

Laboratoire de gestion des réseaux informatiques (GRX)

WMI

Professeur : Alain Bron
Assistant : Rémi Poulard
Version : 3.0

Objectifs

1. Utiliser différents outils pour obtenir des informations sur vos machines Windows via WMI
2. Ecrire un script PowerShell permettant de surveiller l'espace disque d'une machine Windows et de générer un message syslog en cas de problème.

Délai et Consignes

Le fichier PDF du rapport être envoyé au professeur et à l'assistant en principe **avant le début du prochain laboratoire**. Le rapport doit être rédigé de telle sorte à ce qu'un ingénieur qui ne connaît pas la gestion des réseaux puisse refaire les expériences que vous avez menées sans autre documentation que celle de votre rapport. **Veuillez illustrer toutes vos manipulations avec des screenshots et des explications claires. Ajouter en annexe les configurations Cisco.**

Notation

Le laboratoire compte au total 8 points
Note du laboratoire = (Nb points obtenus / 5) + 2
(1 de base + 1 de présence aux labos = 2)
Exemples :
8 points obtenus → +5 → note = 6
6 points obtenus → +3 → note = 5

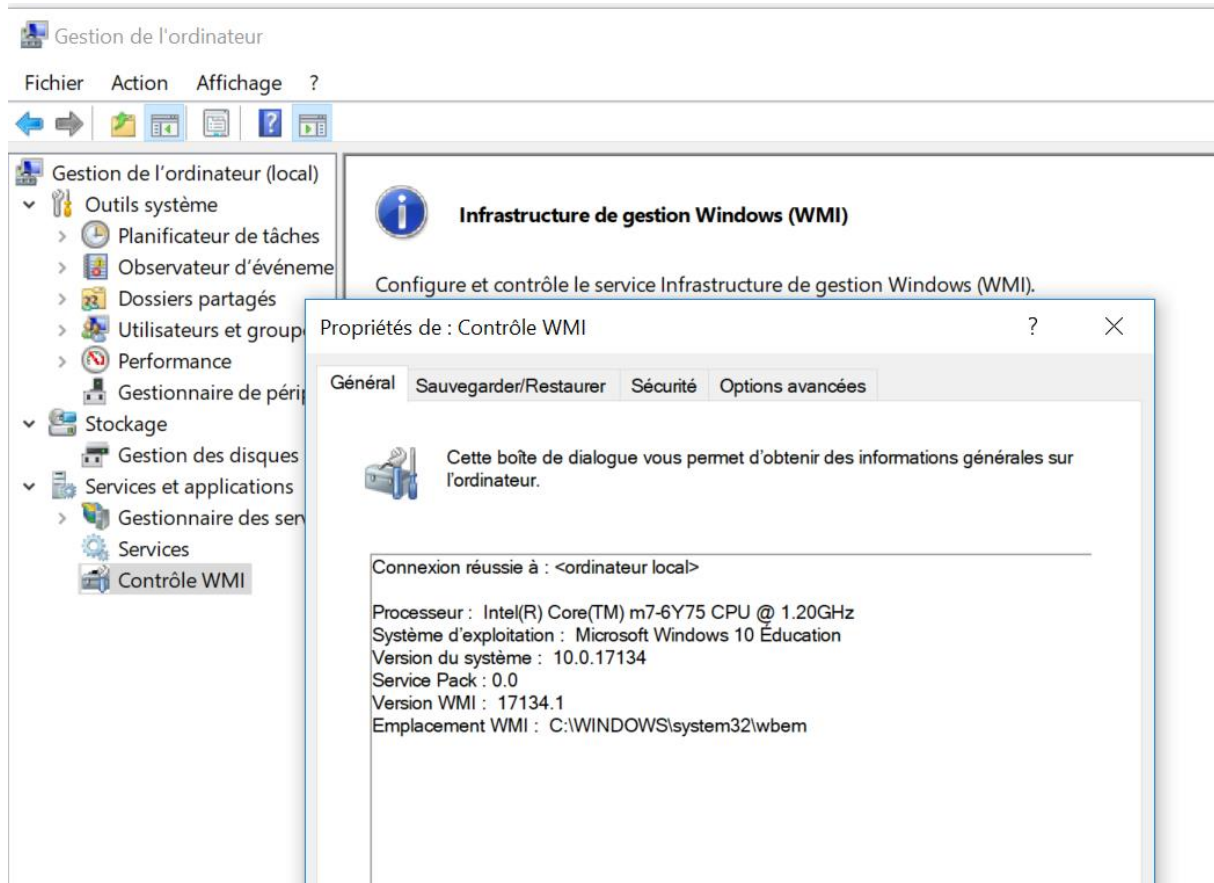
1 Introduction

Ce laboratoire permet la mise en œuvre du protocole SNMP, qui est supporté par une grande majorité des équipements (switchs, routeurs, serveurs, modems, imprimantes, PCs). SNMP se présente sous la forme d'une collection d'objets/attributs constitutifs du système cible géré par un agent SNMP. Chaque objet peut être lu et/ou écrit par le « SNMP Manager » ou console SNMP.

2 Matériel

- L'infrastructure virtuelle est la même que celle utilisée pour le labo syslog. La VM Linux n'est pas utilisée dans le cadre de ce labo.

Préalable : vérifiez que le service WMI est fonctionnel sur votre VM Windows A.



Installez les logiciels WMI Monitor, de SolarWinds et WMI explorer.
(<https://github.com/vinaypamnani/wmie2/releases>) sur la VM Windows A

Depuis la VM Windows A, interrogez la VM Windows A

1. Retrouvez les caractéristiques de votre processeur, en utilisant les différents outils installés
WMI Monitor
WMI explorer

(1 pt)

2. Retrouvez le SID de l'utilisateur Administrateur de votre système, en utilisant les différents outils installés

WMI Monitor
WMI explorer

(1 pt)

3. Retrouvez les routes IPv4 de votre système, en utilisant les différents outils installés

WMI Monitor
WMI explorer

ainsi que les outils Microsoft standards

wmic
wbemtest et
PowerShell

(2 pts)

Depuis la VM Windows A, interrogez la VM Windows A

4. Toujours depuis la VM Windows A, à l'aide de WMI Monitor, affichez la quantité de mémoire disponible sur la machine Windows B.
Montrez le trafic entre la VM Windows A et la VM Windows B à l'aide d'une capture Wireshark.

(2 pts)

5. Toujours depuis la VM Windows A, écrivez un script PowerShell qui permette de lister les partitions de la machine Windows B avec leur lettre de lecteur et de retourner le pourcentage d'espace vide.

En cas d'espace insuffisant, une alarme syslog est générée.

(2 pts)