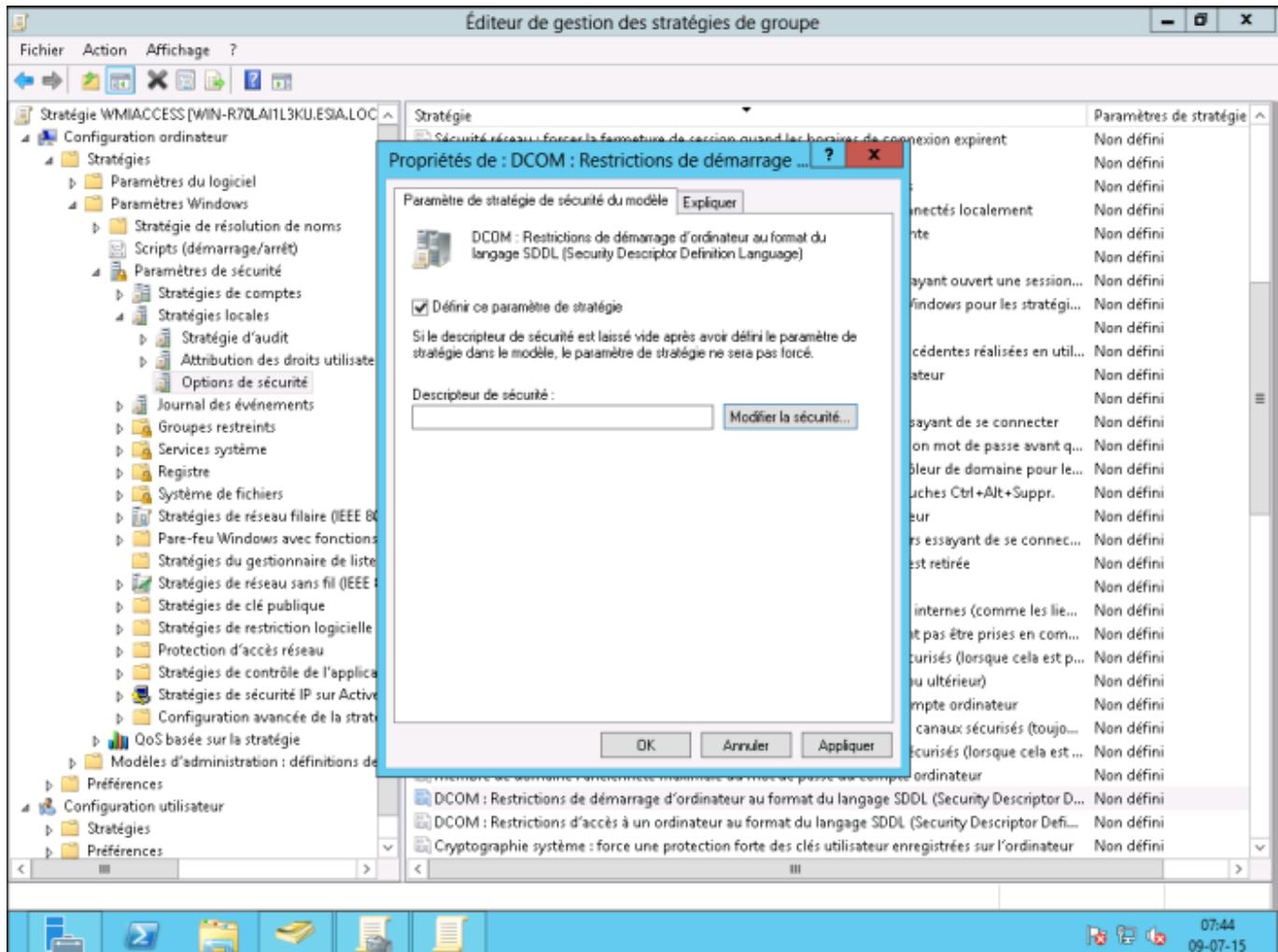
Dans l'onglet paramètre, faites un clic droit et allez ensuite sur "modifier les paramètres". Dans Configuration de l'ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Option de sécurité

Éditeur de gestion des stratégies de groupe

Stratégie

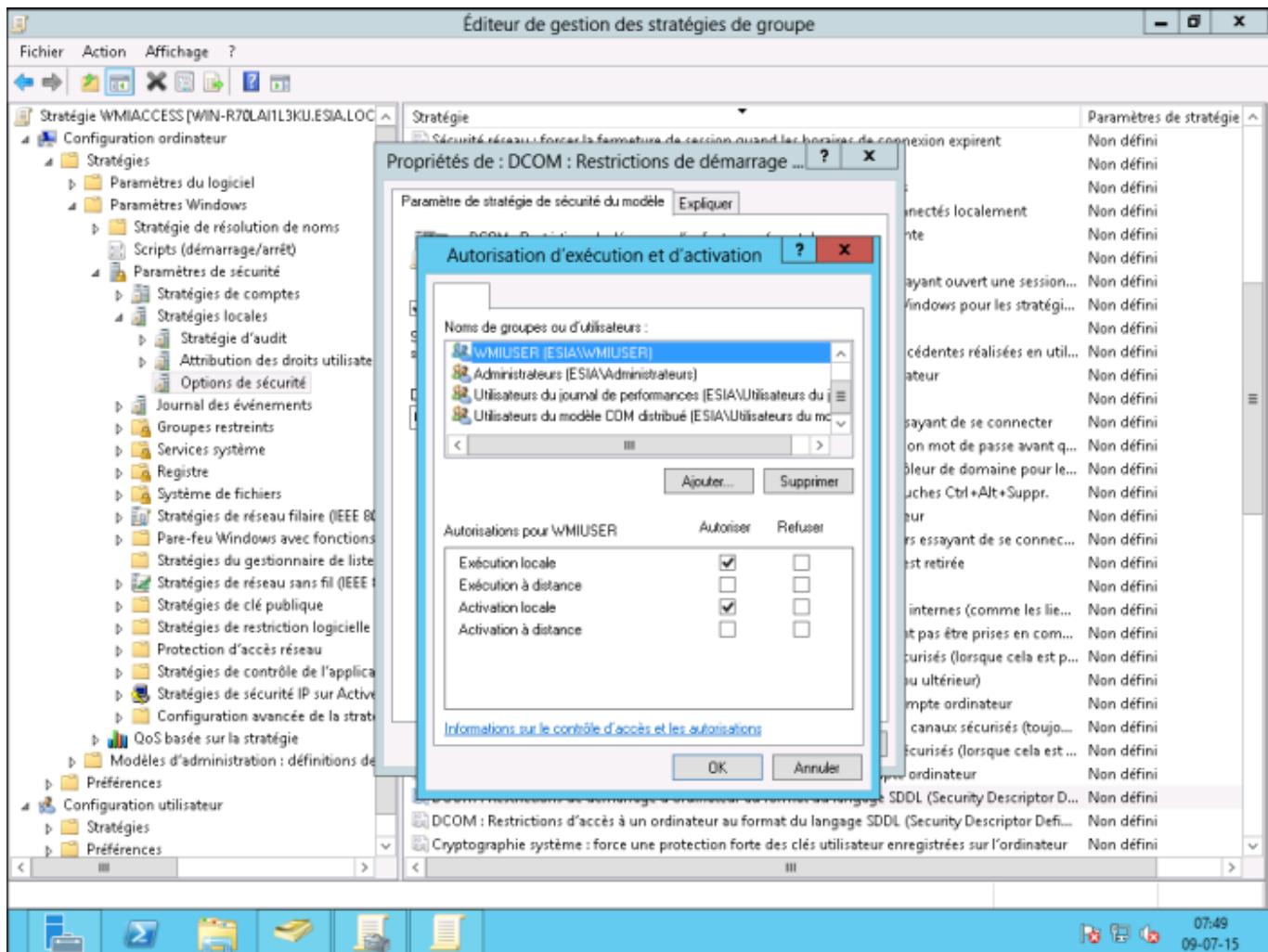
	Paramètres de stratégie
Sécurité réseau : conditions requises pour la signature de client LDAP	Non défini
Pérophériques : permettre le formatage et l'éjection des médias amovibles	Non défini
Pérophériques : ne permettre l'accès aux disques qu'aux utilisateurs connectés localement	Non défini
Pérophériques : empêcher les utilisateurs d'installer des pilotes d'imprimante	Non défini
Pérophériques : autoriser le retrait sans ouverture de session préalable	Non défini
Pérophériques : autoriser l'accès au CD-ROM uniquement aux utilisateurs ayant ouvert une session	Non défini
Paramètres système : utiliser les règles de certificat avec les exécutables Windows pour les stratégies	Non défini
Paramètres système : Sous-systèmes optionnels	Non défini
Ouvertures de sessions interactives : nombre d'ouvertures de sessions précédentes réalisées en utilis...	Non défini
Ouverture de session interactive : seuil de verrouillage du compte d'ordinateur	Non défini
Ouverture de session interactive : limite d'inactivité de l'ordinateur	Non défini
Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter	Non défini
Ouverture de session interactive : prévenir l'utilisateur qu'il doit changer son mot de passe avant q...	Non défini
Ouverture de session interactive : nécessite l'authentification par le contrôleur de domaine pour le...	Non défini
Ouverture de session interactive : ne pas demander la combinaison de touches Ctrl+Alt+Suppr.	Non défini
Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur	Non défini
Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter	Non défini
Ouverture de session interactive : comportement lorsque la carte à puce est retirée	Non défini
Ouverture de session interactive : carte à puce nécessaire	Non défini
Objets système : renforcer les autorisations par défaut des objets système internes (comme les lie...	Non défini
Objets système : les différences entre majuscules et minuscules ne doivent pas être prises en com...	Non défini
Membre de domaine : signer numériquement les données des canaux sécurisés (lorsque cela est poss...	Non défini
Membre de domaine : nécessite une clé de session forte (Windows 2000 ou ultérieur)	Non défini
Membre de domaine : désactive les modifications de mot de passe du compte ordinateur	Non défini
Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujo...	Non défini
Membre de domaine : chiffrer numériquement les données des canaux sécurisés (lorsque cela est poss...	Non défini
Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur	Non défini
DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL (Security Descriptor D...	0:BAG:BAD:(A;;CCDCS...
DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Defi...	0:BAG:BAD:(A;;CCDCCL...
Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur	Non défini
Contrôleur de domaine : refuser les modifications de mot de passe du compte ordinateur	Non défini

Double-cliquez sur « DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL ». Ensuite, sélectionnez la case « définir ce paramètre de sécurité » et cliquez ensuite sur « Modifier la sécurité »



Cliquez sur « Ajouter », tapez WMIUSER (le nom de votre groupe de gestion WMI). Cliquez sur OK.

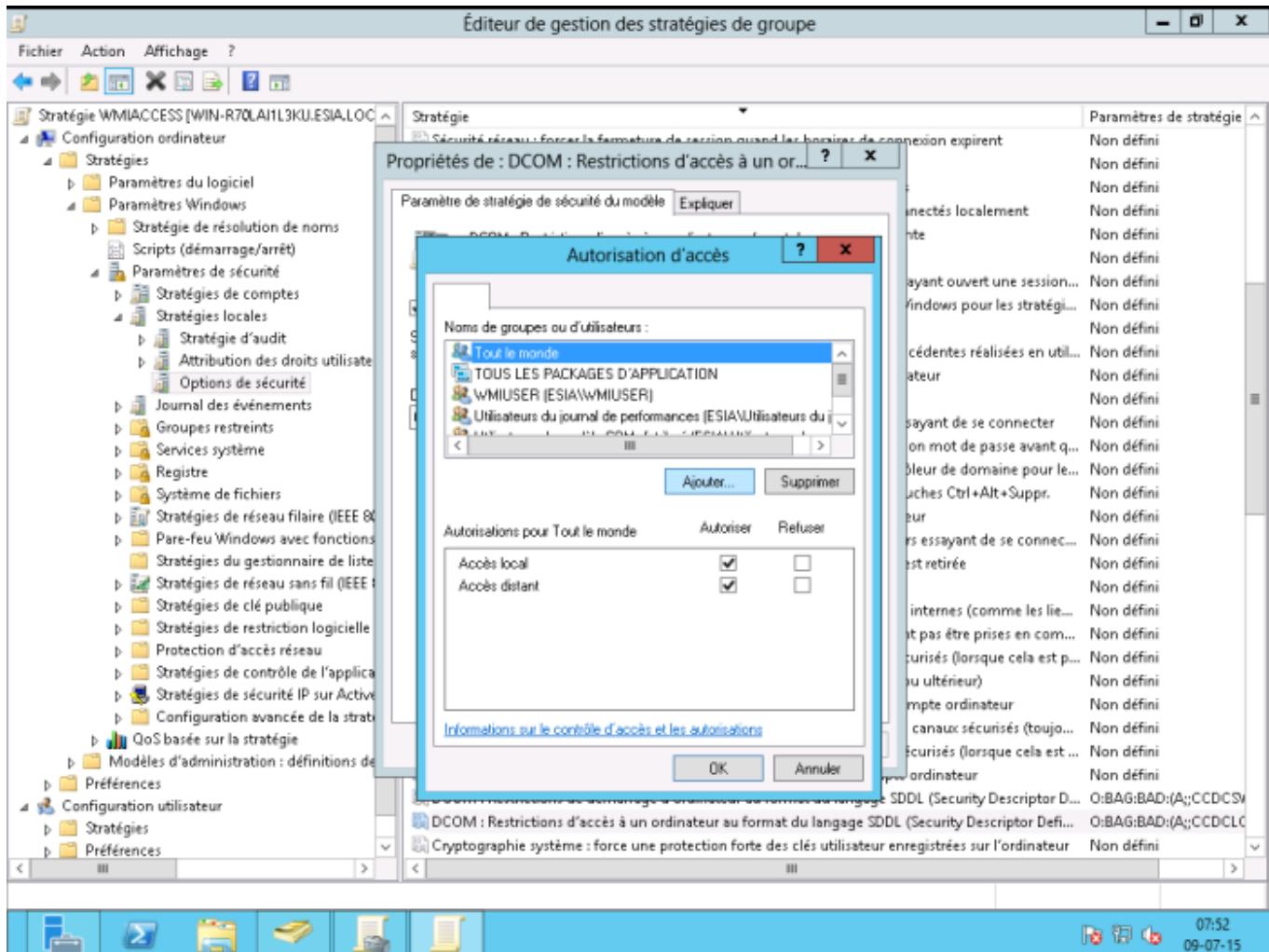
Cocher les cases « Exécution locale » et Exécution à distance ». Cliquez sur OK et de nouveau sur OK.



Double-cliquez sur «DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL». Ensuite, sélectionnez la case « définir ce paramètre de sécurité » et cliquez ensuite sur « Modifier la sécurité »

Cliquez sur « Ajouter », tapez WMIUSER (le nom de votre groupe de gestion WMI). Cliquez sur OK.

Cocher les cases «Accès local » et Accès à distance ». Cliquez sur OK et de nouveau sur OK.



Ne pas oublier de faire un gupdate /force

Configuration du pare-feu Windows

<HTML>

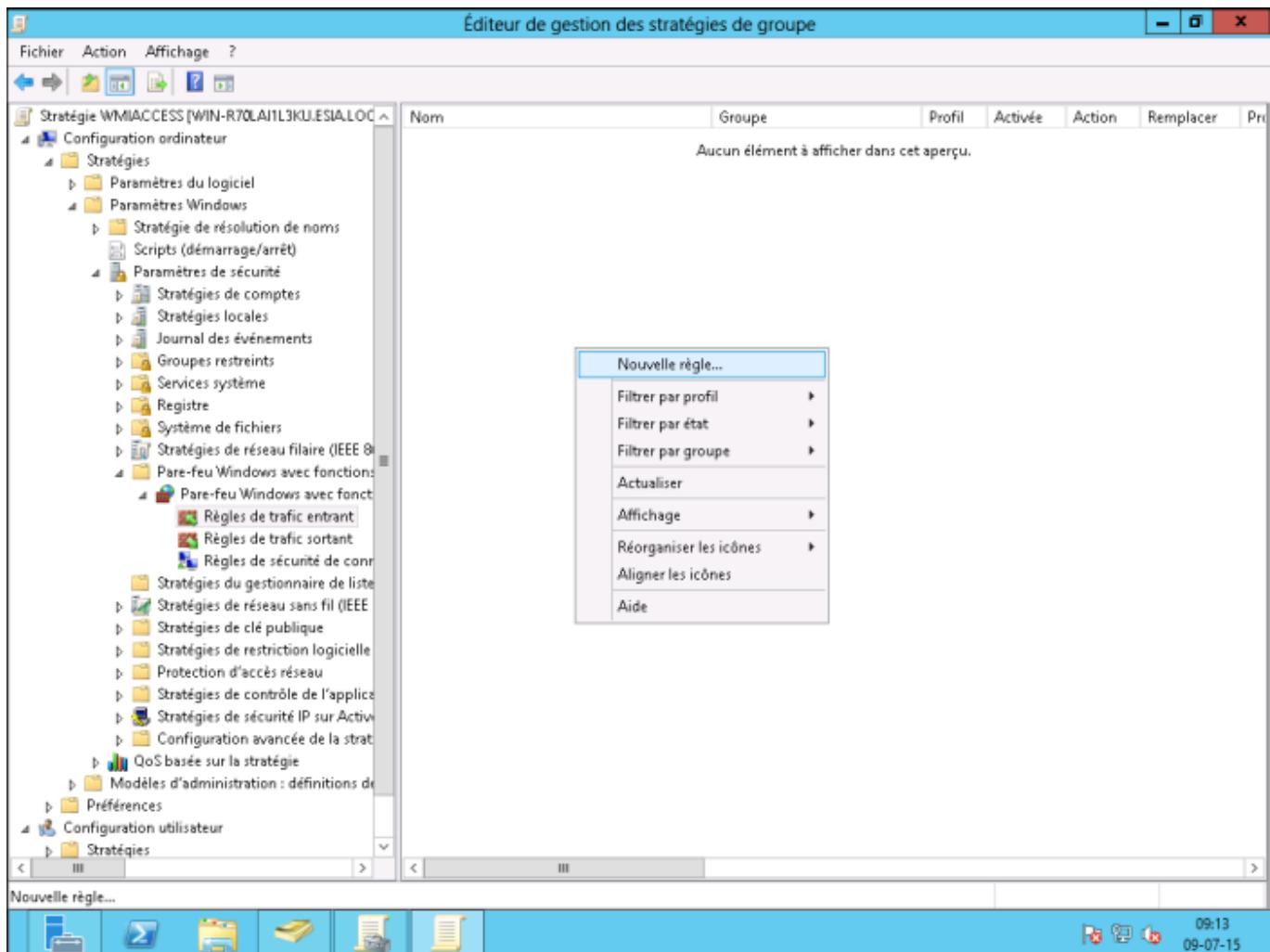
```

<style>
    #configuration_du_pare-feu_windows:after {content: " (Si nécessaire)";
font-size:.75em; font-weight:500;}
</style>

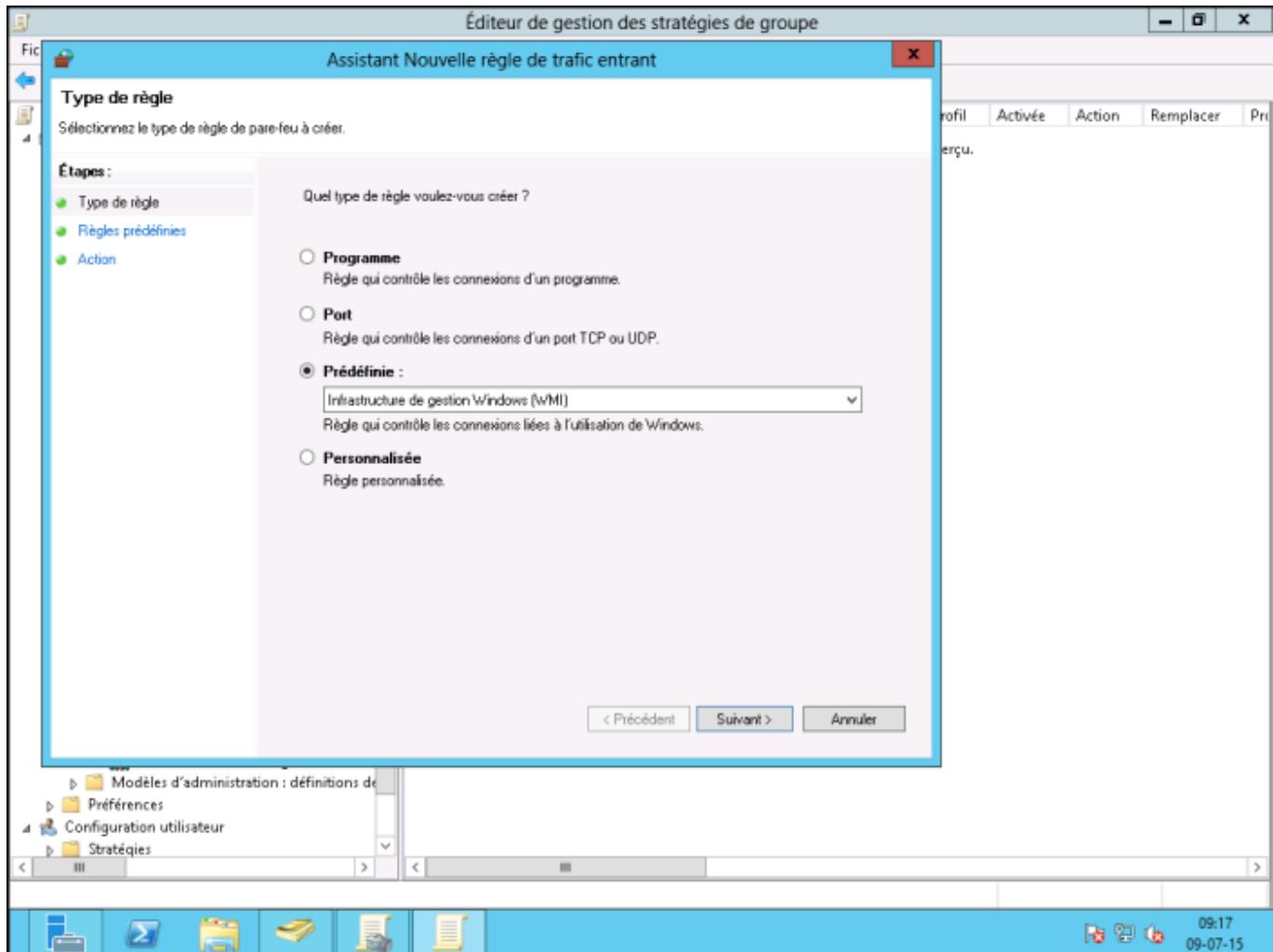
```

</HTML> Dans votre GPO, allez dans Configuration de l'ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Pare-feu Windows avec fonctions avancées de sécurité → Pare-feu Windows avec fonctions avancées de sécurité → Règles de trafic entrant.

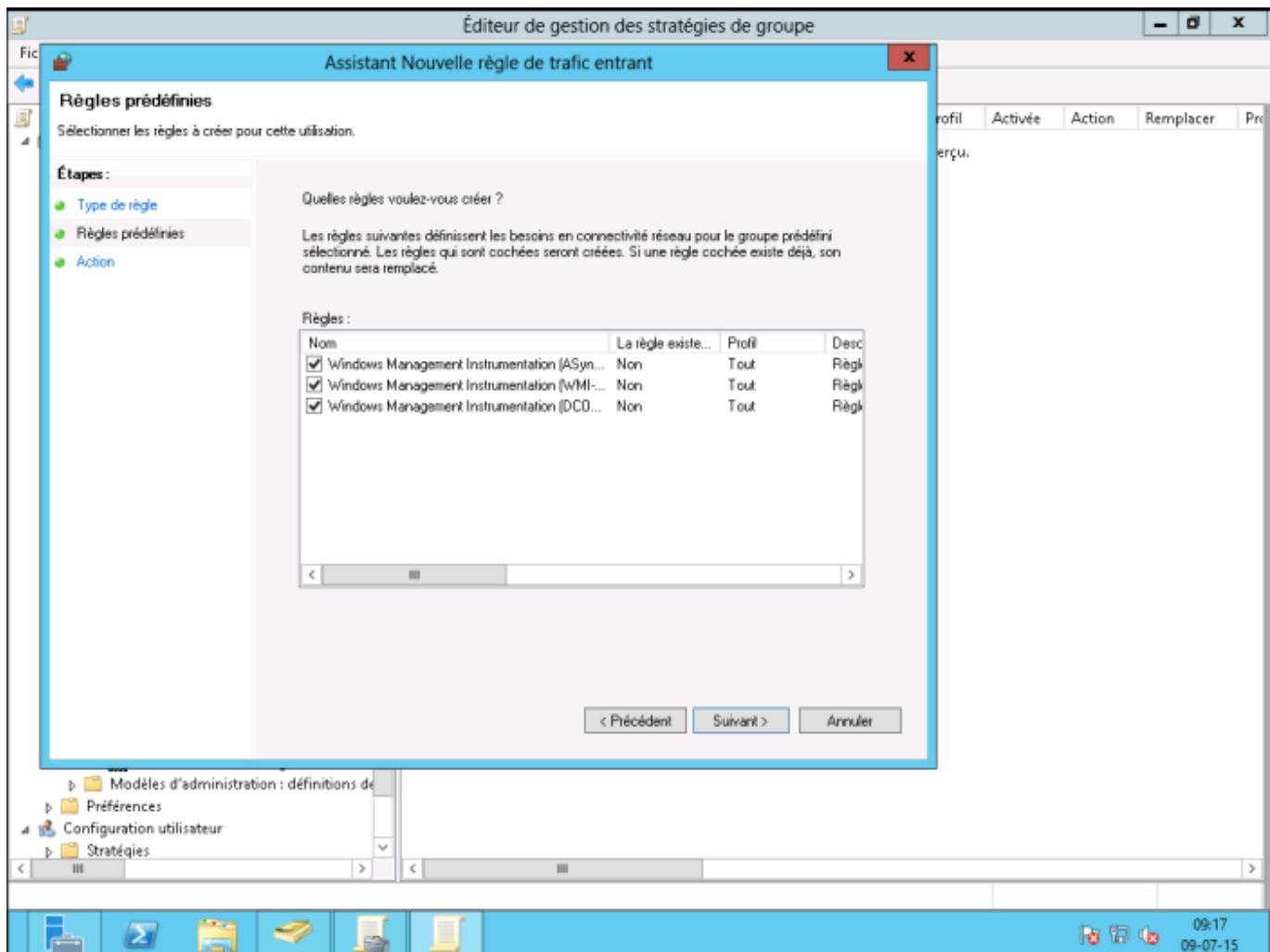
Faites un clic droit pour créer une « Nouvelle règle ... »



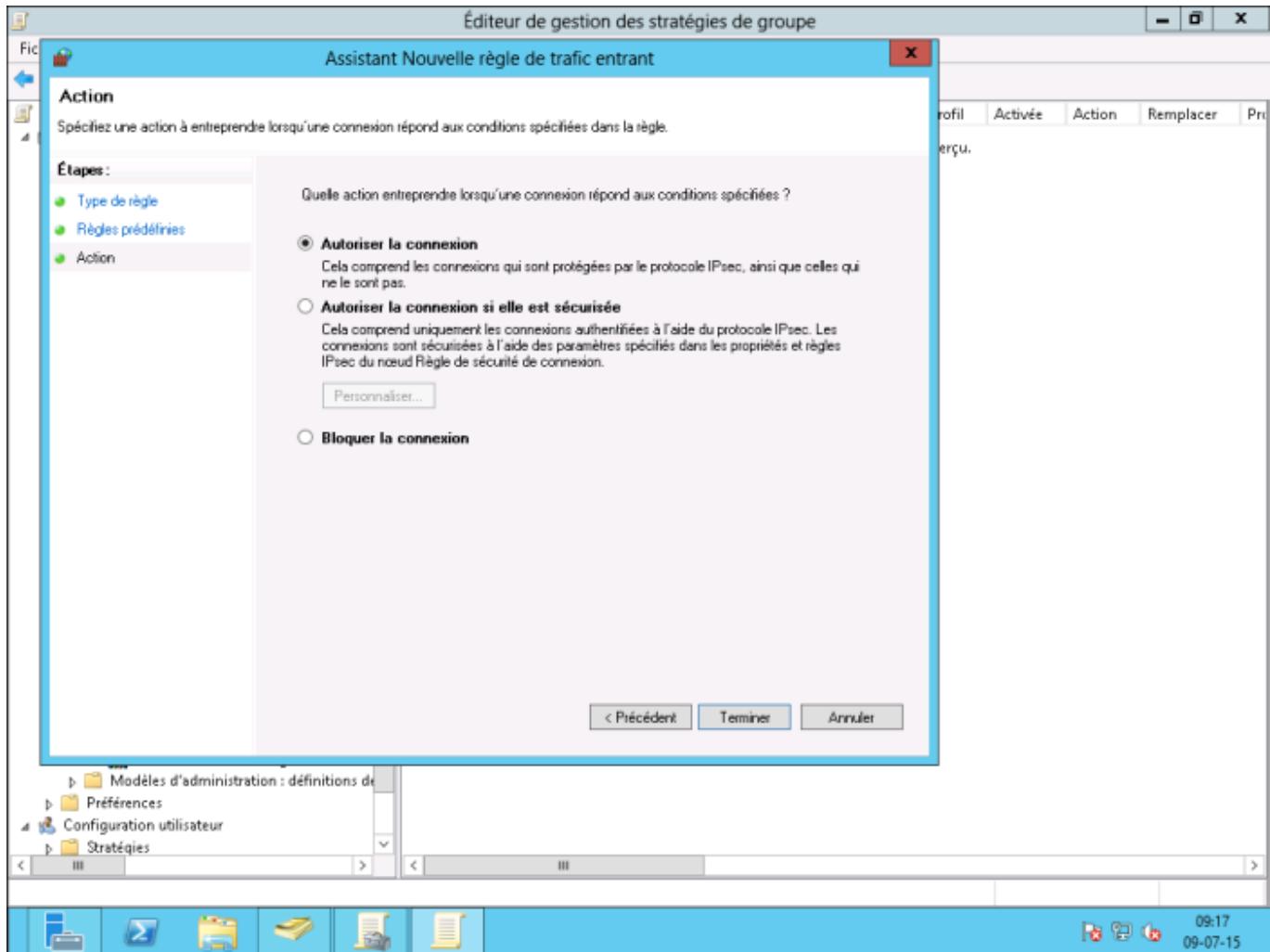
Sélectionnez « Prédéfinie » et choisissez « Infrastructure de gestion WMI ». Cliquez sur suivant.



3 règles de base seront créées, cliquez sur suivant.



Laissez sélectionné « Autoriser la connexion » et cliquez sur terminer.



Ne pas oublier de faire un gupdate /force

Ajout du groupe WMIUSER en tant que simple utilisateur

<HTML>

```

<style>
    #ajout_du_groupe_wmiuser_en_tant_que_simple_utilisateur:after
{content: " (OPTION)"; font-size:.75em; font-weight:500;}
</style>

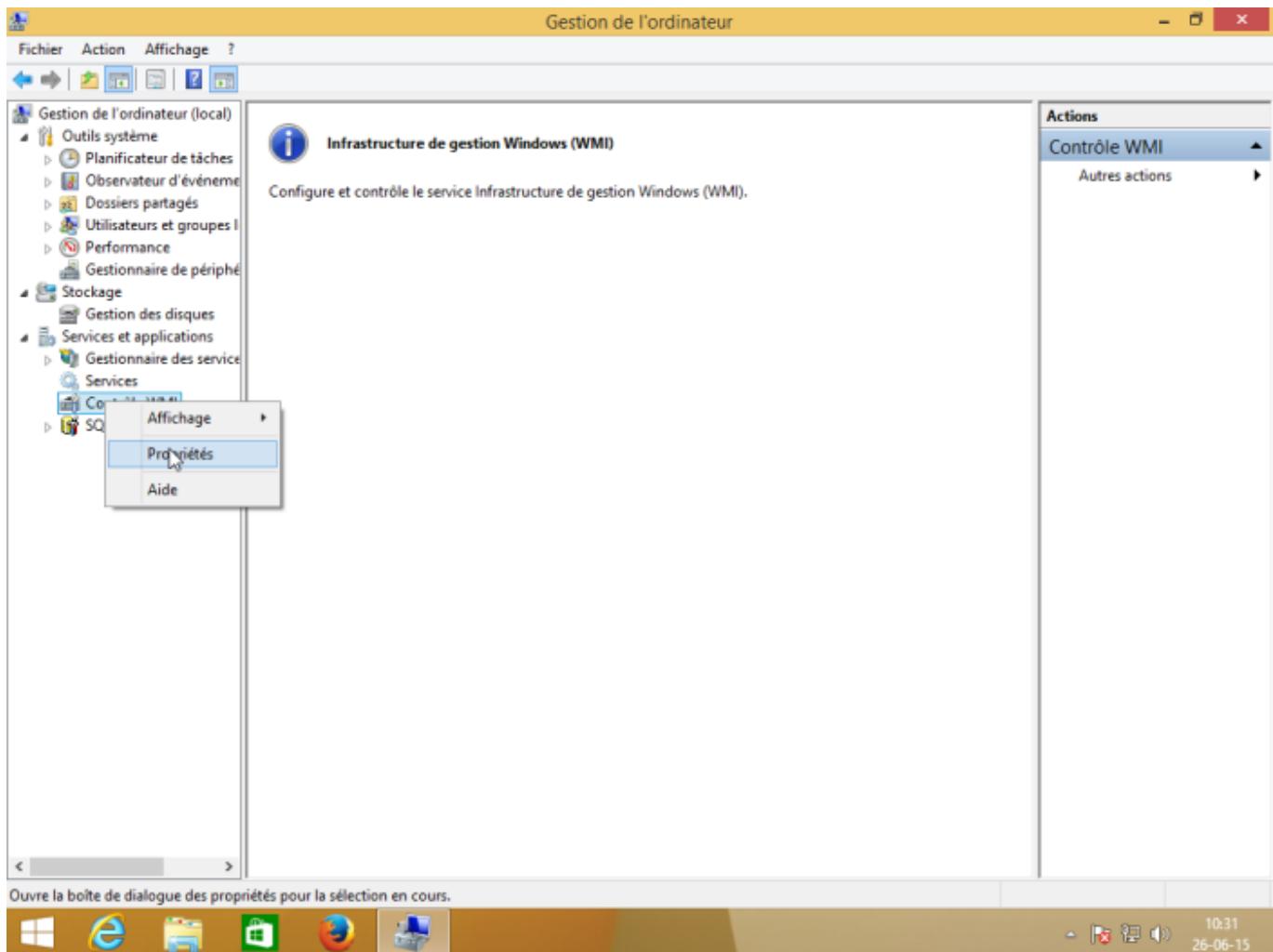
```

</HTML> (! A réaliser sur toute les machines)

Il s'agit ici de donner les droits d'accès distants au compte utilisateur qui sera utilisé par ESIA afin d'accéder aux données WMI. Il est nécessaire de faire cette manipulation sur chacune des machines à interroger.

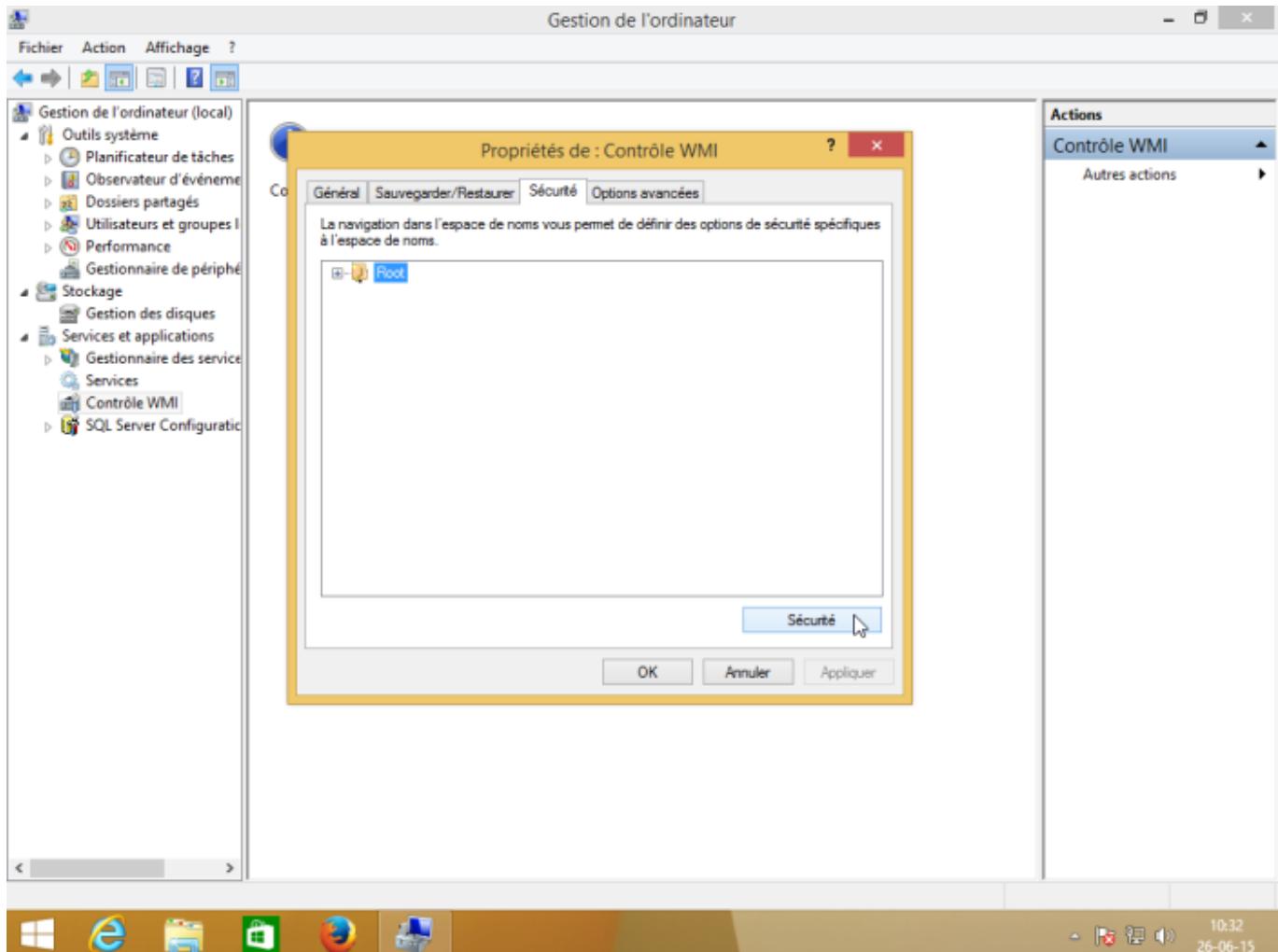
Pour cela :

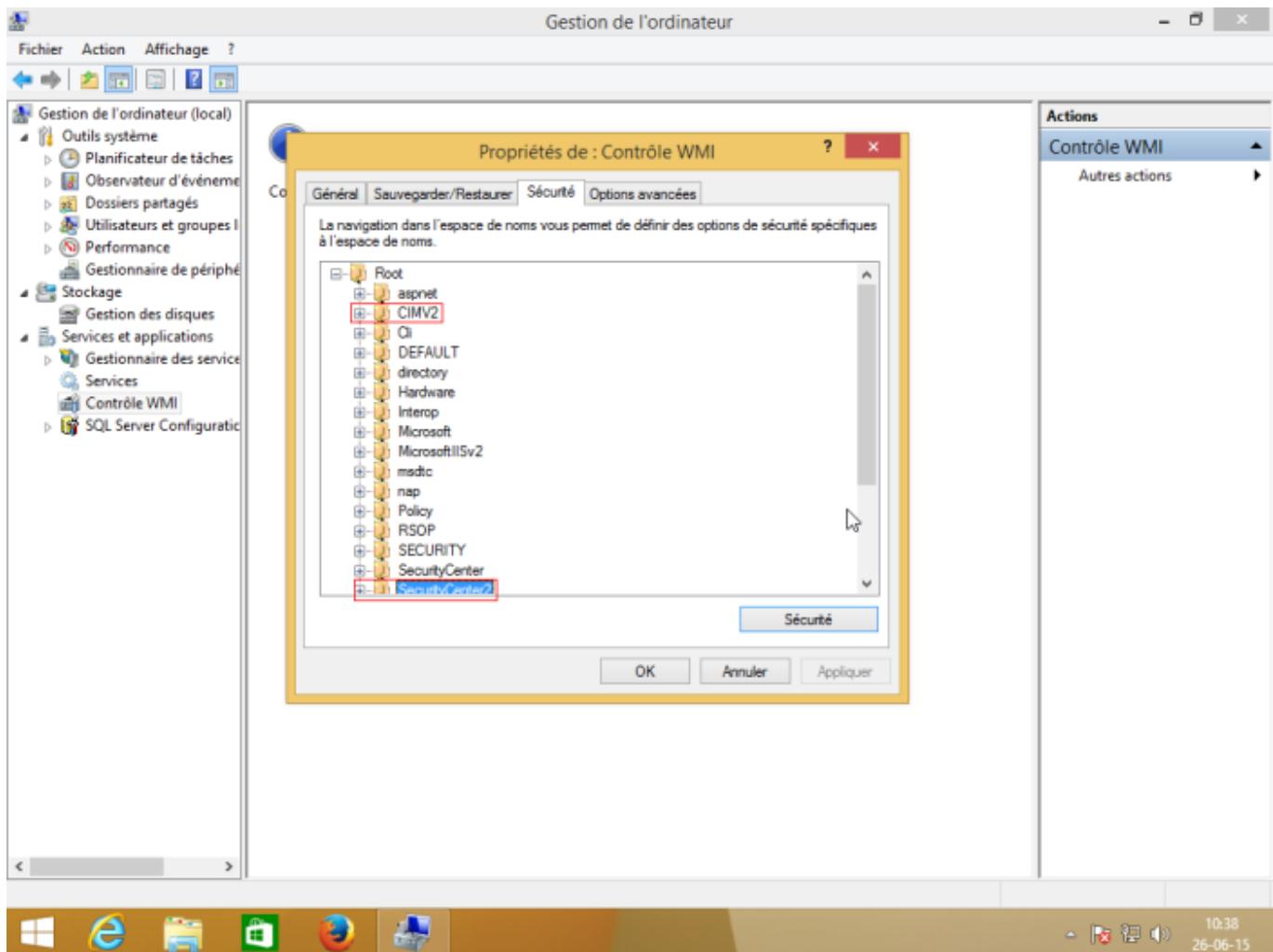
Rendez vous dans « Gestion de l'ordinateur » (ou saisissez la commande «wmimgmt.msc»). Puis, Déroulez « Services et applications » pour pouvoir faire un clic droit sur « Contrôle WMI » et cliquer sur « Propriétés ».



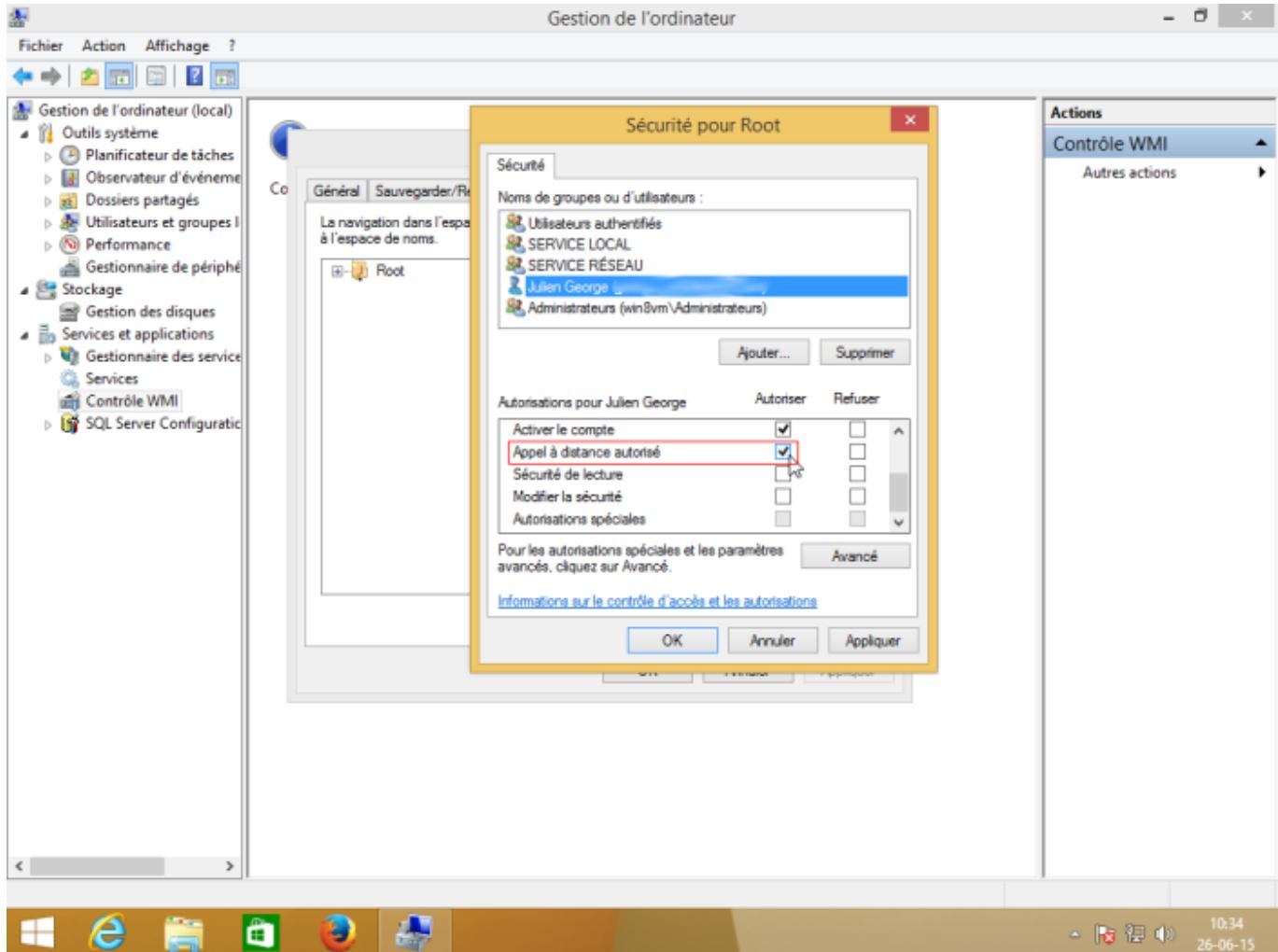
Dans l'onglet « Sécurité » des « Propriétés de : Contrôle WMI », sélectionnez le namespace « Root » et cliquez ensuite sur « Sécurité ».

Si vous souhaitez un réglage plus fin au niveau de la sécurité, les namespaces « Root→CIMV2 » et « Root→SecurityCenter2 » sont ceux utilisés par ESIA.

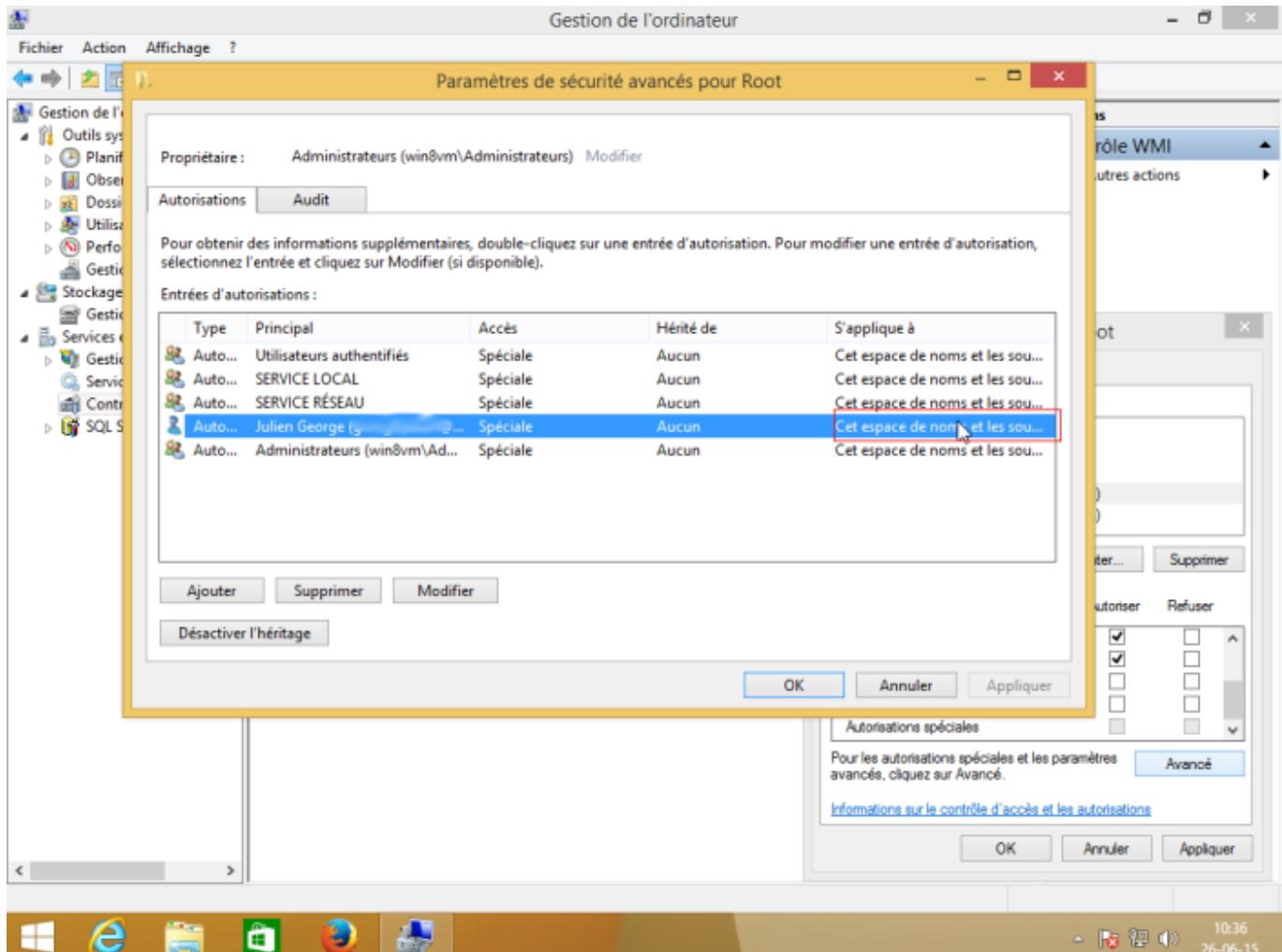




Sélectionnez le compte utilisateur qui sera utilisé pour l'accès distant et cochez les cases « Autoriser » pour « Activer le compte » et « Appel à distance autorisé » qui sont les 2 autorisations nécessaires.



Assurer vous que les autorisations ont été appliquées au namespace sélectionné et à ses sous namespaces en cliquant sur « Avancé » pour vérifier la colonne « S'applique à ».



Voilà, WMI est maintenant activé.

From:
<https://wiki.esia-sa.com/> - **Esia Wiki**

Permanent link:
https://wiki.esia-sa.com/advanced/wmi_win_serveur_2012

Last update: **2023/02/10 10:58**

