TP 2 : Logs et supervision

Architecture

Vous disposez toujours de l'ensemble des machines du TP1. Dans le cadre de ce TP2 vous utiliserez **uniquement les connexions SSH** vers les machines.

Gestion des logs

Sur chacune des machines l'ensemble des opérations d'authentification (locale, SSH, su, sudo) seront *loggées*.

Toutes les opérations réussies seront enregistrées en local sur chaque machine dans le fichier `/var/log/opOK.log`.

Toutes les erreurs seront quant à elles *loggées* sur le serveur Syslog-ng de la machine debian dans différents fichiers. L'architecture des fichiers permettra de repérer la machine et le type d'accès illégal.

Supervision

On souhaite mettre en œuvre une solution de supervision basée sur SNMP. Le NMS sera la machine Ubuntu.

Installez et configurez l'ensemble des paquets nécessaire à la mise en œuvre de SNMP sur l'architecture à disposition.

Configurez l'ensemble des informations standards des différentes machines (nom et adresse de l'administrateur …).

Configurez les machines afin de pouvoir récupérer les informations de charge mémoire, cpu et d'occupation de disque par une requête SNMP que vous écrirez.

Configurez les machines afin de pouvoir récupérer la liste des paquets installés et des utilisateurs connectés sur chaque machine.

Configurez les machines afin de pouvoir "vider" depuis le NMS les fichiers de log des accès réussis présents sur chacune des machines.