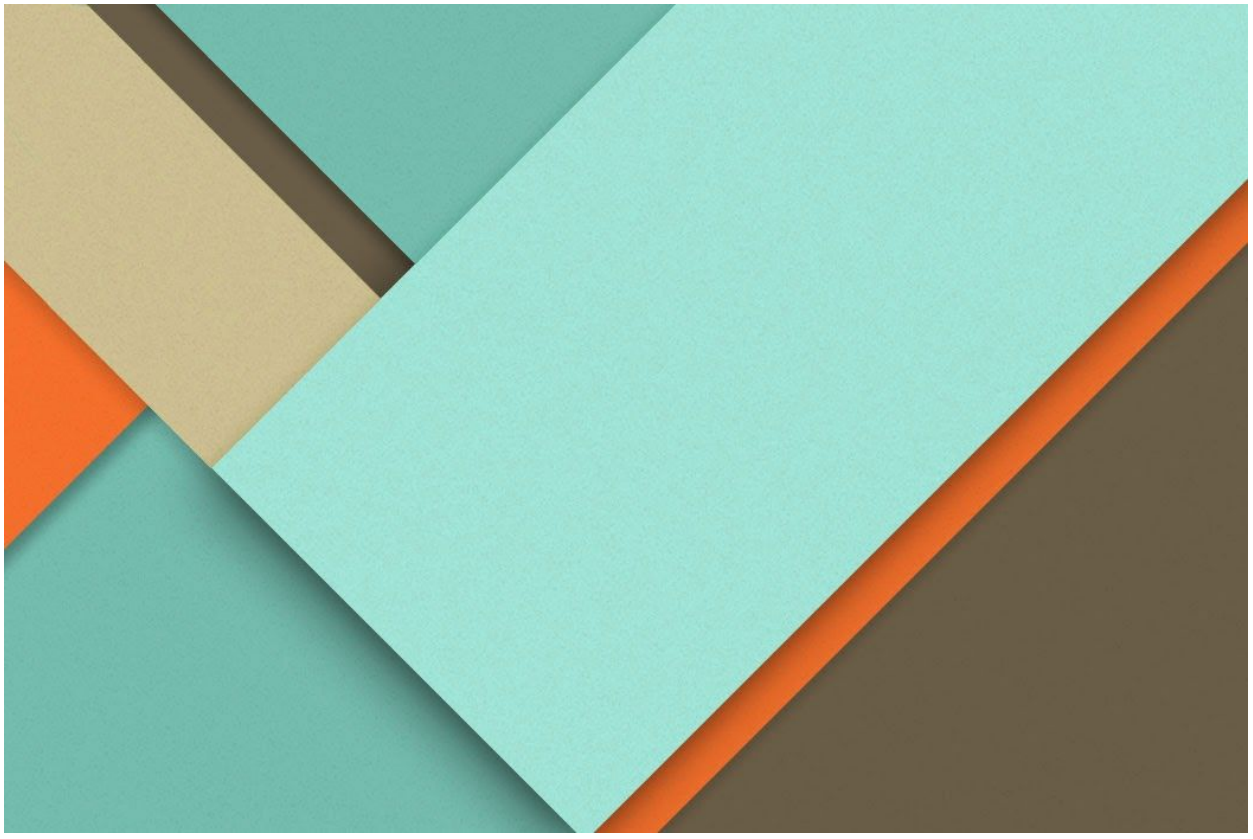

fail2banconfig

Documentation à propos du module Ansible fail2banconfig

Auteur : Biard Dimitri

Version du document : 1.0

Mise à jour le: 18/03/2020

Sommaire

Description 4

Prés-requis 4

- **Ansible** 4
- **Python** 4
- **Fail2ban** 4

Compatibilité 5

Installation 5

Configuration 6

- **Les options** 6
  - **ignoreip** 6
  - **findtime** 6
  - **bantime** 6
  - **maxretry** 6
  - **services** 7
- **Exemple** 7

I - Description

Ce module Ansible à pour objectif de simplifier la configuration de Fail2ban.

Ce module crée un fichier custom.conf (fichier de configuration Fail2ban) avec les paramètres les plus courant par défaut ainsi que les services surveillé que vous aurez choisi. Toutes les configuration par défaut sont éditable à l'aide d'option.

II - Prés-requis

II.1 - Ansible

Ce programme étant un module pour Ansible, vous devez l'avoir installé et préparé la communication entre le node manager et les nodes receveurs. Je vous invite à consulter la doc officielle d'Ansible ou le cour d'Openclassrooms sur le sujet qui est clair et détaillé.

Doc officiel : https://docs.ansible.com/

Openclassrooms :https://openclassrooms.com/fr/courses/2035796-utilisez-ansible-pour-automatiser-vos-taches-de-configuration

II.2 - Python

Ce programme et Ansible d'une manière générale à besoins de python pour fonctionner. Voir la compatibilité dans la section correspondante.

II.3 - Fail2ban

Ce programme configure Fail2ban mais ne le l'installe pas. C'est un choix qui correspond aux principes d'Ansible. En effet Ansible se veut modulaire dans l'organisation de l'automatisation. C'est à dire qu'une tâche complexe sera divisée en plusieurs petites

tâches simple. Il vous faudra donc créer la tâche “Installer Fail2ban” à l’aide du module Ansible “apt” et ensuite créer la tâche “Configuration Fail2ban” à l’aide de fail2banconfig.

III - Compatibilité

Ce programme à été créé et testé sur la configuration suivante :

OS	Debian GNU/Linux 10
Linux version	4.19.0-8-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) 1 SMP Debian 4.19.98-1 (2020-01-26)
Ansible	2.4 et versions supérieurs
Fail2ban	0.11.1 et versions supérieurs
Python	2.7 et versions supérieurs

IV - Installation

- Créer un dossier “library” dans l’environnement de travail.

```
user@NodeManager:~# mkdir library
```

- Déplacez-vous dans le dossier nouvellement créé.

```
user@NodeManager:~/library cd library/
```

- Télécharger l’archive

```
user@NodeManager:~/library wget https://github.com/Dimitri-byte/fail2banconfig-Ansible/archive/master.zip
```

- Dézipper l’archive master

```
user@NodeManager:~/library unzip master.zip
```

- Un dossier “fail2banconfig-Ansible-master” a été créé. Copier le fichier fail2ban.py de ce dossier dans le dossier library.

```
user@NodeManager:~/library cp
fail2banconfig-Ansible-master/fail2ban.py
/home/user/library/fail2banconfig.py
```

Vous pouvez à présent utiliser ce module dans vos “playbooks”.

V - Configuration

V.1 - Les options

ignoreip

L’option ignoreip permet de définir la liste des IP à ignorer. Il est utile d'y mettre sa propre IP afin de ne pas risquer de se faire bannir. **Par défaut** : 127.0.0.1

findtime

L’option findtime définit en secondes le temps depuis lequel une anomalie est recherchée dans les logs. **Par défaut** : 3600 sec

bantime

La durée de bannissement d'une IP est définie par l’option bantime avec une valeur en secondes. **Par défaut** : 86400 sec

maxretry

Cette option définit le nombre de tentative maximum avant le bannissement. **Par défaut**: 3

services

Cette option permet d'ajouter un ou plusieurs services les un à la suite des autres. Le saut de ligne se fait à l'aide du symbole "$" voir la section V.2 -Exemple.

V.2 - Exemple

Ces exemples sont utilisé dans des fichiers de Ansible "playbook" avec l'extention .yml. Reportez-vous à la documentation d'Ansible pour plus d'information.

https://docs.ansible.com/ansible/latest/user_guide/playbooks.html

Example configuration basic avec deux services surveillé

```
- name: "fail2ban ssh et ftp minimum configuration"
  fail2banconfig:
    service = "$[sshd]
              $enable = true
              $$
              $[proftpd]
              $enable = true"
```

Example configuration customisée

```
- name: "fail2ban ssh custom configuration"
  fail2banconfig:
    ignoreip = "127.0.0.1 10.10.0.1 .10.10.0.2"
    findtime = "5000"
    bantime = "600"
    maxretry = "5"
    service = "$[sshd]
              $enable = true
              $logpath = /var/log/auth.log"
```