Réalisation d'une maquette WEF & WEC

Jean-Marc Pouchoulon

octobre 2023

1 Mise en place d'une plateforme windows server 2019

Vous utiliserez les deux machines virtuelles créées lors du TP précédent. win-1 sera le serveur WEC et le contrôleur de domaine et win-2 sera le client WEF.

2 Installation de Sysmon sur win-1 et win-2

Connectez-vous sur les deux machines virtuelles win-1 et win-2.

```
vagrant ssh win-1
vagrant ssh win-2
```

Utilisez le code powershell suivant pour installer Sysmon sur les deux machines virtuelles.

```
Invoke-WebRequest -Uri "https://download.sysinternals.com/files/Sysmon.zip" -OutFile
↪  "c:\users\vagrant\Desktop\Sysmon.zip"
Invoke-WebRequest -Uri
↪  "https://raw.githubusercontent.com/Neo23x0/sysmon-config/master/sysmonconfig-export-block.xml" -OutFile
↪  "c:\users\vagrant\Desktop\sysmonconfig-export-block.xml"
Expand-Archive -F c:\users\vagrant\desktop\Sysmon.zip -DestinationPath c:\users\vagrant\desktop\sysmon
# version amélioré de swift on security
c:\users\vagrant\desktop\sysmon\sysmon64.exe -accepteula -i c:\users\vagrant\desktop\sysmonconfig-export-block.xml
```

Vérifiez que Sysmon alimente bien le journal des événements de Windows et son channel Microsoft-Windows-Sysmon/Operational.

Sauvegarder les logs Sysmon dans un fichier evtx à l'aide wevtutil.exe.

```
wevtutil query-events /c:5  Microsoft-Windows-Sysmon/Operational
wevtutil export-log Microsoft-Windows-Sysmon/Operational sysmon.evtx
wevtutil export-log WecFwdLog-Domain-Members/Security  security-apt.evtx
wevtutil export-log WecFwdLog-Domain-Members/Sysmon  sysmon-apt.evtx
```

3 Installation WEC

3.1 instructions

Utilisez la procédure d'installation d'un serveur WEC en image ici. La machine win-1 sera le serveur WEC.

La VM win-2 initiera les abonnements aux journaux d'événements de win-1 ("source computer initiated") sur le channel "forwarded events". C'est le système de fonctionnement plébiscité par les experts Microsoft.

Les clients WEC seront configurés par GPO. Ainsi chaque nouveau PC ajouté au domaine "forwardera" automatiquement ses logs sur le serveur WEC (win-1).

3.2 Déploiement de la GPO WEF sur win-2

Construisez ensuite une GPO pour déployer la configuration WEF sur win-2. Vous suivrez la procédure suivante ici

3.3 Vérifications et validation

Quelques éléments de vérification avant d'appeler l'enseignant si ça ne fonctionne pas :

- Ping entre les deux machines.
- Vérifiez que win-2 est bien au domaine.
- Résolution de nom de win-1 depuis win-2 et réciproquement.
- Traces du déploiement de la GPO sur win-2 dans la sortie de la commande "gpresult /r".
- Vérifiez que l'URL transmise à win-2 contient bien server=http...
- Firewall ouvert sur win-1 pour le port 5985 (vous pouvez arrêter le firewall même si c'est mal...).

3.4 Vérifications et validation

Quand vous voyez apparaître les logs de win-2 sur l'"event viewer" de win-1 dans le channel "Forwarded" (Sysmon compris) c'est que votre collecte fonctionne.

Appelez alors l'enseignant pour valider.