Installer Lynis

- Ressources : https://cisofy.com/documentation/lynis/get-started/
- Se loguer en tant que *admin* sur le serveur : `ssh admin@<…>-<region>-sinp`
    - Passer en *root* : `sudo -i`
- Se placer dans le dossier */opt/* : `cd /opt`
- Récupérer le code de la dernière version de Lynis : https://github.com/CISOfy/lynis/releases
- Télécharger la dernière version de Lynis : `wget https://cisofy.com/files/lynis-<version>.tar.gz`
- Décompresser l'archive : `tar xfvz lynis-<version>.tar.gz`
- Supprimer l'archive : `rm -f lynis-<version>.tar.gz`
- Se placer dans le dossier de Lynix et commencer à l'utiliser : `cd /opt/lynis`
    - afficher l'aide : `./lynis`
    - vérifier la version : `./lynis update info`
    - auditer le système : `./lynis audit system`
        - consulter le log de l'audit : `vi /var/log/lynis.log`
        - voir le détail d'un test : `./lynis show details <TEST-ID>`
        - relancer un test particulier : `./lynis audit system --tests <TEST-ID>`
- Vérifier et essayer de résoudre les warnings

From:
http://sinp-wiki.cbn-alpin.fr/ - **CBNA SINP**

Permanent link:
http://sinp-wiki.cbn-alpin.fr/serveurs/installation/lynis

Last update: **2024/02/20 14:48**