

Activating powershell in Esia

On the node (Windows)

On the Windows machine, you need to activate powershell remote.

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

You can test from your Windows machine if you have powershell access to it via the command :

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

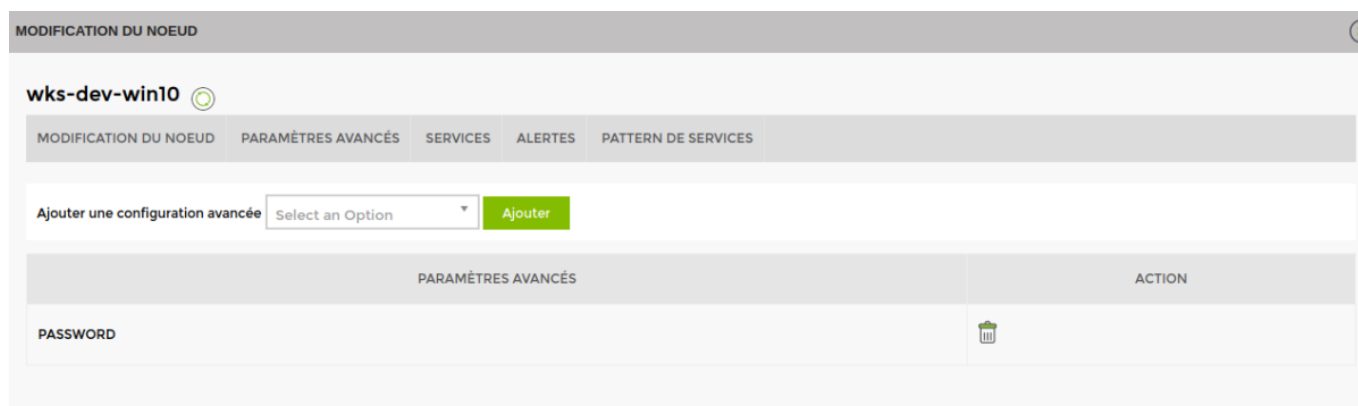
Note for firewalls, the default powershell port is the same as for WinRM: TCP 5985.

On your Esia - Using powershell

Activate powershell on your node

In the advanced settings of your Esia node, add the powershell user and password.

To do this, select the 'Password' type and click Add. Then click on the advanced parameter to configure.



Adding patterns/plugins

You can now add the following patterns and/or plugins to the node configured below:

default_pwsh_windows

Contains the plugins :

- CHECK_ICMP
- CHECK_PWSH_WINDOWS_INTERFACE: Interface bandwidth via powershell
- CHECK_PWSH_WINDOWS_IO: IO/disks
- CHECK_PWSH_WINDOWS_LOAD: CPU load used
- CHECK_PWSH_WINDOWS_MEM: Random Access Memory
- CHECK_PWSH_WINDOWS_STORAGE: hard disk space
- CHECK_PWSH_WINDOWS_TIME: time difference between your Esia and your Windows machine
- CHECK_PWSH_WINDOWS_UPTIME: To detect a recent restart.

Other plugins

- CHECK_PWSH_WINDOWS_SERVICE: Retrieves the status of a service.
- CHECK_PWSH_WINDOWS_SMARTCTL: Recovers the smartctl status of disks.
- CHECK_PWSH_WINDOWS_TASK: retrieves the status of a scheduled task.

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

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

Last update: **2024/01/15 14:53**

