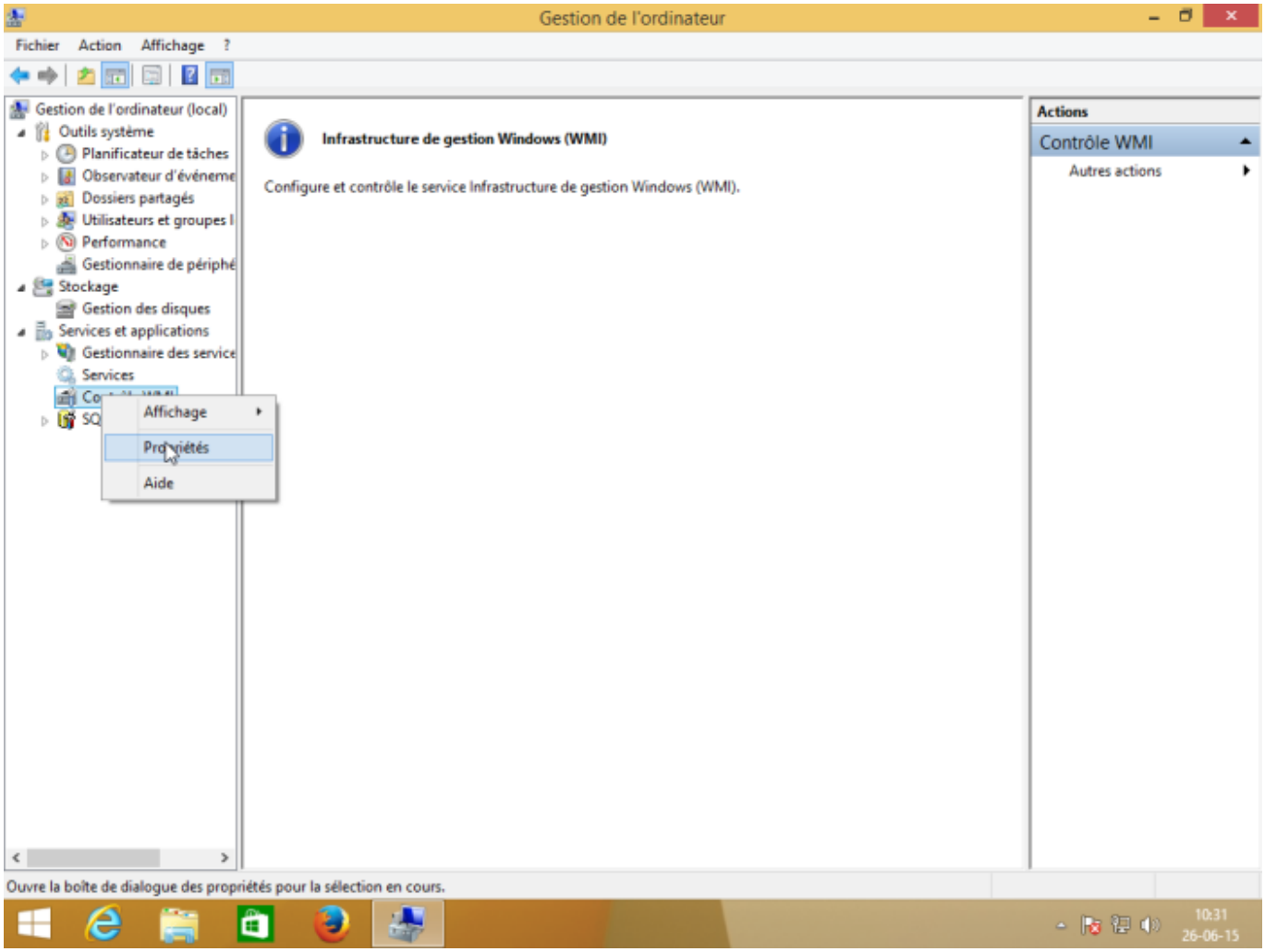
Activer WMI sur Windows 7, 8 & 10

Activer les accès distants à WMI (toujours nécessaire)

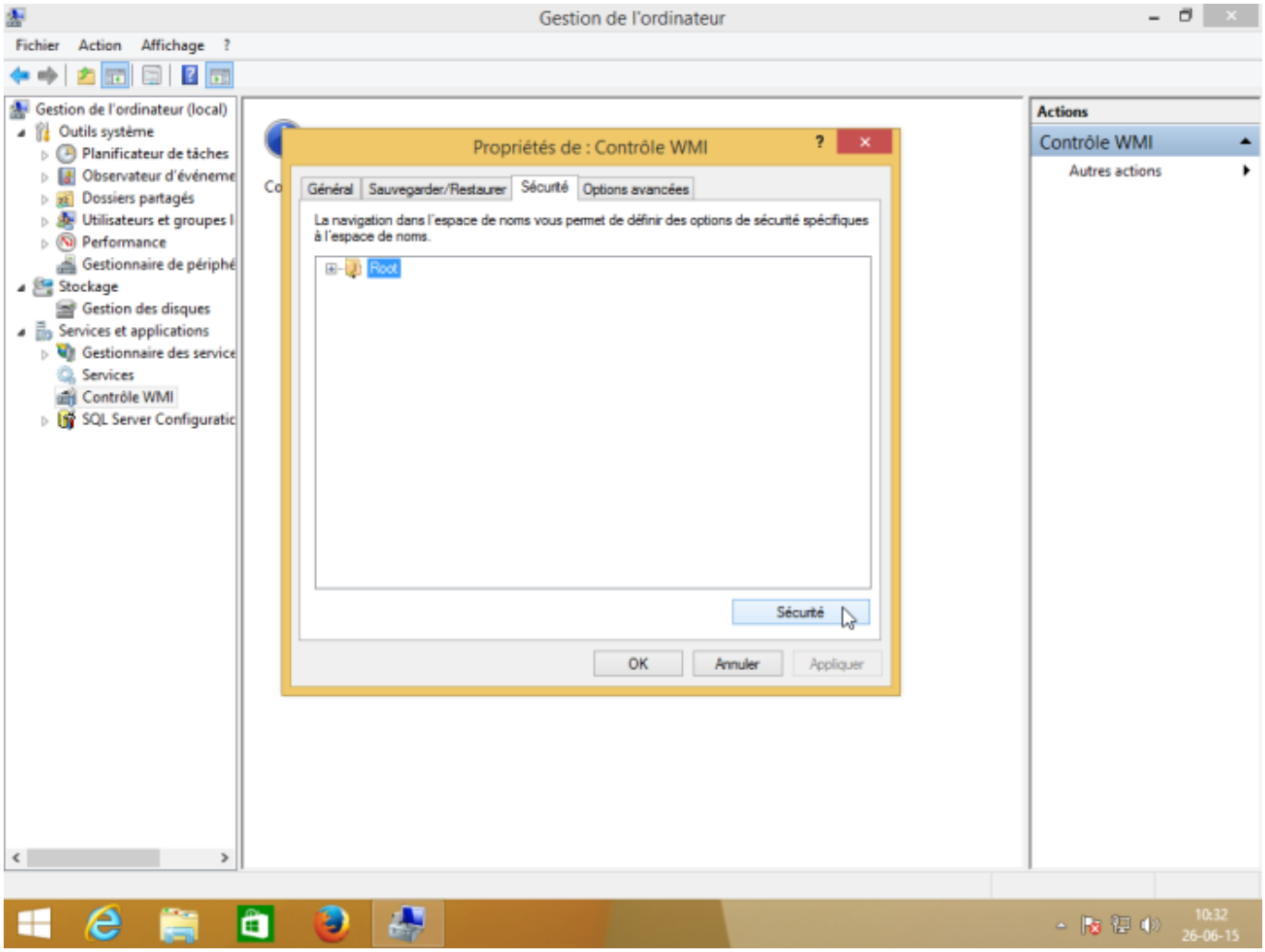
Il s'agit ici de donner les droits d'accès distants au compte utilisateur qui sera utilisé par ESIA afin d'accéder aux données WMI. Pour cela :

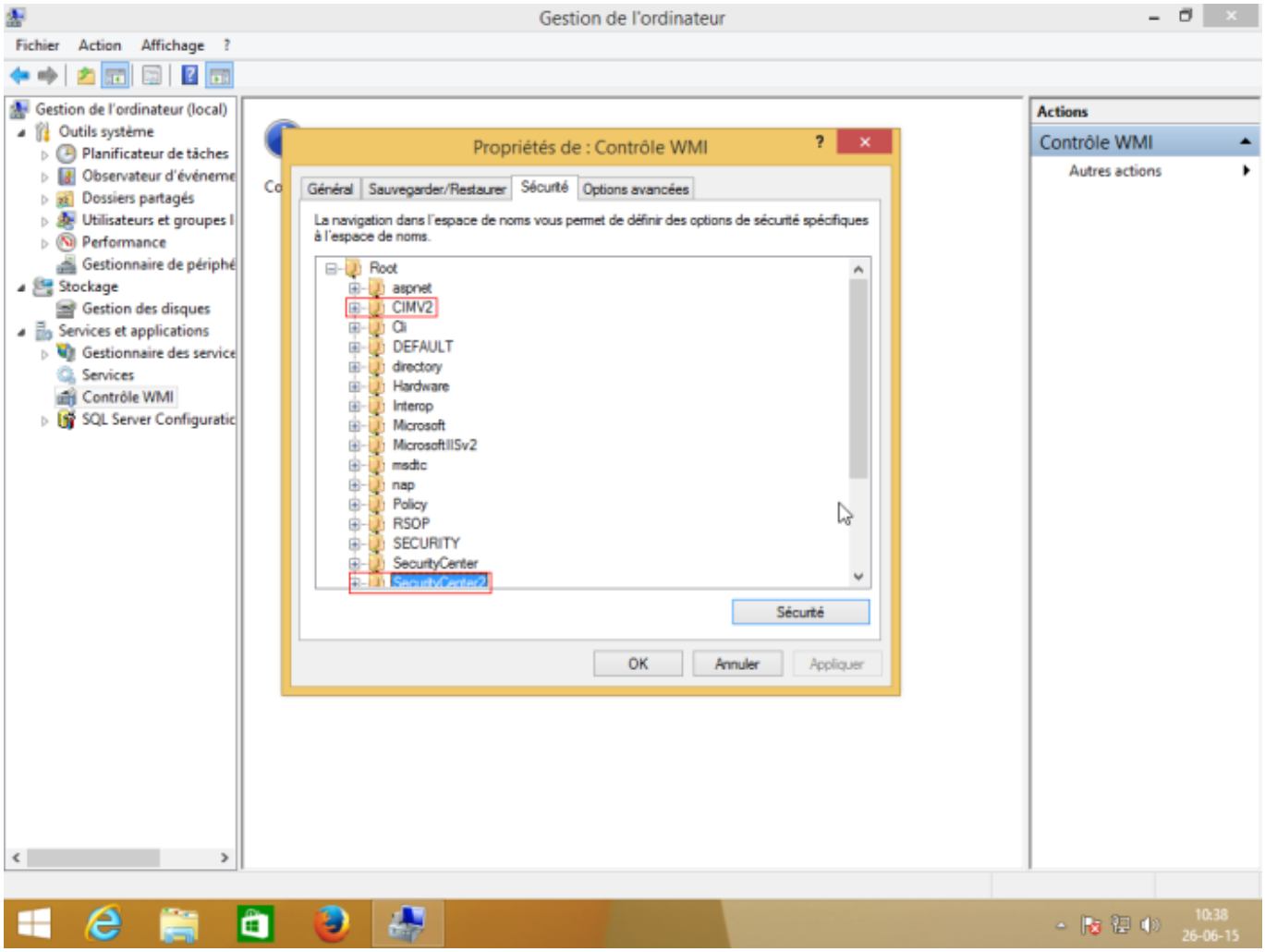
Rendez vous dans « Gestion de l'ordinateur » (ou saisissez la commande « wmimgmt.msc ». Puis, Déroulez « Services et applications » pour pouvoir faire un clic droit sur « Contrôle WMI » et cliquez sur « Propriétés ».



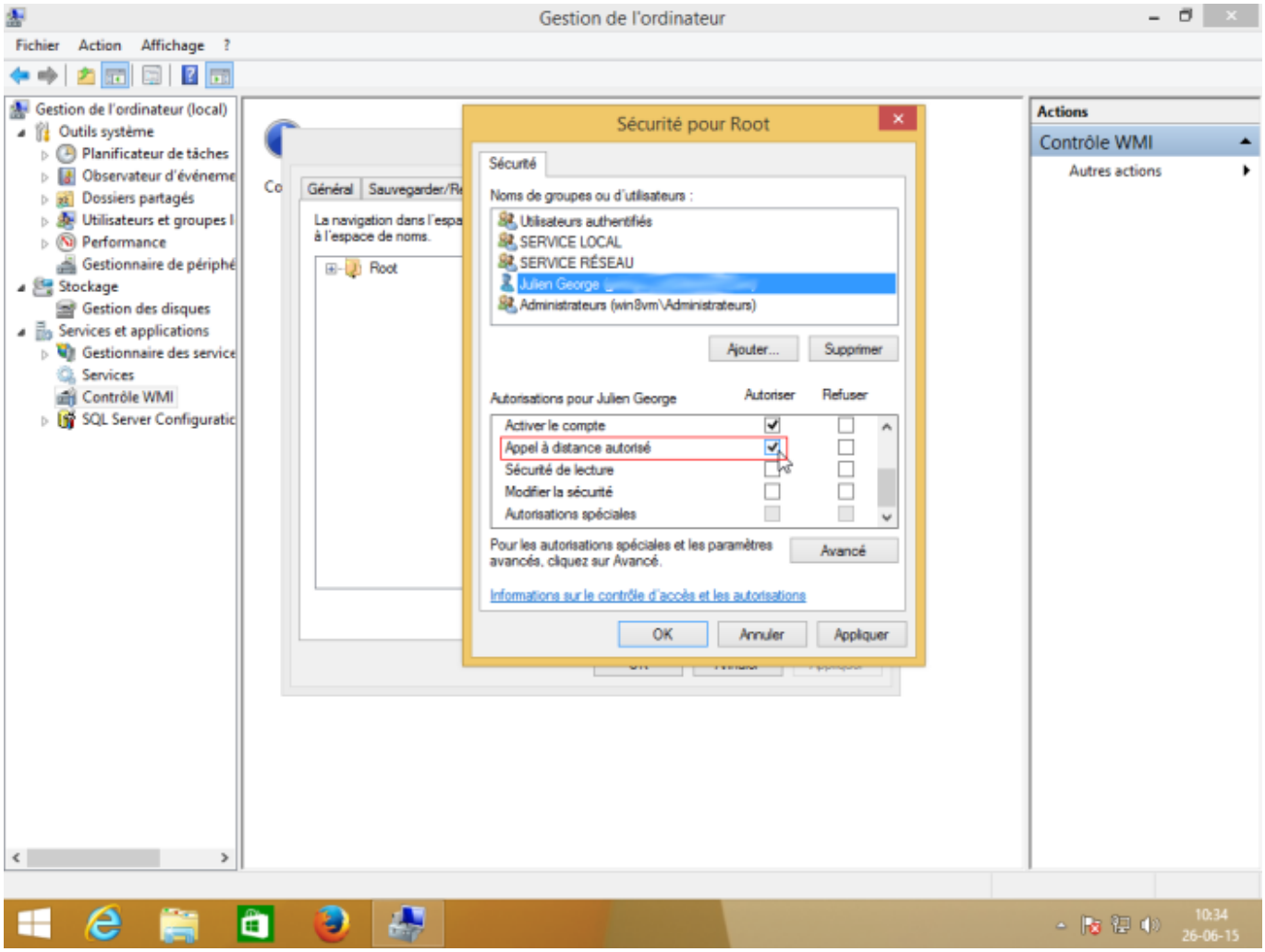
Dans l'onglet « Sécurité » des « Propriétés de : Contrôle WMI », sélectionnez le namespace « Root » et cliquez ensuite sur « Sécurité ».

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

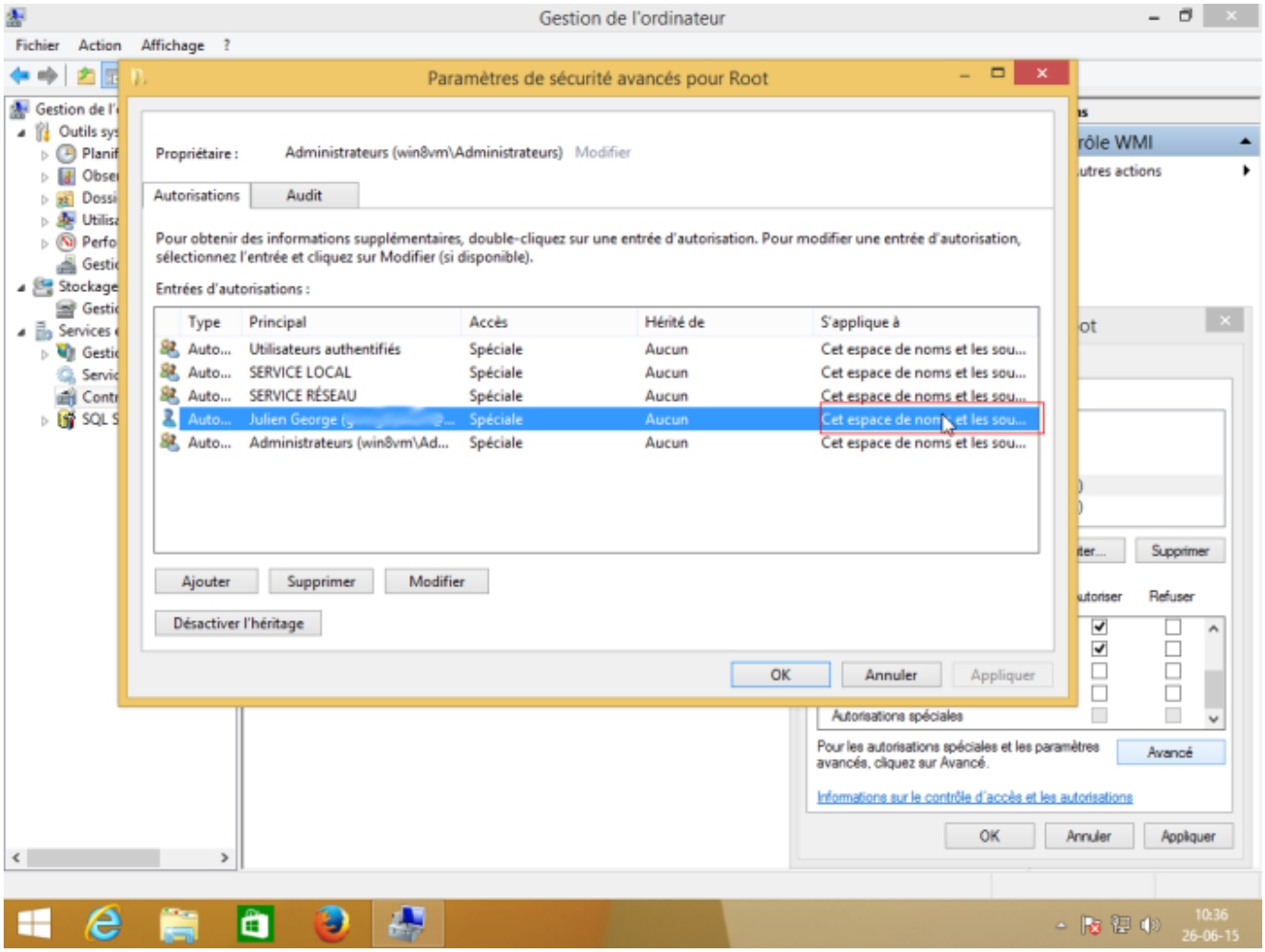

Gestion de l'ordinateur
Fichier Action Affichage ?
Gestion de l'ordinateur (local)
Outils système
Planificateur de tâches
Observateur d'événeme
Dossiers partagés
Utilisateurs et groupes l
Performance
Gestionnaire de périphé
Stockage
Gestion des disques
Services et applications
Gestionnaire des service
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.

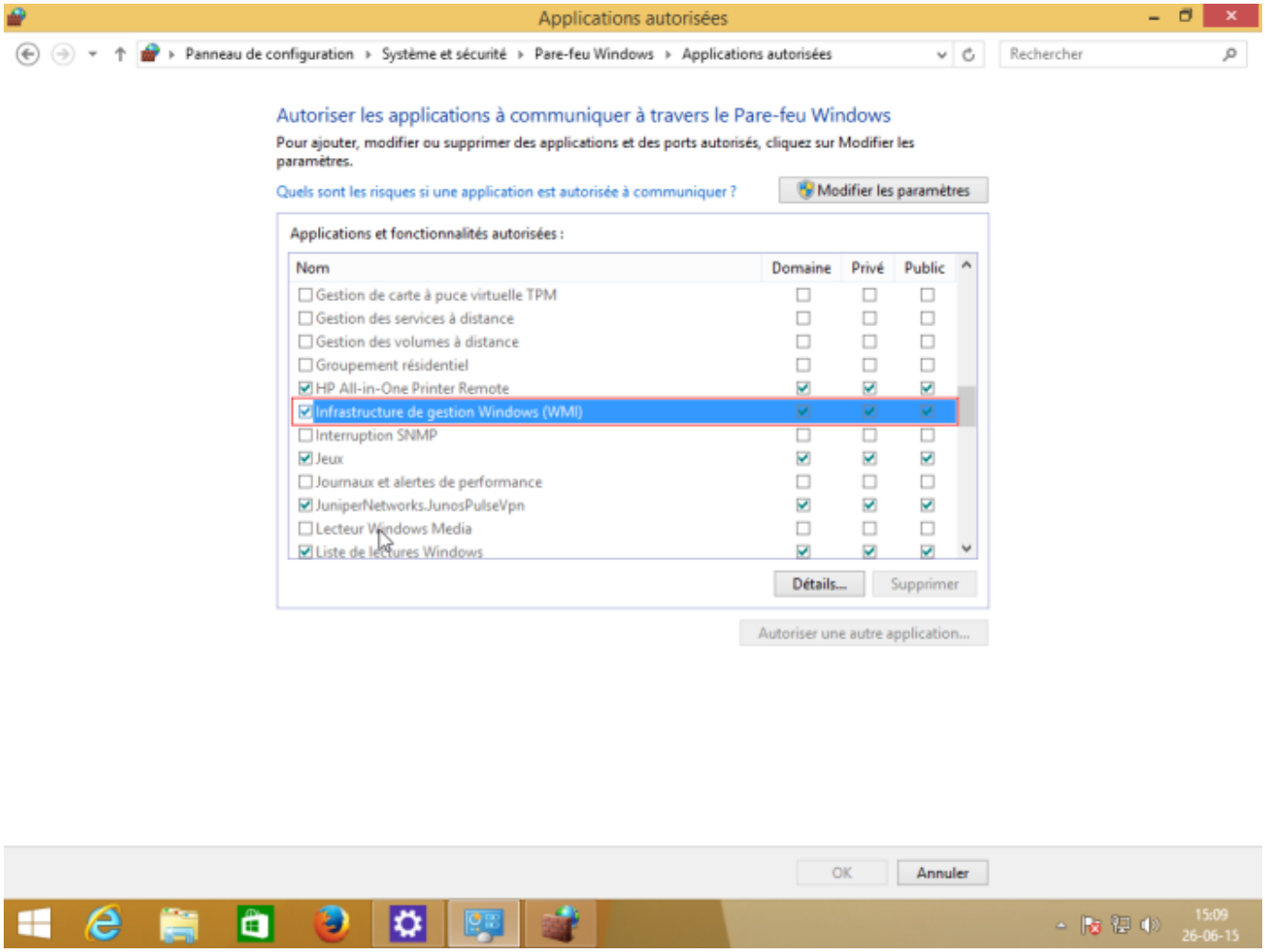


Assurez-vous que les autorisations ont été appliquées au namespace sélectionné et à ses sous namespaces en cliquant sur « Avancé » pour vérifier la colonne « S'applique à ».



Permettre l'accès à travers le pare-feu (Si vous utilisez un pare-feu)

Afin d'éviter que le pare feu ne bloque les requêtes WMI, le plus simple est d'exécuter la ligne de commande suivante en tant qu'Administrateur : « netsh firewall set service RemoteAdmin enable »
Vous pouvez aussi le faire via la page de configuration du pare-feu windows :

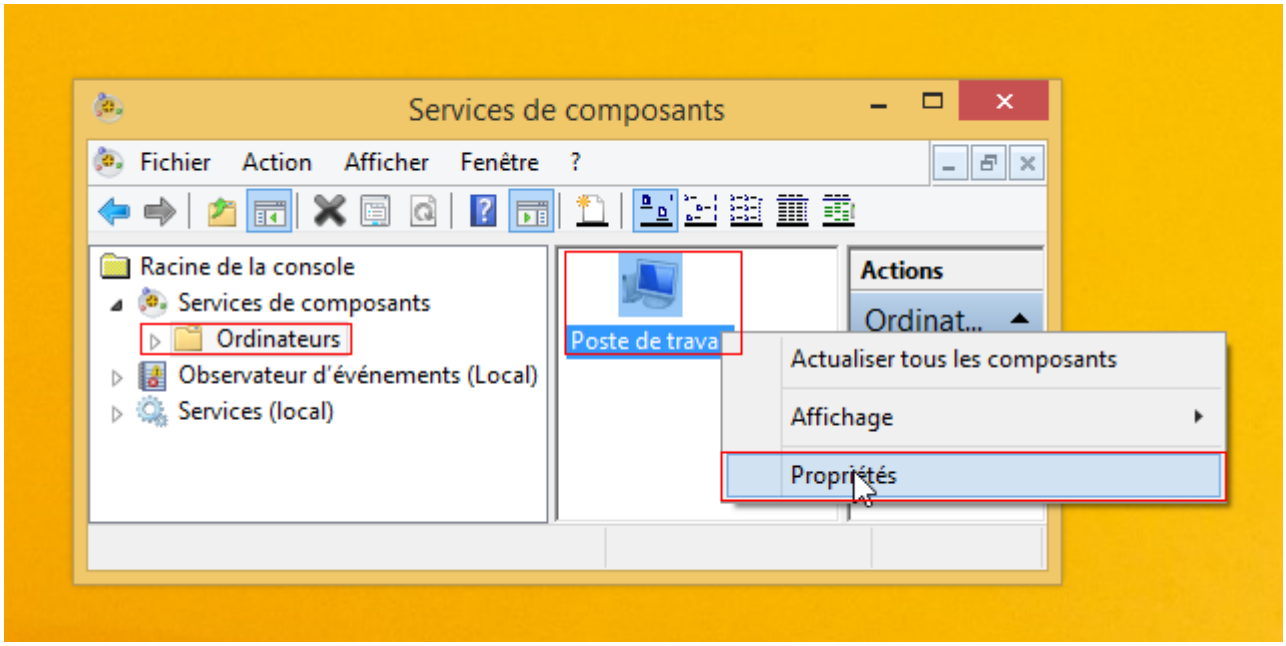


Ajouter l'utilisateur dans un groupe qui a les permissions d'accès à distance

Pour pouvoir accéder à WMI à distance, il faut que WMI fasse partie du groupe « Administrateur ».

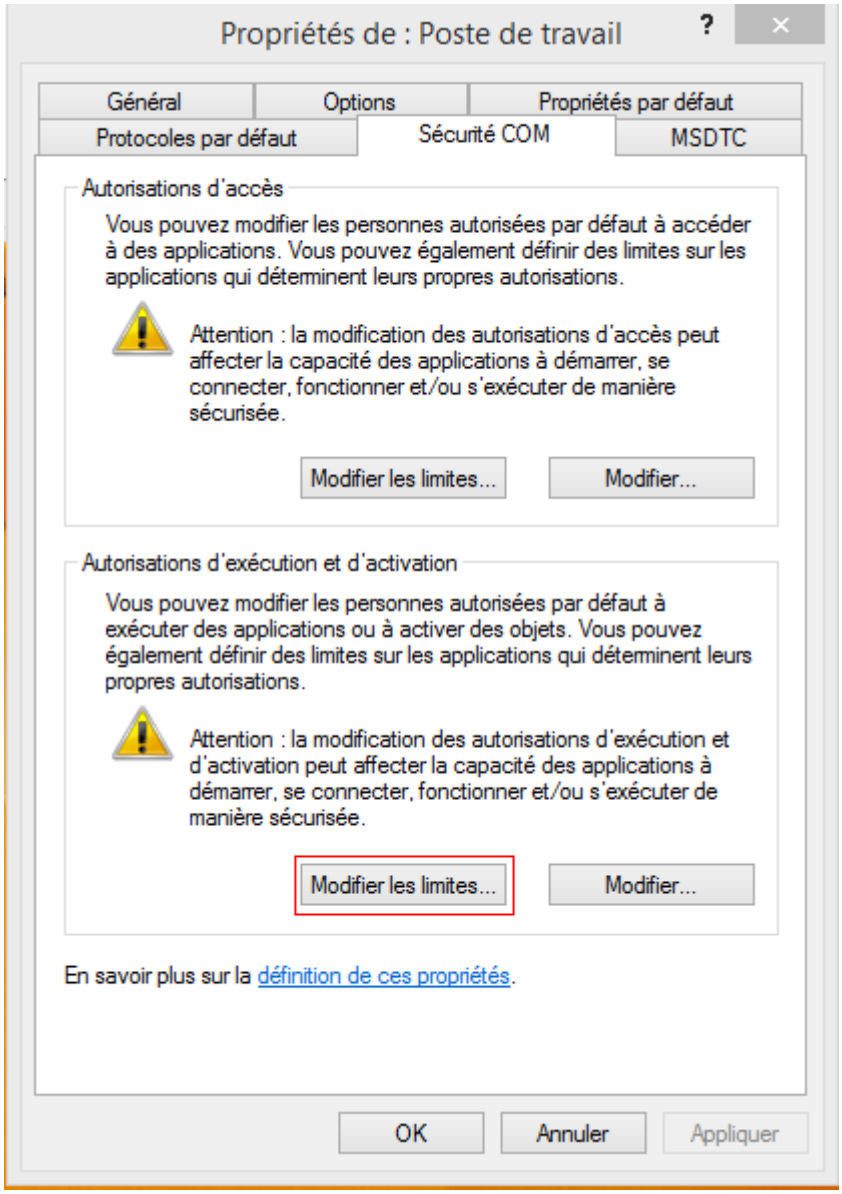
Activer les accès DCOM (si nécessaire)

Exécutez l'application « dcomcnfg »

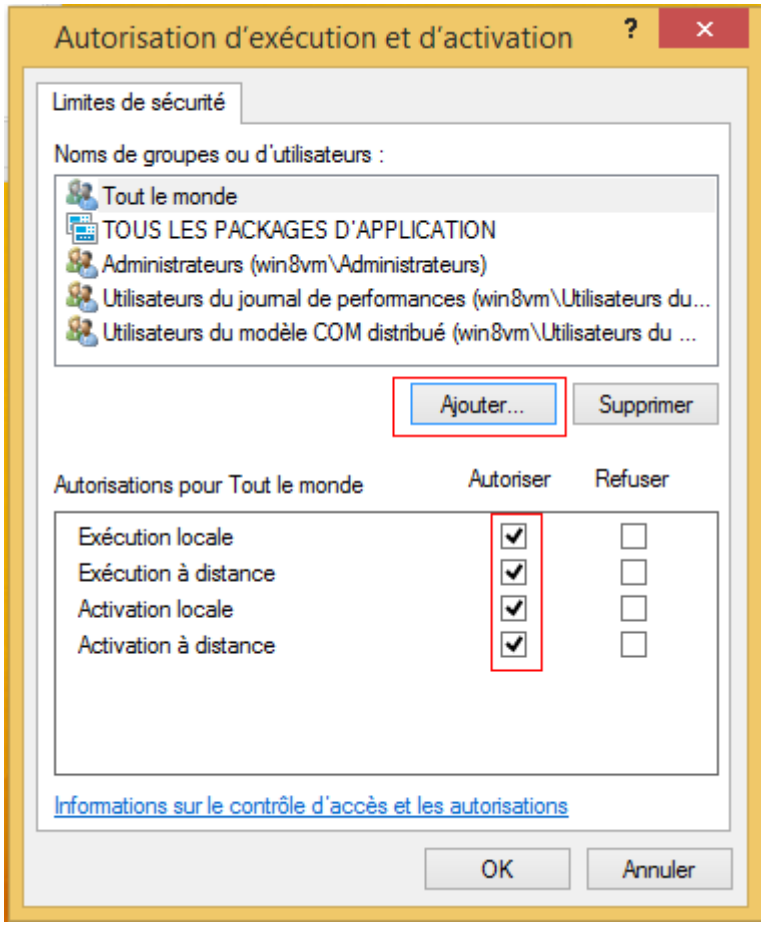


Dans « **Racine de la console → Service de composant → ordinateurs** », faites un clic droit sur « Poste de travail » puis cliquez sur « Propriétés ».

Rendez-vous dans l'onglet « Sécurité DCOM » et, dans « Autorisations d'exécution et d'activation », cliquez sur le bouton « Modifier les limites ».



Ajoutez l'utilisateur pour WMI dans la liste et activez les autorisations distantes :



Remarque : Si cela ne fonctionne pas, essayez toujours l'autre bouton « Modifier limites » et les 2 autres boutons. (« Modifier »).

Groupe de performance

Si vous obtenez une sortie inconnue du type avec un message contenant “2 WMI samples%”. Il faut ajouter l'utilisateur dans le groupe local “Journal de Performance” s'il n'est pas administrateur de la machine

Renseigner les credentials WMI sur le boitier ESIA Unity

L'ensemble des manipulations ci-dessus étant faites, il ne reste plus qu'à renseigner les credentials WMI sur le boitier Unity.

Pour cela, rendez vous sur l'interface web du boitier Unity via son adresse IP et entrez les identifiants. (Comment configurer l'IP d'une Unity ?).

- Le nom d'utilisateur par défaut est : **esia**
- Mot de passe : **gesa**

Ensuite, rendez vous dans l'onglet WMI. Vous pouvez alors renseigner l'utilisateur, le mot de passe et le domaine avec lequel requêter en WMI :