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
```

Il faut autoriser les comptes locaux à se connecter en PowerShell remote.

Vérifier si l'utilisateur peut exécuter des commandes à distance :

copy

```
 Get-ItemProperty
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System |
Select LocalAccountTokenFilterPolicy
```

Si ya **rien** ou **0**, lancez la commande :

copy

```
 New-ItemProperty -Path
'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System'
-Name LocalAccountTokenFilterPolicy -PropertyType DWord -Value 1 -
Force
```

Cette commande ajoute la valeur **1** dans le registre.

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
```

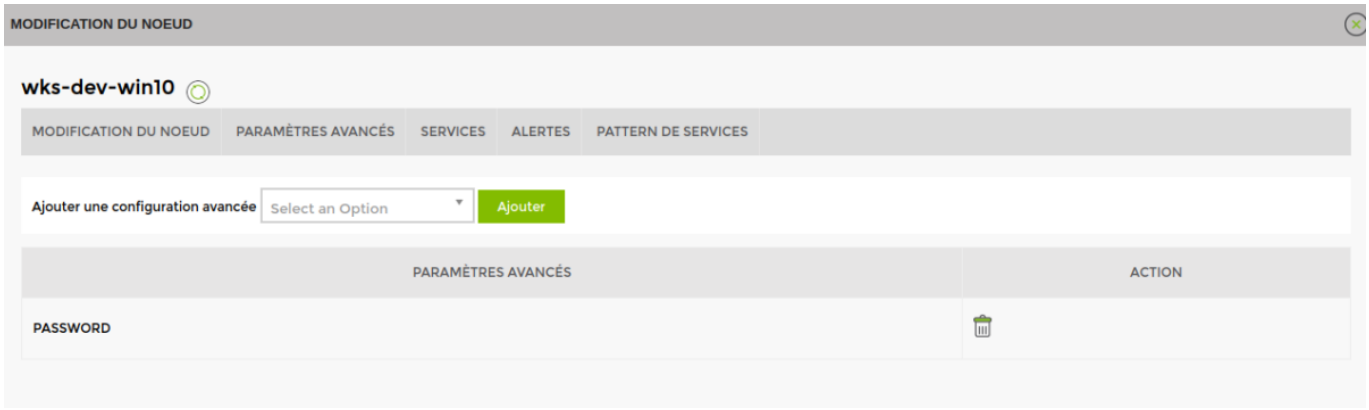
Remarque pour les pare-feu, le port par défaut de PowerShell est le même que pour WinRM : TCP 5985.

Sans Unity 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.



Avec Unity sur sa page web - Utilisation de PowerShell

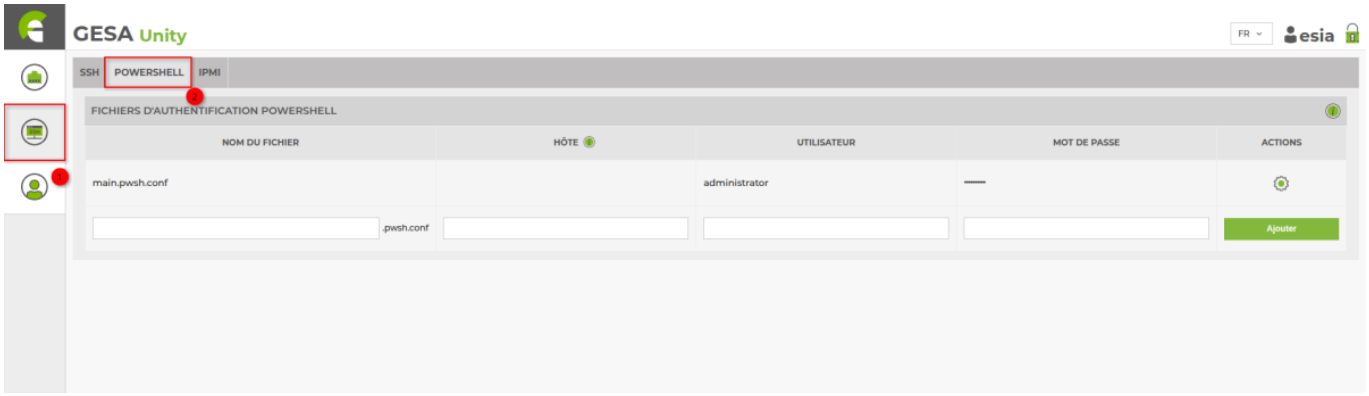
Connectez-vous sur son interfaceweb.

Dans **Protocoles** > **Powershell**

Utilisez le fichier par défaut ou créez-en un nouveau, puis renseignez les credentials :

- nom du fichier
- hôte : si le hostname est renseigné dans les paramètres du service à la place de l'adresse IP, indiquez ce même hostname.
- utilisateur : nom d'utilisateur Windows.
- mot de passe : mot de passe Windows.

l'utilisateur de la machine windows a besoin des droits administrateurs



Ajout de patterns/plugins

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

- GESA_PWSH
- CHECK_PWSH

Dépannage

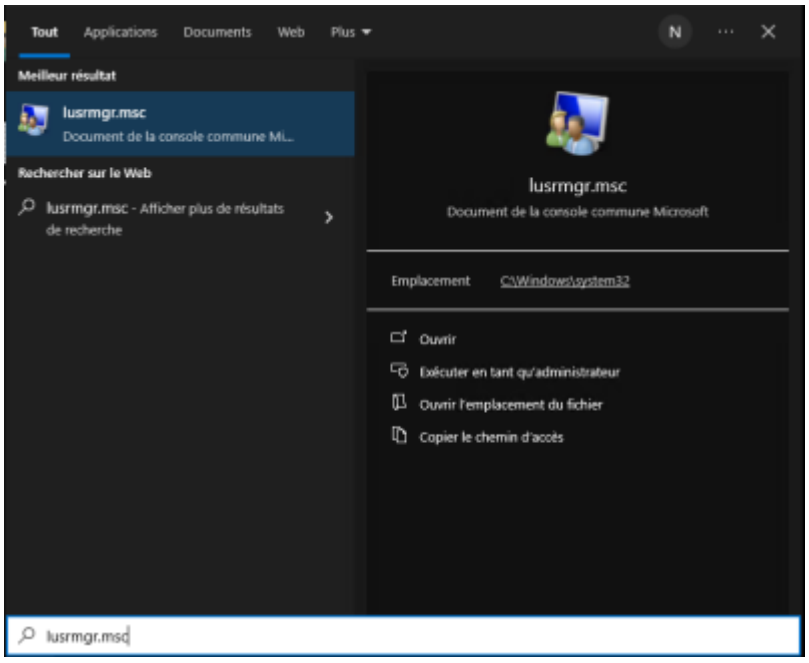
Vérifier les droits d'accès de l'utilisateur

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

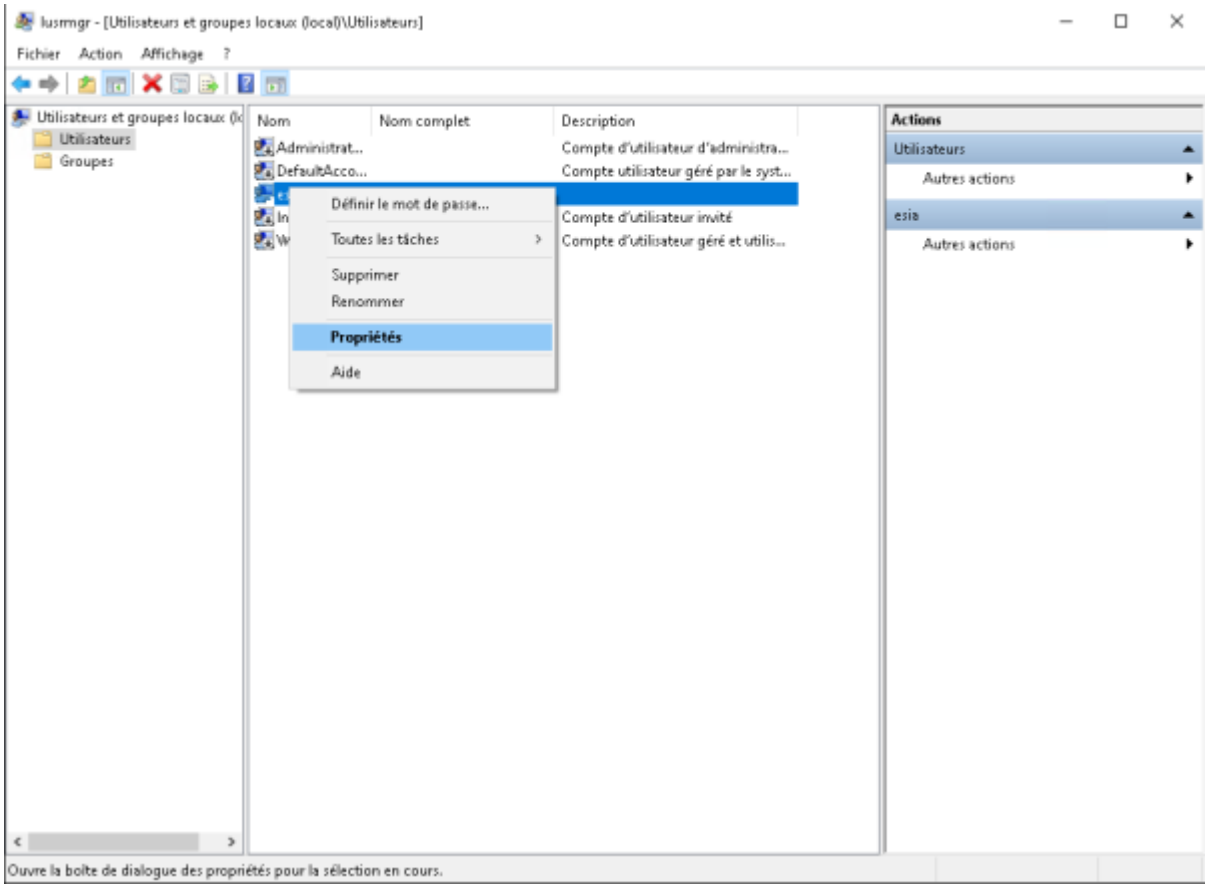
Ouvrez, « L'outil de gestion des utilisateurs et des groupes locaux ».

copy

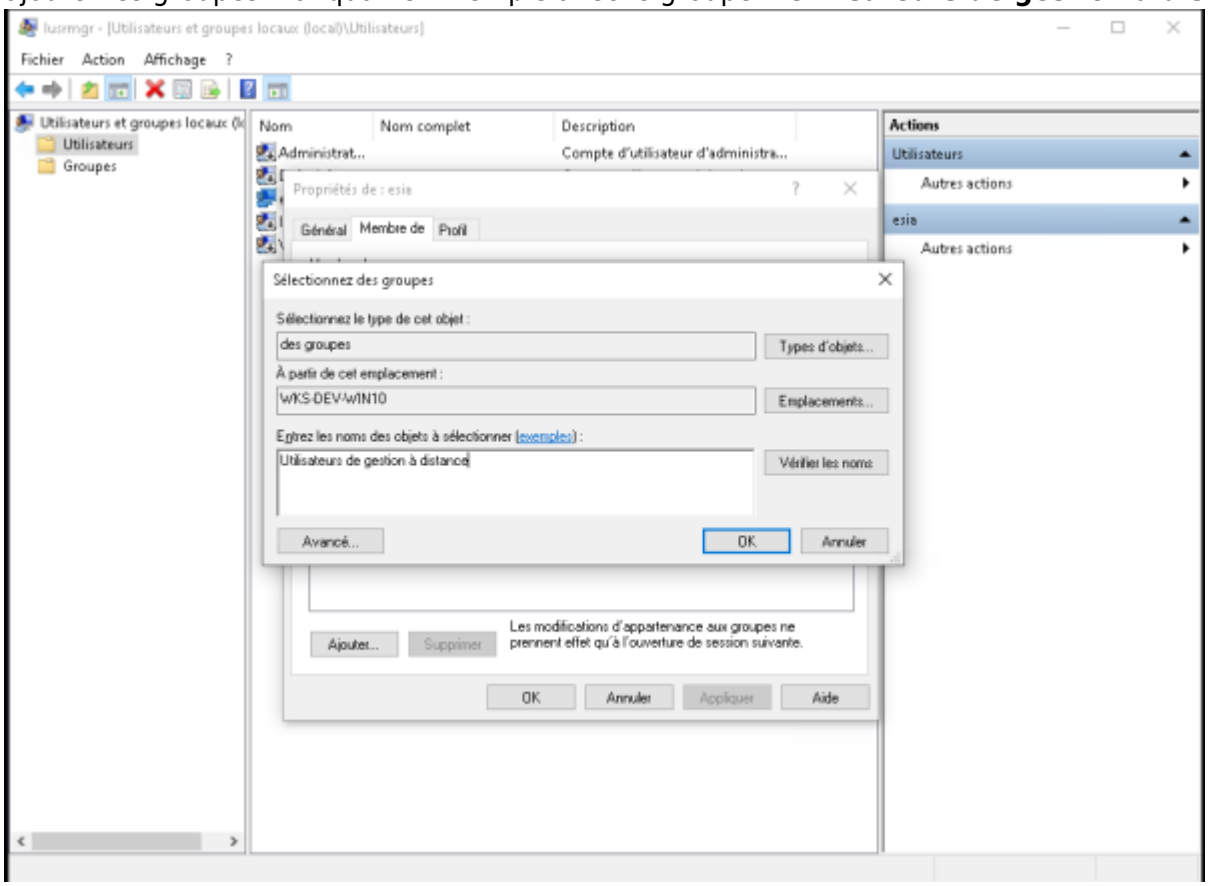
```
lusrmgr.msc
```



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: **2026/10/02 07:58**