MISE EN PLACE D'UNE SOLUTION DE TYPE REVERSE PROXY SOUS LINUX

Document qui explique la mise en place de la solution de type reverse proxy

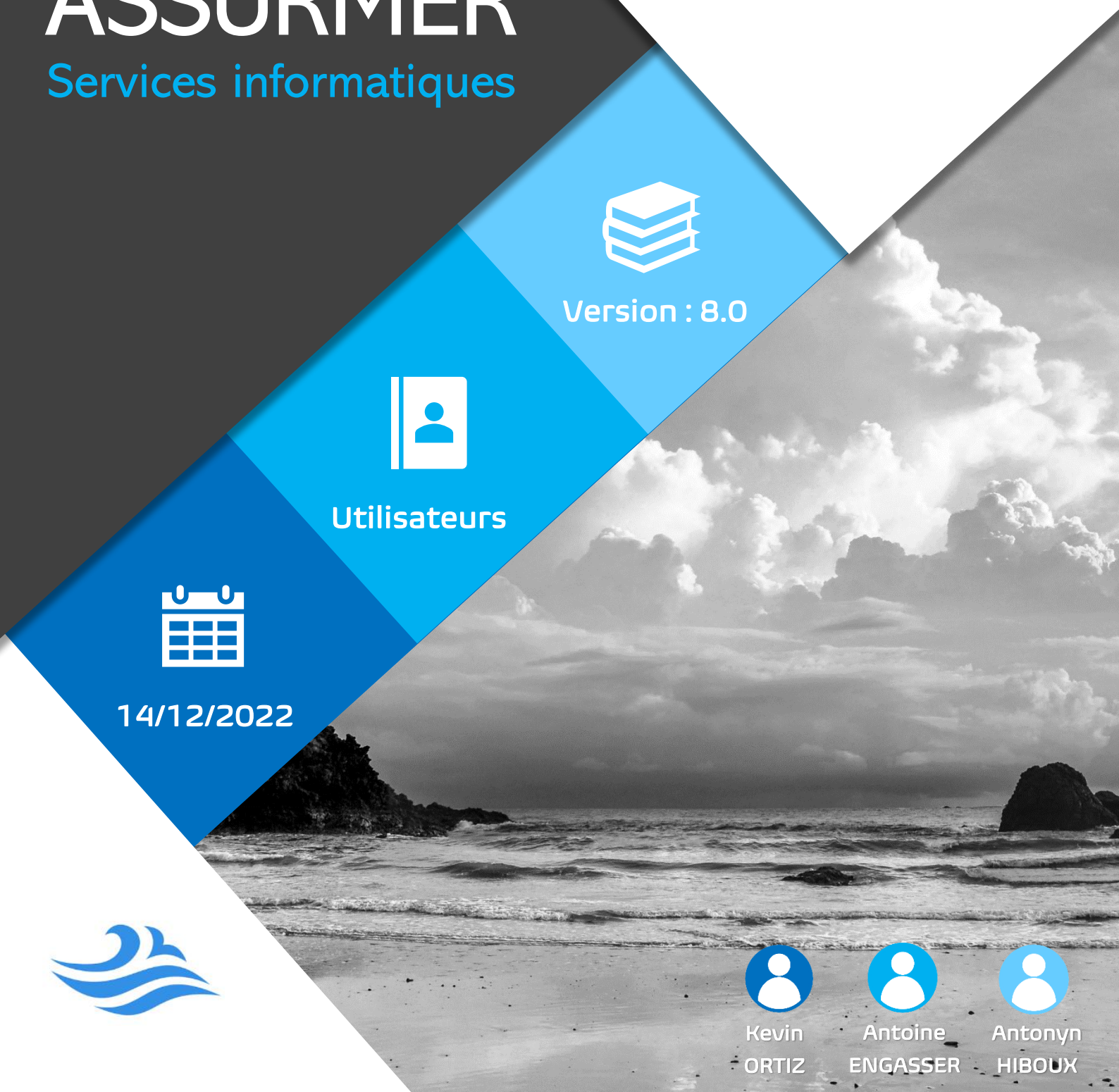
ASSURMER

Services informatiques

Version : 8.0

Utilisateurs

14/12/2022



Kevin ORTIZ

Antoine ENGASSER

Antonyn HIBOUX

DIFFUSION et VISAS

Diffusion			
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**
Assurmer	Service IT	Procédure	Réseau

Visas			
Société / Entité	**Nom**	**Fonction**	**Signature**

SUIVI DES VERSIONS

Versions				
Version	**Date**	**Auteur**	**Raison**	**Nombre de pages**
V 8.0	14/12/2022	Kevin ORTIZ Antoine ENGASSER Antonyn HIBOUX	Solution de stockage	14

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
Kevin ORTIZ	Kevin.ortiz@edu.esiee-it.fr	07.50.03.94.59
Antoine ENGASSER	Antoine.engasser@edu.esiee-it.fr	06.89.03.25.78
Antonyn HIBOUX	Antonyn.hiboux@edu.esiee-it.fr	07.09.23.45.13

Table des matières

I. Introduction et présentation du travail

Afin d'optimiser la monté en charge des connexions sur les serveurs Web Apache 2 d'Assurmer, nous allons installer une des solutions de type Reverse Proxy qui sont : Haproxy et HeartBeat.

Choix de l'outil de type Reverse Proxy

Heartbeat et Haproxy sont deux logiciels couramment utilisés pour surveiller la santé des serveurs et assurer la haute disponibilité des environnements de serveurs. Cependant, il existe quelques différences essentielles entre les deux.

Heartbeat est un programme open-source conçu pour surveiller la disponibilité des serveurs et pour assurer un basculement automatique en cas de défaillance d'un serveur. Il utilise un simple fichier de configuration et peut être facilement configuré pour surveiller la santé des serveurs et des services, et pour prendre les mesures appropriées si un problème est détecté.

Haproxy, quant à lui, est un équilibreur de charge et un serveur proxy plus complet. Il est capable de fournir un équilibrage de charge, une haute disponibilité et des capacités de proxy pour les applications basées sur TCP et HTTP. Il est souvent utilisé conjointement avec Heartbeat afin de fournir une solution complète pour assurer la haute disponibilité et l'équilibrage de charge dans les environnements de serveurs.

En termes de différences, l'une des principales différences entre les deux est que Heartbeat est principalement axé sur la surveillance de la disponibilité des serveurs, tandis que Haproxy est davantage axé sur la fourniture de capacités d'équilibrage de charge et de proxy. En outre, Heartbeat est généralement plus facile à installer et à configurer que Haproxy, qui peut être plus complexe en raison de ses fonctionnalités supplémentaires.

Dans l'ensemble, Heartbeat et Haproxy sont tous deux des outils utiles pour assurer la haute disponibilité et maintenir la santé des environnements de serveurs, mais ils servent des objectifs différents et peuvent être utilisés de différentes manières selon les besoins spécifiques d'une organisation.

Mais Il y a plusieurs raisons pour lesquelles nous préférons choisir Haproxy. Tout d'abord, Haproxy est connu pour être un logiciel très performant et fiable, offrant une latence et une disponibilité élevées. En outre, Haproxy est très configurable et peut être utilisé dans de nombreux environnements différents, ce qui en fait une solution très flexible. Enfin, Haproxy est également très populaire et bien documenté, ce qui signifie qu'il y a une grande communauté d'utilisateurs et de développeurs qui peuvent vous aider si vous rencontrez des problèmes ou si vous avez des questions. En résumé, les raisons pour lesquelles vous pourriez choisir Haproxy incluent sa performance, sa fiabilité, sa flexibilité, sa configurabilisé et sa communauté active.

Donc d'après les différentes études qu'on a réalisé sur les deux outils, nous avons décidé de choisir la solution d'Haproxy car Haproxy est très configurable et fiable, Haproxy nous offre plus de fonctionnalités que HeartBeat. Haproxy nous offre des capacités d'équilibrage de charge et de proxy pour les applications basées sur TCP et http.

II. Les avantages d'un serveur Proxy

Qu'est-ce qu'un Reverse proxy ?

Un Reverse Proxy est un type de serveur qui sert d'intermédiaire entre les clients et d'autres serveurs sur un réseau. Le proxy inverse est souvent utilisé pour améliorer l'évolutivité et la disponibilité d'un site web ou d'une application en permettant à plusieurs serveurs de partager la charge de travail et de travailler plus efficacement. En outre, le Reverse Proxy peut également fournir certaines fonctionnalités supplémentaires, telles que la mise en cache du contenu, le filtrage du trafic et la protection contre les attaques par déni de service. Dans l'ensemble, le proxy inverse est un outil précieux pour toute organisation qui doit améliorer les performances et la sécurité de son site web ou de son application.

Quels sont les avantages d'un serveur Proxy ?

Les avantages d'un serveur proxy peuvent varier en fonction du type de serveur proxy utilisé et de la manière dont il est configuré. Comme pour toutes les technologies, les serveurs proxy ont également des inconvénients, les avantages et inconvénients sont :

Avantages	Inconvénients
• **Meilleure sécurité** : en agissant en tant que relais pour les requêtes des clients, un serveur proxy peut aider à protéger les clients en masquant leur adresse IP et en empêchant les attaquants de cibler directement les clients. • **Meilleures performances** : en stockant en cache les données des réponses aux requêtes fréquemment utilisées, un serveur proxy peut accélérer les temps de réponse pour les utilisateurs et réduire la charge sur les serveurs distants. • **Contrôle de l'accès** : les administrateurs peuvent utiliser un serveur proxy pour contrôler l'accès des clients à Internet en autorisant ou en bloquant l'accès à certaines parties du Web. • **Filtre du contenu** : les administrateurs peuvent utiliser un serveur proxy pour filtrer le contenu qui passe à travers lui en bloquant ou en autorisant l'accès à certains types de contenu en fonction de critères prédéfinis.	• **Coût** : l'installation et la maintenance d'un serveur proxy peuvent être coûteuses, en particulier pour les entreprises qui ont besoin de serveurs proxy puissants pour gérer un grand nombre de requêtes. • **Latence** : en agissant en tant que relais pour les requêtes des clients, un serveur proxy peut ajouter une certaine latence à la communication, ce qui peut ralentir les temps de réponse pour les utilisateurs. • **Faiblesse de sécurité** : bien que les serveurs proxy puissent offrir une certaine sécurité en masquant l'adresse IP des clients, ils peuvent également être la cible d'attaques si les paramètres de sécurité ne sont pas correctement configurés. • **Incompatibilité avec certains protocoles** : certains protocoles de communication, tels que le protocole de transfert de fichiers (FTP) ou le protocole de transfert de courrier électronique (SMTP), ne peuvent pas être utilisés avec certains types de serveurs proxy.

III. Fonctionnement d'Haproxy

Comment fonctionne un Serveur Proxy ?

Un serveur proxy est un serveur qui agit en tant que relais pour les requêtes des clients d'un réseau vers d'autres serveurs. Il peut avoir plusieurs fonctionnalités, notamment :

- **Cacher les détails de l'architecture du réseau des clients** : en agissant en tant que relais, le serveur proxy peut cacher les détails de l'architecture du réseau des clients aux serveurs distants, ce qui peut aider à améliorer la sécurité du réseau en empêchant les attaquants de cibler directement les clients.
- **Contrôler l'accès à Internet** : les administrateurs peuvent utiliser un serveur proxy pour contrôler l'accès des clients à Internet en autorisant ou en bloquant l'accès à certaines parties du Web.
- **Améliorer les performances** : le serveur proxy peut stocker en cache les données des réponses aux requêtes fréquemment utilisées, ce qui peut accélérer les temps de réponse pour les utilisateurs et réduire la charge sur les serveurs distants.
- **Filtrer le contenu** : les administrateurs peuvent utiliser un serveur proxy pour filtrer le contenu qui passe à travers lui en bloquant ou en autorisant l'accès à certains types de contenu en fonction de critères prédéfinis.

En résumé, un serveur proxy peut être utilisé pour améliorer la sécurité, la vitesse et la flexibilité d'un réseau en agissant en tant que relais pour les requêtes des clients.

IV. La Cybersécurité des serveurs Proxy

La cybersécurité des serveurs proxy

La cybersécurité des serveurs proxy est l'ensemble des mesures de sécurité qui visent à protéger les serveurs proxy contre les attaques et les menaces en ligne. Les serveurs proxy peuvent être cibles d'attaques telles que des attaques par déni de service (DoS), des attaques par injection de code, des attaques de phishing, et d'autres types d'attaques visant à compromettre la sécurité des données ou des informations sensibles stockées sur ces serveurs.

Quel est le rôle d'un serveur proxy dans la cybersécurité ?

Le rôle d'un serveur proxy dans la cybersécurité est de fournir une couche de protection supplémentaire pour les réseaux et les systèmes informatiques en agissant en tant que pare-feu et en contrôlant l'accès aux réseaux et aux données sensibles. Un serveur proxy peut être configuré pour filtrer les données entrantes et sortantes, en bloquant les paquets de données malveillants ou non autorisés, et en autorisant uniquement les paquets de données légitimes. En agissant comme une barrière entre les utilisateurs et le réseau ou les systèmes informatiques, un serveur proxy peut aider à prévenir les attaques informatiques et à protéger les données sensibles.

Les attaques le plus fréquentes

Les attaques les plus fréquentes contre les serveurs proxy sont généralement similaires aux attaques courantes contre d'autres types de serveurs, et peuvent inclure des attaques par déni de service (DoS), des attaques par injection de code, des attaques de phishing, et d'autres types d'attaques visant à compromettre la sécurité des données ou des informations sensibles stockées sur ces

Serveurs. Pour protéger les serveurs proxy contre ces attaques, il est important de mettre en place des mesures de sécurité adéquates, telles que des pares-feux et des logiciels de détection d'intrusion, et de mettre à jour régulièrement les logiciels et les systèmes d'exploitation pour éviter les vulnérabilités connues.

V. Fonctionnement et Utilisation

Fonctionnement

Il s'agit de la page d'accueil par défaut utilisée pour tester le bon fonctionnement du serveur Apache après son installation sur les systèmes Debian. Si vous pouvez lire cette page, cela signifie que le serveur HTTP Apache installé sur ce site fonctionne correctement. Vous devez remplacer ce fichier (situé dans **/var/www/html/index.html**) avant de continuer à faire fonctionner votre serveur HTTP.

Si vous êtes un utilisateur normal de ce site Web et que vous ne savez pas de quoi parle cette page, cela signifie probablement que le site est actuellement indisponible pour cause de maintenance. Si le problème persiste, veuillez contacter l'administrateur du site.

Aperçu de la configuration

La configuration par défaut d'Apache2 dans Debian est différente de la configuration par défaut en amont, et est divisée en plusieurs fichiers optimisés pour l'interaction avec les outils Debian. Le système de configuration est entièrement documenté

dans le document rusrshare doc anacheTREADME.Debian.az. Vous pouvez vous y reporter pour la documentation complète.

La documentation pour le serveur web lui-même peut être trouvée en accédant au manuel si le paquet apache2-doc a été installé sur ce serveur.

La disposition de la configuration pour une installation de serveur web Apache2 sur les systèmes Debian est la suivante :

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- ***apache2.conf*** est le fichier de configuration principal. Il rassemble les pièces en incluant tous les autres fichiers de configuration lors du démarrage du serveur web.
- ***ports.conf*** est toujours inclus dans le fichier de configuration principal. Il est utilisé pour déterminer les ports d'écoute.
- Les fichiers de configuration dans les répertoires ***mods-enabled/***, ***conf-enabled/*** et ***sites-enabled/*** contiennent des extraits de configuration particuliers qui gèrent respectivement les modules, les fragments de configuration globale ou les configurations d'hôtes virtuels.