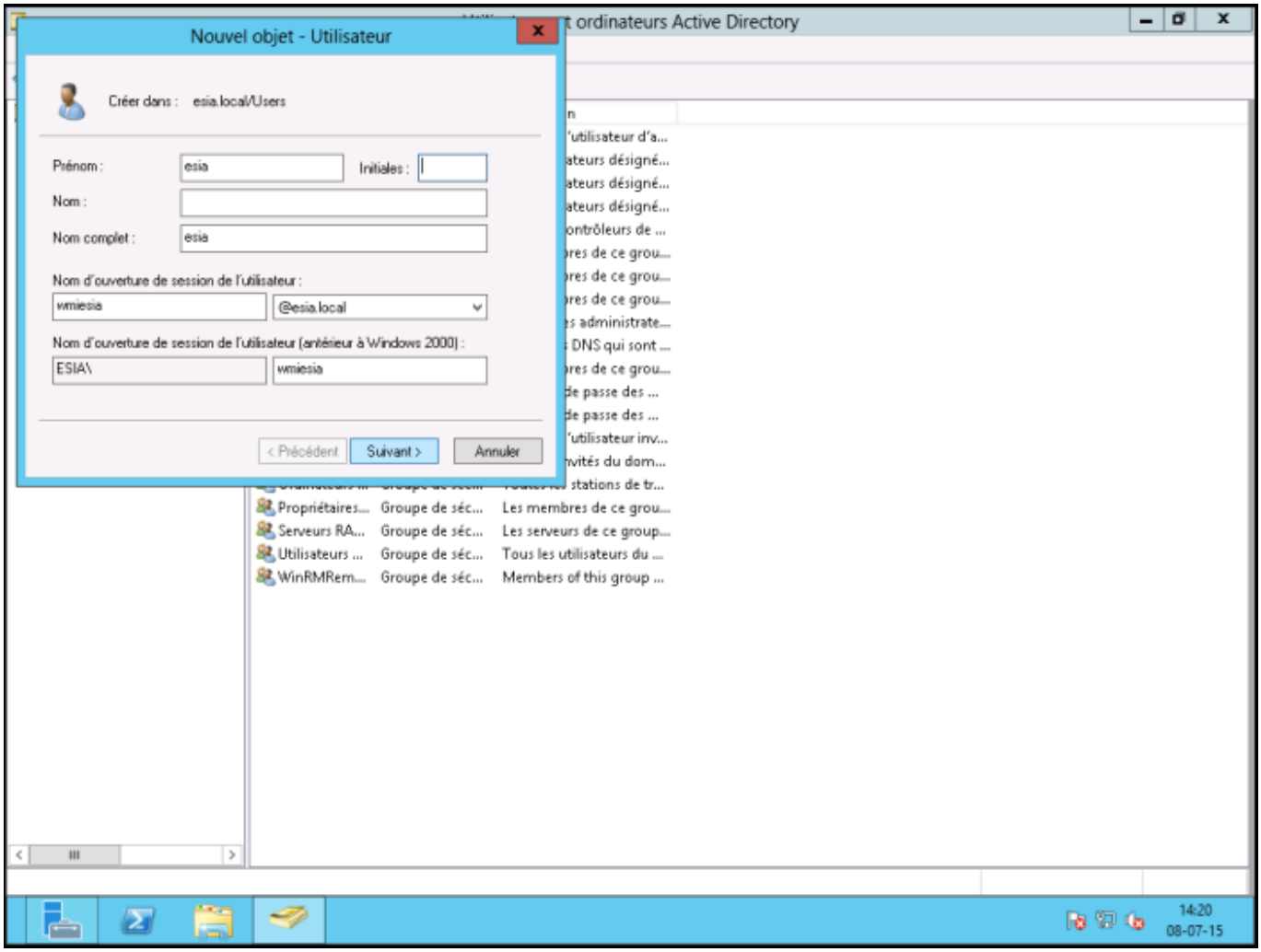
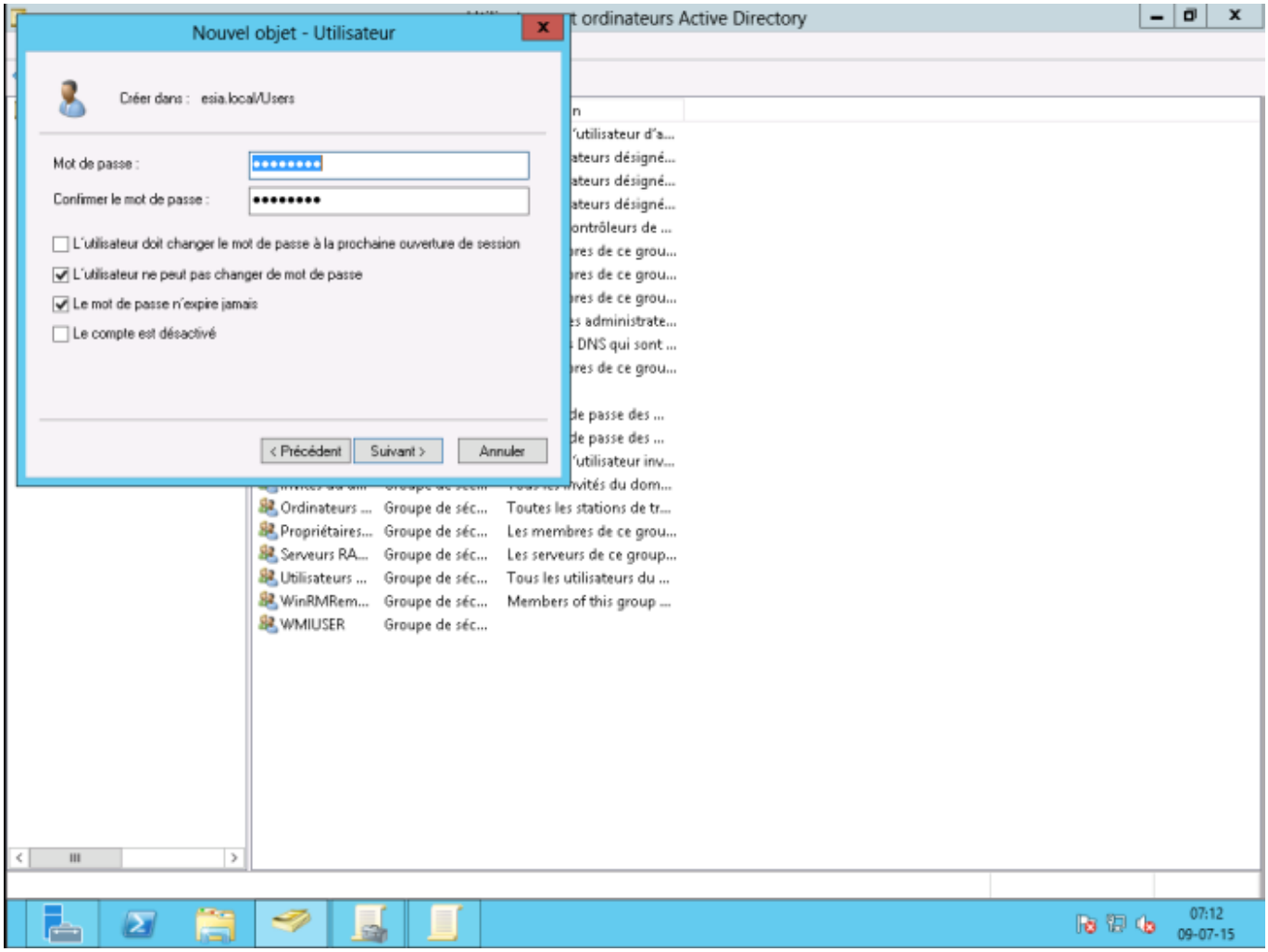
Activer WMI sur Windows Serveur 2012 via GPO

Voici comment activer WMI via les GPO sur un Active Directory

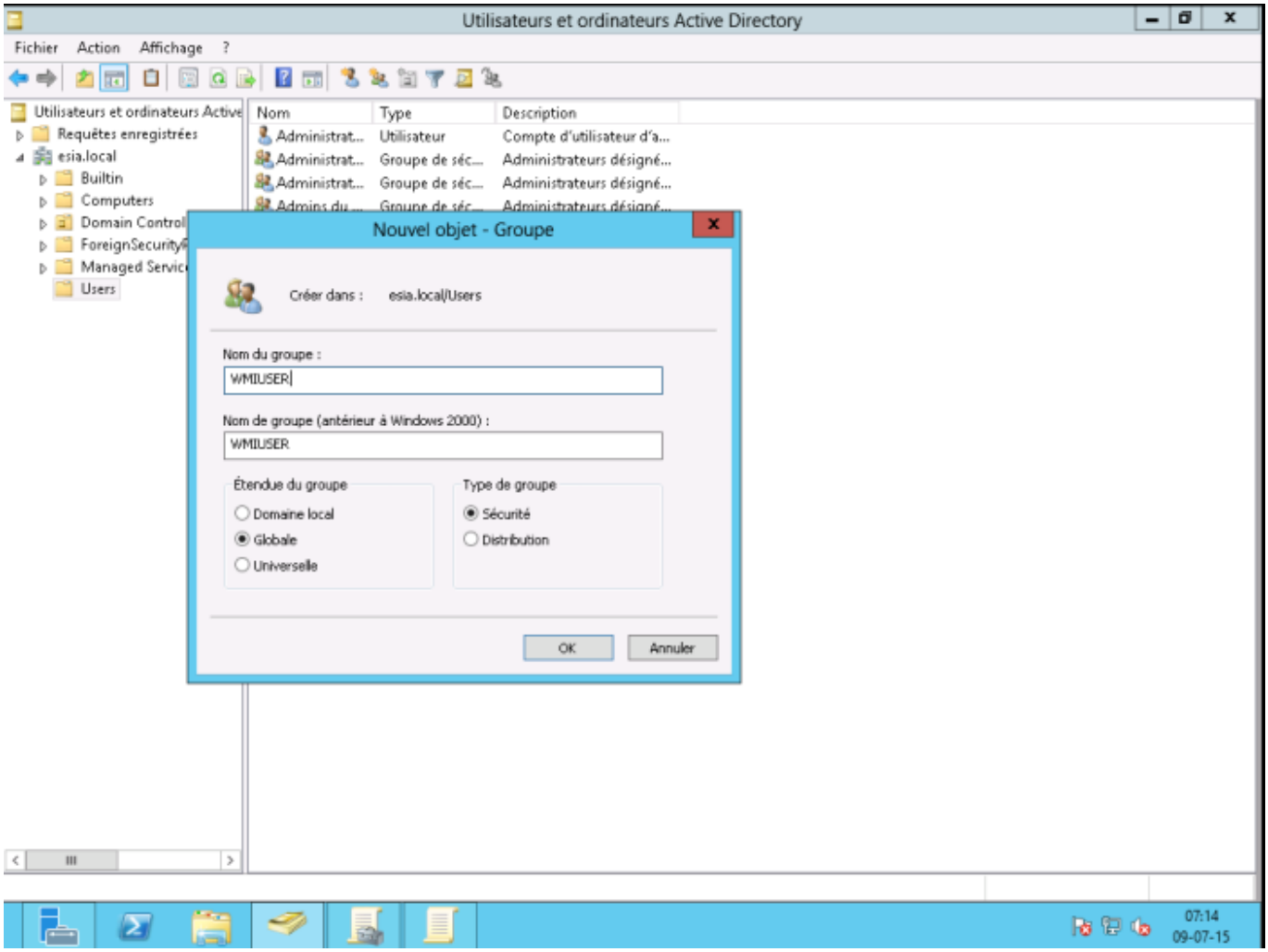
Création de l'utilisateur & du groupe

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 »

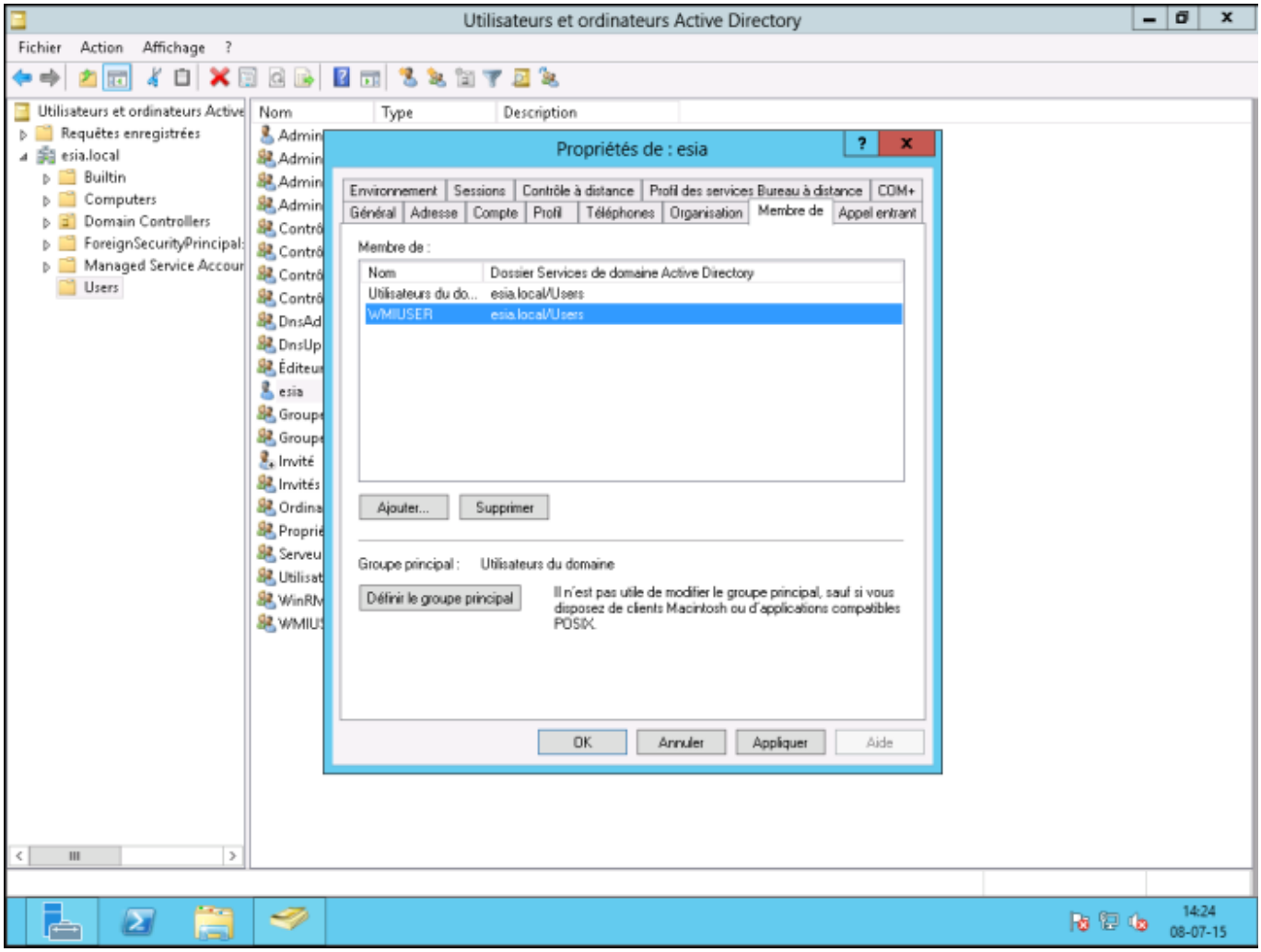




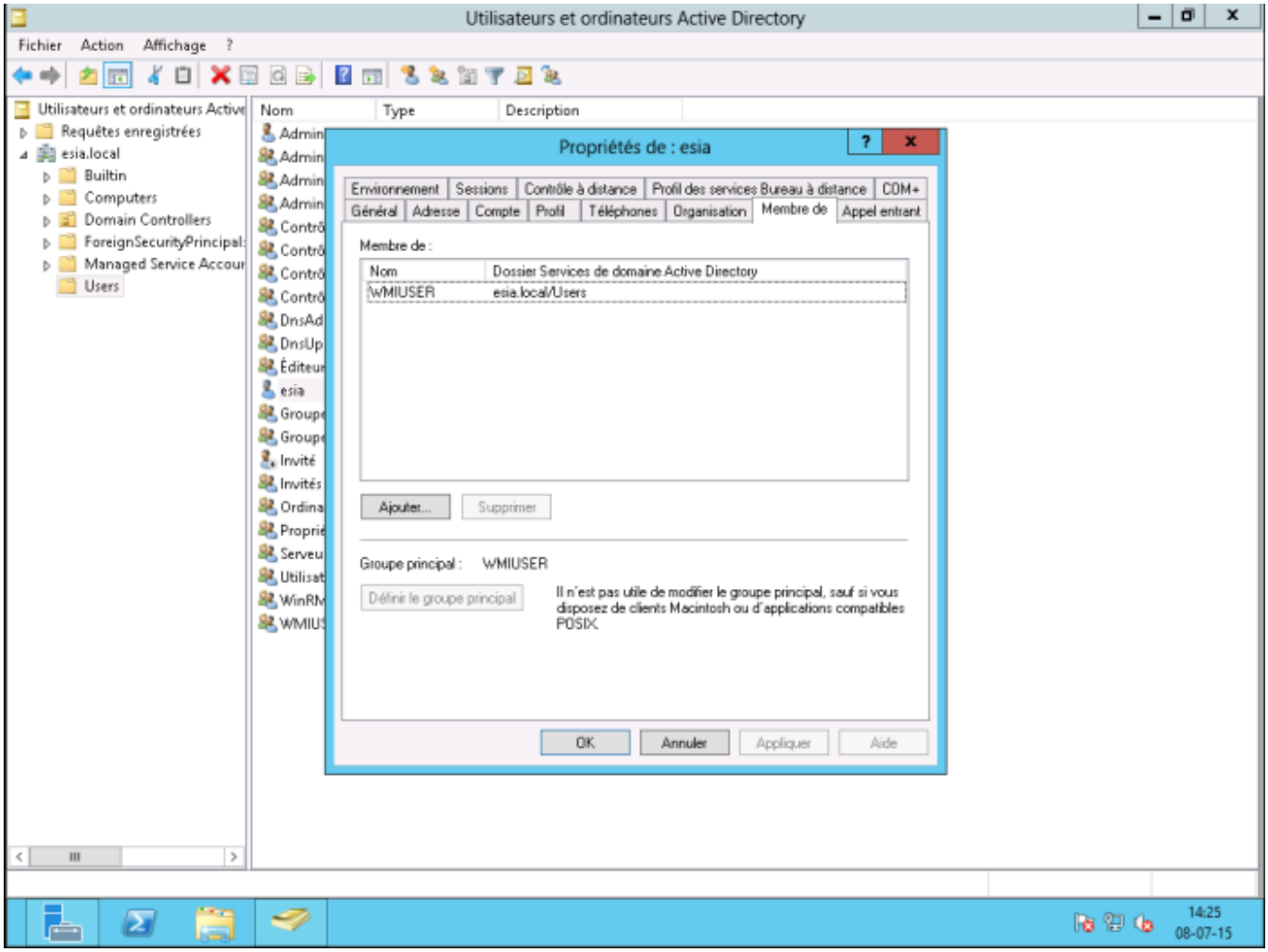
Créer un groupe « WMIUSER » avec un domaine global et comme type de groupe : « sécurité ».



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 :

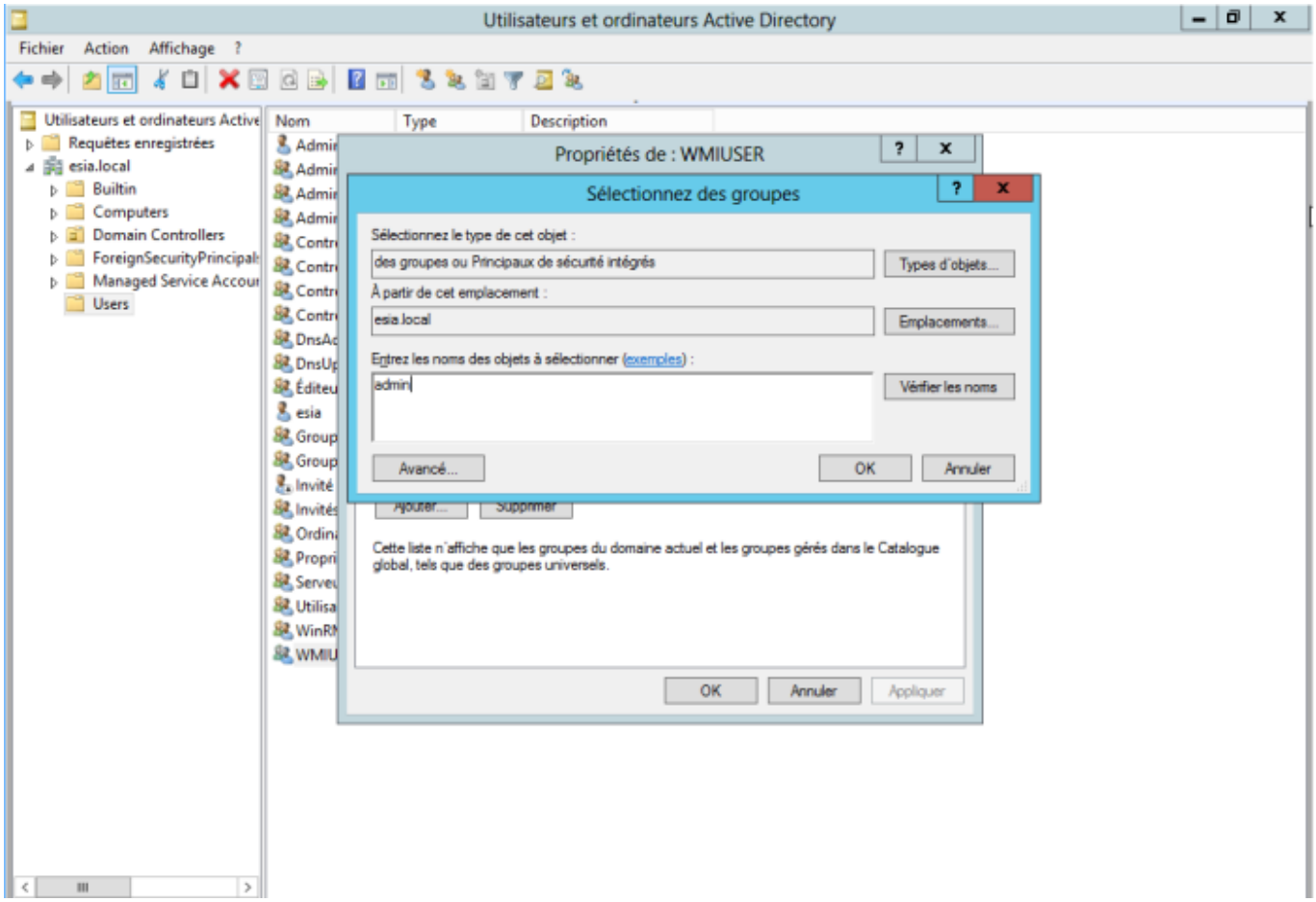


Maintenant 2 solutions s'offrent à vous. Ajoutez le groupe WMIUSER au groupe "**Admins du domaine**", mais ce n'est pas sécurisé ou alors faire une manipulation sur chacune des machines pour autoriser un utilisateur non-administrateur à se connecter.

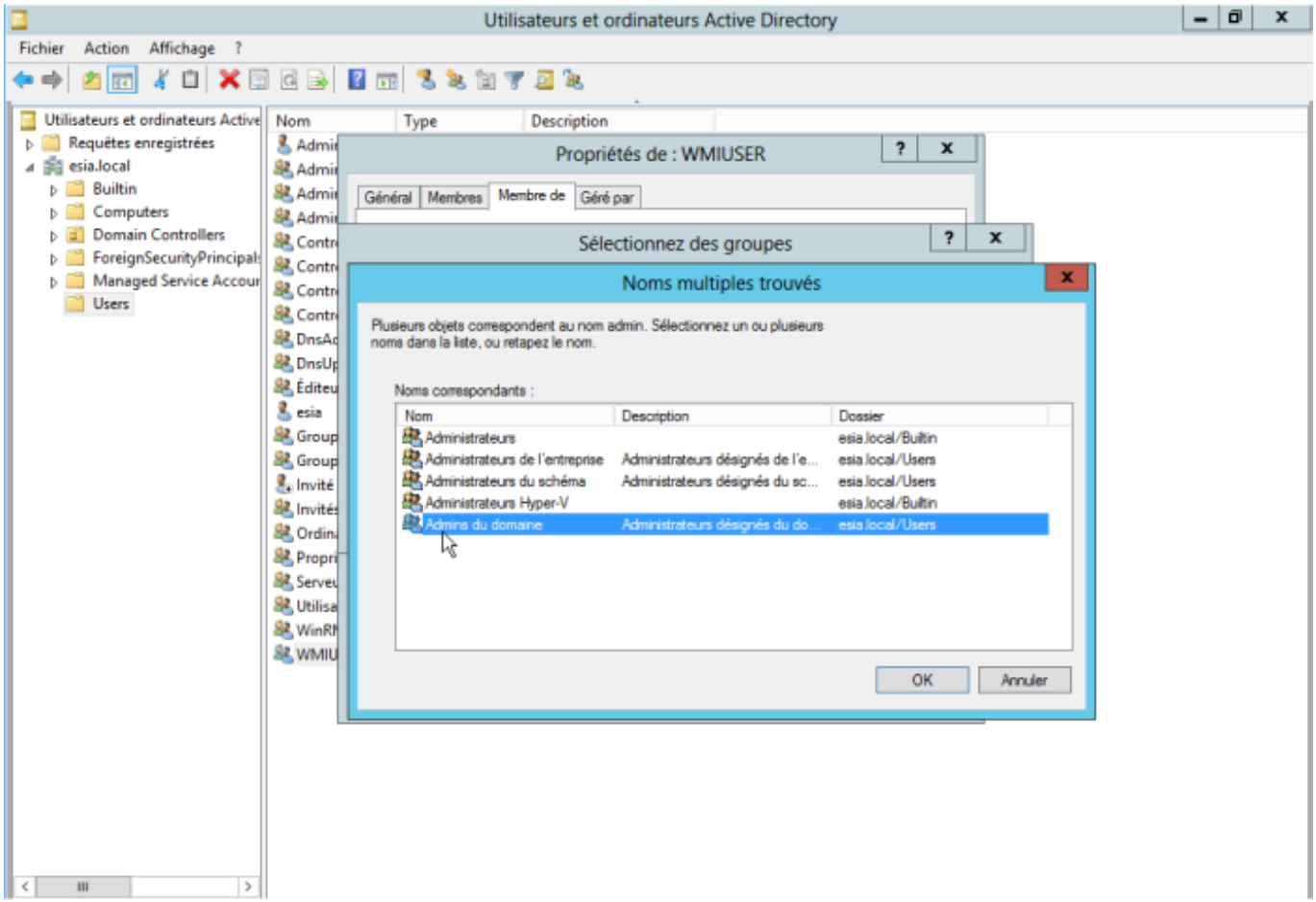
Ajout du groupe WMIUSER en tant qu'administrateur

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 ».

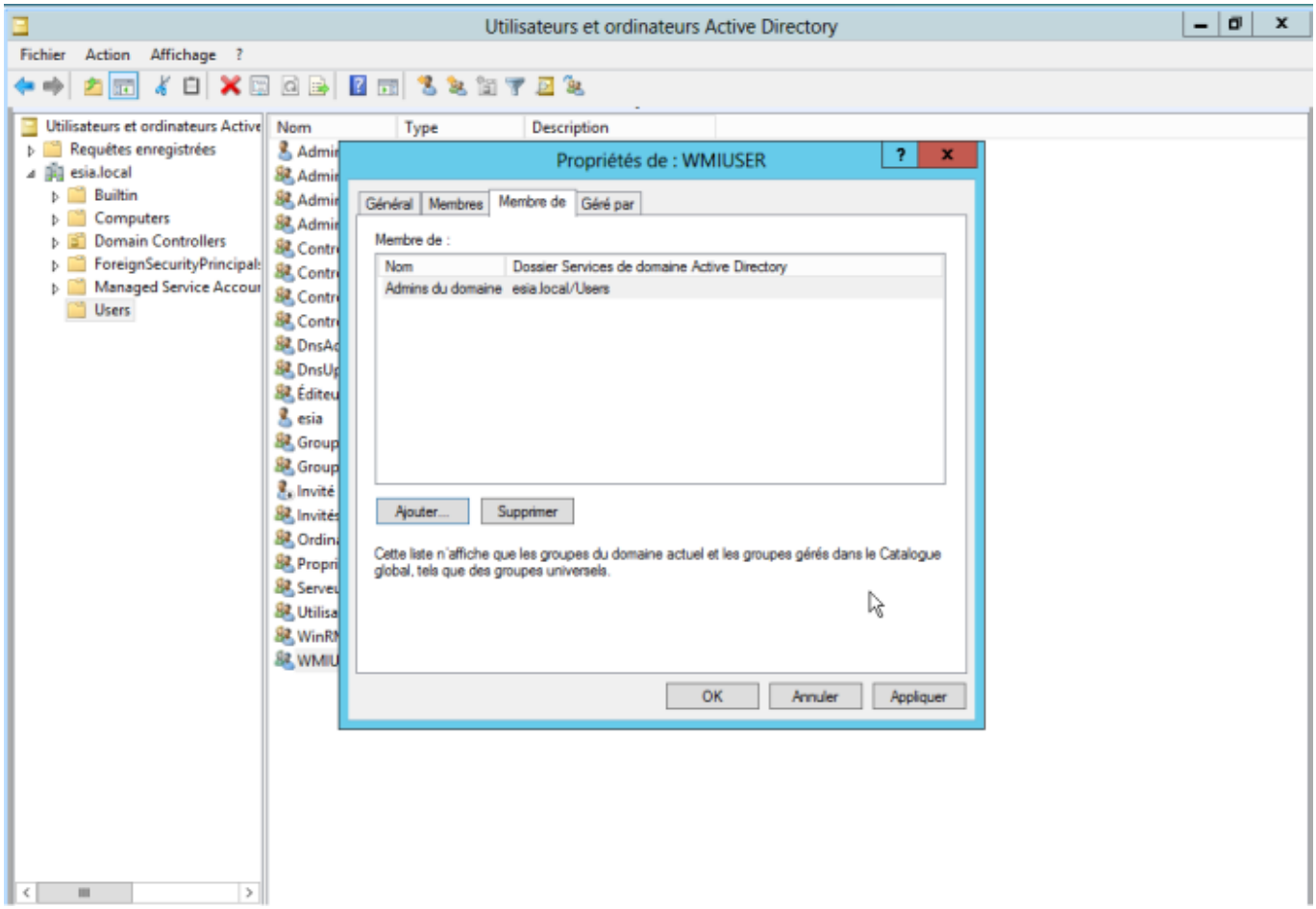
Tapez « admin » puis cliquez sur « Vérifiez les noms »



Sélectionnez, “admin du domaine” et cliquez sur OK.

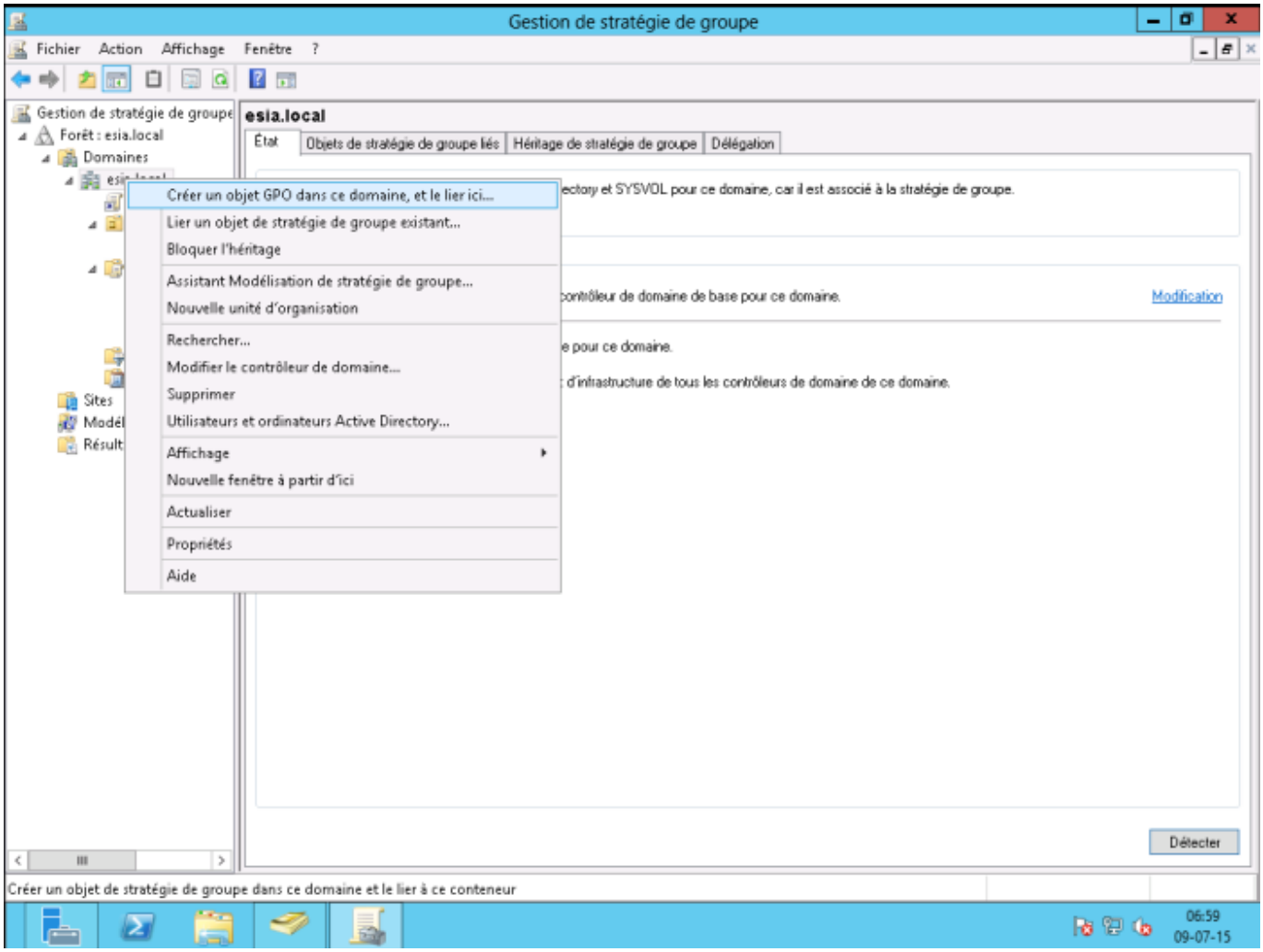


Pour finir, cliquez sur OK.

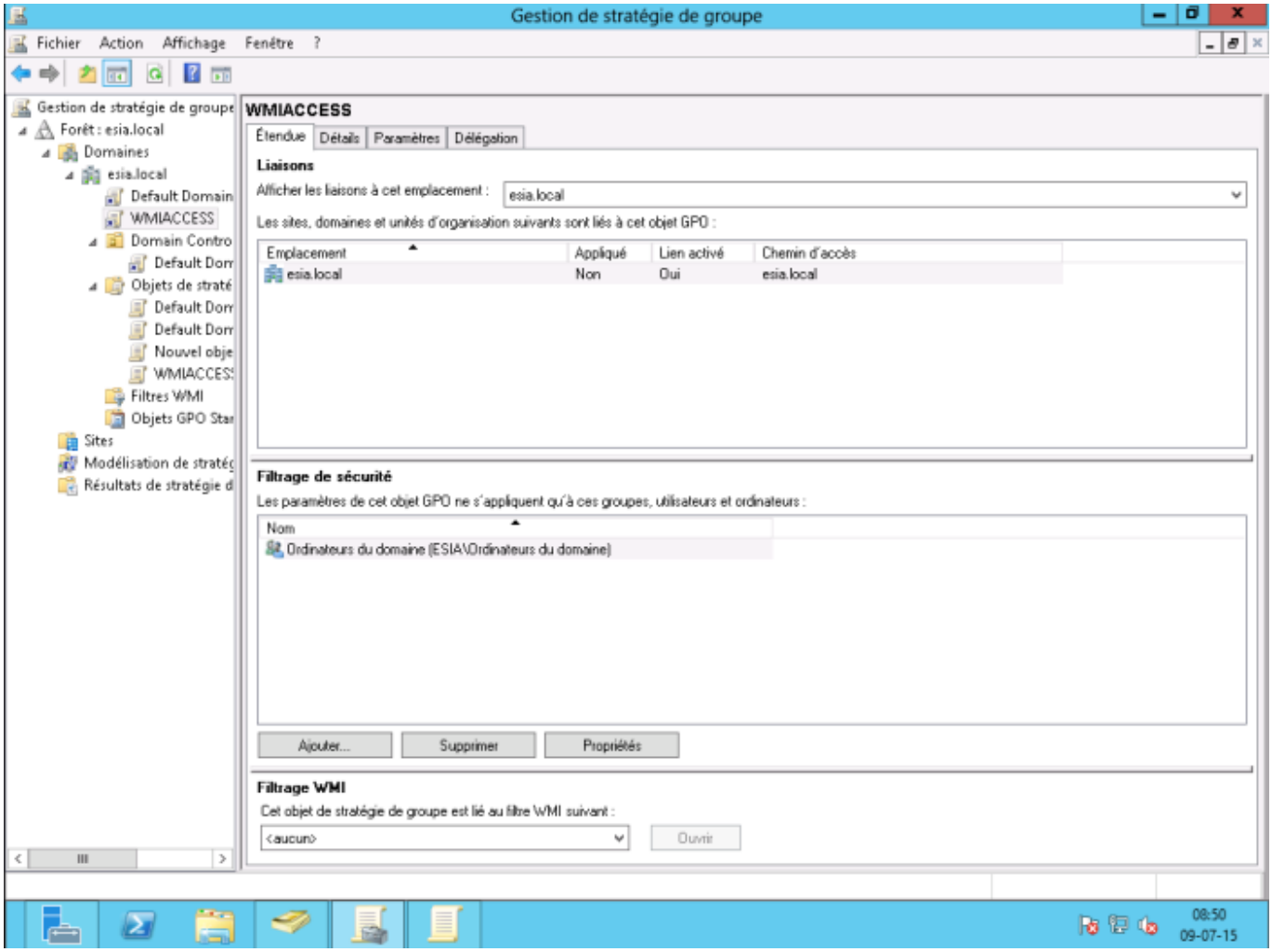


Création de la GPO (Groups Policies Objects)

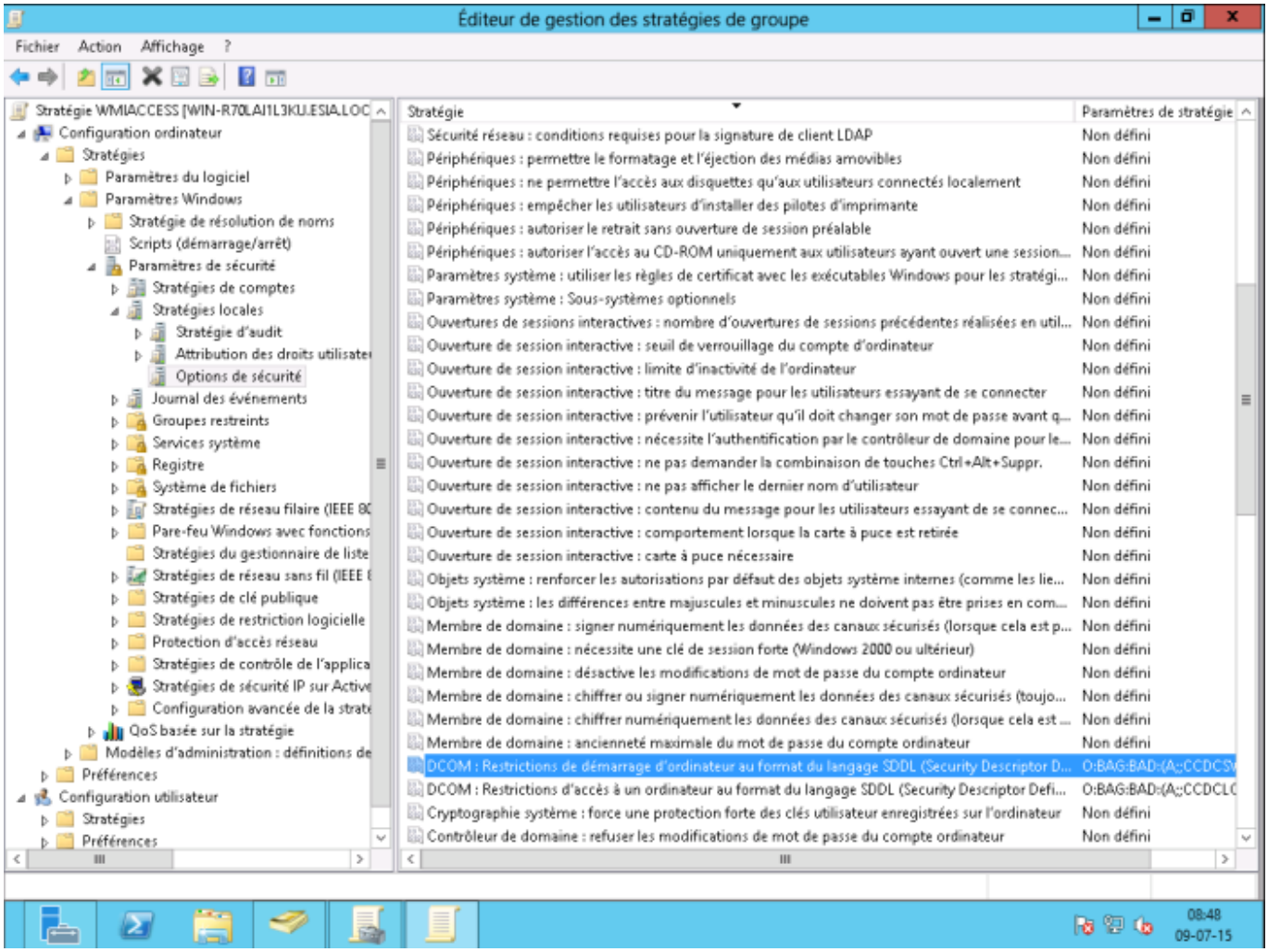
Ouvrez la “Gestion de stratégie de groupe” de votre Active Directory. Faites un clic droit sur votre domaine et créez une nouvelle GPO (ici : WMIACCESS)



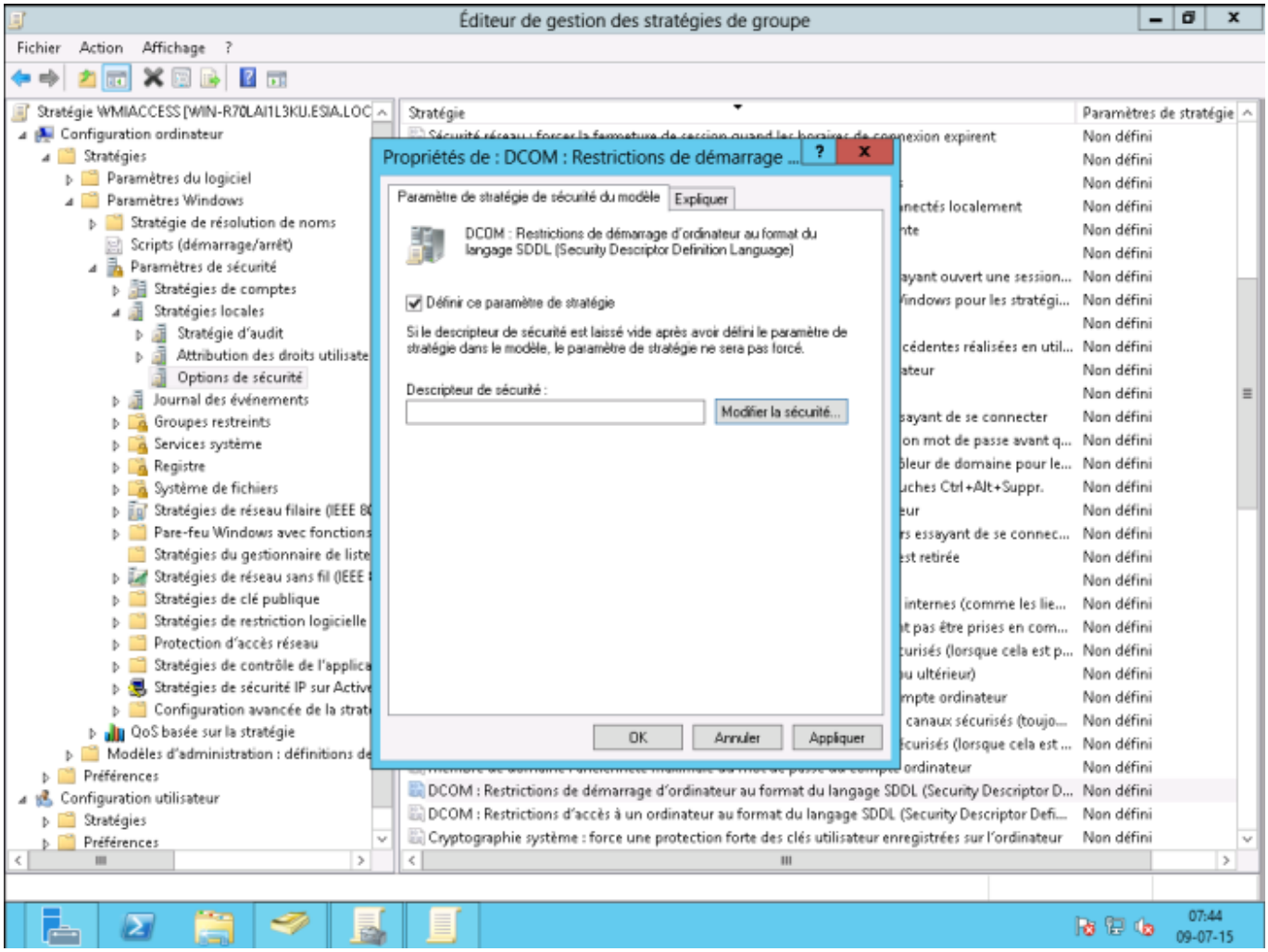
Dans les filtrages de sécurité, supprimez « utilisateurs authentifiés » et ajoutez « ordinateurs du domaine »



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

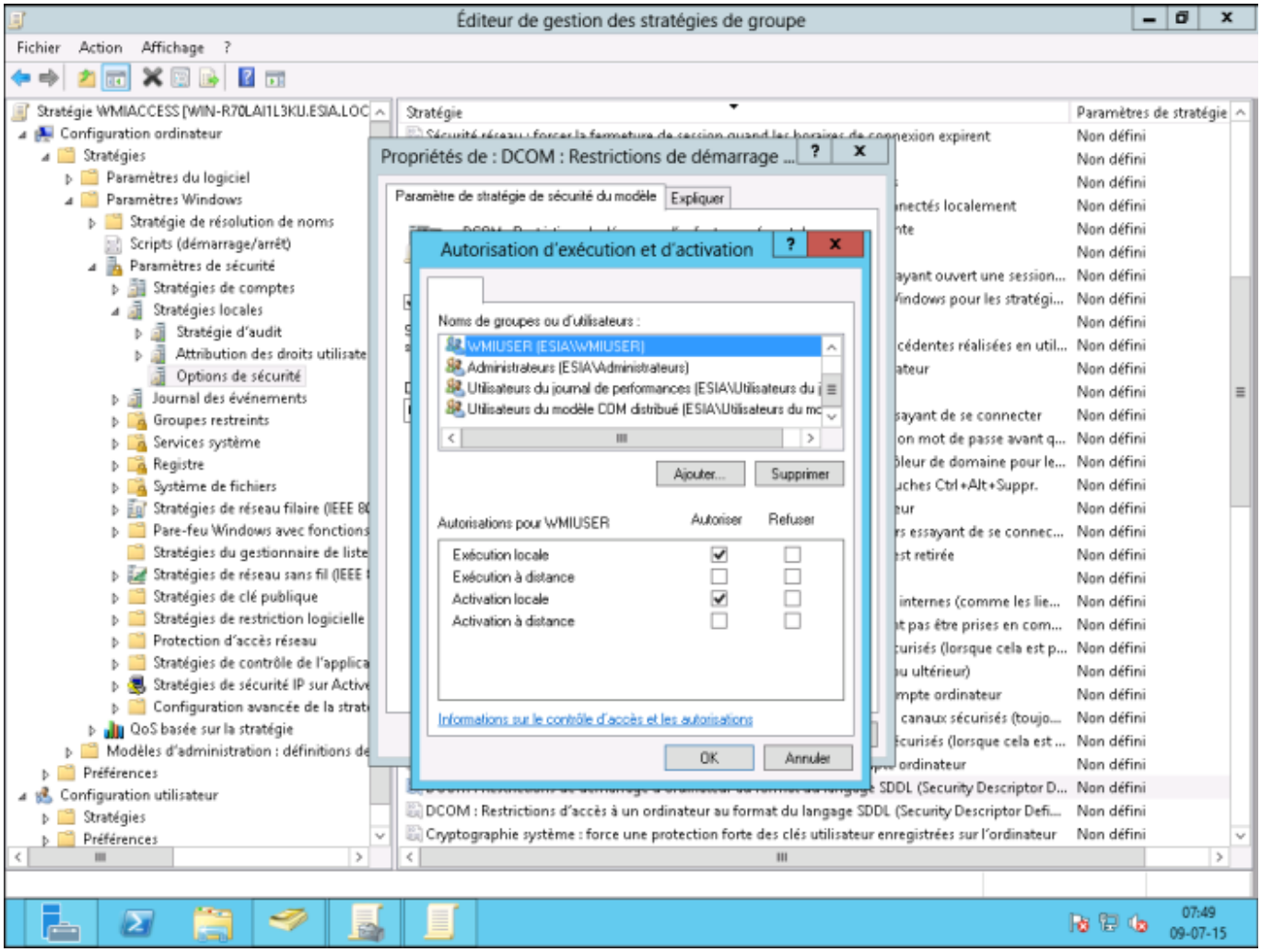


Double-cliquez sur « DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL ». Ensuite, sélectionnez la case « définir ce paramètre de sécurité » et cliquez ensuite sur « Modifier la sécurité »



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

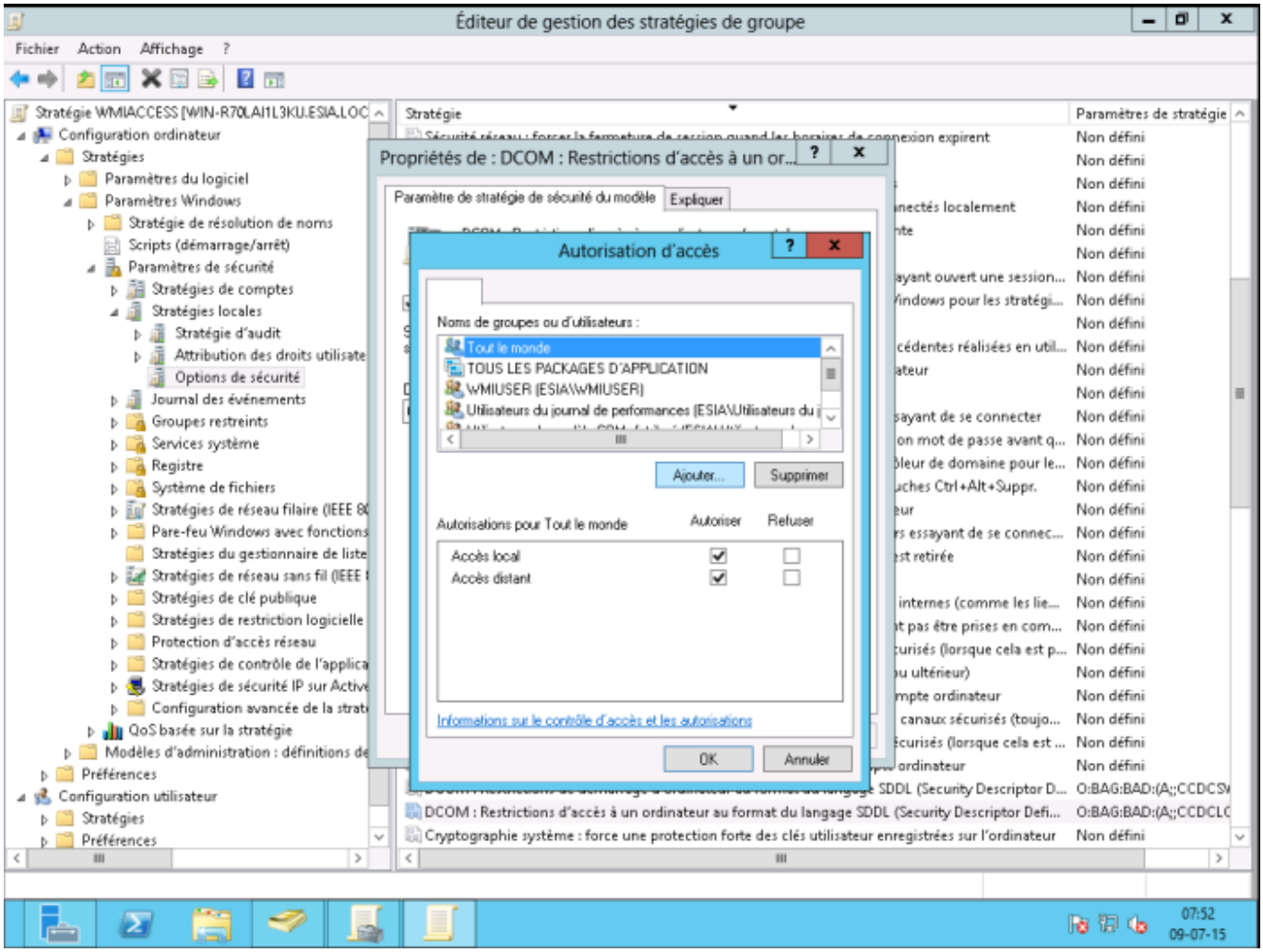
Cocher les cases « Exécution locale » et Exécution à distance ». Cliquez sur OK et de nouveau sur OK.



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 gpupdate /force

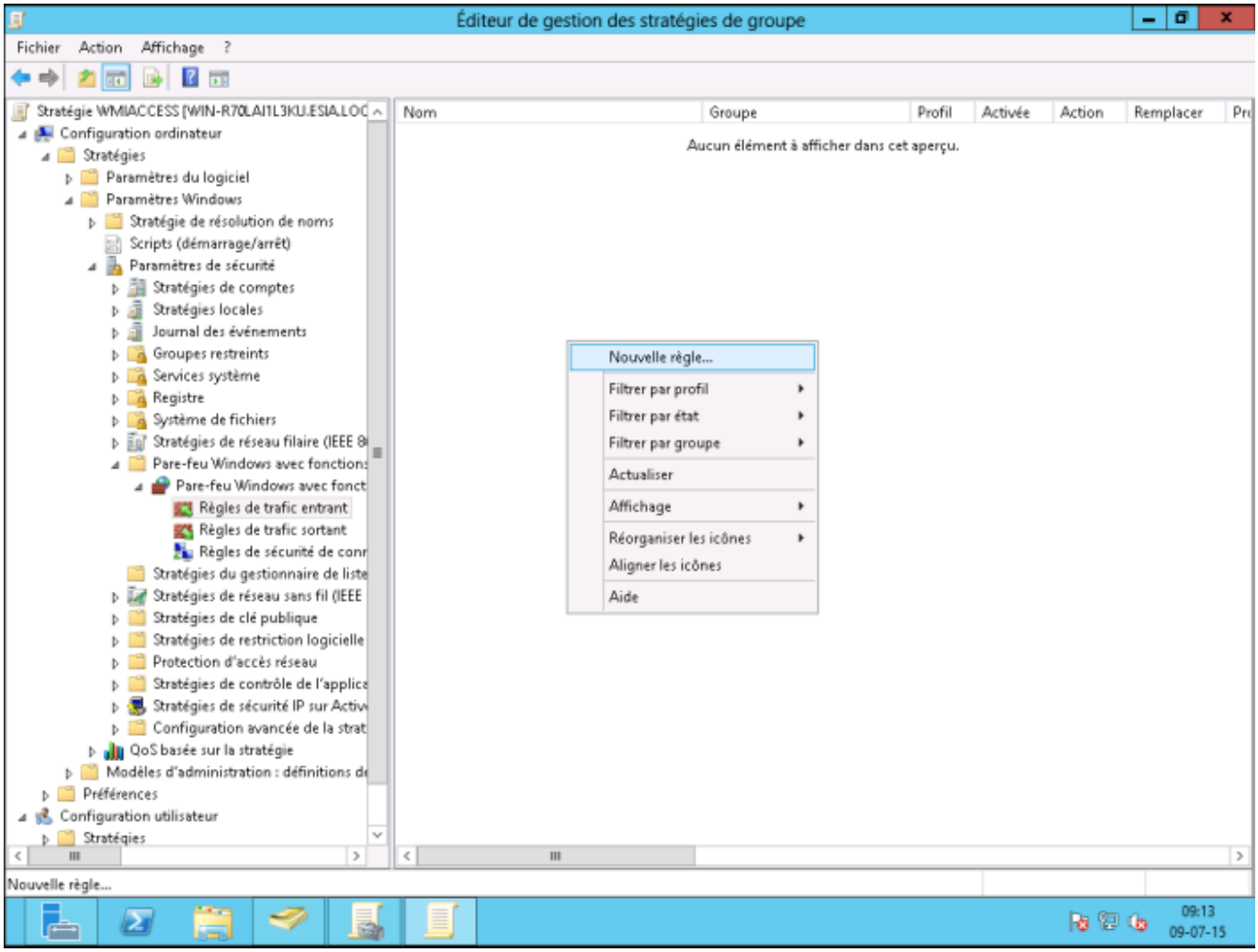
Configuration du pare-feu Windows

<HTML>

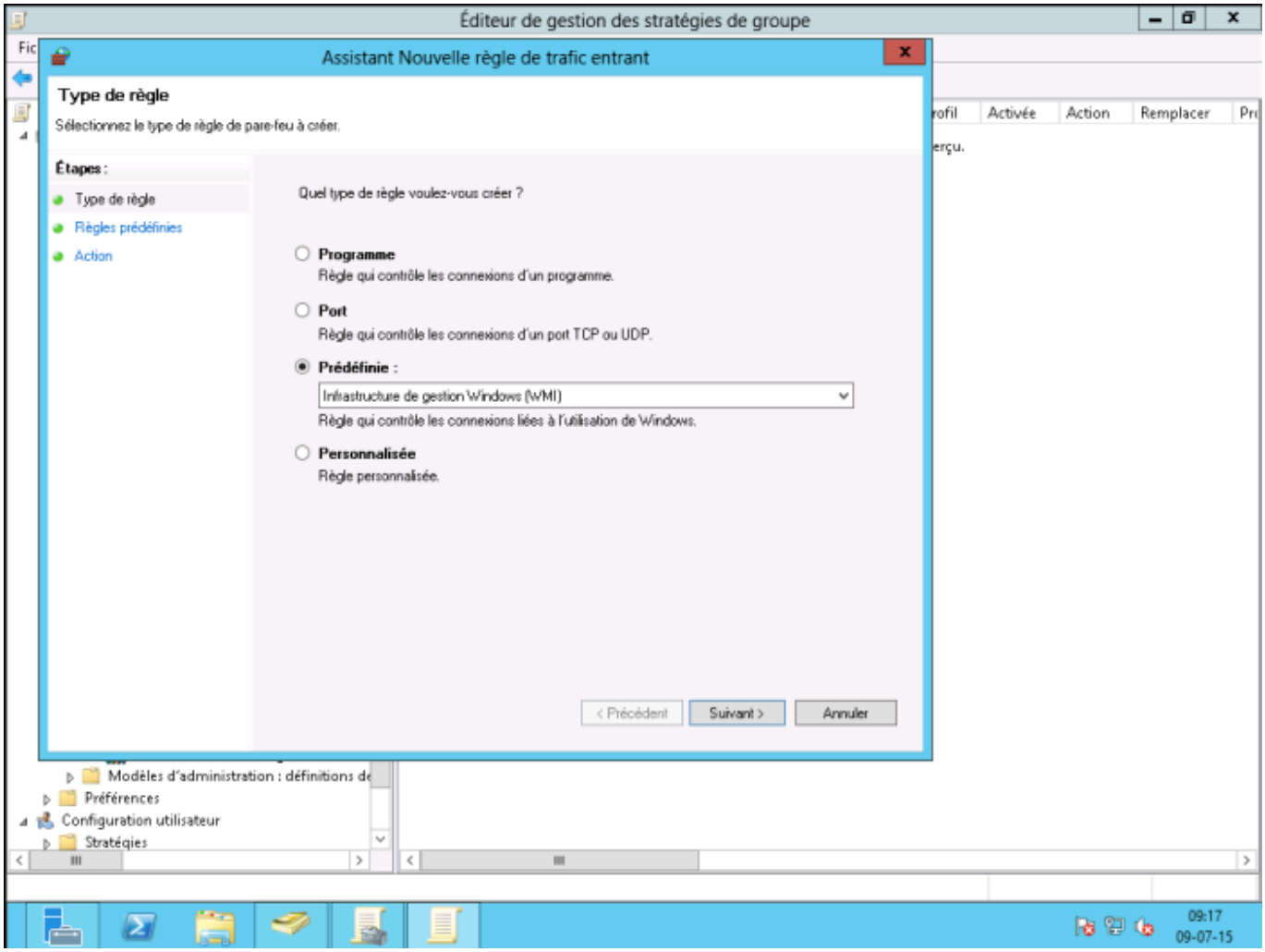
```
  <style>
      #configuration_du_pare-feu_windows:after {content:" (Si nécessaire)";
font-size:.75em; font-weight:500;}
  </style>
```

</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.

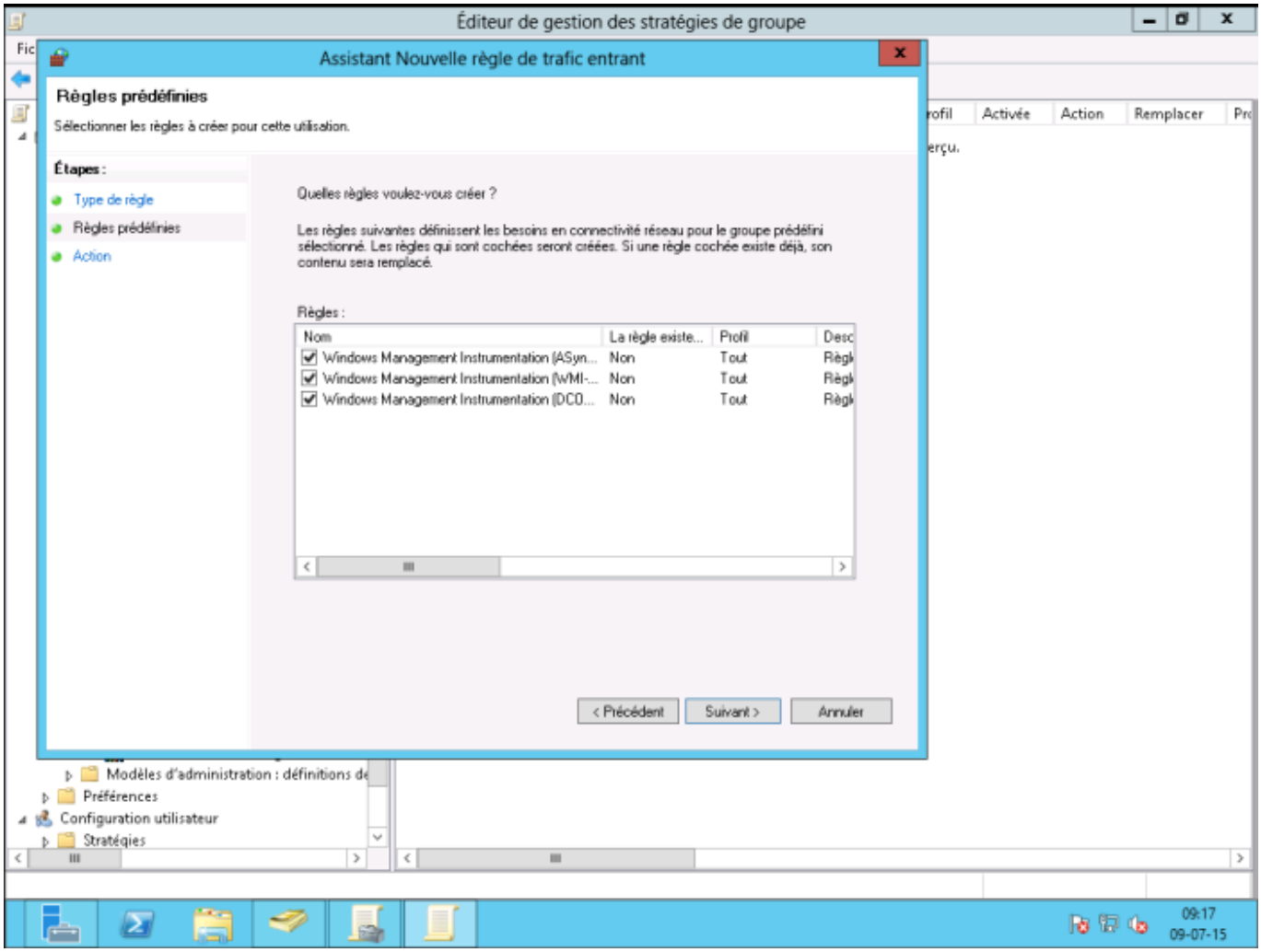
Faites un clic droit pour créer une « Nouvelle règle ... »



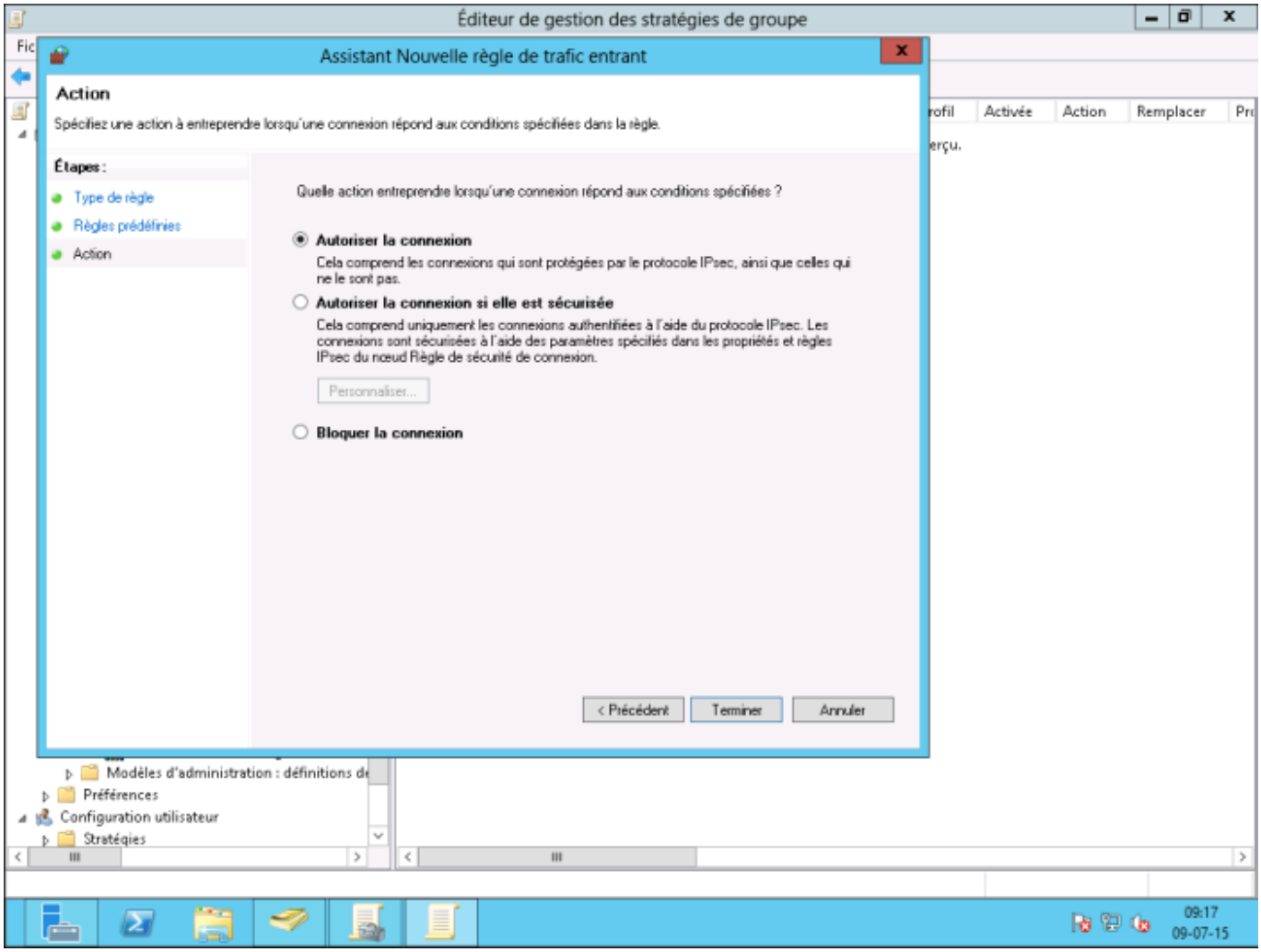
Sélectionnez « Prédéfinie » et choisissez « Infrastructure de gestion WMI ». Cliquez sur suivant.



3 règles de base seront créées, cliquez sur suivant.



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



Ne pas oublier de faire un gpupdate /force

Ajout du groupe WMIUSER en tant que simple utilisateur

<HTML>

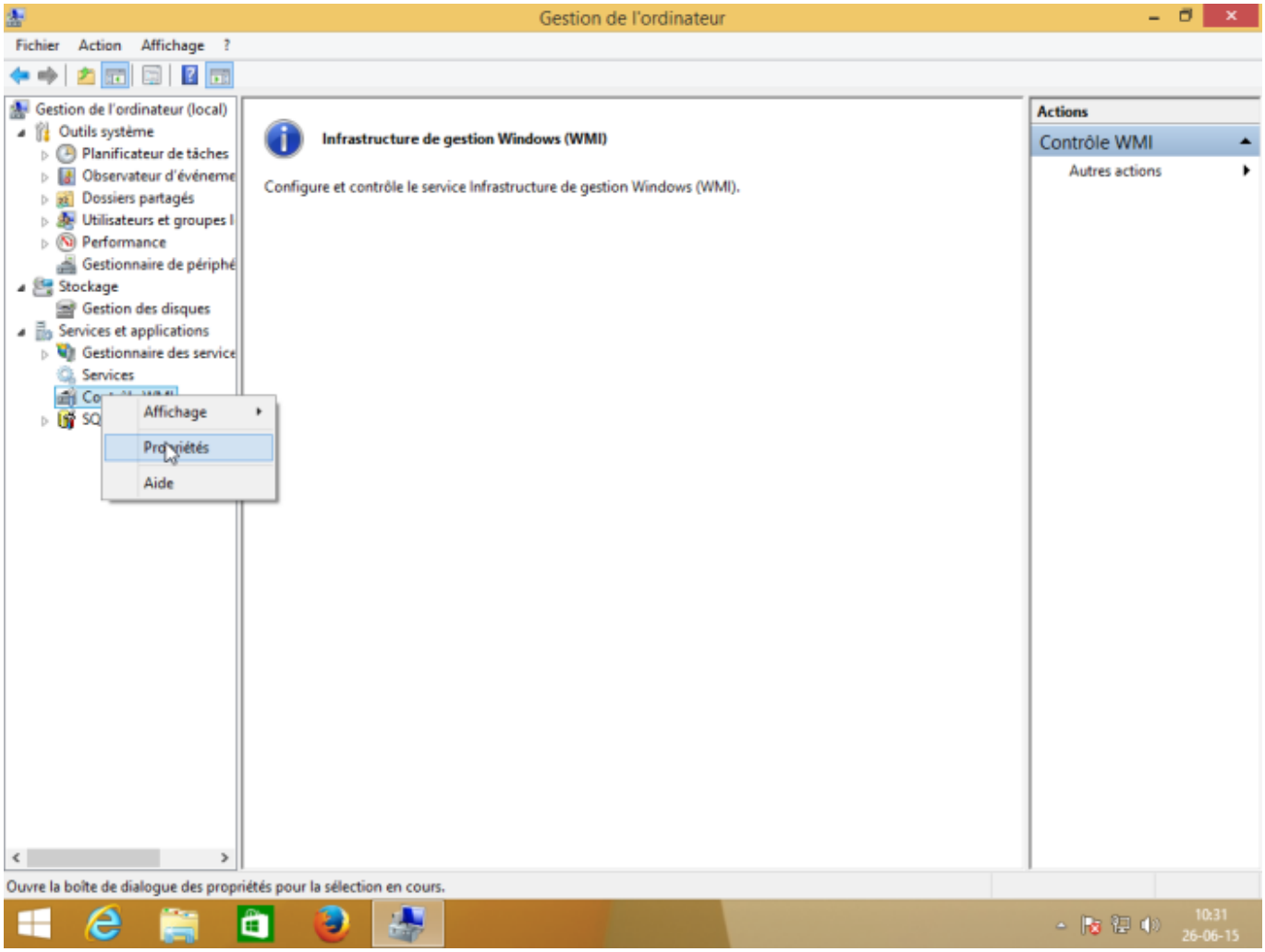
```
  <style>
      #ajout_du_groupe_wmiuser_en_tant_que_simple_utilisateur:after
{content:" (OPTION)"; font-size:.75em; font-weight:500;}
  </style>
```

</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.

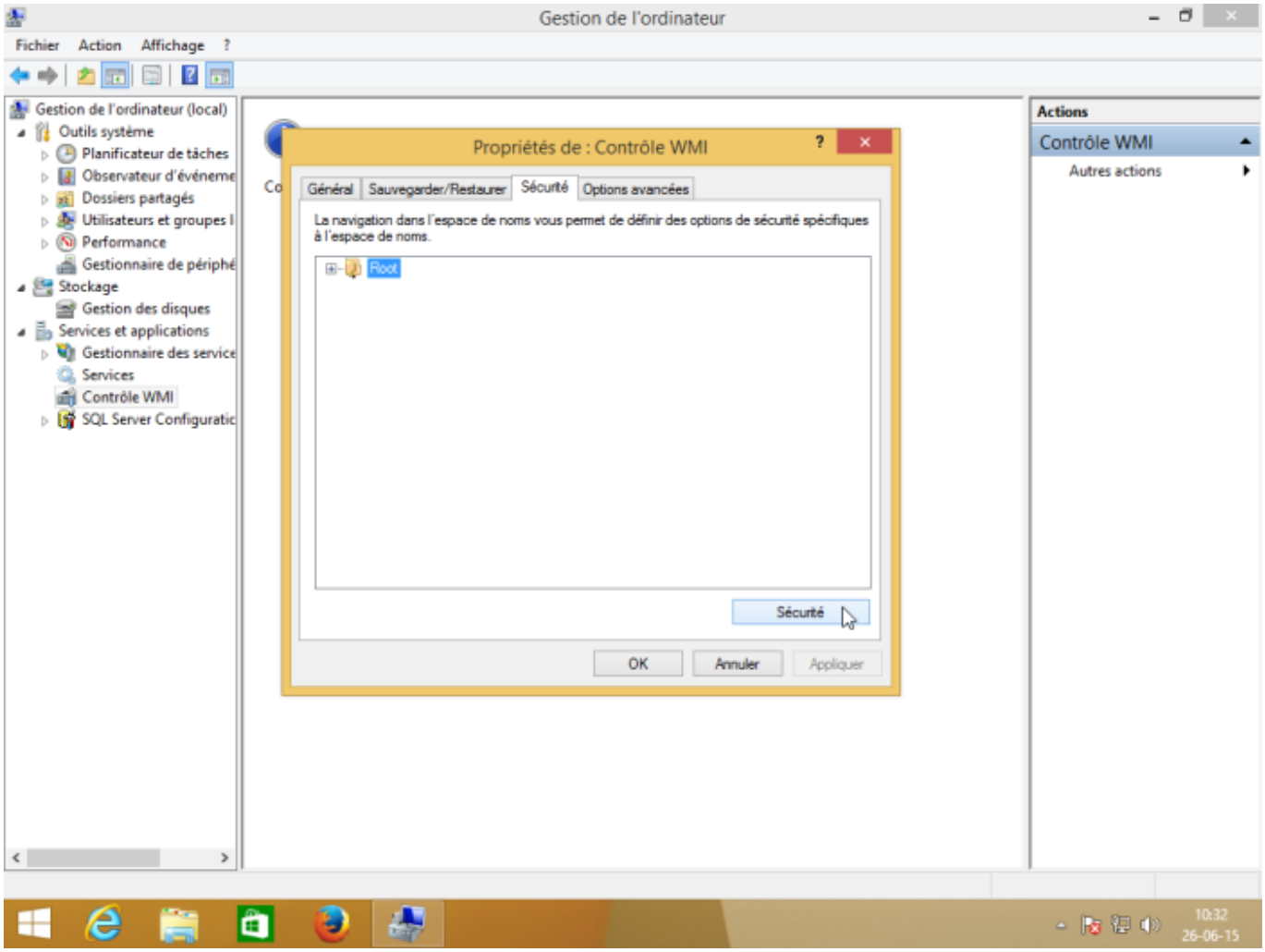
Pour cela :

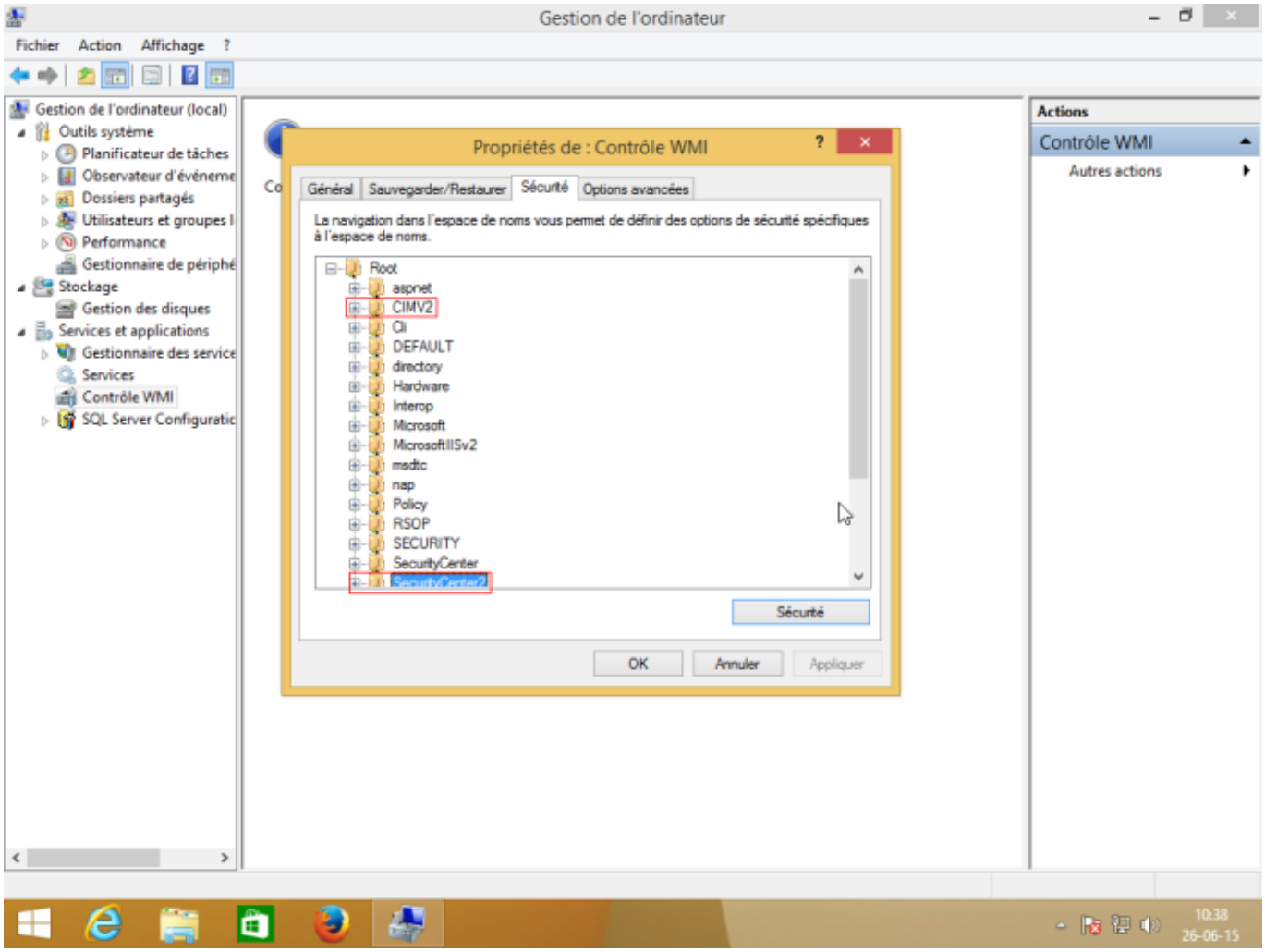
Rendez vous dans « Gestion de l'ordinateur » (ou saisissez la commande «`wmimgmt.msc` ». Puis, Déroulez « Services et applications » pour pouvoir faire un clic droit sur « Contrôle WMI » et cliquer sur « Propriétés ».



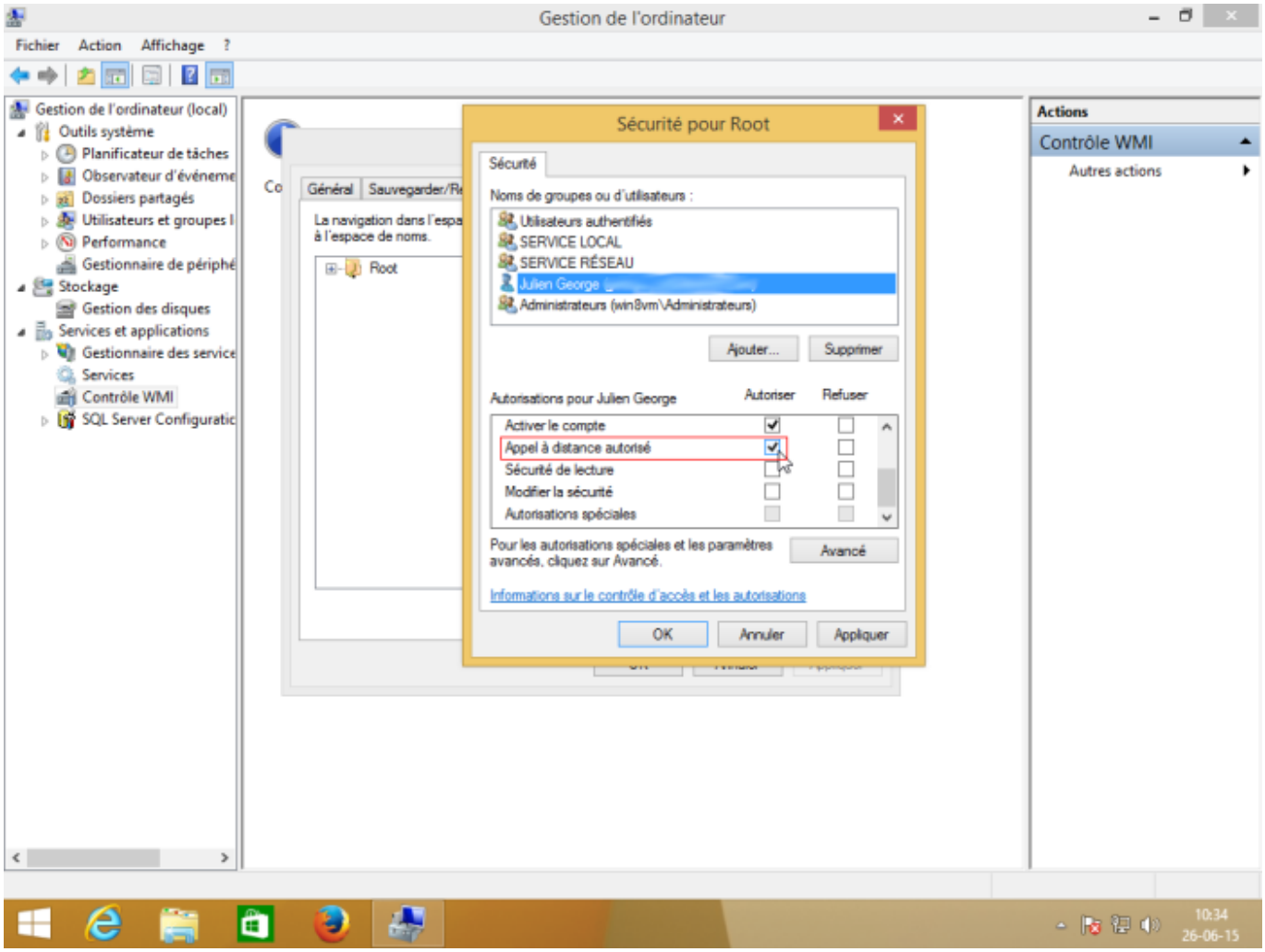
Dans l'onglet « Sécurité » des « Propriétés de : Contrôle WMI », sélectionnez le namespace « Root » et cliquez ensuite sur « Sécurité ».

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

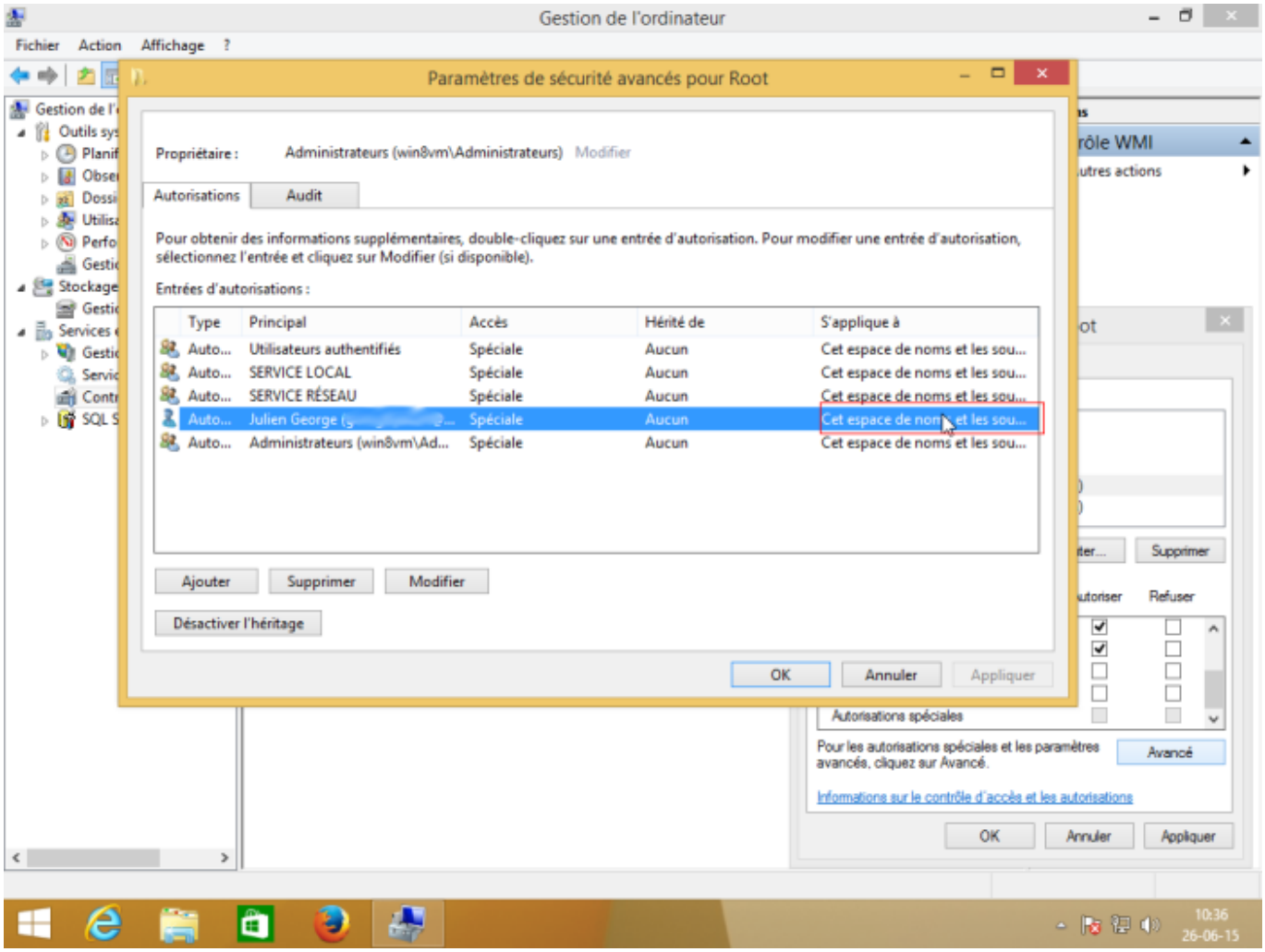

Gestion de l'ordinateur
Fichier Action Affichage ?
Gestion de l'ordinateur (local)
Outils système
Planificateur de tâches
Observateur d'événeme
Dossiers partagés
Utilisateurs et groupes l
Performance
Gestionnaire de périphé
Stockage
Gestion des disques
Services et applications
Gestionnaire des service
Services
Contrôle WMI
SQL Server Configuratic
Propriétés de : Contrôle WMI
Général
Sauvegarder/Restaurer
Sécurité
Options avancées
La navigation dans l'espace de noms vous permet de définir des options de sécurité spécifiques à l'espace de noms.
Root
Sécurité
OK
Annuler
Appliquer
Actions
Contrôle WMI
Autres actions
10:32
26-06-15



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.