Le 29/10/2021,

Objet : Guide accompagnant la mise en place d'une infrastructure VHA multi-hébergeur sous load-balancers

Bonjour,

Vous nous avez sollicité pour mettre en place une infrastructure **VHA (Very High Availability - Très Haute Disponibilité)** multi-hébergeur afin de travailler votre résistance à un **incident global touchant toute l'infrastructure d'un hébergeur** donné (cas d'OVH le 13/10/2021 ayant mis hors service plus de 350 000 serveurs sur 3 continents).

La seule et unique solution pour être **résilient à ce type de dysfonctionnemen**t de gravité sévère est une **infrastructure VHA** composée d'au moins 4 serveurs dans un contexte multi-hébergeurs, au moins deux serveurs type **load-balancer (dénommé LB** pour la suite) et au moins deux **serveurs de production (dénommé PROD** pour la suite), chaque couple LB/PROD étant réparti chez chacun des hébergeurs souhaités par le CLIENT (à date : OVH et Online/Scaleway - les deux plus gros hébergeurs FR et EU).

Pour travailler la résistance à des pénuries de stock d'envergure mondiale (vécue en Automne 2011 et en cours sur la période 2021-2023), nous conseillons fortement à nos clients ayant plus de 2M€ HT de chiffre d'affaires dépendant à la continuité de service de leurs infrastructures de tripler les PRODs.

La mise en place de ce type d'infrastructure VHA engendre des changements qu'il est nécessaire de bien avoir en tête sous peine de générer des dysfonctionnements.

1. Considérations générales à propos des infrastructures VHA

Avant-propos : TW ne propose toujours pas d'infrastructure MASTER-MASTER à date, il s'agit donc toujours d'infrastructure MASTER-SLAVE - Wysiwyg et donc "dev friendly" - souhaité par le marché spécifique des TPE/PME.

Pour fonctionner, les infrastructures VHA exploitent deux mécaniques appelées de "failover".

A/ La première dénommée de "failover DNS' est gérée côté navigateur Internet.

La quasi-totalité des navigateurs Internet grand public (Chrome / FireFox / Safari / Edge / Opéra) ET modernes - datant donc de moins de 3 ans - la gère convenablement.

Pour l'EXEMPLE sur l'infrastructure hébergeant www.touchweb.fr : https://dnschecker.org/#A/www.touchweb.fr (cliquer sur "Search" pour "lancer" la résolution DNS) vous constaterez DEUX adresses IP, correspondant aux DEUX adresses IP des DEUX load-balancers répartis chez les DEUX hébergeurs distincts.

Votre navigateur Internet grand public et moderne va tester chacune des adresses IP fournies par la résolution DNS, si l'une ne répond pas, votre navigateur Internet va automatiquement "tester" l'autre. Ceci constitue la première "failover". Par EXEMPLE, si l'adresse IP du LB chez OVH ne répond pas, votre navigateur testera automatiquement l'adresse IP du LB chez Online/Scaleway.

Pour les plus techniques d'entre vous : les applications systèmes cURL et Wget gèrent également aussi cette mécanique.

ATTENTION : cette mécanique impose que votre équipement réseau dans votre réseau local d'entreprise soit respectueux du protocole DNS et donc qu'aucun équipement réseau de votre réseau local d'entreprise ne mette en cache abusivement et de manière irrespectueuse au regard du protocole DNS, une seule des deux résolutions DNS disponibles.

Par suite d'une découverte chez un CLIENT d'un équipement réseau corrompu, irrespectueux du protocole DNS, il est dorénavant obligatoire que nous réalisions un contrôle de conformité de votre équipement réseau local. En cas de dysfonctionnement, il vous sera demandé de contacter votre prestataire de maintenance informatique gérant votre réseau local d'entreprise afin qu'il remplace ou mette à jour vos équipements réseaux dans votre réseau local d'entreprise.

B/ La deuxième dénommée de "failover IP" est gérée par les load-balancers et neutralise totalement la dépendance aux adresses IP failover d'un hébergeur donné

Vos deux serveurs type load-balancer permettent de basculer manuellement et dans un délai raisonnable (généralement moins de 15 minutes) le trafic réseau depuis une PROD (anciennement MASTER) vers une autre PROD (anciennement SLAVE devenue MASTER).

A date, **ces deux actions sont manuelles**, à savoir : le changement de statut "SLAVE" vers "MASTER" ainsi que la reconfiguration des LBs pour changer le routage réseau vers le nouveau MASTER.

L'automatisation de ces deux actions critiques (car susceptibles de casser complètement le service) est toujours en cours d'étude via un quorum d'au moins cinq serveurs DNS ayant autorité à désigner des MASTER et donc reconfigurer les nœuds : LBs ET PRODs dépendantes via des zones DNS (risque cybersécurité - risque corruption)

2. ATTENTION : Obligation d'externaliser la distribution des emails transactionnels

Il est obligatoire d'externaliser la distribution des emails transactionnels (rappel de mot de passe / confirmation de commandes / etc) vers des tiers spécialisés tel que Mailjet / SendInBlue / Mailchimp.

Pourquoi ? Parce qu'il n'est plus possible d'avoir une reverse DNS CONFORME entre la PROD MASTER qui émet l'email et l'adresse IP de l'application métier contraint à pointer sur les DEUX LBs.

Par EXEMPLE, si l'adresse IP de la PROD MASTER est 1.1.1.1 et que l'expéditeur est test@touchweb.fr, lorsqu'un email va être émis, le tiers (par EXEMPLE Google pour Gmail) qui va le recevoir va contrôler que la reverse DNS de l'adresse IP 1.1.1.1 est égale au domaine de l'expéditeur soit touchweb.fr.

Toujours dans cet EXEMPLE, touchweb.fr est contraint de pointer vers les DEUX adresses IP des DEUX LBs (mécanique inhérente aux infrastructures VHA), et ne vaudra donc jamais 1.1.1.1 (dans cet EXEMPLE, l'adresse IP de la PROD MASTER) ce qui engendrera suivant les tiers des échecs de distribution pour cause d'incohérence contre leurs contrôleurs rDNS / domaine expéditeur.

En résumé : il est obligatoire que TOUS les emails transactionnels transitent par des tiers spécialisés en emailing et plus jamais par le relay SMTP local

3. Traitements informatiques basés sur l'adresse IP du visiteur

Les configurations en place sur les serveurs sous infogérance TOUCHWEB autant côté LBs (HaProxy) que côté frontend sur les PRODs (Apache2) surchargent proprement les variables d'environnement pour que **vous n'ayez pas à vous en soucier.**

Autrement dit **vous pouvez continuer à traiter les adresses IP des visiteurs comme vous avez l'habitude** de le faire que ce soit au niveau de votre applicatif métier (Prestashop / Magento / etc) qu'au niveau d'éventuelles surcharges du frontend Apache2 via le ou les fichiers .htaccess, par exemple pour gérer des redirections en fonction de la géolocalisation du visiteur.

4. Quid des mécaniques de cyber-défense (bannissements)

Un aspect relativement contre-intuitif des infrastructures VHA est que l'on est contraint de déporter les mécaniques de cybersécurité sur les LBs au lieu des PRODs (IDS TW : Intrusion Detection System TouchWeb)

Cela signifie que ce n'est plus les PRODs qui sont susceptibles de vous bannir (car elles ne "voient" que l'adresse IP des LBs), ce sont les LBs eux-mêmes.

Avec une particularité inhérente aux mécaniques de failover DNS (relire point 1/ A/ si nécessaire), c'est que si l'un des LB vous bannit, votre navigateur va vous basculer sur le deuxième LB, qui risque également de vous bannir.

En résumé, votre adresse IP se retrouvera bannie - non plus d'un seul serveur de PROD (cas des infrastructures HA conventionnelles) - mais d'un LB voir des DEUX LBs.

Nous vous suggérons de toujours cocher "Ajouter à tous les serveurs" lorsque vous administrez la liste des adresses IP ne pouvant pas être expulsées.

5. Quid des accès FTP/ES et SSH (SFTP)

Sur les infrastructures HA conventionnelles - mono-hébergeur - vous aviez l'habitude que l'on vous fournisse une adresse IP spécifique, appelée adresse IP failover. On vous expliquait - toujours sur ces infrastructures HA conventionnelles mono-hébergeur - que vous n'aviez pas à vous en soucier, l'adresse IP étant déplacée en toute transparence en fonction du serveur désigné comme PROD MASTER.

Pourquoi privilégier une adresse IP plutôt qu'un sous domaine, par EXEMPLE : ftp.touchweb.fr : **pour éviter d'avoir à gérer des incidents de serveurs de nom** (serveur DNS) générant abusivement du bruit côté CLIENT et la quasi-totalité du temps, de la responsabilité du CLIENT car **de la responsabilité du fournisseur d'accès Internet du CLIENT.**

Par effet de bord, ces adresses IP dénommées "Failover" créent une dépendance forte au Manager / API de l'hébergeur. Cela nous ayant grandement causé du tort par le passé (paralysie du Manager / API de l'hébergeur comme par exemple le 10/03/2021 ou encore le 13/10/2021) engendrant une paralysie totale des adresses IP Failover.

Les infrastructures VHA suppriment définitivement cette dépendance au Manager / API de l'hébergeur, ce sont les LBs qui émulent cette mécanique de failover IP.

Pour les plus techniques d'entre vous : pour des raisons de sécurité, il est totalement exclu de gérer une mécanique de LB over FTP ou over SSH. Pourquoi ? car cela impose de faire du LB over TCP (purement network sans aucun historique lisible par un IDS log-based côté LB), ce sont déjà des couches de complexité forte, il est exclu d'aggraver la complexité de ce type d'infrastructure (synchronisation d'historiques des daemons OpenSSH et ProFTPd / Vsftpd) depuis les PRODs vers les LB ET synchronisation des listes noires (BL) entre les LBs aggravant les scénarios de dysfonctionnement)

Plus concrètement, cela signifie que les emails d'accès FTP/ES et SSH **contiendront TOUTES les adresses IP de TOUS les serveurs éligibles à un statut MASTER** (généralement S1 / S2 / S3) et qu'il sera nécessaire que vous déclariez toutes ces adresses IP dans votre client FTP (Filezilla) avec un suivi de la PROD MASTER bien que facilité par le Manager TW qui l'annonce (colonne Application métier alimentée sur le serveur MASTER) ET par le fait qu'une seule de ces PRODS "répondra" (ces accès étant verrouillés sur les PRODs SLAVE)

.

6. Quid des éventuels accès spécifiques contre MariaDB/MySQL (connexion directe sur le port 3306 - donc n'exploitant pas PHPMyAdmin)

Si vous nous avez réclamé une connexion directe contre le port 3306 de MariaDB/MySQL (MySQL Workbench / Navicat / PrestaManager / etc), nous vous prions également d'utiliser les adresses IP fournies par l'email récapitulatif d'accès pour les mêmes raisons de sécurité que celles détaillées au point 5 (LB over TCP sans historique lisible par un IDS log-based).

Vous êtes susceptible de vous interroger sur le pourquoi cela fonctionne avec PHPMyAdmin, PHPMyAdmin est une application métier standard au même titre que vos sites E-Commerce, vous y accédez donc exactement de la même manière que vos sites E-Commerce via le protocole de communication HTTP - géré par vos DEUX LBs.

Date de dernière mise à jour : 05/11/2021

Si nous bénéficions d'un retour d'expérience de plusieurs années sur les mécaniques de LB sur l'infrastructure de service TW, la mise en œuvre sur des infrastructures CLIENT a démarré en novembre 2021.

Il est probable qu'il y ait des découvertes nécessitant des ajustements soit d'un point de vue technique, soit d'un point de vue documentation, comme à l'accoutumée, nous les traiterons au mieux à détection. Nous vous remercions pour votre patience.

A très vite pour un prochain guide !