Le 23/12/2019,

Objet : Premier pas sur les infrastructures sous infogérance TW

Ce guide est à destination des prestataires externes n'étant pas sur les canaux internes du réseau TW : si c'est la première fois que vous travaillez sur un serveur sous infogérance TW, **nous vous invitons à lire la suite avec attention** pour améliorer votre productivité (ainsi qu'éviter des désagréments anticipables)

Nous sommes une infogérance Européenne respectueuse de la législation en vigueur. Si vous avez l'habitude de travailler sur le marché des TPE à moins de 500K€ de CA / an, certains process sont susceptibles de vous sembler étonnants (bien qu'ils soient communs sur le marché des PME) : il est important de comprendre qu'ils répondent à trois engagements contractuels :

1. garantir une excellente continuité de service en *situation optimale* (nous insistons : en situation optimale - on s'intéresse à bien plus de choses qu'un simple ping) des sites Internet de nos clients (expertise devops senior)

2. garantir un plan d'atténuation des risques professionnel résistant à la majorité des menaces réelles et sérieuses du marché des TPE/PME (du fait des instances CLOUD à quelques centimes l'heure et l'incapacité des hébergeurs à être pro-actifs à ce propos, le volume d'attaques depuis fin 2017 est quadruplé chaque année). Il n'est plus possible d'être laxiste à ce propos.

3. garantir une excellente portabilité des systèmes d'information dans un contexte multi-hébergeur pour qu'aucun de nos clients ne soit dépendant de son infrastructure (PRA professionnel - migration conforme garantie contractuellement - avec moins de 120 secondes d'arrêt de service sur les forfaits HA) - cet engagement nous permet de limiter fortement la durée des pannes ainsi que faire bénéficier nos clients pro-activement des nouvelles gammes de serveur. Déménager un site est quelque chose de normal ici et n'a donc rien d'exceptionnel.

Sommaire :

1/ ATTENTION : Les préproductions sont détruites tous les jours (par défaut)

80% des pannes des sites Internet sont générées par des mises à jour non testées.

Pour répondre à ce problème, **nous mettons à disposition des préproductions *rigoureusement* conformes aux productions**. 99% des projets sous infogérance TW en bénéficient - elles sont facturées à un forfait fixe de 20€ HT / mois (par serveur de préproduction).

Pour s'assurer de la conformité de la préproduction, le Manager TW permet de la détruire soit de manière automatisée (ce qui est toujours le cas par défaut) soit de manière manuelle puis de la reconstruire sur la base de la sauvegarde du matin de la production.

Nous sensibilisons notre clientèle au fait qu**'il est important que leurs préproductions soient tenues à jour**, les mécaniques de reconstruction de leurs préproductions s'inscrivant dans leur PRA (plan de reprise de l'activité) et permettent entre autres choses : de s'assurer que les sauvegardes sont conformes aux attentes.

Par défaut, des alertes sont envoyées par email toutes les 2 semaines si la préproduction n'a pas fait l'objet d'une régénération sur la période invitant (vivement au-delà d'un mois) nos clients à la détruire puis reconstruire (en cliquant sur le bouton rouge relatif sur le Manager TW)

Les préproductions ne sont jamais sauvegardées par défaut partant du principe que pour la quasi-totalité de notre clientèle cela n'a aucun sens de re-sauvegarder une sauvegarde. Cela permet aussi d'éviter des surcoûts discutables sur les contrats de sauvegarde multi-site.

Dans ce contexte : **les préproductions *NE DOIVENT PAS* être utilisées comme environnement de développement.**

ATTENTION à veiller à désactiver la destruction / reconstruction possiblement automatique configurée si nécessaire en :

- réclamant une délégation au Manager TW à notre client commun pour être autonome à ce propos (ne pas hésiter à nous appeler pour une présentation du Manager TW)
- le demandant à notre client commun*****

NB : Les préproductions et de manière générale les liens ne devant pas être exposées à tous (incluant PMA) sont protégées par un htpasswd (login/password réclamés dans une popup). Pour vous éviter d'avoir à saisir ces paramètres d'identification, nous livrons toujours des liens sécurisés (contenant le login/password relatif)

Dans l'éventualité d'un bug de votre navigateur, affichant la popup malgré la présence du login/password dans le lien sécurisé, nous vous invitons à découper le lien sur un bloc note : https://LOGIN:PASSWORD@URL. **Par exemple, si le lien est : https://test1:test2@www.test.fr : le login est test1, le mot de passe est test2** et l'URL : https://www.test.fr

2/ Gestion des droits (GDRP/RGPD COMPLIANT)

En l'accord avec les besoins du DPO - fonction devenue obligatoire depuis mai 2018 : https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo, les accès au système d'information sont nominatifs afin de les aider à tenir un registre.

Sur les systèmes GNU/Linux : seul le propriétaire d'un fichier/dossier peut éditer les droits (chmod/chown) - c'est une limitation système de base inhérente à GNU/Linux qui n'a rien avoir avec TOUCHWEB.

Pour aider à l'identification de l'origine d'un dysfonctionnement, le serveur Web utilise son propre utilisateur (www-data ou user personnalisé) qui n'est jamais le même que les utilisateurs livrés (sur les liens FTPES/SSH).

Si d'un côté nous nous assurons d'effectuer tous les réglages nécessaires pour que votre groupe d'utilisateurs ait les pleins pouvoirs sur le fragment du système dont vous avez besoin (umask et droits hérités conformes), d'un autre côté, il peut arriver ponctuellement que vous ayez besoin de chmod/chown.

Si vous souhaitez chmod/chown un fichier/répertoire dont vous n'êtes pas le propriétaire, le système vous l'interdira (opération non permise)

SOLUTION :

En créant un fichier dans /path_to_cms/tw_supervisor/api/ dénommé "reset_rights", cela remettra en conformité les droits. La prise en charge par le superviseur d'application métier se fera dans la minute.

Le chmod / chown qui passe en récursif est configurable - ne pas hésiter à nous contacter à ce propos.

3/ Historiques du serveur Web : où sont-ils ?

Pour les stacks Web : les historiques des daemons HAProxy, Apache2, NGinx et FPM sont dupliqués toutes les minutes sur l'hyperviseur : https://manager.touchwweb.fr

Si vous intervenez sur le projet, **nous vous invitons à réclamer à notre client commun une délégation à son Manager TW : *vous en aurez besoin*.** (Manager TW | Infrastructure | Serveurs)

Si vous avez besoin de consulter en temps réel les historiques, nous vous invitons à réclamer un accès SSH.

Par ailleurs, vous êtes sur une infrastructure professionnelle qui bénéficie d'historiques avancés (en plus des historiques standards), pour aider les pools de développement SENIOR :

- les scripts PHP dont le temps d'exécution dépasse 3 à 5 secondes sont auto-profilés et ce profiling est historisé : voir /var/log/php/*.slow - cela peut vous éviter des heures de recherche.

- pour les bases de données : les structures et index des tables sont photographiées régulièrement et un delta avec l'état antérieur est disponible ici /var/log/mysql/btws_integrity.log - cela peut aussi vous éviter des heures de recherche (mise à jour de module en anomalie, tiers malveillant qui DROP une clé primaire dans une table, etc)

- pour les bases de données et si le serveur bénéficie d'une réplication active (infra HA - haute disponibilité) - les logs binaires contenant toutes les requêtes SQL altérant les datas donc ALTER / UPDATE / INSERT / DELETE, sont disponibles dans /var/log/mysql/*bin* - cela peut vous permettre d'obtenir un horodatage précis d'une requête SQL lancée par un script PHP en anomalie. Le binaire nécessaire à la lecture de ces historiques : mysqlbinlog est disponible dans votre chroot. Suivant l'OS (Stretch), il peut y avoir une anomalie de charset (https://jira.mariadb.org/browse/MDEV-15835), si cela vous arrive, nous vous invitons à spécifier mysqlbinlog --no-defaults /path_to_binlog/ ou à nous réclamer une suppression du default-charset sur la configuration [client] (attention aux effets de bord)

4/ Erreur 408 - Timeout - Détecter une expulsion (bannissement)

Cette erreur est la plus commune que l'on peut rencontrer ici (pour les admins/prestataires techniques), dans 99% des cas il s'agit d'une expulsion (bannissement par l'IDS TW) - nous vous invitons à ajouter l'IP bannie à la liste blanche du serveur via le Manager TW.

Pour se faire, nous vous suggérons de réclamer une délégation au Manager TW du client.

Nous vous prions de considérer ceci : les serveurs en ligne sont exposés à différentes menaces, la mise en place d'une politique de sécurité (via un PAR : plan d'atténuation des risques) impose obligatoirement une mécanique d'expulsion. Sans expulsion, il est impossible d'avoir un service stable.

Il est important de comprendre que c'est précisément pour cette raison que les hébergements mutualisés sont notoirement connus pour être instables car il est impossible sur ce type d'hébergement d'avoir une mécanique de liste blanche - prérequis indispensable pour la mise en place d'une mécanique d'expulsion.

Pour les plus techniques d'entre vous, nous vous invitons également à considérer ceci : nous gérons plus de 2 500 modules Prestashop / Magento / Wordpress / Drupal dont plus de 200 ont des APIs gérées par des tiers qui dans 40% des cas ne sont pas capables de nous fournir des IP fixes. Dans ce contexte précis, il est inenvisageable de mettre en place une solution anti-ddos basée sur du challenging JS/Recaptcha et nécessaire de conserver en l'état l'IDS LB + liste blanche. C'est le seul compromis viable sur le marché particulier des TPE ayant expressément besoin de flexibilité.

Il existe une méthode simple et rapide pour constater que votre adresse IP a été bannie : tenter d'accéder au site via une autre adresse IP (comme celle de votre téléphone portable connecté sur un réseau mobile 3G/4G). Si cela fonctionne sur cette autre IP mais pas celle de votre ordinateur, alors il s'agit d'un ban.

Le fait de vous ajouter en liste blanche, en plus d'éviter de vous faire bannir vous évitera aussi de subir des micro-bans de 10 secondes (ce qui peut arriver à ceux qui sont victimes d'ongletite chronique aigüe - ou le syndrome du clic molette en mitraillette - à bon entendeur)

5/ Mise à jour d'une image / js / css non prise en charge

Si vous êtes confronté à une persistance non souhaitée de contenu, nous vous invitons à vérifier que :

A/ Votre navigateur est hors de cause

Certains navigateurs mettent en cache (parfois abusivement) certains contenus. Sous Firefox et Chrome, veillez à bien cocher la box dans la console (F12 - onglet Network) : "Disable cache"

***Attention 1* aux configurations qu'un tiers a pu mettre dans le .htaccess racine relatives à mod_expires.**
Si Google conseille des valeurs élevées d'expiration et donc suggère aux développeurs de configurer mod_expires, cela peut vous causer du tort. Nous vous laissons le soin d'effectuer un arbitrage à ce niveau : souhaitez-vous vous plier aux doléances de Google au risque d'avoir des persistances contre-intuitives de contenu OU souhaitez-vous améliorer votre productivité ?

NB : Nous déconseillons la mise en place de mod_expires si des tiers ayant des compétences de niveau JUNIOR interviennent sur le projet.

***Attention 2* : les redirections 301** (permanentes - qui s'opposent à des redirections 302, temporaires) **sont souvent gardées en mémoire** - cette mécanique 100% liée à votre navigateur cause souvent du tort aux consultants SEO. Si vous souhaitez que votre navigateur "oublie" une redirection 301, il est nécessaire de le relancer (Attention avec Chrome - fermer le navigateur ne suffit pas toujours - conseil pour les non techniciens : passer sous Firefox ou redémarrer l'ordinateur)

B/ Le CDN est hors de cause

En l'accord avec les doléances de Google, la majorité des projets supervisés par TW bénéficie d'une MEDIA URL (media.DOMAINE) et sur les sites en production : ces MEDIA URL sont déployées sur un CDN.

Nous attirons votre attention sur le fait qu'une MEDIA URL et un CDN sont 2 choses bien distinctes et la présence de l'une n'entraîne pas nécessairement la présence de l'autre.
Par exemple, si le site de production bénéficie d'une MEDIAL URL (quasiment toujours déployée sur CDN), par soucis de cohérence et pour vous aider à capturer en amont d'éventuelles anomalies de CORS Policy (pour ne citer qu'elles), la préproduction associée bénéficiera aussi d'une MEDIA URL - cependant spécifiquement sur les préproductions, la MEDIA URL de préproduction n'est jamais déployée sur CDN (pour éviter que le CDN ne vous cause du tort).

Si vous ne savez pas ce qu'est un CDN, pour faire simple et éviter de rentrer dans les détails de cette technologie de pointe (DNS Anycast sur une infrastructure mondiale) : c'est un cache.

Comme tous les systèmes de cache : ils fonctionnent de la même manière, SI le lien ne change pas ET que personne ne vide le cache ALORS le contenu du cache est mis à jour à la durée de vie configurée, variable suivant les doléances du client (12h à 1 mois - vous pouvez nous réclamer une mise à jour à ce niveau)

Pour savoir si c'est un cache non souhaité au niveau du CDN, nous vous invitons à mettre à la fin du lien du fichier incriminé une séquence aléatoire de ce type : ?t=<nombre aléatoire> - SI le contenu affiché via ce lien réécrit ne change pas ALORS cela ne vient pas du CDN (mais du serveur OU dans de rare cas d'un proxy entre votre ordinateur et le serveur) SINON vous avez 3 options :
- réclamer un accès au compte OVH du CLIENT pour être autonome sur la purge du CDN (il faudra aussi nous réclamer de lui transférer les pleins pouvoirs à ce propos)
- nous réclamer une purge du CDN (à éviter - cela neutralise son effet - certaines infrastructures pour faire économiser de l'argent au CLIENT sont sous dimensionnées compte tenu de la présence d'un CDN)
- faire en sorte que le lien du contenu soit différent

***Attention 3* :** si vous comptez éditer de nombreux contenus exploitant la MEDIA URL ET que cette MEDIA URL est déployée sur CDN, nous vous suggérons de supprimer temporairement la MEDIA URL (partout - attention aux contextes multi-boutiques qui nécessitent parfois une désactivation manuelle sur l'ensemble des sous boutiques)

C/ Le cache serveur est hors de cause

Si notre client commun nous a réclamé mod_pagespeed pour Apache2, il est tenu de vous en informer (voir lettre d'information TW de Juin 2019 https://www.touchweb.fr/lettre-information-19061)
Nous vous invitons à lui réclamer un détail technique pour forcer un refresh ou le cas échéant à réclamer une désactivation de mod_pagespeed

Vous pouvez voir si ce module est activé via le Manager TW (Infrastructure | Serveurs | cliquer sur le serveur hébergeant le site | déplier la box Système à droite | constater si PageSpeed est désactivé - cela sera écrit)

Pour détecter si c'est un cache serveur qui pose soucis (sous réserve que vous ayez mis hors de cause un éventuel CDN), il existe une méthode simple, rajouter un paramètre aléatoire à la fin de votre lien ?t=<chaîne aléatoire>

6/ D'où vient une redirection 301 / 302 ?

Lorsque vous êtes confronté à une redirection 301 ou 302, cela peut venir de :

- la configuration du front end (HAProxy/Apache2/Nginx) - le TTFB de la 301/302 sera inférieur à 50ms
NB : la majorité de nos fronts ends est configurée pour rediriger automatiquement les requêtes HTTP effectuées de manière non sécurisée (protocole HTTP sur port 80) vers leurs variantes sécurisées (protocole HTTPS sur port 443) en l'accord avec les doléances de Google - hors demande expresse du client OU module non compatible (ATOS)
- un .htaccess - le TTFB de la 301/302 sera aussi inférieur à 50ms - S'IL n'y a rien dans le .htaccess ALORS c'est la configuration du front end.
- l'application métier (Prestashop/Magento/Drupal/Wordpress) - le TTFB devrait être au moins cinq fois supérieur (>250ms)

Pour isoler le TTFB sur Google Chrome et Firefox (F12 - Onglet network - CTRL + F5 - puis regarder le temps de distribution de la page initiale ayant souffert de la 301/302) - en veillant à cocher "Preserve logs"

7/ Sauvegarde - préservation et récupération

Du fait des mécaniques de sauvegarde multi-site et multi-hébergeur, les sauvegardes du système d'information sont disponibles sur demande via email.

Ce type de demande est généralement traité sous 15 minutes sur les périodes couvertes par le contrat d'infogérance.

Fréquence des sauvegardes :

- les fichiers sont sauvegardés exhaustivement (hors fichier auto-reconstructible tel que les caches)
Ces snapshots sont conservés sur 4 jours (entrées de gamme), 10 jours (OMNI+) ou 30 à 60 jours (sur-mesure)
Pour les préservations sur 4 jours et 10 jours glissants, les snapshots du premier jour des 2 derniers mois sont aussi conservés (incluant mécaniquement le mois en cours)

- les bases de données sont sauvegardées sur 60 jours glissants + conservation variable au-delà.

En plus de cela pour les infrastructures HA (haute-disponibilité), sur le serveur secondaire de production :
- les bases de données sont sauvegardées toutes les demies-heures (* 0,30) avec préservation sur les dernières 24 heures (sauf en cas d'undersizing de la réplication, dans ce cadre : * 30)
- les fichiers sont sauvegardés toutes les heures (* 15) sans préservation donc avec écrasement de l'état antérieur du fait de la volumétrie de données

Vous pouvez nous réclamer à tout moment une restauration de données sur les périodes couvertes par le contrat d'infogérance - les restaurations totales sont incluses dans tous nos contrats d'infogérance. Nous vous conseillons de nous réclamer de forcer une sauvegarde lorsque vous savez que vous allez mettre en production une évolution à risque.

NB : les restaurations partielles (reconstruction d'un fragment de table, etc) ne sont pas incluses.

8/ Géolocalisation professionnelle par pays (DB PRO Maxmind)

Si vous avez besoin d'effectuer de la géolocalisation par pays, nous vous encourageons à exploiter des bases professionnelles (MaxMind) *régulièrement* mises à jour (au moins une fois par mois)

La pénurie d'IPv4 (novembre 2019) a pour conséquence d'engendrer plus fréquemment des redistributions des pays d'attribution de blocs IP (revente) : il convient donc de tenir à jour vos bases de données à ce propos sous peine de bloquer abusivement des tiers.

Les forfaits d'infogérance TW incluent un support professionnel à ce propos via mod_maxminddb pour Apache2 incluant une mise à disposition de la base PRO IP/Country au format mmdb ainsi que des mises à jour fréquentes. N'hésitez pas à nous demander de vous mettre à disposition ce module et la base professionnelle qui l'accompagne (financée par TW).

Vous pourrez ainsi configurer via vos .htaccess d'éventuelles redirections ou des blocages. Code pays : https://dev.maxmind.com/geoip/legacy/codes/iso3166/ - le module est préconfiguré par nos soins (entre autres choses initialisation des variables d'environnement MM_COUNTRY_CODE et GEOIP_COUNTRY_CODE)

Exemple d'un blocage (Ukraine et Brésil) que vous pouvez ajouter à la fin de votre .htaccess :

```
SetEnvIf GEOIP_COUNTRY_CODE ^(UA|BR) BlockCountry
Deny from env=BlockCountry
```

Exemple d'une redirection (avec création d'une nouvelle variable d'environnement - généralement à insérer en entête du .htaccess pour la bonne prise en charge) :

```
SetEnvIf GEOIP_COUNTRY_CODE FR VISITOR_COUNTRY=FR
SetEnvIf GEOIP_COUNTRY_CODE UK VISITOR_COUNTRY=US
SetEnvIf GEOIP_COUNTRY_CODE US VISITOR_COUNTRY=US

RewriteEngine On
RewriteCond %{ENV:VISITOR_COUNTRY} ^FR$
RewriteRule ^(.*)$ http://www.test-redirection.fr/$1 [L,R=302]
RewriteCond %{ENV:VISITOR_COUNTRY} ^US$
RewriteRule ^(.*)$ http://www.test-redirection.com/$1 [L,R=302]
```

9/ Cloner le système d'information sur un environnement distant (ou effectuer une migration)

Nous vous invitons à réclamer un accès SSH si vous souhaitez cloner le système d'information (fichiers et bases de données) de manière rigoureuse. Les accès FTPES ne permettent pas de garantir professionnellement l'intégrité du miroir réalisé et souvent, le timeout du front-end (ou des fronts-ends si reverse proxy) peuvent vous déranger pour créer un dump SQL via nos PHPMyAdmin sécurisés.

Nos chroots jails sont compliant avec les prérequis de Magento 2 - ils sont donc (très) permissifs et bien fournis en binaire (hors sudo/su et certains sbin pour honorer l'engagement contractuel relatif à la portabilité garantie du système non dépendante à une machine virtuelle/conteneur - donc hautement résistante à des corruptions majeures générées par un éventuel piratage). **Entre autres choses, les binaires rsync et mysqldump sont disponibles.**

Nous attirons votre attention sur le fait que notre méthode de sauvegarde multi-site est *très* consommatrice d'espace disque (100Mo de datas incompressibles = de 3,5Go à 7Go de datas sauvegardées), si d'un côté cela nous permet d'affirmer que notre engagement de préservation de données a toujours été honoré depuis plus de 10 ans, de l'autre, nous vous invitons à ne pas exploiter les productions de nos clients pour stocker des données dupliquées qui alourdissent inutilement le poids des sauvegardes.

NB : si vous utilisez un système de supervision de code source tel que Git - s'il vous plait - ne clonez pas les images OU demandez nous d'exclure des répertoires de la sauvegarde multi-site.

TOUCHWEB est là pour vous aider. Si vous rencontrez des difficultés, n'hésitez pas à nous envoyer un email sur contact at touchweb.fr ou à nous appeler au 09 70 44 42 84.

Chaque année, nous injectons 80 000€ à 150 000€ dans notre recherche et développement (R&D) pour vous proposer toujours plus de fonctionnalités et tenir à jour nos outils sur toujours plus de systèmes/daemons.

Si vous pensez qu'une fonctionnalité manque et/ou si vous pensez que l'on peut automatiser la détection/réparation d'un défaut pour vous aider, n'hésitez pas à nous en parler.

Les demandes ayant du sens et pouvant être mutualisées sur l'ensemble de la clientèle TW sont toujours prises en charge totalement gratuitement.

TOUCHWEB a une approche DEVOPS - nous ne sommes pas une infogérance conventionnelle. Nous travaillons main dans la main avec les pools DEV pour améliorer nos productivités mutuellement en bonne intelligence.

Dernière mise à jour : 27/02/2020

Changelog : https://www.touchweb.fr/aide