INSTITUT PAUL LAMBIN - INFORMATIQUE DE GESTION

Guide d'installation de la data diode

Stage à l'École Royale Militaire

MANSOURI Zacharia

Le 15 Mai 2020

Table des matières

Informations préliminaires

Dans la suite, il est préférable de ne pas installer tout ce qui est en rapport avec le module NTP, ce dernier n'étant pas terminé (si, par curiosité, ce dernier est installé, alors il faut décommenter la ligne 22 du fichier Vagrantfile).

Le fichier Vagrantfile permet de visualiser le réseau de machines. Seules les machines diodein, diodeout et secure importent.

Pour les tests sur machines virtuelles, il existe deux dossiers :

- Separate : contient les tests que l'on peut effectuer d'une traite indépendamment sur diodein ou diodeout ;
- Parallel : contient les tests qui doivent être d'abord effectués sur diodein, pour l'être ensuite sur diodeout à peu près 10 secondes plus tard. Chacun de ces tests est à effectuer séparément des autres tests du même dossier. Il faut donc lancer chaque test de ce dossier sur diodein, attendre 10 secondes, le lancer sur diodeout et attendre que le test soit terminé sur chaque machine avant de passer au suivant.

Installation diodein

L'ensemble des commandes à utiliser se situe dans le fichier `/vagrant/diode-in.sh`. Des explications seront données sur les différentes lignes de ce fichier, précisant ce qu'il faut installer. À noter qu'une connexion internet est nécessaire et que l'ensemble des commandes est à exécuter en tant que root. Un utilisateur nommé *www-data* doit aussi être présent sur la machine.

Astuce : une commande avec des pipes, des chevrons, etc peut etre exécutée en tant que root de la manière suivante : sudo sh -c 'commande entre apostrophes'.

Ligne 2 : seulement utile pour l'installation automatisée par vagrant. La valeur *noninteractive* correspond au comportement suivant : *This is the anti-frontend. It never interacts with you at all, and makes the default answers be used for all questions. It might mail error messages to root, but that's it ; otherwise it is completely silent and unobtrusive, a perfect frontend for automatic installs. If you are using this front-end, and require non-default answers to questions, you will need to preseed the debconf database ; see the section below on Unattended Package Installation for more details.* [1]. Il ne faut donc pas exécuter cette commande.

Lignes 3-4 : à exécuter pour installer tous les programmes nécessaires à diodein.

Lignes 5-15 : à exécuter pour pouvoir déployer l'interface web de diodein sur le port 80.

Lignes 16-32 : à remplacer par un git clone vers l'url du projet git de la data diode. Cela doit se faire à la racine `/var/www/`, de manière à avoir le projet `/var/www/data-diode/`.

Lignes 33-41 : à exécuter pour permettre à Laravel d'installer les dépendances, d'obtenir diverses configurations et de générer une clé et une base de données.

Ligne 42 : à remplacer par une commande qui permet de placer le dossier BlindFTP_0.37 à la racine `/var/www/data-diode/`.

Ligne 44 : à exécuter pour prendre en compte les modifications faites ci-dessus.

Lignes 48-49 : à exécuter pour installer supervisor.

Lignes 51-54 : à exécuter pour lancer et permettre le relancement au démarrage de supervisor.

Ligne 56 : à exécuter pour installer python-pypi-mirror.

Lignes 58-59 : à exécuter pour installer python-dotenv.

Lignes 61-74 : ces lignes correspondant à la configuration du serveur NTP. Le module NTP n'étant pas entièrement terminé, ces lignes ne sont pas à exécuter.

1. `https://askubuntu.com/questions/972516/debian-frontend-environment-variable`

Lignes 76-77 : à exécuter pour octroyer des droits sur divers dossiers à l'utilisateur *www-data*. Si les lignes 61-74 n'ont pas été exécutées, il faut retirer `/etc/ntp.conf` de la ligne 77.

Lignes 79-80 : à exécuter pour permettre le packet forwarding.

Ligne 81 : à exécuter pour octroyer des droits sur divers scripts à l'utilisateur *www-data*.

Lignes 83-85 : ces lignes correspondant au module NTP, ce dernier n'étant pas entièrement terminé, elles ne sont pas à exécuter, sauf si les lignes 61-74 ont été exécutées.

Installation diodeout

L'ensemble des commandes à utiliser se situe dans le fichier `/vagrant/diode-out.sh`. Des explications seront données sur les différentes lignes de ce fichier, précisant ce qu'il faut installer. À noter qu'une connexion internet est nécessaire et que l'ensemble des commandes est à exécuter en tant que root. Un utilisateur nommé *www-data* doit aussi être présent sur la machine.

Astuce : une commande avec des pipes, des chevrons, etc peut etre exécutée en tant que root de la manière suivante : sudo sh -c 'commande entre apostrophes'.

Ligne 2 : seulement utile pour l'installation automatisée par vagrant. La valeur *noninteractive* correspond au comportement suivant : *This is the anti-frontend. It never interacts with you at all, and makes the default answers be used for all questions. It might mail error messages to root, but that's it ; otherwise it is completely silent and unobtrusive, a perfect frontend for automatic installs. If you are using this front-end, and require non-default answers to questions, you will need to preseed the debconf database ; see the section below on Unattended Package Installation for more details.* [1]. Il ne faut donc pas exécuter cette commande.

Lignes 3-4 : à exécuter pour installer tous les programmes nécessaires à diodeout.

Lignes 5-15 : à exécuter pour pouvoir déployer l'interface web de diodeout sur le port 80.

Lignes 16-32 : à remplacer par un git clone vers l'url du projet git de la data diode. Cela doit se faire à la racine `/var/www/`, de manière à avoir le projet `/var/www/data-diode/`.

Lignes 33-41 : à exécuter pour permettre à Laravel d'installer les dépendances, d'obtenir diverses configurations et de générer une clé et une base de données.

Ligne 42 : à remplacer par une commande qui permet de placer le dossier BlindFTP_0.37 à la racine `/var/www/data-diode/`.

Ligne 44 : à exécuter pour prendre en compte les modifications faites ci-dessus.

Lignes 48-49 : à exécuter pour installer supervisor.

Lignes 51-54 : à exécuter pour lancer et permettre le relancement au démarrage de supervisor.

Ligne 56 : à exécuter pour installer python-pypi-mirror.

Lignes 58-59 : à exécuter pour installer python-dotenv.

Lignes 61-69 : ces lignes correspondent à la configuration du serveur NTP. Le module NTP n'étant pas entièrement terminé, ces lignes ne sont pas à exécuter.

1. `https://askubuntu.com/questions/972516/debian-frontend-environment-variable`

Lignes 71-72 : à exécuter pour octroyer des droits sur divers dossiers à l'utilisateur *www-data*. Si les lignes 61-69 n'ont pas été exécutées, il faut retirer `/etc/ntp.conf` de la ligne 72.

Lignes 74-75 : à exécuter pour permettre le packet forwarding.

Ligne 76 : à exécuter pour octroyer des droits sur divers scripts à l'utilisateur *www-data*.

Lignes 79-81 : à exécuter pour créer le dossier qui contiendra les dossiers zippés.

Lignes 84-94 : ces lignes correspondant au module NTP, ce dernier n'étant pas entièrement terminé, elles ne sont pas à exécuter, sauf si les lignes 61-69 ont été exécutées.

Installation secure

L'ensemble des commandes à utiliser se situe dans le fichier `/vagrant/secure.sh`. Des explications seront données sur les différentes lignes de ce fichier, précisant ce qu'il faut installer. À noter que l'ensemble des commandes est à exécuter en tant que root. Le réseau peut contenir plusieurs machines secure.

Astuce : une commande avec des pipes, des chevrons, etc peut etre exécutée en tant que root de la manière suivante : sudo sh -c 'commande entre apostrophes'.

Ligne 2 : seulement utile pour l'installation automatisée par vagrant. La valeur *noninteractive* correspond au comportement suivant : *This is the anti-frontend. It never interacts with you at all, and makes the default answers be used for all questions. It might mail error messages to root, but that's it ; otherwise it is completely silent and unobtrusive, a perfect frontend for automatic installs. If you are using this front-end, and require non-default answers to questions, you will need to preseed the debconf database ; see the section below on Unattended Package Installation for more details.* [1]. Il ne faut donc pas exécuter cette commande.

Lignes 3-4 : à exécuter pour installer tous les programmes nécessaires à diodeout. Si le module NTP n'a pas été installé sur diodein et diodeout, il faut retirer `ntp` de la ligne 4.

Lignes 6-7 : à exécuter pour installer python-pypi-mirror.

Lignes 9-32 : à ne pas exécuter si le module NTP n'a pas été installé sur diodein et diodeout.

Ligne 37 : permet d'établir la communication NTP entre secure et diodeout. À ne pas exécuter si le module NTP n'a pas été installé sur diodein et diodeout. Si exécuté, il est nécessaire de lier l'adresse IP 192.168.102.1 avec une addresse MAC (ici : 00AABBBBAA00, cf Vagrantfile ligne 22).

Ligne 42 : programmes nécessaires à l'installation d'Opera depuis la data diode. Cette ligne est présente à cause des dépendances dont Opera a besoin et qui ne pouvaient pas être téléchargées vu que le miroir présent sur la data diode n'était pas complet lors des tests, il s'agissait d'un simple miroir Opera et non d'un miroir APT. À ne pas exécuter mais il faut s'assurer de bien avoir un miroir APT complet sur la data diode.

Lignes 9-32 : à exécuter afin de vider le fichier `/etc/apt/sources.list` qui sera rempli lors de l'utilisation de la data diode (voir mini guide APT sur l'interface web de diodeout pour plus d'informations).

1. `https://askubuntu.com/questions/972516/debian-frontend-environment-variable`