**Installation OpenVas**

2019-06-07

**Historique des versions**

|  |  |  |
| --- | --- | --- |
| Date | Author | Description |
| 06/06/2019 | Vincent ROSET | Document creation |
|  |  |  |
|  |  |  |
|  |  |  |

**Sommaire**

[1 Installation d’openVas 2](#_Toc18073580)

[1.1 Mise en place 2](#_Toc18073581)

[1.2 Choix d’installation 2](#_Toc18073582)

[1.3 Ajout du dépôt tiers 3](#_Toc18073583)

[1.4 Installation du paquet OpenVas 3](#_Toc18073584)

[1.5 Mise à jour des feeds du scanner 3](#_Toc18073585)

[1.6 Configuration des services 3](#_Toc18073586)

[1.7 Ajout des utilisateurs 4](#_Toc18073587)

[1.8 Redirection des ports 4](#_Toc18073588)

# Installation d’openVas

## Mise en place

Afin de pouvoir installer proprement OpenVas sur un serveur, il est nécessaire d’avoir une VM Ubuntu Server 18.04 pouvant s’authentifier sur le proxy de Klépierre. Plus précisément une VM qui peut :

* Mettre à jour ses dépôts ;
* Modifier le fichier de configuration des dépots ;
* Télécharger des fichiers via la commandes wget ;
* Avoir un service rsync correctement configuré ;

## Choix d’installation

Installer OpenVas directement par les dépôts officiels d’Ubuntu ne fonctionnait pas. L’un des composants (Openvas-Scanner) était buggé.

Donc afin de pallier à ce problème 4 autres idées furent trouvés :

* Installer et compiler sur la vm les composants d’openvas
* Utiliser un docker openvas
* Utiliser une iso officielle du constructeur greebone (qui vend aussi des appliances)
* Utiliser un dépôt tiers

La meilleure solution fut celle d’utilisait un dépôt tiers à savoir celui de Mohamed Razavi.

En voici le lien ci-dessous.

<https://launchpad.net/~mrazavi/+archive/ubuntu/gvm>

## Ajout du dépôt tiers

|  |
| --- |
| add-apt-repository ppa:mrazavi/openvas  nano /etc/apt/sources.list.d/mrazavi-ubuntu-openvas-bionic.list |

Dans le fichier nano /etc/apt/sources.list.d/mrazavi-ubuntu-openvas-bionic.list décommenter la ligne deb-src.

Puis mettre à jour les dépôts :

|  |
| --- |
| apt update |

## Installation du paquet OpenVas

Pour installer le pacquet openvas 9 adéquat (et non celui du dépôt officiel d’ubuntu) il faut indiquer openvas9 et non openvas lors de la requête d’installation.

|  |
| --- |
| apt install -y openvas9 |

L’option –y permettra d’ajouter les dépendances nécessaires au cours de son installation.

## Mise à jour des feeds du scanner

L’étape intermédiaire consiste à télécharger la dernière base de données des vulnérabilités. Ce qui se fait avec les commandes ci-dessous :

|  |
| --- |
| # la synchronisation peut échouer due à des problèmes de proxy  # il vaut en cas d'erreur relancer plusieurs fois la synchronisation des tests de vulnérabilités  # a noter que ceci prends du temps  greenbone-nvt-sync --rsync  greenbone-nvt-sync  greenbone-scapdata-sync  greenbone-certdata-sync |

La commande greenbone-nvt-sync est répétée deux fois, car elle est sujette à des problèmes réseaux.

## Configuration des services

Il faut désormais configure les services d’OpenVas pour qu’ils soient accessible de l’extérieur :

|  |
| --- |
| #Configuration de l'interface Web  # il se met en écoute sur le port 9390 et 4000  service openvas-scanner stop  service openvas-manager stop  service openvas-gsa stop  echo "LISTEN\_ADDRESS=\"0.0.0.0\"" >> /etc/default/openvas-gsa  echo "MANAGER\_ADDRESS=\"0.0.0.0\"" >> /etc/default/openvas-gsa  echo "MANAGER\_PORT\_NUMBER=9390" >> /etc/default/openvas-gsa  echo "LISTEN\_ADDRESS=\"0.0.0.0\"" >> /etc/default/openvas-manager  echo "PORT\_NUMBER=9390" >> /etc/default/openvas-manager  systemctl daemon-reload  systemctl start openvas-scanner  systemctl start openvas-gsa |

## Ajout des utilisateurs

Afin d’accéder au portail, il faut définir un compte administrateur et un un compte utilisateur.

|  |
| --- |
| # ajout des users admin et omp (mdp par défaut)  openvasmd --create-user=admin --role=Admin  openvasmd --create-user=omp --role=Admin  openvasmd --user=admin --new-password=admin  openvasmd --user=omp --new-password=omp  #démarrage du service  systemctl start openvas-manager |

## Redirection des ports

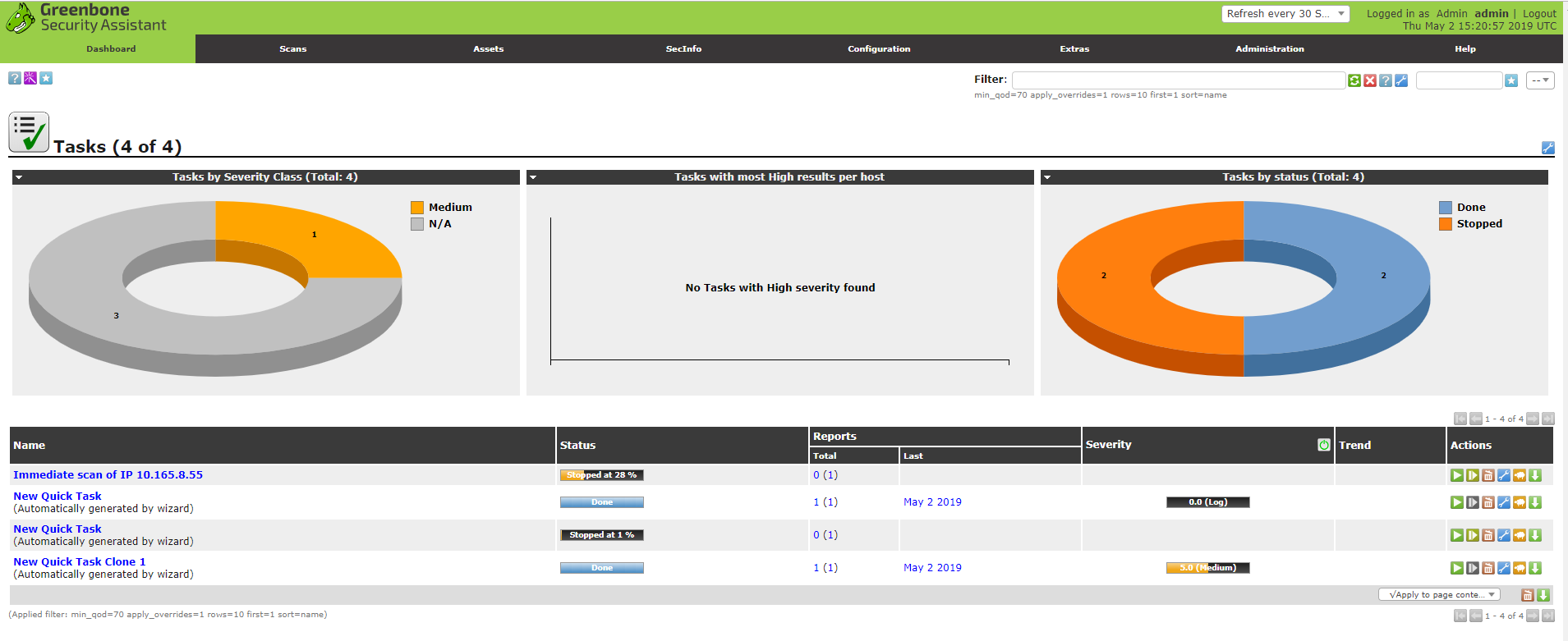
En fonction des paramètres réseaux de la VM il peut être nécessaire de faire une redirection de Port. Notamment si l’interface réseau est en NAT.

Le service d’openvas gsad chargé de démarrer l’application, écoute sur le port 4000. Il est nécessaire de vérifier que celui-ci écoute bien sur le port 4000 avec les commandes ci-dessous :

|  |
| --- |
| #normalement gsad écoute sur le port 4000  netstat -antp  #gsad, openvassd et openvasmd sont lancés  ps -ef | grep openvas  ps -ef | grep gsad |

Après avoir correctement configuré les redirections de ports, l’url d’accès à l’interface web est :

https://localhost :4000



*Page principale d’OpenVas*