Gestion des réseaux et sécurité opérationnelle (GRS)

Syslog

Professeur : Alain Bron

Assistant :

Version : 2.1

Objectifs

1. Configurer un serveur et des clients Syslog
2. Configurer Syslog sur des composants du réseau
3. Rediriger les événements Windows sur un serveur Syslog

Délai

La date de remise (via le formulaire cyberlearn) sera définie en classe.

Introduction

Dans ce laboratoire, vous allez utiliser un premier protocole standard utilisé dans la gestion des réseaux, Syslog, supporté par la plupart des équipements (réseau, imprimantes, ordinateurs sous Windows ou Linux) et permettant à chaque client/agent d'envoyer ses logs sur un serveur central. Ce protocole est utilisé dans la gestion des systèmes informatiques, pour des audits de sécurité, ainsi que pour l'analyse et le dépannage dans un cadre plus général.

Notation

Notation sur 15 points (note finale = 1.0 + nb de point /3)

Infrastructure

L'infrastructure virtuelle utilisée est celle mise en place au labo 0.

Les programmes `SyslogGenerator.exe` et `visualsyslog_setup.exe` sont disponibles sur la VM Windows 10.

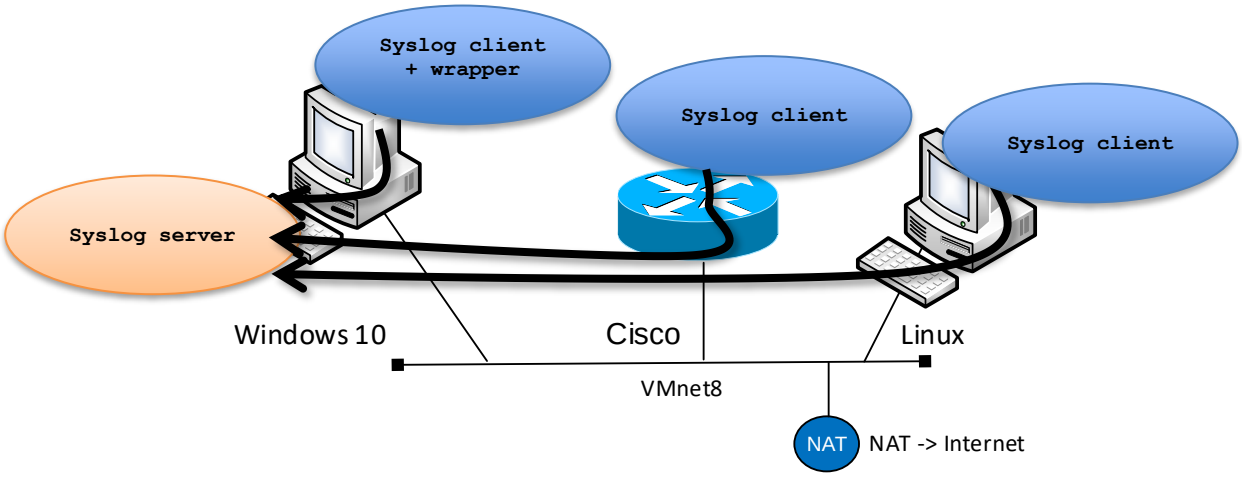
`rsyslog` est installé sur le noeud Linux.

Son fichier de configuration principal est /`etc/rsyslog.conf` et les fichiers liés se trouvent dans le répertoire `/etc/rsyslog.d/`

Gestion manuelle du daemon : `sudo systemctl start|stop|restart|status rsyslog`

La nœud Windows 10 opère en tant que serveur de collecte Syslog.

Les nœuds Windows 10, Linux et Cisco seront configurés pour transmettre des événements au serveur Syslog.



1 Configurer un serveur Syslog

Sur le nœud PC Windows 10.

- Démarrez le serveur `Visual Syslog Server`.
- Lancez `SyslogGenerator`. A l'aide de cet outil vous pouvez tester que votre serveur Syslog reçoit bien les messages générés localement. Faites quelques tests avec différents types de message et notamment un message contenant votre nom.

1. Montrez, avec une copie d'écran, les événements reçus par votre serveur Syslog

2 Configurer un client Linux

Sur le nœud Linux.

- Configurer Syslog (`rsyslog`), en modifiant le fichier de configuration qui se trouve dans le répertoire `/etc/rsyslog.conf/` pour qu'il redirige les logs sur le serveur situé sur le PC Windows 10 (Port UDP 514).

2. Montrez votre fichier de configuration (les commandes importantes)

- Générez des messages depuis la VM Linux (`reboot`, `sudo` et en utilisant la commande `logger`) et capturez simultanément le trafic Syslog à l'aide de Wireshark.

3. Montrez les messages reçus sur la console du serveur Syslog distant (Windows 10).
4. Donnez plusieurs exemples de messages qui vous semblent utiles dans la gestion des réseaux.
5. Que pouvez-vous dire sur la sécurité des échanges de messages Syslog ?
6. Présentez et expliquer la captures wireshark d'un message Syslog.
7. Modifiez votre configuration afin que les messages Syslog générés par la commande `sudo` (et exclusivement ceux-ci) soient stockés dans le fichier local `/var/log/sudos.log`

3 Configurer Syslog sur un équipement réseau

Sur le nœud Cisco.

- Configurez votre routeur de manière à récupérer les messages de niveau Debug, en tant que Local_3, sur votre serveur Syslog.

8. Montrer les commandes IOS que vous avez utilisé.

- Configurer votre routeur afin qu'il soit possible d'assurer une corrélation précise (précision à la milliseconde) des événements reçus par le serveur Syslog, en utilisant le protocole NTP.

9. Montrer les commandes IOS que vous avez utilisé.

- Configurez votre routeur Cisco de manière à récupérer un message contenant la commande utilisée, lors d'une modification de la configuration. Par hypothèse, les logs sont maintenant fixés au niveau Warning et plus Debug.

10. Montrer les commandes IOS que vous avez utilisé.
11. Montrer le message reçu.

4 Rediriger les événements Windows sur un serveur Syslog

Sur le nœud Windows 10.

- A l'aide de la commande `logger.exe`, envoyez un message à votre serveur Syslog.

  12. Montrez la commande et le message reçu sur le serveur Syslog

- Générez un message Syslog à l'aide de la cmdlet `Send-SyslogMessage` (module `Posh-SYSLOG`) en mode RFC 3164 et 5424 et comparez les messages

  13. Montrez la commande utilisée et les messages reçus par le serveur Syslog

- Créez un script PowerShell qui vérifie toutes les 2 minutes la présence d'un processus p (par exemple cmd.exe) et qui génère un message Syslog en cas d'absence.

  14. Montrez le contenu du script et le message reçu par le serveur Syslog

A l'aide de https://www.solarwinds.com/free-tools/event-log-forwarder-for-windows ou le cmdlet `Send_syslogMessage`:

- Redirigez, vers le serveur Syslog, l'événement Windows (Observateur d'événements) liés à un échec de login local.

  15. Montrez le bon fonctionnement de la redirection à l'aide d'une copie d'écran du serveur Syslog

5 Utilisation de Sysmon

Sur le nœud Windows 10.

- Installez l'extension `sysmon` (*Microsoft Sysinternals*) et configurez-le, via un fichier XML, de manière que les connexions vers le port `80` et les requêtes DNS sur le site `lematin.ch` soient journalisée et visible dans l'Observateur d'événements.

16. Montrez le contenu de votre fichier XML.
17. Montrez le message reçu.