


E4-Mission1-HomeLab-Baptiste-Grimaldi

Liens utiles:

Article Home-Lab

Check out the portfolio of Baptiste Grimaldi, a full-stack web developer specializing in creating dynamic and responsive websites. Explore his projects and contact him for your next web development project.

 <https://portfolio.baptistegrimaldi.info/projects/view/home-lab>

Article de mon portfolio



SOMMAIRE

Liens utiles:

Introduction

- Contexte de la mission
- Objectifs de la mission
- Présentation de l'infrastructure
- Schéma de liaison
- Tableau de références

Configurations

- Note sur l'ip dynamique.
- Configuration de la Livebox 4
 - PPPoE
 - DHCP sur le Vlan de Orange
- Configuration du routeur pfSense
 - Configuration du VPN OpenVPN pour l'accès à distance sécurisé
 - Le pare-feu de pfSense
 - Redirection vers les serveurs web
- Configuration du serveur Ubuntu
 - Traefik
 - Connexions par ssh avec RSA
 - Endless shh
 - Les prisons ssh et sftp
 - Backups
- Configuration du DNS BIND9
 - Configuration du serveur DNS BIND9
- Configuration du serveur HomeBridge
- Configuration du serveur OctoPrint
- Configuration du serveur de cloud gaming
 - Architecture
- Haute disponibilité

Point Environnemental

- Impact du numérique sur l'environnement
- Avancée du numérique responsable
- Implication personnelle dans la conception de l'infrastructure

Monitoring

- Uptime Robot
- NetData Cloud & mails
- Traefik & ssl

Conclusion

- Résumé de la mission
- Bilan et perspectives d'avenir

Introduction

Contexte de la mission

Dans le cadre d'une volonté d'en apprendre plus sur les bonnes pratiques en réseau, et sur ce que l'on appelle plus généralement du DevOps, j'ai commencé mon propre HomeLab qui est maintenant une architecture stable type entreprise.

Un HomeLab est une infrastructure de laboratoire informatique personnel que l'on peut installer chez soi. Elle peut être utilisée pour apprendre et expérimenter de nouvelles technologies, tester de nouvelles configurations, ou pour développer des projets personnels ou professionnels. Un HomeLab peut être composé de différents éléments, tels que des routeurs, des serveurs, des NAS, des équipements de surveillance, etc. L'objectif est de créer un environnement de test et de développement pour les technologies de l'information et de la communication.

Objectifs de la mission

Les objectifs de cette mission étaient de créer un HomeLab pour apprendre et expérimenter de nouvelles technologies, ainsi que de développer des projets personnels ou professionnels.

Je voulais une infrastructure avec des composants que je n'aurais pas à acheter ou alors avec un très bon rapport qualité prix.

Présentation de l'infrastructure

Mon architecture actuelle est définie par les éléments suivants:

- Une Livebox 4 avec un boîtier ONT: Celle-ci ne sert qu'à passer le trafic vers mon routeur pfSense. Elle est configurée avec une DMZ pointant vers mon routeur pfSense.
- Un routeur pfSense sur une carte mère d'un hp 240 g7 configuré pour renforcer la protection de mon réseau interne comme externe. Un serveur OpenVPN est configuré dessus et utilise la base de données utilisateur du pfSense. Le serveur OpenVPN est configuré pour utiliser des certificats ainsi qu'un couple nom d'utilisateur et mot de passe pour l'authentification.
- Un serveur sous ubuntu serveur LTS 22 sur une carte mère d'un hp 240 g7. Dessus tourne un ensemble de scripts docker. Ceci est le sujet d'une de mes missions E4 dans le cadre de mon BTS SIO option SLAM.
Un Traefik est déployé sur ce serveur pour gérer le load balancing de mes docker

ainsi que les certificats ssl avec OVH et let's encrypt. Le serveur est construit pour créer des prisons pour des utilisateurs sftp.

- Un DNS local sous BIND9
- Un NAS Qnap TS412 configuré pour le iscsi pour la sauvegarde et la redondance de mon serveur web.
- Un serveur HomeBridge pour transformer ma maison connectée sous FlexHom en maison HomeKit.
- Un serveur OctoPrint pour mon imprimante 3D
- Un serveur de cloud gaming utilisant le serveur OpenVPN.
- Un Netgear WAX214 - AX1800 WiFi 6 Dual Band PoE. C'est un très bon access point d'un niveau d'entreprise, avec un bon rapport qualité-prix.

Schéma de liaison

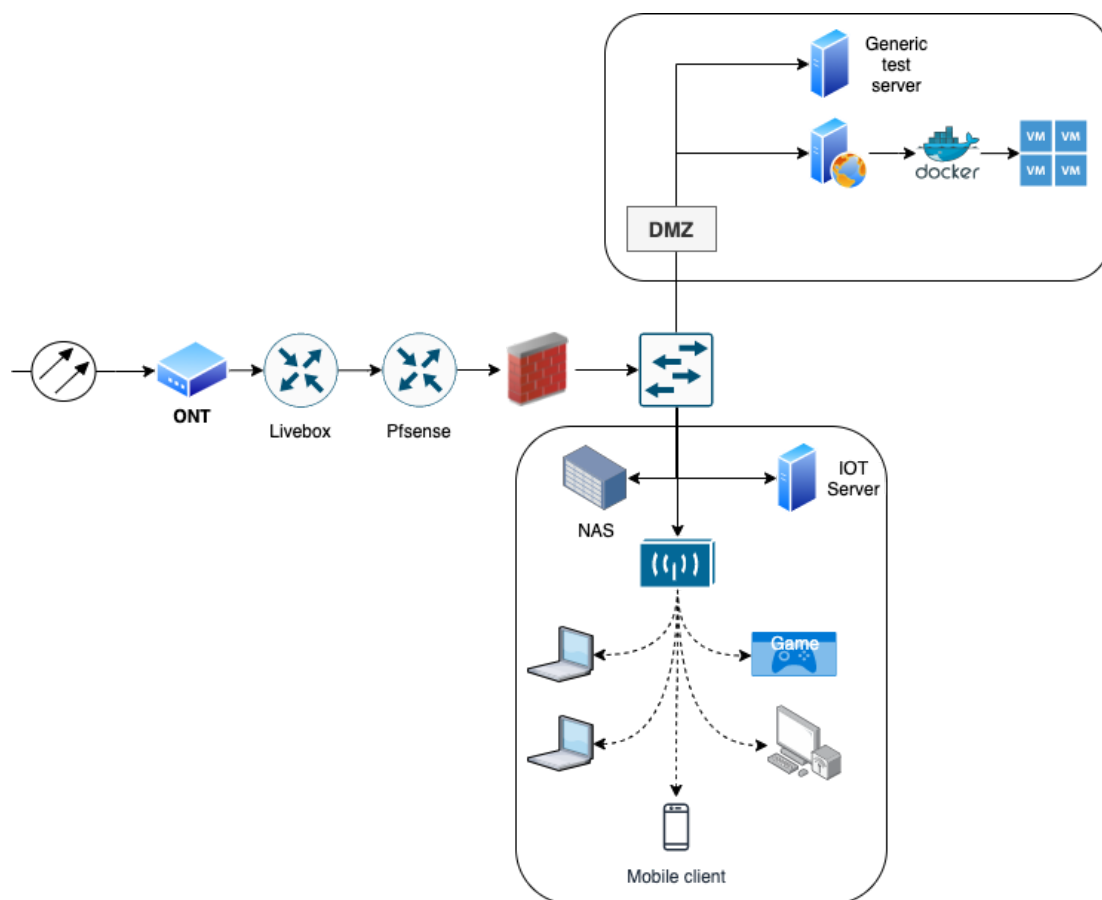


Schéma conventionnel

Tableau de références

Matériel	Référence
Accès réseau publique	Livebox 4 + ONT
Routeur pfSense	HP 240 G7
Serveur Ubuntu	HP 240 G7
DNS	BIND9 en docker
NAS	Qnap TS412
Serveur HomeBridge	Raspberry pi WH 2
Serveur OctoPrint	Raspberry pi WH 2
Point d'accès WIFI	Netgear WAX214 AX1800 WiFi 6

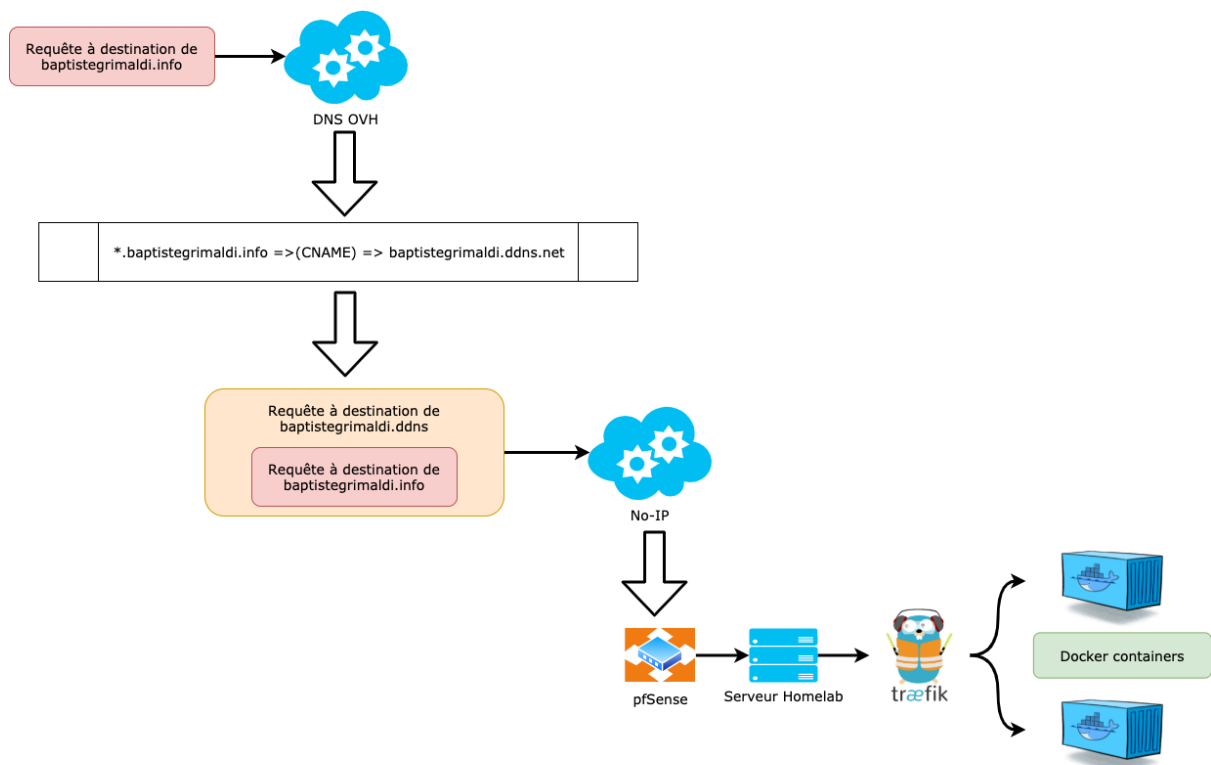
Configurations

Note sur l'ip dynamique.

Dans la démarche d'économie et de garder le plus de mon anciens système, un problématique c'est posée: Comment résoudre le problème de l'IPv4 dynamique sous payer?



Chez Orange, une IP dynamique est une adresse IP qui change régulièrement. Elle est attribuée aux particuliers qui n'ont pas souscrit à l'option "IP fixe". Cela signifie que l'adresse IP publique de votre box internet peut changer à chaque connexion ou toutes les quelques heures. Cela peut poser des problèmes si vous souhaitez accéder à votre réseau de l'extérieur ou si vous utilisez des services qui nécessitent une adresse IP fixe, tels que les serveurs web ou les services VPN. Pour contourner ce problème, il est possible de souscrire à l'option "IP fixe" auprès de votre fournisseur d'accès internet. Cette option permet d'obtenir une adresse IP publique fixe pour votre box internet, ce qui facilite l'accès à votre réseau de l'extérieur.



Configuration de la Livebox 4

La configuration de la Livebox 4 consiste principalement à activer le mode DMZ pour rediriger tout le trafic vers le routeur pfSense. Pour cela, il faut se connecter à l'interface de la Livebox 4 et activer le mode DMZ, puis indiquer l'adresse IP locale du routeur pfSense.

Il va de paire que l'ip du routeur pfSense est fixe sur la box orange

Actuellement l'équipement intégré à la DMZ est :

pfSense (adresse ip: 192.168.10.10)

Intégrer un autre équipement

Équipement	<input type="text" value="pfSense"/>
Adresse IP statique	192.168.10.10
Adresse MAC	80:E8:2C:4F:E6:8B

La DMZ sur la livebox

En outre, il est recommandé de désactiver les fonctionnalités de routage et de firewall de la Livebox 4 pour éviter tout conflit avec le routeur pfSense.



Le remplacement d'une Livebox par un routeur personnel sur une fibre Orange peut ne pas être autorisé par votre fournisseur d'accès internet. Vérifiez les conditions d'utilisation de votre abonnement avant de procéder.

Si vous êtes autorisé à remplacer votre Livebox par un routeur personnel, voici les étapes à suivre:

PPPoE

1. Configurez votre routeur personnel avec les mêmes identifiants que votre Livebox. Vous pouvez trouver ces informations dans l'interface de gestion de votre Livebox.
2. Configurez votre routeur pour qu'il utilise le protocole PPPoE avec les mêmes identifiants que votre Livebox.
3. Configurez votre routeur pour qu'il utilise les mêmes adresses IP que votre Livebox.
4. Configurez votre routeur pour qu'il utilise les mêmes paramètres DNS que votre Livebox.
5. Configurez votre routeur pour qu'il utilise les mêmes paramètres de sécurité que votre Livebox (WPA, clé de sécurité, etc.).
6. Connectez votre routeur personnel à votre fibre optique en utilisant le câble fourni par Orange.

DHCP sur le Vlan de Orange

je renvoi à:

https://wiki.virtit.fr/doku.php/kb:linux:pfSense:remplacer_sa_box_orange_par_un_pfsense

Ou bien l'excellent forum:

lafibre.info

Actuellement ma Livebox est encore utilisé car je n'avais pas réussi à récupérer le PPPoE. Ma Livebox recevant son adresse IP de la part de orange sous DHCP, il faut modifier récupérer une requête DHCP de la part de orange, en analyser la trame et en extraire certaines authentification en hexadécimal.

Configuration du routeur pfSense

Le routeur pfSense joue un rôle clé dans l'infrastructure HomeLab. Il est utilisé pour renforcer la sécurité du réseau interne et externe.

Je précise qu'aucunes sauvegardes ni de redondance n'est mise en place. Néanmoins, la configuration de base de mon routeur est exporté et stocké séparément du bâtiment.

La configuration du routeur pfSense réside sur ces axes principaux:

- Configuration du VPN OpenVPN pour l'accès à distance sécurisé
- Configuration des règles de pare-feu pour la protection du réseau
- Redirection vers les serveurs web
- Configuration de la surveillance réseau avec les outils de monitoring

Configuration du VPN OpenVPN pour l'accès à distance sécurisé






OpenVPN est un logiciel de réseau privé virtuel (VPN) open source utilisé pour créer des connexions sécurisées et chiffrées sur Internet. Il est utilisé pour fournir un accès à distance sécurisé à l'infrastructure HomeLab.

L'authentification par certificat est une méthode d'authentification forte qui utilise des certificats pour identifier les clients VPN. Cette méthode d'authentification est plus sécurisée que l'authentification par mot de passe car elle ne nécessite pas l'échange de mots de passe sur Internet.



Un certificat est un fichier numérique qui contient les informations d'identification d'un utilisateur. Dans le cas d'OpenVPN, un certificat est utilisé pour identifier un client VPN. L'authentification par certificat est une méthode d'authentification forte qui utilise des certificats pour identifier les clients VPN. Cette méthode d'authentification est plus sécurisée que l'authentification par mot de passe car elle ne nécessite pas l'échange de mots de passe sur Internet.

Le processus de création d'un certificat pour OpenVPN implique la création d'un certificat racine, d'un certificat de serveur et d'un certificat de client. Le certificat racine est signé par l'autorité de certification (CA) et est utilisé pour créer des certificats de serveur et de client. Le certificat de serveur est utilisé pour identifier le serveur OpenVPN auprès des clients VPN et le certificat de client est utilisé pour identifier les clients VPN auprès du serveur OpenVPN.







Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-GRIMALDEV-OPENVPN	✓	self-signed	3	ST=Grand-Est, OU=It-departement, O=Grimaldev, L=Strasbourg, CN=grimaldev, C=FR <small>Valid From: Fri, 22 Apr 2022 19:58:12 +0200 Valid Until: Mon, 19 Apr 2032 19:58:12 +0200</small>	OpenVPN Server	  

Autorité de certification

Les certificats sont créés à l'aide d'un outil appelé EasyRSA, qui est inclus dans le package OpenVPN. Le processus de création de certificats est assez complexe et nécessite une connaissance approfondie de la configuration d'OpenVPN et de la création de certificats. Il est recommandé de suivre un guide détaillé pour créer des certificats pour OpenVPN.

Une fois que les certificats sont créés, ils doivent être distribués aux clients VPN. Les clients VPN doivent installer le certificat de serveur sur leur ordinateur pour se connecter au serveur OpenVPN. Les certificats de client sont distribués individuellement aux clients VPN pour leur permettre de s'authentifier auprès du serveur OpenVPN.

Il est important de noter que les certificats doivent être protégés avec des mots de passe forts pour garantir la sécurité du système VPN.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 964 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-128-CBC, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN SSL - GRIMALDEV	  
WAN	UDP / 965 (TUN)	10.10.100.0/24 FE80::AAAA:AAAA:0000/64	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-128-CBC, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	php-users-opnevpn	  

Deux serveurs VPN

Ici, deux serveurs VPN sont utilisés, un pour l'administrateur, et l'autre pour les utilisateurs de mes serveurs. (ex: *connexion sftp*). Cela me permet d'appliquer des règles de pare-feu spécifique à certains réseaux OpenVPN.

Le pare-feu de pfSense



Un pare-feu ?

Un pare-feu est un dispositif de sécurité qui contrôle les connexions réseau entrantes et sortantes. Il est utilisé pour protéger un réseau contre les attaques informatiques et pour surveiller le trafic réseau. Les pare-feux peuvent être configurés pour bloquer les connexions non autorisées et pour alerter les administrateurs système en cas de tentative d'accès non autorisé au réseau. Les pare-feux sont souvent utilisés en combinaison avec d'autres dispositifs de sécurité, tels que des systèmes de détection d'intrusion et des antivirus.

Le pare-feu de pfSense est utilisé pour protéger le réseau interne et externe de l'infrastructure HomeLab. Le pare-feu permet de bloquer les connexions non autorisées et de surveiller le trafic réseau.

Le pare-feu de pfSense est configuré à l'aide de règles qui définissent les connexions réseau autorisées et bloquées. Les règles sont configurées en fonction des adresses IP, des ports et des protocoles réseau.

Les règles de pare-feu sont organisées en groupes appelés "alias". Les alias sont des groupes de règles qui peuvent être utilisés pour simplifier la configuration du pare-feu. Les alias permettent de regrouper des adresses IP, des ports et des protocoles réseau similaires.

Les règles de pare-feu sont configurées dans l'interface web de pfSense. Pour créer une nouvelle règle de pare-feu, il faut sélectionner l'interface réseau à laquelle la règle s'applique, spécifier l'adresse IP source, l'adresse IP de destination, le port et le protocole de la connexion. Il est également possible de spécifier un alias pour la source, la destination, le port et le protocole.

Le pare-feu de pfSense est configuré pour bloquer les connexions non autorisées et pour surveiller le trafic réseau. Les journaux du pare-feu sont consultables dans l'interface web de pfSense.

Il est important de noter que la configuration du pare-feu de pfSense peut être complexe et nécessite une connaissance approfondie de la configuration de pfSense et du pare-feu en général. Il est recommandé de suivre un guide détaillé pour configurer le pare-feu de pfSense.

Redirection vers les serveurs web

La configuration de la redirection vers les serveurs web est effectuée à l'aide de la fonctionnalité de redirection NAT (Network Address Translation) de pfSense. La

redirection NAT permet de rediriger le trafic entrant d'une adresse IP et d'un port donnés vers une adresse IP et un port différents.

La redirection du trafic des ports 80 et 443 vers le serveur web est nécessaire pour permettre aux utilisateurs d'accéder au site web via le protocole HTTP et HTTPS. Le port 80 est utilisé pour les connexions HTTP non sécurisées, tandis que le port 443 est utilisé pour les connexions HTTPS sécurisées. En redirigeant le trafic des ports 80 et 443 vers le serveur web, toutes les requêtes HTTP et HTTPS destinées à l'adresse IP publique de l'infrastructure HomeLab seront envoyées au serveur web. Le serveur web pourra alors traiter les requêtes et renvoyer les pages web demandées aux utilisateurs. Il est important de noter que la redirection du trafic des ports 80 et 443 doit être configurée de manière sécurisée pour éviter les attaques de type man-in-the-middle ou les injections de code malveillant. Il est recommandé d'utiliser des certificats SSL pour chiffrer les connexions HTTPS et de configurer des règles de pare-feu pour bloquer les connexions non autorisées.

Configuration du serveur Ubuntu

Le serveur Ubuntu est utilisé pour exécuter des scripts Docker et pour fournir une plateforme de développement pour des projets personnels ou professionnels. Le serveur est équipé de Traefik pour gérer le load balancing de mes docker et pour gérer les certificats SSL avec OVH et Let's Encrypt. Le serveur est également configuré pour créer des prisons pour des utilisateurs SFTP.

Traefik



Traefik est un reverse proxy et un load balancer open source conçu pour gérer le trafic HTTP et TCP. Il est utilisé pour distribuer le trafic entre plusieurs serveurs web afin d'améliorer les performances et la disponibilité des applications. Traefik prend en charge plusieurs protocoles, tels que HTTP, HTTPS, TCP, UDP et WebSocket, et peut être configuré pour fonctionner avec des conteneurs Docker, des instances Amazon EC2, des serveurs bare-metal, etc. Il est également équipé de fonctionnalités de surveillance et de journalisation pour aider les administrateurs système à diagnostiquer les problèmes de réseau.

Traefik est actuellement configuré dans une docker avec une configuration persistante et redondante.

Accueil des requêtes web: Les requêtes web venant de la zone DNS baptistegrimaldi.info sont redirigées en fonction du sous-domaine. Dans la configuration

de la zone DNS, tout les sous-domaines redirigent vers mon réseau, le load-balancer de Traefik redirige ensuite vers le service concerné.

Connexions par ssh avec RSA



Le protocole SSH (Secure Shell) est un protocole de communication sécurisé qui permet aux utilisateurs d'accéder à un ordinateur distant de manière sécurisée. Il permet aux utilisateurs de se connecter à un ordinateur distant et d'exécuter des commandes à distance. Les connexions SSH sont chiffrées, ce qui les rend plus sûres que les connexions telnet ou FTP.

Le protocole SSH utilise une infrastructure de clés publiques et privées pour authentifier les utilisateurs. Lorsqu'un utilisateur se connecte à un ordinateur distant via SSH, le serveur vérifie que l'utilisateur dispose d'une clé privée correspondante à la clé publique stockée sur le serveur. Si la clé privée est valide, l'utilisateur est autorisé à se connecter.

Le protocole SSH prend en charge plusieurs algorithmes de chiffrement, tels que AES, Blowfish, 3DES, etc. Il est également équipé de fonctionnalités de compression de données pour améliorer les performances de la connexion.



La clé RSA est un algorithme de chiffrement asymétrique utilisé pour la génération de paires de clés publique/privée. La paire de clés RSA est utilisée pour chiffrer et déchiffrer des données sensibles, telles que des mots de passe et des informations d'authentification. La clé publique est utilisée pour chiffrer les données, tandis que la clé privée est utilisée pour déchiffrer les données.

Il est important de noter que la configuration de SSH peut être complexe et nécessite une connaissance approfondie de la sécurité des systèmes informatiques. Il est recommandé de suivre un guide détaillé pour configurer SSH correctement.

```

Include /etc/ssh/sshd_config.d/*.conf

Port 5099
#AddressFamily any
ListenAddress 192.168.100.200
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
RekeyLimit 512M 120

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

```

Base de configuration de sécurité ssh

La propriété `RekeyLimit` du fichier de configuration `sshd_config` permet de spécifier la fréquence à laquelle les clés de chiffrement sont renégociées pour les connexions SSH. Cette propriété est utilisée pour améliorer la sécurité des connexions SSH en réduisant le risque d'attaques par force brute et de compromission de clés.

La propriété `RekeyLimit` prend deux paramètres: le premier paramètre spécifie le temps écoulé avant qu'une clé de chiffrement ne soit renégociée, et le second paramètre spécifie la quantité de données échangées avant qu'une clé de chiffrement ne soit renégociée. Par exemple, la propriété `RekeyLimit 1G 1h` signifie que les clés de chiffrement seront renégociées toutes les heures ou après l'échange de 1 Go de données, selon la première limite atteinte.

Il est important de configurer correctement la propriété `RekeyLimit` pour garantir la sécurité des connexions SSH. Une valeur trop basse peut entraîner une surcharge de trafic et une baisse de performance, tandis qu'une valeur trop élevée peut compromettre la sécurité des connexions SSH. Il est recommandé de suivre les bonnes pratiques de sécurité pour configurer la propriété `RekeyLimit`, en fonction des besoins spécifiques de chaque système.

On note les propriété suivantes et leurs paramètres:

--	--

Propriété	valeur
PermitRootLogin	prohibit-password
MaxAuthTries	6
PubkeyAuthentication	yes

Endless ssh

La librairie Endless SSH est une librairie open-source pour Linux qui permet de maintenir des connexions SSH persistantes. Elle permet notamment de reconnecter automatiquement une session SSH en cas de perte de connexion, de redémarrage ou de mise en veille de l'ordinateur client ou du serveur distant.

Il est possible d'utiliser la librairie Endless SSH comme honeypot pour détecter les tentatives d'intrusion sur le serveur Ubuntu. Un honeypot est un dispositif de sécurité qui simule un système vulnérable pour attirer les attaquants et les empêcher d'attaquer le système réel.

Pour utiliser Endless SSH comme honeypot, il faut configurer le serveur Ubuntu pour qu'il accepte les connexions SSH sur un port différent du port standard (22). Il est recommandé de choisir un port élevé et peu commun pour éviter les tentatives d'intrusion automatisées.

Une fois que le serveur Ubuntu est configuré pour accepter les connexions SSH sur un port différent, il faut installer la librairie Endless SSH et la configurer pour qu'elle surveille le port choisi. Endless SSH sera alors prêt à détecter les tentatives d'intrusion sur le port surveillé.

Il est important de noter que l'utilisation d'un honeypot peut être risquée et nécessite une connaissance approfondie de la sécurité des systèmes informatiques. Il est recommandé de suivre un guide détaillé pour configurer un honeypot correctement.

Après avoir fait beaucoup de serveur ssh, je notes ces best-practices:

- Créer user autre et le mettre sudoer
 - Connection par clé rsa
 - Client:
 - ssh-keygen (ne rien rentrer dans les propositions)
 - ssh-copy-id user@ip
- Désactiver connection root et par mot de passe
 - Host:
 - Modifier /etc/ssh/sshd_config

- PermitRootLogin no
 - PermitPassword no
- Changer le port de base:
 - Host:
 - Modifier /etc/ssh/sshd_config
 - Port xxxx
- Installer fail2ban:
 - Host:
 - Sudo apt-get install update; sudo apt-get install upgrade; sudo apt-get install fail2ban
- Restart les services:
 - Host:
 - Sudo systemctl restart sshd
 - Sudo systemctl enable fail2ban
 - Sudo systemctl start fail2ban
- Endless SSH
 - Honeypot

Les prisons ssh et sftp



Une prison SSH, ou chroot jail en anglais, est un mécanisme de sécurité qui permet d'isoler les utilisateurs d'un serveur SSH dans un environnement contrôlé. En utilisant une prison SSH, les utilisateurs peuvent se connecter au serveur SSH et exécuter des commandes, mais ils sont limités à leur propre environnement et ne peuvent pas accéder aux fichiers ou aux services du système hôte.

La prison SSH est configurée en créant un répertoire de base pour l'utilisateur dans lequel se trouvent toutes les ressources nécessaires pour exécuter les commandes. L'utilisateur est ensuite limité à ce répertoire et ne peut pas naviguer en dehors de celui-ci. Cela permet de limiter les risques de piratage et de compromission du système hôte. La prison SSH est généralement utilisée pour les utilisateurs SFTP, qui ont besoin d'un accès restreint à des fichiers spécifiques sur le serveur.

Il est important de noter que la configuration de la prison SSH peut être complexe et nécessite une connaissance approfondie de la sécurité des systèmes informatiques. Il est recommandé de suivre un guide détaillé pour configurer la prison SSH correctement.

Backups

Les backups sur un serveur target iSCSI depuis un Linux peuvent être effectués à l'aide d'un outil de backup tel que `rsync`.

Pour effectuer des backups avec `rsync`, il faut tout d'abord monter le disque iSCSI comme un disque local. Cela peut être fait en utilisant l'outil `iscsiadm` qui est inclus dans la plupart des distributions de Linux.

Une fois que le disque iSCSI est monté, il est possible d'utiliser `rsync` pour copier les données de la source vers le disque iSCSI. Il est recommandé d'utiliser l'option `-a` pour copier les fichiers avec les mêmes permissions, propriétaires et dates de modification, ainsi que l'option `-v` pour afficher les fichiers qui sont copiés.

La commande `rsync` peut être exécutée à partir d'un script qui est exécuté à une heure précise, ou elle peut être exécutée à l'aide d'une tâche cron pour automatiser les backups.

Il est important de noter que les backups doivent être effectués régulièrement pour garantir la sécurité des données. Il est également recommandé de tester régulièrement les backups pour s'assurer qu'ils peuvent être restaurés en cas de besoin.

Configuration du DNS BIND9

Configuration du serveur DNS BIND9

Le serveur DNS BIND9 est utilisé pour gérer la résolution de noms de domaine pour les clients sur le réseau interne et externe de l'infrastructure HomeLab. Le serveur DNS permet de traduire les noms de domaine en adresses IP, ce qui permet aux clients d'accéder aux services et aux sites web sur Internet.

La configuration du serveur DNS BIND9 implique la création de zones de recherche directes et inverses pour les noms de domaine. Les zones de recherche directe sont utilisées pour traduire les noms de domaine en adresses IP, tandis que les zones de recherche inverses sont utilisées pour traduire les adresses IP en noms de domaine.

La configuration du serveur DNS BIND9 est effectuée à l'aide du fichier de configuration `named.conf`. Ce fichier de configuration contient les paramètres de configuration pour les zones de recherche directe et inverses, les serveurs de noms autoritaires, les enregistrements DNS, etc.

Il est important de noter que la configuration du serveur DNS BIND9 peut être complexe et nécessite une connaissance approfondie de la résolution de noms de domaine et de la configuration de DNS. Il est recommandé de suivre un guide détaillé pour configurer le serveur DNS BIND9 correctement.

Une fois que le serveur DNS BIND9 est configuré, il doit être configuré sur les clients pour qu'ils puissent utiliser le serveur DNS pour la résolution de noms de domaine. Les clients peuvent être configurés manuellement en modifiant les paramètres de configuration du réseau, ou ils peuvent être configurés automatiquement à l'aide de DHCP.

Il est important de noter que la configuration du serveur DNS BIND9 doit être régulièrement mise à jour pour garantir la sécurité et la disponibilité du système. Les mises à jour de sécurité doivent être installées dès que possible pour éviter les vulnérabilités de sécurité.

```
$TTL 2d
$ORIGIN grimaldev.local.

@           IN      SOA    ns.grimaldev.local. contact@baptistegrimaldi.info (
                                2023013104      ; serial
                                12h              ; refresh
                                15m              ; retry
                                3w               ; expire
                                2h               ; minimum ttl
                                )

           IN      NS     ns.grimaldev.local.

ns         IN      A      192.168.100.200

; -- dns records

srv        IN      A      192.168.100.200
nas        IN      A      192.168.100.205
*.srv      IN      A      192.168.100.200

; -- home infra

router     IN      A      192.168.100.1
orange     IN      A      192.168.10.1
ap         IN      A      192.168.100.4
gaming     IN      A      192.168.100.155
rasp       IN      A      192.168.100.156
```

Configuration du serveur HomeBridge

Le serveur HomeBridge est utilisé pour transformer ma maison connectée sous FlexHom en maison HomeKit. HomeBridge est une plate-forme open source qui permet de connecter des appareils non compatibles HomeKit à HomeKit. Le serveur est configuré pour contrôler les lumières, les volets, les thermostats et autres appareils que j'ajoute.

Configuration du serveur OctoPrint

Le serveur OctoPrint est utilisé pour contrôler une imprimante 3D. Il permet de visualiser les modèles 3D, de les préparer pour l'impression et de contrôler l'imprimante 3D à distance. Le serveur est configuré pour fonctionner avec une imprimante 3D Creality Ender 3.

Configuration du serveur de cloud gaming

Architecture

- Laptop configuré pour du jeu
 - GeForce® GTX 1070 with 8GB GDDR5
 - 32GB de RAM
 - SSD & HDD
 - LAN NIC Gigabit
 - Windows spectre
- Nvidia Geforce Shield Server / Sunshine
- Moonlight client

Windows Spectre est une version personnalisée de Windows 10 conçue pour les gamers. Elle est optimisée pour les performances de jeu et inclut des fonctionnalités telles que l'installation de pilotes graphiques automatique et la désactivation des services inutiles pour améliorer les performances. Windows Spectre est également équipé de logiciels de monitoring pour surveiller les performances du système et détecter les problèmes de compatibilité avec les jeux.

Windows spectre est un windows très léger sans tout les logiciels par défaut de windows.

Au démarrage de l'ordinateur, une session utilisateur secondaire est automatiquement lancée sans mot de passe. Cette session démarre automatiquement un serveur de connexion distante spécialisé dans la rapidité et la fluidité: **Nvidia Geforce Shield Server**.



Nvidia Geforce Shield serveur est un ancien programme de Geforce qui, en achetant le "nvidia shield", une sorte de chrome cast du gaming, permettait de se connecter à distance dans le même lan, ou pas, à un pc.

Nvidia révolutionne le marché en offrant un nouveau protocole propriétaire ultra rapide. Plus tard un groupe de développeurs de la communauté open-source programment un client lourd qui offre la même chose: **“sunshine”**.

Côté client, **“moonlight”** apparaît, un client capable de faire pareil que le shield mais en temps que client lourd sur n'importe quelle machine.

Haute disponibilité

Un système de haute disponibilité est un système qui vise à garantir un haut niveau de disponibilité et de continuité de service pour une application ou un service en cas de panne ou de défaillance d'un composant.

Dans le cas d'un système de haute disponibilité pour un site web, par exemple, on peut mettre en place un système de dns-failover. Cela consiste à avoir un script qui vérifie en permanence si le serveur primaire est disponible. Si ce n'est pas le cas, le script change automatiquement les enregistrements DNS de la zone OVH pour pointer vers un serveur de secours.

Pour mettre en place un tel système, il faut tout d'abord disposer d'un serveur de secours qui est configuré pour prendre le relais en cas de défaillance du serveur primaire. Ensuite, il faut écrire un script qui vérifie régulièrement si le serveur primaire est disponible. Si le serveur est disponible, le script ne fait rien. Si le serveur est indisponible, le script utilise l'API de OVH pour changer les enregistrements DNS de la zone OVH afin de pointer vers le serveur de secours.

Il est important de noter que la mise en place d'un système de haute disponibilité peut être complexe et nécessite une connaissance approfondie de la sécurité des systèmes informatiques. Il est recommandé de suivre un guide détaillé pour configurer un tel système correctement.

Point Environnemental

Impact du numérique sur l'environnement

Le numérique a un impact significatif sur l'environnement, il représente 4% des émissions totales de gaz à effet de serre. Les centres de données, qui stockent et traitent une grande quantité de données, consomment énormément d'énergie. Selon une étude menée par l'Agence Internationale de l'Énergie, la consommation électrique des centres de données a augmenté de 6 % en 2020, ce qui équivaut à la consommation totale d'énergie de l'Espagne. De plus, la production de matériel informatique nécessite l'extraction de matières premières et la production de déchets électroniques. En 2019, environ 54 millions de tonnes de déchets électroniques ont été générées dans le monde

selon l'Organisation des Nations unies. Il est donc important de prendre en compte cet impact environnemental lors de la conception et de l'utilisation de technologies numériques.

Avancée du numérique responsable

L'avancement numérique du travail est un mouvement important qui cherche à intégrer le travail social et environnemental avec le développement et l'utilisation des technologies numériques. Les technologies numériques ont un impact croissant sur notre société, et il est nécessaire de prendre les mesures nécessaires pour réduire leurs effets négatifs.

- Selon une étude des Nations Unies, la génération de déchets électroniques dans le monde a atteint 53,6 millions de tonnes en 2019. Ce nombre devrait atteindre 74,7 millions de tonnes en 2030. Cela représente une croissance de 21 % en seulement 5 ans. De plus, selon une étude de la Commission européenne, on s'attend à ce que les émissions de gaz à effet de serre de l'industrie des technologies de l'information et de la communication (TIC) doublent d'ici 2025.
- Ces chiffres montrent la rapidité d'adoption des pratiques numériques importantes. De nombreuses entreprises ont déjà commencé à prendre des mesures pour soutenir la technologie qui a un rôle. *Par exemple, Apple s'efforce de n'utiliser que des matériaux recyclés pour ses produits, et Google utilise des énergies renouvelables pour alimenter ses centres de données.*

Les gouvernements et les organisations internationales jouent également un rôle important dans la promotion des technologies nécessaires. L'Union européenne a lancé une stratégie numérique qui met l'accent sur la promotion des technologies numériques, et les Nations unies ont lancé un programme intitulé "Action pour le climat et technologies numériques", qui vise à réduire l'impact environnemental de la technologie.

Implication personnelle dans la conception de l'infrastructure

C'est donc avec ces notions environnementales que j'ai créé mon infrastructure. Mes serveurs sont des laptops basse consommation avec une carte mère modifiée pour en prendre que les composants réellement utiles pour le serveur et pour le debug.

C'est également dans cette implication que j'utilise docker. Docker est bien moins gourmand en ressources que d'autres technologies d'isolation de systèmes.

Mes serveurs minimaux sont sur des Raspberry Pi Zero WH 2. Les serveurs minimaux dans l'infrastructure sont sur des Raspberry Pi Zero WH 2, une version légère du célèbre Raspberry Pi. Ils sont très peu gourmands en énergie et sont donc économiques et

écologiques. Ils sont également pratiques pour des tâches simples telles que la surveillance des systèmes. Il peuvent tourner sur une paire de pile, c'est impressionnant

Monitoring

Uptime Robot



Le monitoring est une pratique importante pour garantir la disponibilité et la performance des systèmes informatiques. Uptime Robot est un service de surveillance de site web qui permet de surveiller la disponibilité des sites web et des services. Le service envoie des alertes par e-mail ou SMS en cas de défaillance ou d'interruption.

Uptime Robot est un service de surveillance de site web qui permet de surveiller la disponibilité des sites web et des services. Le service envoie des alertes par e-mail ou SMS en cas de défaillance ou d'interruption. Il est un outil essentiel pour la surveillance de l'infrastructure HomeLab.

Grâce à Uptime Robot, il est possible de surveiller la disponibilité des serveurs et des applications en temps réel. En cas de défaillance, le service envoie une alerte immédiate par e-mail ou SMS, permettant de réagir rapidement et de minimiser les temps d'arrêt. Uptime Robot est configuré pour surveiller tous les services de l'infrastructure HomeLab, y compris les serveurs web, les serveurs de bases de données, les serveurs de messagerie, les serveurs de fichiers, etc.

Uptime Robot est également configuré pour surveiller les temps de réponse des serveurs et des applications. Cette fonctionnalité permet de détecter rapidement les problèmes de performance et de réagir avant qu'ils n'affectent l'expérience utilisateur.

Enfin, Uptime Robot fournit des rapports de disponibilité et de performance détaillés pour chaque service surveillé. Ces rapports permettent de suivre les tendances de disponibilité et de performance sur une période donnée, ce qui est utile pour identifier les problèmes récurrents et les tendances à long terme.

NetData Cloud & mails



NetData est un outil de surveillance des systèmes qui fournit des informations en temps réel sur les performances du système, les statistiques de trafic réseau, la charge du processeur et de la mémoire, etc. NetData m'aide à surveiller l'utilisation des ressources sur mes serveurs et à détecter les problèmes de performance avant qu'ils ne deviennent critiques.

NetData est également capable de générer des alertes en cas de dépassement de seuils de performance. Ces alertes peuvent être envoyées par e-mail ou par SMS, ce qui me permet de réagir rapidement en cas de problème.

En utilisant NetData Cloud, je peux surveiller mes serveurs à distance depuis n'importe quel appareil. Les données de surveillance sont stockées dans le cloud, ce qui me permet de les consulter en temps réel, même lorsque je suis en déplacement.

En outre, NetData Cloud fournit des fonctionnalités de suivi des versions et de gestion des mises à jour, ce qui facilite la maintenance de mes serveurs. Je peux être sûr que mes serveurs sont toujours à jour et sécurisés grâce à NetData Cloud.

En somme, NetData est un outil de surveillance essentiel pour tout propriétaire de serveur. Il permet de surveiller les performances en temps réel, de détecter les problèmes de performance et de les résoudre rapidement. Grâce à NetData Cloud, je peux surveiller mes serveurs à distance et être sûr qu'ils sont toujours à jour et sécurisés.

Traefik & ssl



Traefik peut surveiller les certificats SSL pour les sites Web en utilisant la propriété `tls.certResolver` dans le fichier de configuration Traefik. Cette propriété permet de configurer un résolveur de certificats SSL qui peut être utilisé pour surveiller les certificats SSL pour les sites Web.

Pour utiliser cette fonctionnalité, vous devez d'abord configurer un résolveur de certificats SSL dans le fichier de configuration Traefik. Le résolveur de certificats SSL peut être configuré pour utiliser un fournisseur de certificats SSL tiers, tel que Let's Encrypt, ou pour utiliser des certificats SSL auto-signés.

Une fois que le résolveur de certificats SSL est configuré, vous pouvez l'utiliser pour surveiller les certificats SSL pour les sites Web en utilisant la propriété `tls.certResolver` dans le fichier de configuration Traefik. Cette propriété spécifie le nom du résolveur de certificats SSL à utiliser pour le site Web.

Si le certificat SSL pour un site Web expire ou devient invalide, Traefik peut automatiquement renouveler le certificat SSL en utilisant le résolveur de certificats SSL configuré. Traefik peut également envoyer des alertes par e-mail pour informer l'administrateur système en cas de problème avec un certificat SSL.

Il est important de configurer correctement la surveillance des certificats SSL pour garantir la sécurité des sites Web. Les certificats SSL expirés ou invalides peuvent rendre les sites Web vulnérables aux attaques de sécurité. Il est donc recommandé de suivre les bonnes pratiques de sécurité pour surveiller les certificats SSL de manière appropriée.

Conclusion

Résumé de la mission

Cette mission consiste en la définition, la fabrication, l'installation ainsi que la configuration d'un système et d'un réseau de type entreprise dans ma maison. Ce système est capable de s'adapter à mes besoins et saura grandir avec mes besoins.

Bilan et perspectives d'avenir

Le bilan de cette mission est très positif. L'infrastructure mise en place est efficace, économique et écologique, tout en répondant aux besoins de l'utilisateur. Les choix de technologies ont été faits en tenant compte de l'impact environnemental et de la sécurité des systèmes informatiques.

Pour l'avenir, il est recommandé de suivre les bonnes pratiques de sécurité pour maintenir la sécurité et la disponibilité du système. Il est également important de continuer à surveiller l'impact environnemental du système et de prendre les mesures nécessaires pour réduire cet impact. Enfin, il est recommandé de continuer à suivre les tendances et les développements dans le domaine des technologies numériques pour s'assurer que l'infrastructure reste à la pointe de la technologie.

Je souhaite améliorer beaucoup de choses et ne prétend en aucuns cas mon système comme infaillible.

Enfin, il est important de suivre les tendances et les développements dans le domaine de la haute disponibilité pour garantir la disponibilité continue du système en cas de panne ou de défaillance d'un composant. Les solutions de haute disponibilité telles que le DNS failover peuvent aider à garantir la continuité de service en cas de panne.

Il est important de noter que la sécurité et la disponibilité des systèmes informatiques sont des préoccupations importantes pour toute organisation. Il est recommandé de

suivre les bonnes pratiques de sécurité et de surveiller régulièrement l'infrastructure pour détecter les anomalies ou les vulnérabilités de sécurité.



Cette documentation est la propriété intellectuelle de Grimaldi Baptiste.
portfolio.baptistegrimaldi.info/legal

Avis de droits d'auteur

Informations légales sur les droits d'auteur de cette documentation

Cette documentation a été créée par moi, Grimaldi Baptiste, en tant qu'étudiant. Tous les droits d'auteur sur cette documentation sont réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système de récupération ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre, sans l'autorisation préalable écrite de l'auteur.

Toute utilisation non autorisée de cette documentation peut constituer une violation des lois sur les droits d'auteur et entraîner des poursuites judiciaires.

Si vous souhaitez utiliser cette documentation à des fins éducatives ou autres, veuillez contacter l'auteur pour obtenir l'autorisation écrite nécessaire.

Copyright Grimaldi Baptiste, 2023.

Par Baptiste Grimaldi