

Activation de PowerShell dans Esia

Sur la machine Windows

Sur la machine Windows, il faut activer PowerShell remote.

copy

```
Enable-PSRemoting -Force  
Restart-Service WinRM
```

Vous pouvez tester à partir de votre machine Windows si vous avez accès à celle-ci en PowerShell via la commande :

copy

```
Enter-PSSession -ComputerName <nom de votre machine> -Credential  
<utilisateur> -Authentication Negotiate
```

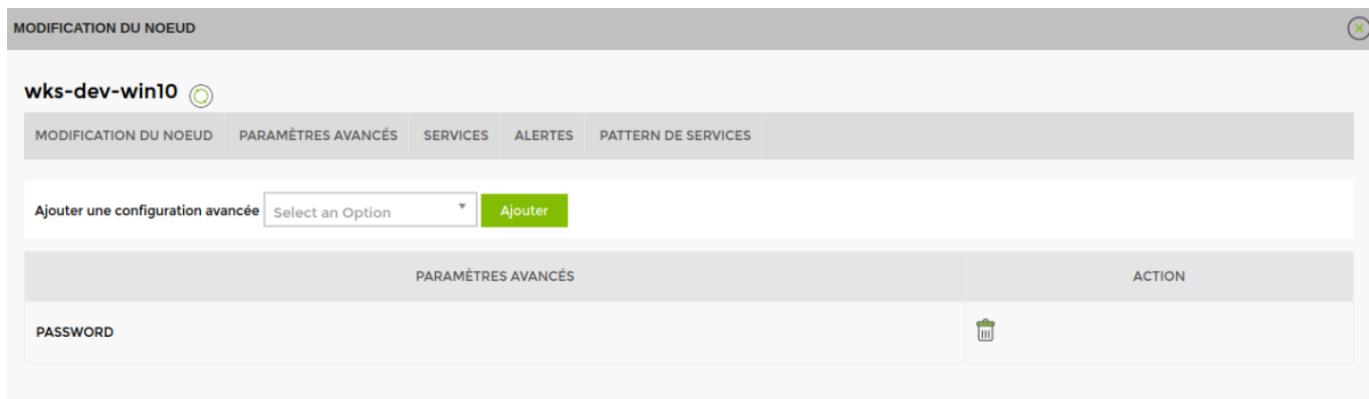
Remarque pour les pare-feu, le port par défaut de PowerShell est le même que pour WinRM : TCP 5985.

Sur votre Esia - Utilisation de PowerShell

Activer Powershell sur votre noeud

Dans les paramètres avancés de votre noeud Esia, il faut ajouter l'utilisateur et le mot de passe PowerShell.

Pour cela, sélectionnez le type 'Password' et cliquez sur Ajouter. Cliquez ensuite sur le paramètre avancé pour configurer.



The screenshot shows the 'MODIFICATION DU NOEUD' (Node Configuration) interface for a node named 'wks-dev-win10'. The 'PARAMÈTRES AVANCÉS' (Advanced Parameters) tab is selected. A table titled 'PARAMÈTRES AVANCÉS' (Advanced Parameters) is displayed. The first row contains a 'PASSWORD' column and an 'ACTION' column with a delete icon. Above the table, there is a button labeled 'Ajouter une configuration avancée' (Add advanced configuration) and a dropdown menu 'Select an Option'. The 'Ajouter' (Add) button is highlighted in green.

Ajout de patterns/plugins

Vous pouvez alors ajouter sur le noeud configuré ci-dessous le pattern et/ou les plugins suivants :

default_pwsh_windows

Contient les plugins :

- CHECK_ICMP
- CHECK_PWSH_WINDOWS_INTERFACE : Bande passante de l'interface via PowerShell
- CHECK_PWSH_WINDOWS_IO : IO/disques
- CHECK_PWSH_WINDOWS_LOAD : Charge CPU utilisée
- CHECK_PWSH_WINDOWS_MEM : Mémoire vive
- CHECK_PWSH_WINDOWS_STORAGE : Espace d'un disque dur
- CHECK_PWSH_WINDOWS_TIME : Ecart de temps entre votre Esia et votre machine Windows
- CHECK_PWSH_WINDOWS_UPTIME : Pour détecter un restart récent.

Autres plugins

- CHECK_PWSH_WINDOWS_SERVICE : Récupère le status d'un service.
- CHECK_PWSH_WINDOWS_SMARTCTL : Récupère le status smartctl des disques
- CHECK_PWSH_WINDOWS_TASK : Récupère le status d'une tâche planifiée
- CHECK_PWSH_REMOTE : [Permet d'utiliser un exécutable/script sur la machine Windows](#)

Dépannage

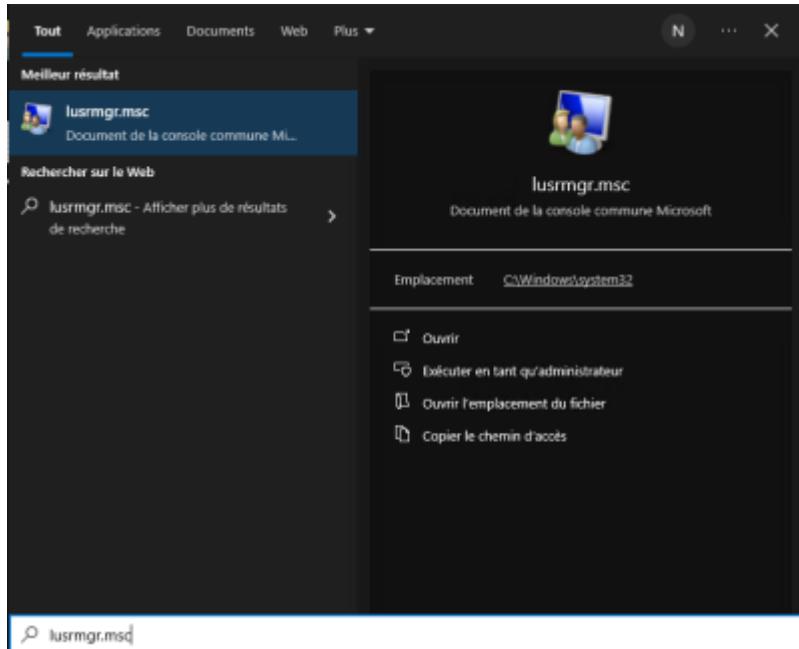
Vérifier les droits d'accès de l'utilisateur

L'utilisateur doit être membre des groupes "Administrator" et "**Remote Management Users**". En français, « Administrateurs » et « **Utilisateurs de gestion à distance** ».

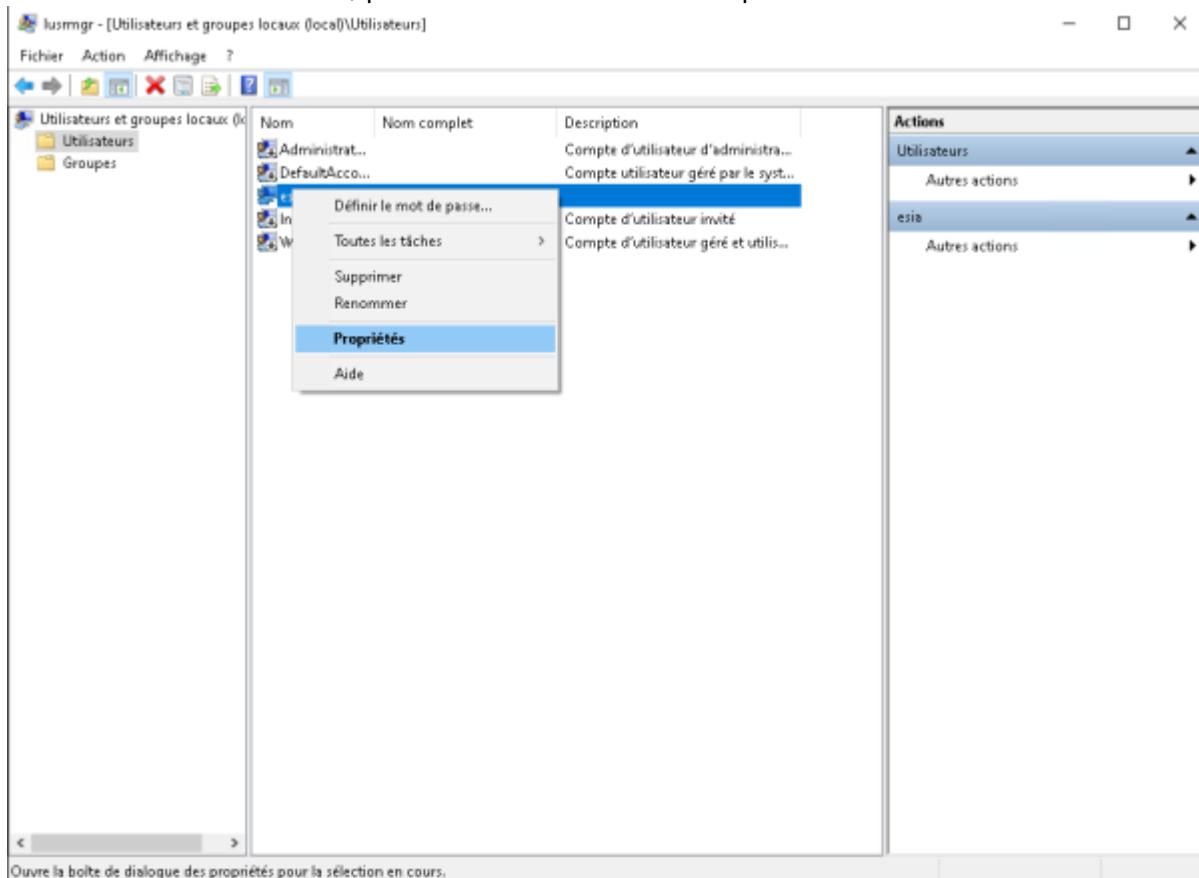
Ouvrez, « L'outil de gestion des utilisateurs et des groupes locaux ».

[copy](#)

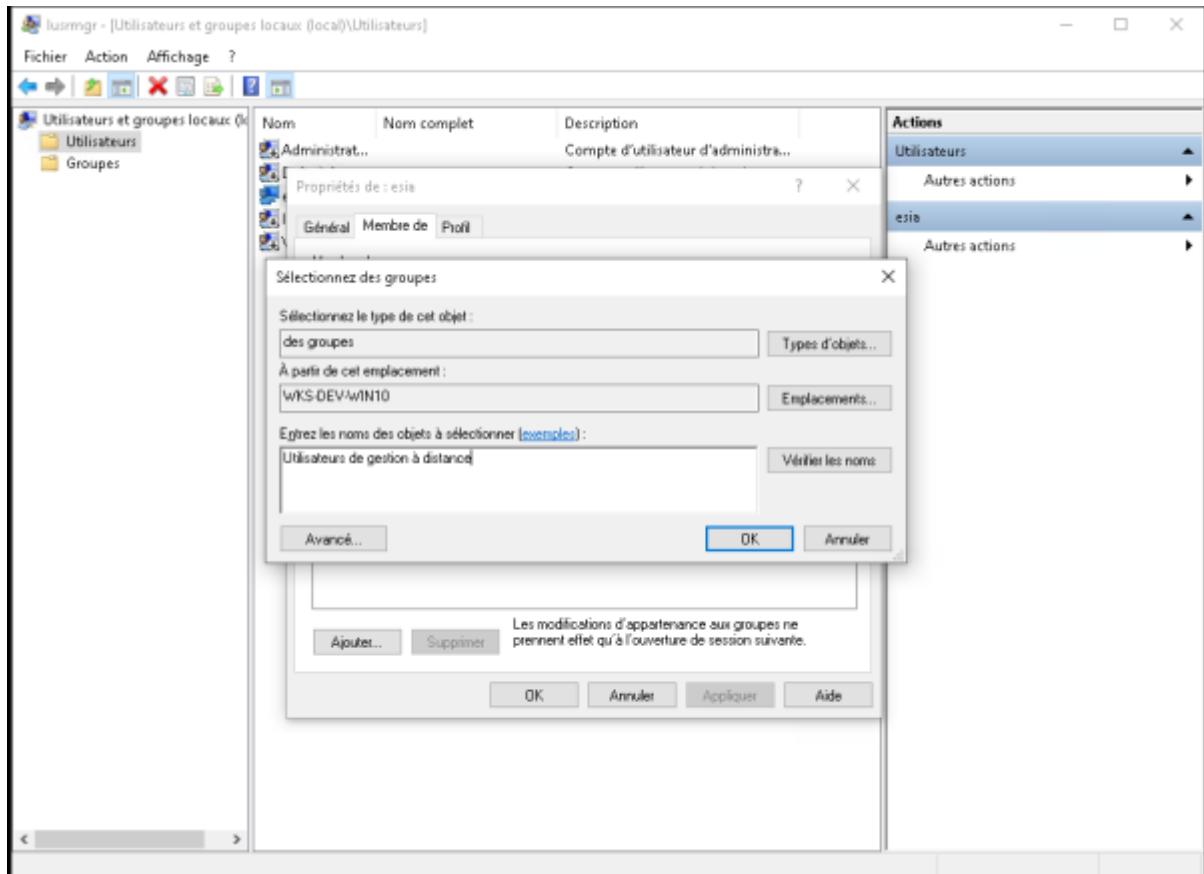
```
lusrmgr.msc
```



Allez dans « Utilisateurs », puis faites un clic droit « Propriétés » sur l'utilisateur concerné.



Allez dans l'onglet « Membre de ». Si les deux groupes ne sont pas listés, cliquez sur « Ajouter » pour ajouter les groupes manquants. Exemple avec le groupe « **Utilisateurs de gestion à distance** »



Une fois ajoutés vous devriez avoir ceci :

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

Permanent link:
https://wiki.esia-sa.com/protocols/powershell_enable

Last update: **2025/04/25 12:39**

