|  |  |
| --- | --- |
| pfSense Cluster avec Wazuh | |
| Cluster de pfsense et Wazuh | |
|  | |
| **Référence :** Promu246 | |
| **Auteur**(s) :  Rosmade Maxime  Poulade Samuel | **Destinataire**(s) :  Easyformer |

|  |  |  |
| --- | --- | --- |
|  | Date de modification : 14/04/24 | Version : 1 |
|  | | |

Sommaire page

1 Introduction 3

1.1 TEST 3

1.1.1 TEST 3

TEST 3

1. Définition des termes du projets
   1. C’est quoi pfSense

pfSense est une distribution open-source de pare-feu et de routeur basée sur FreeBSD, un système d’exploitation UNIX-like. Il est conçu pour être flexible et adaptable à divers environnements réseau, allant des petites entreprises aux grands déploiements commerciaux.

pfSense offre une gamme de fonctionnalités avancées telles que le filtrage de paquets, la disponibilité grâce le filtrage de paquets, la surveillance du trafic, la prise en charge de VPN, la gestion de la bande passante, la haute disponibilité grâce à la redondance de pare-feu et bien plus encore.

Il est souvent utilisé comme solution de sécurité réseau complète et économique, offrant des performances élevées et une grande stabilité grâce à sa base sur FreeBSD. De plus, pfSense dispose d'une interface utilisateur conviviale basée sur le Web, facilitant sa configuration et sa gestion même pour les utilisateurs moins expérimentés en réseau.

* 1. C’est quoi Wazuh

Wazuh est une plateforme open-source de détection et de réponse aux incidents de sécurité (SIEM) conçue pour surveiller et analyser les journaux de sécurité, les événements système et les activités réseau dans un environnement informatique. Il offre des fonctionnalités avancées telles que la détection d'intrusion, la corrélation d'événements, la surveillance de la conformité et la réponse aux incidents en temps réel.  
  
Wazuh agrège et analyse les données de sécurité à partir de différents types de sources, y compris les journaux de fichiers, les flux réseau, les fichiers de configuration et les alertes générées par d'autres outils de sécurité. Il utilise des techniques sophistiquées pour détecter les menaces potentielles, les comportements suspects et les activités malveillantes, ce qui permet aux équipes de sécurité de prendre des mesures correctives rapidement et efficacement.  
  
En plus de ses capacités de détection avancées, Wazuh offre une interface utilisateur conviviale, des tableaux de bord personnalisables et des fonctionnalités de reporting pour aider les organisations à mieux comprendre et à gérer leur posture de sécurité. Il est largement utilisé dans les environnements d'entreprise pour renforcer la sécurité des systèmes informatiques et des réseaux contre les cybermenaces.

* 1. La haute disponibilité avec CARP

De nos jours, les organisations requièrent une connexion Internet fiable et permanente pour garantir la disponibilité de leurs services. Même une perte de connexion de quelques minutes peut entraîner d'importantes pertes financières. Pour assurer une "haute disponibilité", ce tutoriel propose d'expliquer comment mettre en place une redondance de routeurs pfSense en utilisant le protocole CARP (Common Address Redundancy Protocol).

Le CARP, ou "Protocole de Redondance d'Adresse Commune", permet à plusieurs hôtes sur un même réseau local de partager un ensemble d'adresses IP. Ce protocole est couramment utilisé pour la répartition de charge ou la tolérance aux pannes sur des routeurs. Il constitue une alternative sécurisée et libre aux protocoles tels que le Virtual Router Redundancy Protocol (VRRP), le Hot Standby Router Protocol (HSRP) et le Foundry Standby Router Protocol (FSRP), ayant été développé pour contourner des brevets.

Le fonctionnement du CARP consiste à regrouper plusieurs hôtes (formant un groupe de redondance) qui partageront une adresse IP "virtuelle". Sous cette adresse IP virtuelle se trouvent plusieurs hôtes, dont un maître qui traitera toutes les requêtes destinées à cette adresse. Chaque groupe utilisant le CARP est appelé un "groupe de redondance", partageant une adresse IP entre ses membres. À l'intérieur de ce groupe, un hôte est désigné comme "maître" tandis que les autres sont des "esclaves". Le maître répond à tout trafic ou requête ARP à destination de l'adresse partagée, tandis que chaque hôte possède une seconde adresse IP unique et peut appartenir à plusieurs groupes de redondance.

Une application courante du CARP est la création de groupes de pare-feu redondants. L'adresse IP virtuelle attribuée au groupe de redondance est utilisée comme adresse du routeur par défaut sur les machines clientes. En cas de panne du pare-feu maître ou de sa déconnexion du réseau, l'adresse IP virtuelle est prise en charge par l'un des pare-feu esclaves, assurant ainsi la continuité du service sans interruption. Le CARP prend en charge à la fois IPv4 et IPv6, avec le numéro de port TCP 112.

1. Préparation des machines virtuelles

Prérequis :

Pour réaliser ce tutoriel, utilisation d’un environnement de virtualisation (VMware Workstation 17) des plusieurs réseaux VMnet telle que le VMnet0 : Bridged qui représente le WAN et le VMnet8 : NAT qui représente le LAN dans notre architecture.

Dans ce tutoriel, nous allons mettre en place une haute disponibilité en créant 2 routeurs pfSense rebondants, et un cluster de serveurs Wazuh.

Chaque VM (Virtuel machine) de pfSense posséder 2 interfaces réseaux :

* Une interface « WAN »
* Une interface « LAN »

Dans le LAN nous allons installer, le cluster de serveurs Wazuh sur un Linux Ubuntu 22.04 LTS avec une interface VMnet8.

1. Schéma et adressage de l’architecture réseau

Schéma provisoire\*

Une image contenant texte, capture d’écran, affichage, diagramme

Description générée automatiquement

Lors de la réalisation de tutoriel, chaque routeurs pfSense est connecté à la même interface « WAN » qui est configurée ainsi :

|  |  |  |
| --- | --- | --- |
| pfSense 1 - Maître | 192.168.1.251/24 | DHCP non active |
| pfSense 2 - Backup | 192.168.1.252/24 | DHCP non active |
| Virtual IP WAN | 192.168.1.253/24 |  |

Chaque routeurs pfsense aura une interface « LAN » configurée ainsi.

|  |  |  |
| --- | --- | --- |
| pfSense 1 - Maître | 192.168.8.251/24 | DHCP non active |
| pfSense 2 - Backup | 192.168.8.252/24 | DHCP non active |
| Virtual IP LAN | 192.168.8.254/24 |  |

1. Préparation des VMs pfSense sur VMware Workstation 17

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Configuration des VMs pfSense 1 et 2 :

Mémoire :

Régler sur l’option recommander par VMware

Processeur :

Nb de processeur 1 et nb de cœur 1

Disque dur :

15 Go largement suffisant pour OS

Adaptateur réseau :

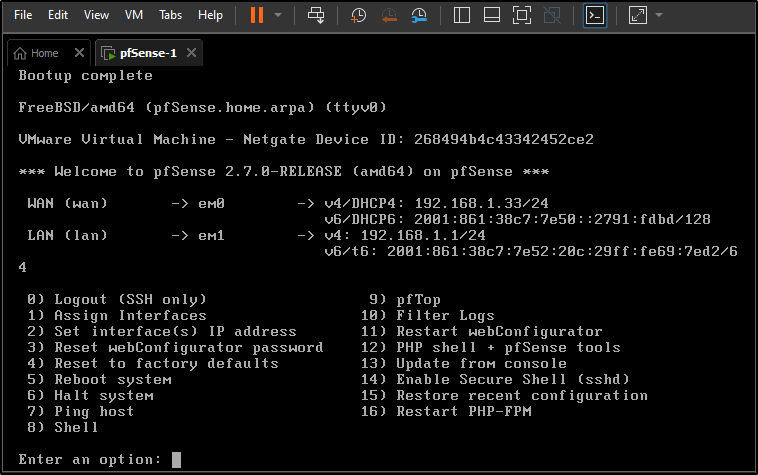
VMnet0 : Réseau WAN \*Bridge

VMnet8 : Réseau LAN \*NAT

Voici un lien qui vous permettra de vous aide pour installation de pfSense si vous ne l’avez jamais fait.

<https://all-it-network.com/pfsense-2-6-0-installation/>

Un fois installation terminer vos pfSense sont comme celui ci-dessous.

Nous allons procéder à configuration des interfaces WAN et LAN, en IP statique. \*page 6

Pour la configuration l'interface WAN.

Ne jamais configurer une interface sur un pfSense en DHCP.

Enter l’IP WAN de votre pfSense, ensuit son masque de sous réseau /24.

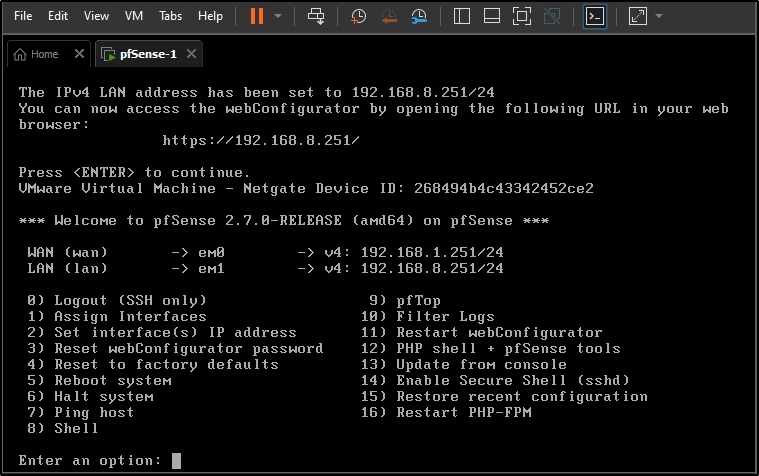
Pour la upstream gateway dans le contexte de pfSense, désigne généralement un routeur ou un périphérique réseau situé plus en amont dans le réseau, souvent du côté de l'ISP (Fournisseur d'Accès Internet). C'est l'élément de réseau auquel pfSense envoie le trafic qui n'est pas destiné aux réseaux locaux configurés dans pfSense lui-même.

Donc upstream gateway en fonction de votre réseau dans mon cas 192.168.1.254

Dans ce TP nous n'utilisons pas ipv6.

Pour interface LAN.

Nous allons configurer l’interface avec ip 192.168.8.251/24. Il n’y a pas de upstream gateway a configurer, ne pas installer le service DHCP sur l’interface en ligne de commande et toujours pas ipv6.

Voici le résultat que vous devez obtenir à la fin de la configuration des interfaces pfSense en ligne de commande.

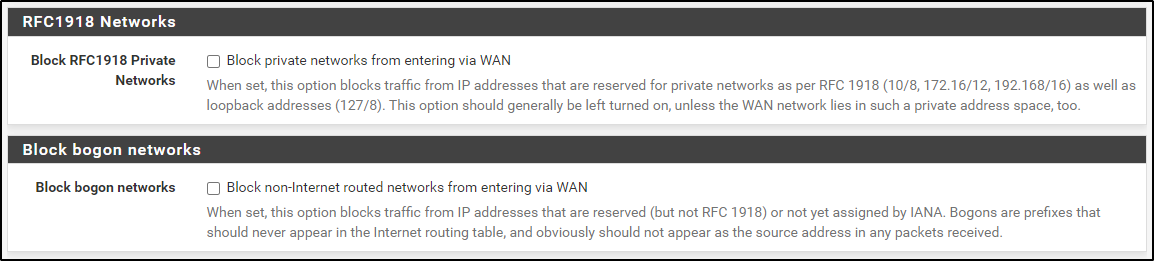
Nous allons pouvoir avoir accès à l’interface graphique de configuration pfSense.

Voici un petit code aide pour ceux qui ont du mal 😉

|  |  |
| --- | --- |
| Pour Interface WAN | Pour Interface LAN |
| 2  1  n  192.168.1.251  24  192.168.1.254  y  n  entre \*la touche merci  n  n | 2  2  n  192.168.8.251  24  entre  n  entre  n  n |

1. Configuration du cluster sur pfSense interface web

Pour accéder à l’interface graphique de pfSense le login et le mot de passe sont respectivement « admin » « pfsense ».

Pendant le Setup Wizard : à l’étape 4 décoche les options block RFC1918 et bogon networks. A effectue pour ce lab non en production.

Voici notre interface pfSense interface Web ci-dessous.Une image contenant texte, capture d’écran, logiciel, Page web

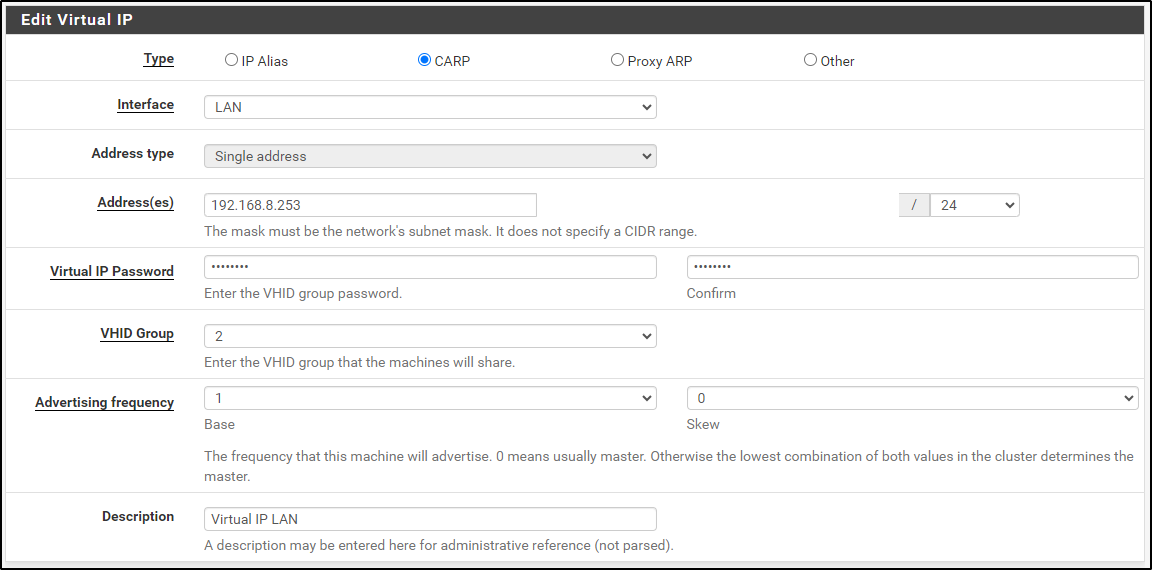
Description générée automatiquement

* 1. Mise en place de la haute disponibilité pfSense
     1. Création des « Virtual IP » sur chaque routeur pfSense
* Sur le pfSense 1 MASTER, cliquez le menu « Firewall » - « Virtual IPs » puis « add ».

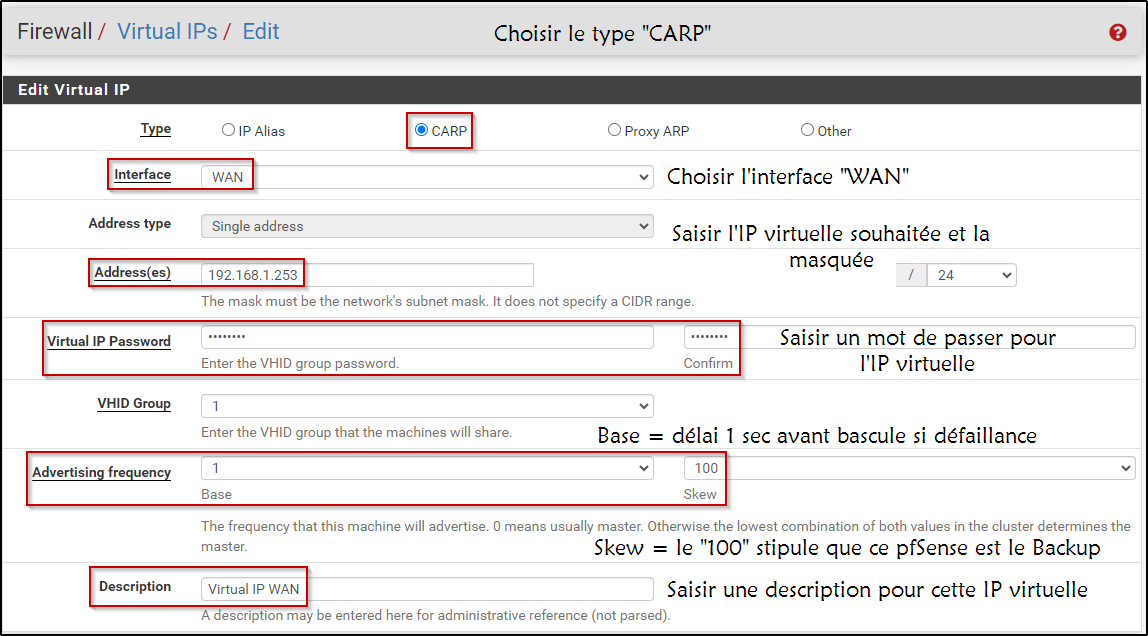
Une image contenant texte, Appareils électroniques, capture d’écran, nombre

Description générée automatiquement

* Cliquez les boutons « Save » et « Apply Changes » pour valider vos paramètres.
* Nous allons procéder de la maniére précédant pour l’interface LAN.



* Sur le pfSense 2 Backup, clique menu « Firewall » - « Virtual IPs » puis « add ».



* Pour nous avons saisi une valeur de 100 Supérieur au pfSense 1 (Master) du groupe VHID 1 afin qu’il soit considéré comme le backup
* Nous Effectuons la même configuration pour l’interface LAN

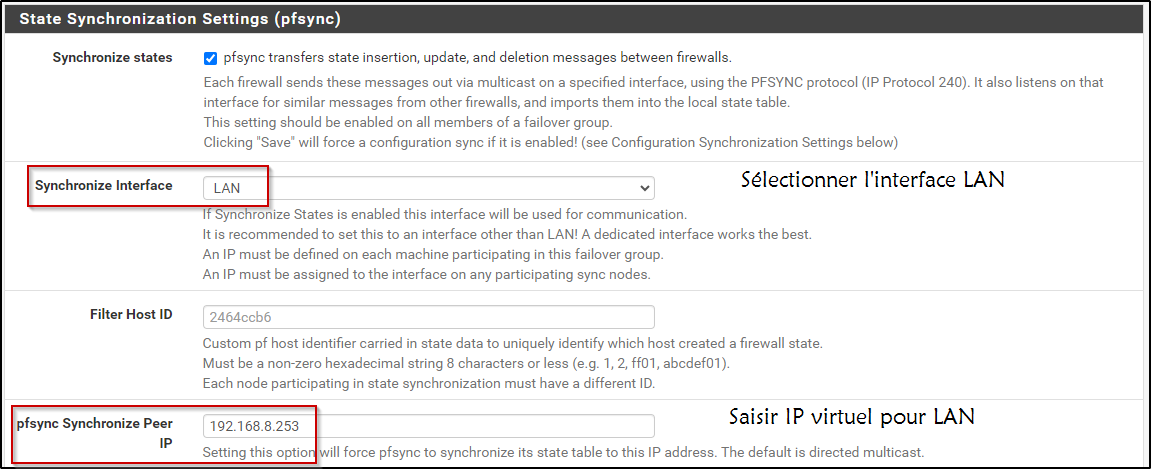
Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Une fois que les adresses IP virtuelles sont paramétrées de manière identique sur les 2 pfSense, nous avons paramétrer le pfSense 1 pour être le Master et le pfSense 2 le backup.

* + 1. Mise en place de la haute disponibilité (depuis le pfSense Master) :
* Cliquez sur le menu « System » - « High availability »
* Configurez la haute disponibilité de cette façon :

A réaliser sur le pfSense 1 (Master), pas de manipulation à faire sur le pfSense 2 puisque la réplication effectuera le travail pour vous.

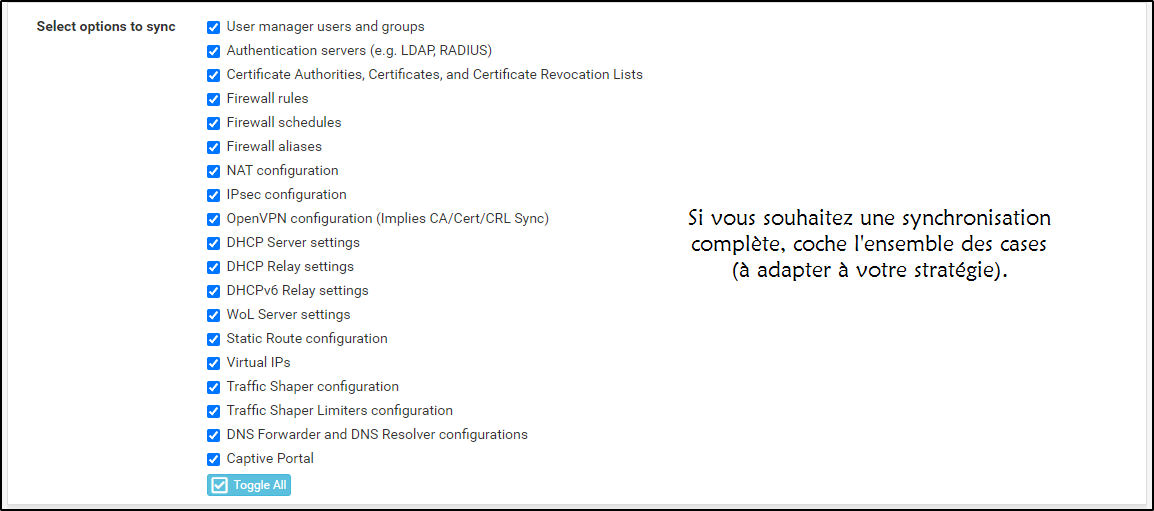


1er partie

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

2ème partie



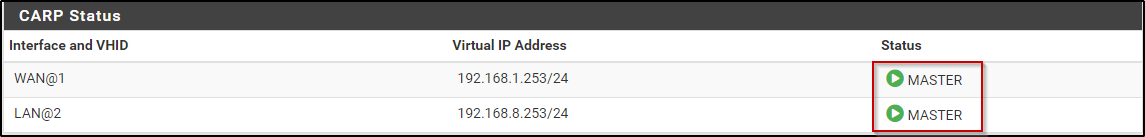
3ème partie

* Cliquez sur le bouton « Save » pour valider vos paramètres.
  + 1. Vérification du bon fonctionnement de la réplication

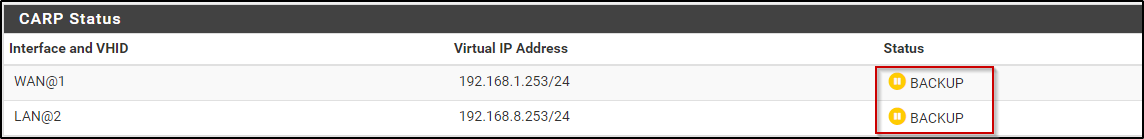
Les IP virutelles, la haute disponibilité et les règles de pare-feu étant configurées, nous pouvons déjà vérifier si le statut CARP de notre pfSense Master est fonctionnel.

* Cliquez sur le menu « Status » - « CARP (failover) » ; une fenêtre s’affiche :

On peut constater, ici, que notre pfSense Master a bien le statut de « Master ». L’interface « CARP » et l’interface « LAN » sont bien répliquée sur l’autre routeur.

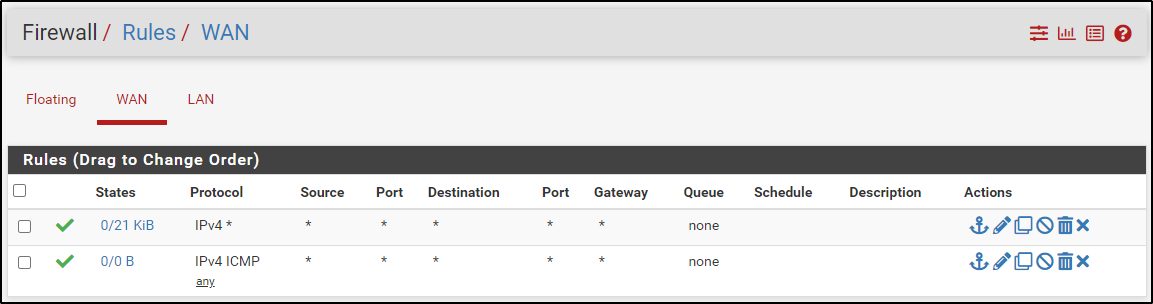


* Nous allons vérifier le pfSense 2 a bien le statut « BACKUP ».



On peut constater, ici, que notre routeur pfSense 2 a bien le statut de « backup » qui signifie qu’il est « backup » dans le cluster. La haute disponibilité est fonctionnelle est puisque la communication est établie !

* Cliquez, sur le routeur pfSense backup, le menu « Firewall » - « Rules » ; vous constaterez que les « Règles » saisies dans le routeur pfSense master ont été intégralement répliquées (!) :



Test de la haute disponiblilite du cluster pfSense

Nous allons, ici, simuler une « panne » pfSense Master. Plutôt que de l’arrêter, on peut stopper le protocole CARP en cours sur celui-ci. Pour cela, effectuez les manipulations suivantes :

Arrêt du protocole « CARP » sur le routeur Master (simulation de panne)

* Cliquez sur le menu « Status » - « CARP (failover) »
* Une image contenant texte, capture d’écran, Police

  Description générée automatiquementCliquez sur le bouton orange « Temporarily Disable CARP »

Le statut du routeur Master passe en mode « DISABLED »

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Sur le pfSense backup et vérifiez son statut ; votre routeur pfSense backup est maintenant passé au statut Master. La haute disponibilité est pleinement fonctionnelle :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquementLe pfSense 2 backup devient maintenant le « maître » et assure la disponibilité des services de manière transparente.

Bravo vous avez réussi la vérification de la haute disponibilité

Configuration étape par étape de Wazuh sur 3 serveurs (Master, Worker, Dashboard) linux Ubuntu 22.04 LTS.

Bienvenue dans notre guide complet sur l'installation de Wazuh, une puissante solution open-source de gestion des informations et des événements de sécurité (SIEM).

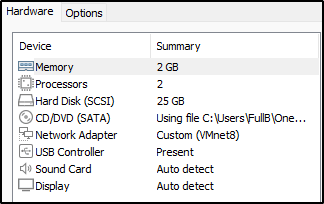
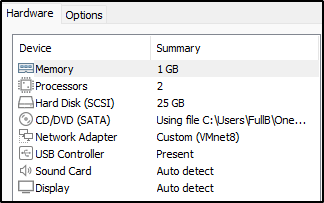
Wazuh fournit une plateforme robuste pour la détection des menaces, la réponse aux incidents et la gestion de la conformité.

Une image contenant texte, capture d’écran, logo, Police

Description générée automatiquement

Pour cette partie du Lab les configurations VM ware sont les suivantes :

1 ordinateur avec 16 gigas de RAM vous permet de réaliser ce Lab (Vous pouvez éteindre le pfSense 2 backup) avec un serveur Linux Ubuntu à 2 giga de RAM un sévère un serveur Linux avec également 2 giga ram et un 3 serveur Linux avec un gigagram pour le dashboard

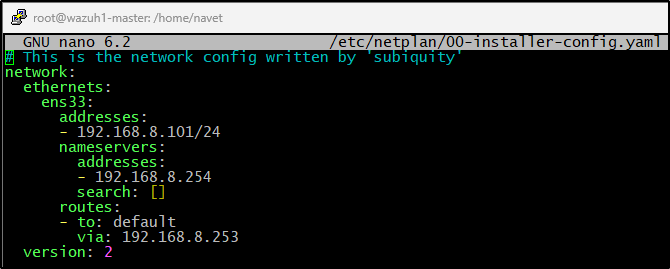


Configuration Serveurs Wazuh Master et Worker

Serveur Dashboard

Avec cette configuration je me permets de vous dire que vous pouvez aussi éteindre la BMPS backup et avec cette configuration vous n’aurai pas de problème afin de démarrer le démon Wazuh. Car il faut au minimum 2 Go de RAM sur le serveur Master et Woker.

* Procéder à la configuration réseau des Serveurs Linux les adresses IP sont disponible sur le schéma page 3.
* Voici une illustration du netplan du Serveurs Master



* Adresse ip 192.168.8.101/24
* DNS : 192.168.8.254 (gateway réseau VMnet 8 NAT)
* Routes « Gateway » : 192.168.8.253 (IP
* virtuel pfSense)

Avant de commencer le processus d'installation, il est essentiel de s'assurer que votre référentiel APT (Advanced Package Tool) est à jour. Cette étape permet de s'assurer que vous avez accès aux dernières informations et versions des paquets.

# apt update

# apt upgrade

* Création des certificates sur le Wazuh Master :

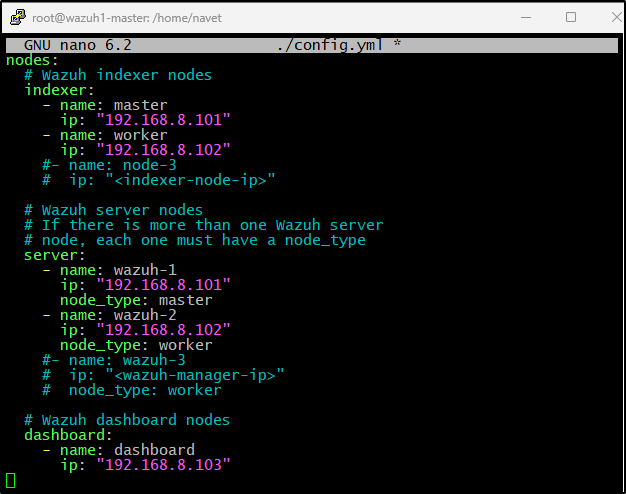
# curl -sO https://packages.wazuh.com/4.7/wazuh-certs-tool.sh

# curl -sO https://packages.wazuh.com/4.7/config.yml

* Modifiez le fichier ./config.yml en substituant les appellations et les adresses IP actuelles par les désignations.

# nano ./config.yml

* Voici une représentation du fichier à adapter en fonction de vos IP



* Pour un cluster multi-nœuds, ces certificats doivent être déployés ultérieurement sur toutes les instances Wazuh de votre cluster.

# bash ./wazuh-certs-tool.sh -A

* Créez une archive tar nammée « wazuh-certificates », en incluant tous les fichiers et répertoires contenus dans le répertoire « ./wazuh-certificates/»

# tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .

# rm -rf ./wazuh-certificates

* Attention copiez le wazuh-certificates.tar fichier sur les serveurs Worker et Dashboard.
* La commande sera : (à adapter selon vos besoin)

# scp wazuh-certificates.tar navet@192.168.8.102:/home/navet

Installation des nœuds

# apt-get install debconf adduser procps

Ajouter du référentiel Wazuh

* Installez les paquets suivants s’ils manquent.

# apt-get install gnupg apt-transport-https

* Installez la GPG Key.

# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | \

gpg --no-default-keyring –keyring \

-- keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg \

--import && \

chmod 644 /usr/share/keyrings/wazuh.gpg

* Ajouter le référentiel.

# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] \

https://packages.wazuh.com/4.x/apt/ stable main" | \

tee -a /etc/apt/sources.list.d/wazuh.list

* Mise à jour des informations sur les paquets.

# apt-get update

Installation de l’indexeur Wazuh

* Installer le paquetage de l’indexeur Wazuh

# apt-get -y install wazuh-indexer

Configuration de Wazuh indexer

# nano /etc/wazuh/opensearch.yml

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

Déploiement de certificats

Exécutez les commandes suivantes en remplaçant <indexer-node-name> par le nom du nœud de l’indexeur Wazuh que vous configurez, tel que défini dans config.yml. Par exemple, node-1. Ceci déploie les certificats SSL pour cryter les communications entre les composants centraux de Wazuh.

# NODE\_NAME=master

# mkdir /etc/wazuh-indexer/certs

# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem

# mv -n /etc/wazuh-indexer/certs/$NODE\_NAME.pem /etc/wazuh-indexer/certs/indexer.pem

# mv -n /etc/wazuh-indexer/certs/$NODE\_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem

# chmod 500 /etc/wazuh-indexer/certs

# chmod 400 /etc/wazuh-indexer/certs/\*

# chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs

Starting the service

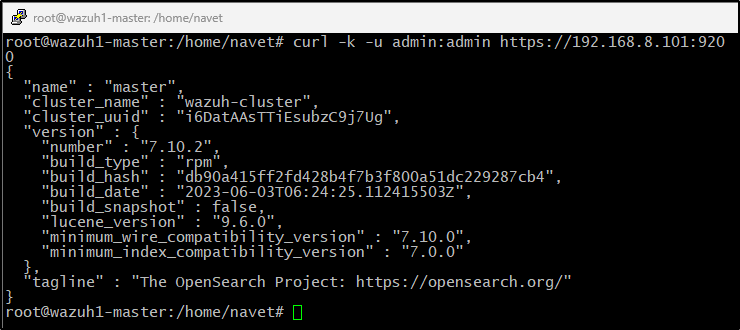
# systemctl daemon-reload

# systemctl enable wazuh-indexer

# systemctl start wazuh-indexer

Répétez cette étape du processus d'installation pour chaque nœud d'indexation Wazuh dans votre cluster.

Procédez ensuite à l'initialisation de votre cluster à un ou plusieurs nœuds dans l'étape suivante.



* Remplacez <WAZUH\_INDEXER\_IP> et exécutez la commande suivante pour vérifier si le cluster à un ou plusieurs nœuds fonctionne correctement.