



Duplication à l'identique d'un blog WordPress censuré

Par [Sami Ben Gharbia](#), [Rebekah Heacock](#) et [Jeremy Clarke](#). - Traduit par [Anna Guève](#)

Ce guide s'adresse aux blogueurs utilisant le logiciel libre [WordPress](#) qui soupçonnent certains gouvernements de bloquer ou filtrer leur blog. Ce guide les aidera à utiliser un site dupliqué et ainsi rendre le contenu censuré lisible.

Pour les blogs sous  **WORDPRESS.ORG** seulement.



Pour accéder à des sites et blogs bloqués, la plupart de ceux qui défendent la liberté d'expression sur le web se concentrent sur la manière de contourner la censure en s'aidant d'outils.

Bien que cela soit important, apprendre aux utilisateurs d'internet la manière de contourner la censure ne suffit pas. La plupart des personnes ne connaissent pas ou n'ont pas accès à ces outils permettant de contourner la censure, car les pays qui filtrent internet ont également tendance à bloquer les serveurs proxy (providers) et autres technologies de contournement. L'utilisation des outils de contournement affecte souvent la vitesse de connexion, ce qui rend l'accès à internet encore plus difficile là où la connexion est déjà lente.

Une façon de faciliter l'accès des sites bloqués aux utilisateurs d'internet dans les pays qui filtrent le contenu en ligne se fait en recopiant les données à l'identique : dupliquer le contenu d'un site sur un autre nom de domaine ou sous-domaine. Les sites dupliqués recopient les données à l'identique, en temps réel, les changements apportés au site d'origine, permettant aux blogueurs de contourner la censure en fournissant plusieurs possibilités aux lecteurs d'accéder à leur contenu.

Ce guide est destiné aux blogs auto-hébergés et utilisant le logiciel de publication libre WordPress. Un blog auto-hébergé sur WordPress n'est pas hébergé sur le service gratuit de blogging WordPress.com, mais sur un serveur distinct qui utilise la plateforme de publication WordPress.org. Pour plus d'information, voir <http://wordpress.org/> qui s'adresse aux sites pouvant être bloqués par des filtres gouvernementaux. Son but est d'aider les blogueurs à utiliser une duplication à l'identique afin que les lecteurs aient quand même accès aux contenus censurés en dépit de ces filtres. Il contient des instructions étape-par-étape pour la mise en place d'une duplication à l'identique du blog (« source ») WordPress.

Table des matières

1. Copier votre contenu sans dupliquer à l'identique
2. Sécuriser votre blog
3. Introduction aux techniques de filtrages internet
4. Déterminer comment votre blog a été censuré
5. Duplication à l'identique de votre blog WordPress
 - a. Obtenir et configurer votre nouveau domaine et sous-domaine
 - b. Choisir, télécharger et installer un module d'extension (plugin) de duplication à l'identique WordPress
 - c. Configurer le module d'extension
 - d. S'occuper des risques pour votre référencement
 - e. Informer vos lecteurs de l'existence de blog dupliqué



1- Copier le contenu de votre site sans le dupliquer



Une façon simple de permettre à vos lecteurs d'avoir accès à votre site lorsqu'il est bloqué est d'en dupliquer le contenu sur d'autres sites. Même si les adresses URL ou IP de votre site sont bloquées, les services qui republient votre contenu peuvent être disponibles. Des outils comme [Google Reader](#), [FriendFeed](#), [Google Buzz](#), [Facebook](#) et autres [RSS readers](#) offrent plus de possibilités aux visiteurs d'accéder à votre site en republiant votre contenu en plusieurs endroits.

Pour pouvoir utiliser ces services, il vous faut publier en flux [RSS](#) ou [Atom](#). WordPress crée automatiquement ces flux de votre blog ; toutefois, si vous avez l'intention d'utiliser ces outils pour rendre accessibles les contenus censurés, soyez sûr :

- **D'inclure la totalité de votre contenu dans votre flux, et pas seulement les titres, les sous-titres et des extraits.** Sous WordPress, cela se fait dans Réglages > Lecture (Options de lecture). Sous « Pour chaque article, fournir » assurez-vous que «Le texte complet » est sélectionné.
- **De vérifiez que les fichiers multimédia incorporés dans le contenu du blog ne sont pas bloqués pour vos lecteurs.** Si les images / vidéos / audio incluses ou accessibles à partir de vos billets sont hébergées dans votre domaine, les lecteurs ne seront peut-être pas en mesure de les visionner, même s'ils peuvent lire vos flux RSS. Au lieu d'héberger vos contenus multimédia sur votre site censuré, essayez d'utiliser des sites de médias sociaux qui ne sont pas bloqués dans le pays que vous ciblez. Transférer vos contenus vers des sites comme [YouTube](#), [Flickr](#), [blip.tv](#), ou [archive.org](#). Faire un lien à partir de votre blog peut aussi les rendre accessibles aux visiteurs qui, autrement, ne pourraient voir que vos textes.



Vous devez vous assurer que les services que vous choisirez ne sont pas censurés dans le pays que vous ciblez. L'OpenNet Initiative a une [carte](#) actualisée qui montre les pays qui bloquent Facebook, Flickr et YouTube.



Avant de commencer le processus de duplication de votre blog pour contourner la censure, vous devez vous assurer que vous êtes bien visé par un gouvernement, que vous ne rencontrez pas des problèmes de sécurité n'ayant rien à avoir avec la politique. WordPress, en raison de sa popularité, est la cible d'une fervente armée de pirates-spammeurs créatifs qui s'introduisent dans les sites administrés sous WordPress pour y ajouter des liens spammeurs ou autres moyens illégaux et espion d'optimisation de moteurs de recherche (SEO) qui exploitent la popularité de votre site. Un des effets possibles de ces intrusions est que votre site peut être bloqué par un logiciel de filtrage ou même Google pour contenir un contenu inapproprié (mis sur votre site par les pirates) ou pour alimenter en logiciels malveillants / espions les visiteurs, une autre stratégie courante des pirates qui s'emparent des sites WordPress.

Veiller à ce que votre site soit sécurisé et sous votre contrôle total, quel qu'en soit la raison, mais si vous pensez que vous êtes censuré, le fait d'examiner la sécurité peut donner des indices orientant vers un problème plus terre à terre. Si vous découvrez que votre site a été infecté et que vous êtes en mesure de régler le problème, alors vous pouvez faire réintégrer votre site dans Google ou faire retirer des filtres commerciaux en demandant que votre site soit passé en revue (voir plus bas).

De même, si vous pensez que vous pouvez être censuré, avoir un site particulièrement sécurisé est une bonne idée, car il permettra de le protéger ainsi que vos informations personnelles contre les tentatives malveillantes de piratage politique.

Le Codex WordPress donne des conseils sur la manière de consolider WordPress pour le rendre plus sécurisé. [Ce qu'il faut faire si vous pensez que votre site a été piraté](#) et [la manière de consolider WordPress pour le rendre moins vulnérable](#). Les objectifs fondamentaux sont de s'assurer que nul ne vienne sur votre site de façon anonyme et que les seuls fichiers présents sur votre serveur sont ceux qui doivent y être. Les pirates téléchargent de nouveaux fichiers et les utilisent pour vous re-pirater si vous êtes hors-ligne. Ils ajoutent également du contenu à votre base de données et cachent des utilisateurs pour que vous ne puissiez pas les trouver.

La meilleure façon de vérifier votre site est d'utiliser certains des [nombreux plugins \(modules d'extension\) de sécurité WordPress](#) qui existent à cet effet. Voici une petite liste de quelques-uns des meilleurs d'entre eux (vous n'avez pas besoin de les installer tous, mais regarder ce qu'ils offrent est utile) :



Liste de plugins pour mieux sécuriser votre blog Wordpress

- ★ [WP Security Scan](#) : Scanne votre installation WordPress pour rechercher les failles au niveau de la sécurité et suggère des actions pour les prévenir.
- ★ [WordPress Firewall Plugin](#) : Recherche les requêtes Web avec de simples historiques spécifiques à WordPress pour identifier et arrêter les attaques les plus évidentes.
- ★ [WordPress File Monitor](#) : Surveille sur votre installation WordPress les fichiers ajoutés / supprimés / changés. Lorsqu'un changement est détecté une alerte e-mail peut être envoyée à une adresse spécifiée au préalable.
- ★ [WordPress Database Backup](#) : Crée des sauvegardes de votre base de données, y compris de celles qui sont automatiques et régulières. Cela est particulièrement important parce que si vous êtes piraté vous aurez besoin d'une base de données sauvegardée dont vous savez qu'aucun contenu malveillant n'y aurait été ajouté.
- ★ [Secure WordPress](#) : Aide à sécuriser votre installation WordPress : supprime les informations d'erreur sur la page de connexion, ajoute un index.html au répertoire du plugin (module d'extension), supprime le fichier wp-version, sauf dans la zone « administrateur ».
- ★ [Maximum Security for WordPress](#): Protège des intrusions, détecte pléthore d'incidents, bloque les contenus malveillants qui pourraient nuire à vos lecteurs et à votre référencement sur les moteurs de recherche et comprend un pare-feu web puissant incluant un système complet de prévention d'intrusion.
- ★ [Login LockDown WordPress Security](#) : Enregistre l'adresse IP et l'horodatage de chaque tentative de connexion WordPress ayant échoué. Si plus d'un certain nombre de tentatives sont détectées dans un laps de temps court depuis la même adresse IP, alors la fonction de connexion est désactivée pour toutes les demandes suivantes de cette adresse.
- ★ [ChapSecureLogin](#) : Vous pouvez utiliser ce plugin (module d'extension) pour le cryptage de votre mot de passe. Le processus de cryptage est créé par le protocole CHAP, ce qui est particulièrement utile lorsque vous ne pouvez pas utiliser SSL (TSL) ou tout autre type de protocole de sécurisation.
- ★ [Theme Authenticity Checker](#) : TAC recherche les fichiers source de tous les thèmes installés pour des signes de codes malveillants. S'il y trouve un code malveillant, TAC dévoile le chemin vers le fichier du thème, le numéro de ligne et un petit extrait du code suspect.



L'[OpenNet Initiative](#) un centre de recherches de l'Université de Harvard, définit le [filtrage d'internet](#) comme des « approches techniques pour contrôler l'accès à l'information sur internet. ». Le filtrage du web n'est qu'une partie de la censure du web, qui comprend également des tactiques telles que [menacer les](#) blogueurs et retirer des sites gênants du web en envoyant des avis de fermeture ou de radiation des noms de domaine. Dans ce guide, nous nous concentrerons sur les diverses modalités techniques du filtrage du web, qui peut être divisé en quatre grandes approches.

Filtrage de l'annuaire des domaines

La façon la plus commune de censurer un site web est de bloquer l'accès à son nom de domaine dans toute une région, par exemple en interdisant tout accès à monblog.com. Dans ces cas les sites bloqués sont souvent accessibles avec d'autres noms de domaine ou sous-domaine desdits sites : si monblog.com est bloqué, blog.monblog.com peut toujours être accessible.

Filtrage de l'adresse universelle/adresse réticulaire (URL)

Une autre méthode courante consiste à bloquer l'accès à des informations spécifiques (des pages ou des billets) sur un site web ou un blog en empêchant l'accès à certaines URL. Ce blocage sélectif ne cible que des sous-domaines ou des pages spécifiques sans affecter le reste du site. Par exemple, un censeur peut filtrer le sous-domaine [advocacy.globalvoicesonline.org](#) tout en laissant le site général [globalvoicesonline.org](#) non filtré, ou vice versa.

Filtrage de l'adresse IP

Bloquer les [adresses IP](#) des serveurs hébergeant les sites web indésirables est la forme la plus simple de la censure du net. L'adresse IP est le numéro utilisé pour identifier de manière unique chaque ordinateur sur internet, donc bloquer l'adresse IP d'une machine la rend inaccessible. Bien que le filtrage d'IP soit le moyen le plus simple et le moins cher d'interdire les contenus non désirés, il peut facilement conduire à trop censurer une large gamme de sites. Si une adresse IP associée à un site web particulier est bloquée, tous les autres sites qui partagent la même adresse IP sur le serveur le sont également.

Filtrage de mots-clés

Certains pays, comme la Chine et la Tunisie, bloquent l'accès à tout URL contenant un mot-clé spécifique. Par exemple, la Tunisie bloque le domaine [nawaat.org](#) ainsi que le mot-clé « nawaat » dans toutes les adresses universelles (URL). Cela signifie que le compte Twitter [@Nawaat](#) (<http://twitter.com/nawaat>) est automatiquement bloqué, comme le compte Facebook de Nawaat ainsi que tous les caches Google et les pages de résultats de recherches qui contiennent « nawaat » dans leurs URL.



4- Déterminer si et comment votre site est bloqué



Si vous pouvez identifier quelles techniques sont utilisées pour censurer votre blog, vous pouvez déterminer la meilleure façon de le rendre à nouveau accessible aux utilisateurs bloqués. Un bon début est de vérifier la [description du pays](#) de l'OpenNet Initiative pour avoir une idée sur les méthodes de filtrage utilisées là où vous pensez que votre blog est bloqué.

Déterminer si votre site est bloqué est une partie importante de ce processus. Il est possible que des problèmes de connectivité, de configuration, ou même de sécurité, plutôt que la censure, soient ce qui rend le site inaccessible aux lecteurs. Pour bien déterminer la nature du filtrage ou blocage de votre site, vous aurez besoin de communiquer avec les personnes concernées et de leur demander de vous aider à tester la situation. Établir des liens avec un groupe de testeurs est susceptible de se révéler utile. Si vous voulez soustraire les tests, vous pouvez consulter [Herdict](#), un site qui, en vous localisant, accède à votre blog et crée une carte des endroits où vous êtes probablement bloqué.

Outils de censure

Certains pays utilisent des logiciels de filtrage (outils de censure), tels que Websense ou SmartFilter, qui bloquent l'accès à des sites selon leur indexation comme « nuisible », « jeu », « spam », etc. Si vous pensez que votre site est bloqué parce qu'il a été signalé comme dangereux ou spam (voyez le paragraphe sur la sécurité ci-dessus), vous pouvez utiliser l'outil de diagnostic Google de navigation sécurisée (allez voir sur <http://www.google.com/safebrowsing/diagnostic?site=> [votre URL, comme <http://globalvoicesonline.org.>]) ou celui de McAfee [SiteAdvisor](#) pour vérifier ce qu'il en est. Ce verrouillage peut résulter d'un site peu sûr devenu source de logiciels malveillants parce que piraté. Si vous avez résolu le problème de sécurité, que votre blog a été signalé par erreur, [contactez Google pour faire réexaminer votre site](#).

Blocage de l'IP

La première étape pour déterminer si votre adresse IP est bloquée est de connaître votre adresse IP. Vous pouvez utiliser l'outil [IP Lookup: Domain](#) pour trouver quelle adresse IP correspond avec le nom de domaine de votre blog. L'étape suivante consiste à vérifier si cette adresse IP est bloquée.

Il est possible que l'adresse IP de votre site soit bloquée non pas à cause de votre contenu, mais parce qu'un autre site avec la même adresse IP sur l'hébergeur commun a été bloqué. Pour voir quels sites ont une même adresse IP, vous pouvez effectuer une [recherche inversée d'IP](#). Si vous pensez que votre site est bloqué par erreur parce qu'il partage son adresse IP, vous pouvez contacter votre service d'hébergement et leur demander de la changer (par exemple, en le déplaçant vers un autre serveur ou groupe). Il se peut que vous ayez à acheter une adresse IP pour ce faire, ce qui peut être cher. Une autre solution, peu pratique, pour le filtrage IP, serait de déplacer entièrement votre site vers un nouvel hôte, ce qui vous procurerait une nouvelle adresse IP.

Filtrage de mot-clé

Si votre blog est victime de filtrage par mot-clé, vous devrez acheter un autre nom de domaine. Vous devez également éviter d'utiliser ce mot-clé dans le nom de votre blog, les titres de vos billets et pages, vos citations et catégories, vos images et vos fichiers multimédia. Comme expliqué ci-dessus, le filtrage de mot-clé cible un mot spécifique, et la solution ultime est d'éviter l'utilisation de ce mot dans toutes vos adresses URL.

Le filtrage de mot-clé est particulièrement difficile à traiter, puisque vous aurez besoin de changer toutes les URL de votre site pour éviter d'utiliser le mot bloqué. Dans le processus, vous perdrez des liens entrants, pingbacks et des liens provenant de moteurs de recherche et des agrégateurs courants. Vous pouvez essayer d'utiliser le [plugin Permalink Migration WordPress](#), qui vous permettra de changer vos URL sans affecter vos référencement dans les moteurs de recherche ou rompre des liens préexistants sur votre site.



La duplication est le processus qui consiste à avoir deux ou plusieurs noms de domaine ou sous-domaine contenant les mêmes mises à jour de données. Dans ce guide, nous montrerons la duplication synchronisée d'un blog auto-hébergé sur WordPress. Dans la duplication synchronisée, les données sont mises à jour dans les deux sens, en gardant les deux ou plusieurs blogs en synchronisation en utilisant les mêmes installations WordPress et base de données. Lorsque vous ajoutez, modifiez ou supprimez tout type de contenu (billets, pages, commentaires, images, etc.) du blog « principal » sur son domaine normal ou dans le(s) blog(s) « cibles » sur le(s) domaine(s) dupliqué(s), le même contenu sera ajouté, modifié ou supprimé dans les autres blogs.

Malheureusement, dupliquer votre blog n'est pas une solution définitive ou permanente face à la censure. Dans la plupart des cas, les censeurs découvriront votre blog dupliqué dans un temps plus ou moins long et le bloqueront à nouveau. S'ils surveillent très étroitement vos activités en ligne, il leur sera très facile de bloquer tous vos blogs dupliqués. Rappelez-vous que la censure est un jeu du chat et de la souris et que la technique de duplication expliquée ici n'est peut être pas la solution idéale pour vous. Il vous aidera seulement à exploiter la brèche dans le mur de la censure en rendant votre contenu disponible pour un certain laps de temps, dont la durée dépend de la vigilance des censeurs.

Toutefois, les plugins (modules d'extension) de duplication présentés dans ce guide vous permettront de créer et de gérer autant de blogs dupliqués que vous le souhaitez. Il vous sera ainsi plus facile de garder une longueur d'avance sur la censure en étant prêt à dupliquer votre contenu autant de fois que nécessaire. Même si votre blog n'est pas encore censuré, le dupliquer peut servir comme une solution de repli en cas de censure et de sauvegarde.

Pour dupliquer votre blog, il vous faut suivre les étapes suivantes :

- a. Obtenir et configurer un nouveau domaine ou sous-domaine
- b. Choisir, télécharger et installer un plugin (module d'extension) de duplication WordPress
- c. Configurer le plugin (module d'extension)
- d. Soustraire votre blog dupliqué des recherches Google
- e. Faire connaître votre site dupliqué à vos lecteurs



Afin de dupliquer votre blog sur une autre URL, la première chose dont vous avez besoin est une URL de substitution. Il peut s'agir d'un sous-domaine du site que vous avez déjà (i.e. dupliquer.monblog.com) ou un domaine entièrement nouveau (dupliquermonblog.com). Savoir ce qui est mieux pour vous est complexe et dépend de la nature exacte de la censure / du filtrage qui bloque votre site.

Rappelez-vous que si vous êtes bloqué au niveau de l'adresse IP, un site miroir hébergé sur le même serveur, quel que soit son domaine, sera également bloqué. Voir la section sur le filtrage des adresses IP ci-dessus pour obtenir des conseils sur la façon de traiter ce cas.

Utiliser un sous-domaine (i.e. dupliquer.monblog.com)

Parfois, un sous-domaine de l'URL habituelle de votre site passe par des filtres qui bloquent votre site principal, certainement parce que le filtre cible seulement votre URL exacte (« <http://monblog.com> » plutôt que « monblog.com » ou « monblog »). Dans ce cas, dupliquer en utilisant un sous-domaine, est le choix idéal. Il sera familier aux lecteurs existants, nécessitera moins de configuration et, dans la plupart des cas, n'entraînera pas de frais supplémentaires auprès de votre hébergeur.

La plupart des hébergeurs vous permettent d'ajouter et de configurer les sous-domaines à partir du panneau de contrôle de votre compte. Lisez le mode d'emploi de votre hébergeur ou demandez lui de l'aide si vous n'êtes pas sûr de savoir comment le faire.

Tester si un sous-domaine permettra aux utilisateurs bloqués d'accéder à votre site est assez facile :

- Créez un sous-domaine de test auprès de votre hébergeur et redirigez-le vers un répertoire vide du serveur.
- Téléchargez une simple page index.html contenant un message de test.
- Demandez à un utilisateur bloqué sur votre site principal d'y aller.

Si la page test n'est pas bloquée pour la personne qui ne peut accéder à votre blog principal, alors un site dupliqué fonctionnera certainement dans un sous-domaine. Sinon, un nouveau nom de domaine peut s'avérer nécessaire.

Enregistrer un nouveau nom de domaine

Il faut un domaine complètement nouveau si le filtrage se fait par domaines nuancés ou par mots-clés. Dans ces deux cas, les sous-domaines seront bloqués en même temps que le site principal, et même de nouveaux domaines contenant les mots-clés bloqués pourront être

inaccessibles. Vous devrez particulièrement faire attention au choix de votre nouveau domaine :

- Il faut payer pour enregistrer des noms de domaine.
- Si vous êtes censuré par mot-clé, vous aurez besoin d'un domaine qui ne contienne pas ce mot-clé.
- Dans l'idéal, ce domaine devrait être caractéristique et évocateur aux lecteurs existants et aux nouveaux.

De nouveaux domaines peuvent être enregistrés, soit auprès de votre d'hébergeur ou par des sociétés que ne font que cela, telle [GoDaddy](#). Si votre hébergeur propose l'enregistrement de domaine, il vaut mieux utiliser ses services, car cela simplifie pour vous le processus de configuration du domaine comme il gèrera les paramètres DNS pour vous.



Beaucoup d'hébergeurs pratiquent des tarifs exorbitants pour enregistrer de nouveaux domaines par rapport aux sociétés comme GoDaddy qui ne font que cela (un domaine .com/.net/.org coûte environ 10\$ US / par an), de sorte que le travail supplémentaire consistant à soumettre un nouveau domaine avec DNS (annuaire des domaines) à votre hébergeur peut valoir la peine à long terme .Vous devez comparer les prix de votre hébergeur avec ceux des concurrents avant de décider.


Une fois un nouveau domaine est enregistré, il faut entre 12 et 72 heures pour qu'il soit actif parce que les paramètres DNS (annuaire des domaines) se propagent lentement à travers l'internet. En attendant, vous devez vous préparer pour des tâches ci-dessous. Vous pourrez continuer lorsque votre navigateur peut aller sur le domaine que vous avez créé et voir la page de destination que votre hébergeur vous a créée.

Configuration de DNS (annuaire des domaines)

L'étape suivante consiste à vous connecter à la page d'accueil de votre interface web (dans les exemples qui suivent nous avons utilisé l'hébergeur DreamHost) et à sélectionner *Domains > Manage Domains*. Votre domaine principal (celui qui est bloqué) doit être entièrement hébergé. Pour le domaine ou sous-domaine que vous souhaitez définir comme duplicata, cliquez sur le bouton « *edit* » (modifier). Sur l'écran d'édition, vous verrez plusieurs options. Par exemple, DreamHost offre cinq options :

6. *Fully Hosted* (entièrement hébergé) ;
7. *Redirected* (redirigé) ;
8. *Mirrored* (dupliqué);
9. *Parked* (stationné) ;
10. *Cloaked* (dissimulé).

Sélectionnez l'option « *Mirrored* » (duplicué), et définissez le domaine à dupliquer (dupliquermonblog.com) pour utiliser votre nom de domaine entièrement hébergé (monblogbloqué.com) :

 **Mirrored**
(Use the same files from a fully hosted site you have at DreamHost, but display them at a different address.)

Create the mirror at:
sub-domains are okay!

Mirror this site: ↕

[Change settings](#)

Modification de l'hébergeur virtuel

Si vous n'utilisez pas DreamHost comme hébergeur, demandez l'aide de votre hébergeur sur la façon de configurer les hébergeurs virtuels et modifier les paramètres DNS (annuaire des domaines). Normalement, vous n'aurez qu'à diriger vers votre nouveau domaine ou sous-domaine (exemple : 4.fartattou.com) dans le répertoire racine de votre blog principal (exemple : /kitab.nl) :

* Edit Virtual Host

Subdomain

Link to path *2



b. Choisir, télécharger et installer un plugin de duplication



Choisir un plugin (module d'extension)

Plusieurs plugins (modules d'extension) WordPress existent pour vous aider à dupliquer. Nous vous recommandons d'utiliser une des options suivantes :

- [Domain Mirror Plugin](#) par David McAleavy
- [Domain Theme](#) par Stephen Carroll

Les deux plugins (modules d'extension) permettent à une seule installation WordPress d'afficher différents URLs (adresses universelles), titres de blog et domaines. Ils vous permettent également d'associer des thèmes et des domaines différents, ce qui signifie que vous pouvez utiliser un style de thème Web 2.0 dynamique pour votre blog principal et un thème minimaliste pour le blog dupliqué qui accélère les temps de chargement et minimise l'utilisation de la bande passante. Les [thèmes Wordpress minimalistes](#) sont recommandés pour les blogs censurés. Des temps rapides de chargement de pages sont cruciaux pour les



Ce guide contient des instructions pour configurer le plugin du domaine dupliqué. Pour des instructions sur l'utilisation du thème du plugin du domaine, allez sur le site de [Stephen Carroll](#).

visiteurs voulant accéder à des blogs bloqués en passant par des copies, ainsi que pour ceux qui vivent dans des endroits à connexion lente.

Télécharger et installer le plugin (module d'extension)

[Télécharger le plugin \(module d'extension\) du domaine dupliqué](#), décompressez-le et téléchargez-le sur le dossier wp-content/plugins / via FTP (protocole de transfert de fichiers). Vous pouvez également installer le plugin directement depuis le tableau de bord en allant à WordPress Plugins > « Add New » (Ajouter) et cherchez le nom du plugin. Après l'avoir trouvé, cliquez sur « Install » (Installer), lien à droite du résultat des recherches :

Name	Version	Rating	Description	Actions
Domain Mirror	1.1	★★★★★	If you have more than one domain and want to point both of them at the same Wordpress installation, you'll find that it doesn't really work very well. Wordpress creates its own internal URLs based on the settings in General Options. This Plugin allows multiple domains to be configured within Wordpress and updates the Weblog Title, Wordpress Address URL and Blog Address URL on-the-fly based on the ... By Dave McAleavy.	Install



Si vous décidez d'installer le plugin du [domaine dupliqué](#) en passant par l'interface de l'administrateur WordPress, vous devrez renommer le répertoire téléchargé « domaine-dupliqué » : « AA-DomainDupliqué » afin que ce plugin se télécharge d'abord, ce qui empêchera les problèmes de compatibilité avec d'autres plugins. Pour ce faire vous aurez besoin d'un accès FTP (protocole de transfert de fichiers) au répertoire des plugins.

Avant

plugins

Name	Date	Owner	Kind	Permissions	
akismet	1/15/10	nawaato	Folder	drwxr-xr-x	
bad-behavior	1/15/10	nawaato	Folder	drwxr-xr-x	
breadcrumbs	2/10/10	nawaato	Folder	drwxr-xr-x	
category-icons	2/10/10	nawaato	Folder	drwxr-xr-x	
customizable-c...ent-listings.php	12/22/09	nawaato	BBEd...ent	-rw-r--r--	2
disable-wordpress-core-update	1/15/10	nawaato	Folder	drwxr-xr-x	
disable-wordpress-plugin-updates	1/15/10	nawaato	Folder	drwxr-xr-x	
domain-mirror	Today	nawaato	Folder	drwxr-xr-x	
excerpt-editor	1/15/10	nawaato	Folder	drwxr-xr-x	
extended-comment-options	1/15/10	nawaato	Folder	drwxr-xr-x	
flickr-rss	2/10/10	nawaato	Folder	drwxr-xr-x	

Après

plugins

Name	Date	Owner	Kind	Permissions	
AA-DomainMirror	Today	nawaato	Folder	drwxr-xr-x	
akismet	1/15/10	nawaato	Folder	drwxr-xr-x	
bad-behavior	1/15/10	nawaato	Folder	drwxr-xr-x	
breadcrumbs	2/10/10	nawaato	Folder	drwxr-xr-x	
category-icons	2/10/10	nawaato	Folder	drwxr-xr-x	
customizable-c...ent-listings.php	12/22/09	nawaato	BBEd...ent	-rw-r--r--	2
disable-wordpress-core-update	1/15/10	nawaato	Folder	drwxr-xr-x	
disable-wordpress-plugin-updates	1/15/10	nawaato	Folder	drwxr-xr-x	
excerpt-editor	1/15/10	nawaato	Folder	drwxr-xr-x	
extended-comment-options	1/15/10	nawaato	Folder	drwxr-xr-x	
flickr-rss	2/10/10	nawaato	Folder	drwxr-xr-x	



c. Configurer le plugin du domaine dupliqué



Sur votre interface d'administration WordPress, allez sur l'onglet Plugins et activez le plugin que vous avez installé. Puis, allez sur l'onglet Réglages > Domain Mirror (tableau de bord> Paramètres> domaine dupliqué) et remplir les informations appropriées pour vos noms de domaine.

La section #1 du domaine doit contenir les informations de base de votre blog principal. Cliquez sur « *Get Current domain* » (obtenir le domaine actuel) pour obtenir les valeurs de la base de données enregistrées dans vos paramètres généraux WordPress. La section #2 du domaine doit contenir les détails du domaine dupliqué. Après l'ajout de cette information, cliquez « *Save Changes* » (Enregistrer les modifications). Vous pouvez ajouter autant de domaines dupliqués que vous le souhaitez en cliquant sur le bouton « *Add New Domain* » (Ajouter un nouveau domaine).

Domains

Domain #1

Domain: X

Weblog title: X [dmBlogTitle]

Tagline: X [dmTagLine]

Wordpress address (URL): X [dmWpAddr]

Blog address (URL): X [dmBlogAddr]

Clear all: X

Delete Domain

Get Current Domain

Domain #2

Domain: X

Weblog title: X [dmBlogTitle]

Tagline: X [dmTagLine]

Wordpress address (URL): X [dmWpAddr]

Blog address (URL): X [dmBlogAddr]

Clear all: X

Delete Domain

Get Current Domain

Si vous avez suivi les étapes ci-dessus, vous avez maintenant deux copies de votre blog. Lorsque vous allez sur votre domaine principal, votre blog reste inchangé. Lorsque vous allez sur votre site dupliqué, le blog apparaît comme s'il avait été configuré pour ce domaine. Vous pouvez voir un exemple du blog collectif tunisien qui utilise cette technique : le blog principal est sur nawaat.org et le blog dupliqué sur twitter.nawaat.org. Vous remarquerez que le blog principal (à droite) a un thème complexe, tandis que le blog dupliqué (à gauche) utilise un thème minimaliste pour assurer un temps rapide de chargement des pages.





Les censeurs, comme les utilisateurs réguliers d'internet, utilisent souvent Google et autres moteurs de recherche pour trouver du contenu en ligne. Si votre site dupliqué est référencé sur Google, la censure pourra le trouver et le bloquer très vite. Pour que cela n'arrive pas, vous pouvez empêcher les robots de recherche Google et autres d'indexer vos blogs dupliqués. Cela peut également rendre plus difficile aux nouveaux lecteurs l'accès à votre blog. Pour cette raison, nous vous recommandons de faire connaître votre blog dupliqué par Twitter, mails, Facebook, Google Buzz et autres outils de médias sociaux.

Vous pouvez empêcher Google d'indexer votre blog dupliqué en créant ou modifiant un protocole d'exclusion de robots (également connu sous le nom robot.txt). Ce fichier indique aux moteurs de recherche où et quand ne pas regarder le contenu de votre serveur et empêchera l'indexation de votre domaine dupliqué, ce qui réduit le risque que la censure trouve votre blog dupliqué.

Si un fichier robots.txt n'existe pas dans le dossier qui contient le contenu de votre site dupliqué, vous devez en créer un. Vous pouvez pour cela utiliser n'importe quel logiciel d'édition de texte (Notepad ou Wordpad pour Windows, TextEdit sous Mac OS, Vi ou Emacs pour Linux). Une fois que vous avez créé le fichier (ou après avoir ouvert le fichier existant), ajoutez le texte suivant :

```
# Disallow Googlebot
User-agent: Googlebot
Disallow: /

User-agent: *
Disallow: /
```

Enregistrez le fichier sous robot.txt et transférez-le à votre dossier dupliqué. Veillez à ne pas mettre le fichier dans le dossier qui contient votre blog principal, car vous empêcheriez les moteurs de recherche d'indexer tout votre site.

Faire connaître votre site dupliqué à vos lecteurs

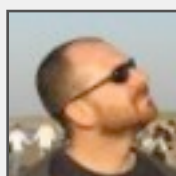
Après la mise en place du domaine dupliqué de votre blog, l'étape suivante est d'informer les lecteurs du nouveau lien. Il y a plusieurs façons de le faire :

- Ajouter un avis sur l'en-tête de votre flux RSS informant vos abonnés RSS de la duplication. Stylisez l'avis grâce aux feuilles de style en cascade (CSS) afin qu'il soit visible. Vous pouvez utiliser le module d'extension [RSS plugin](#) pour ajouter et styliser l'avis.

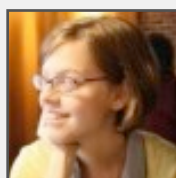
- Si vous avez une liste d'adresse[s] courriels, envoyez le nouveau lien à vos abonnés.
- Si vous utilisez [TwitterFeed](#) pour publier automatiquement les mises à jour de votre blog sur Twitter, assurez-vous de changer le lien du flux RSS du blog au fil RSS de votre site dupliqué. Cela fera en sorte que tous les liens publiés sur Twitter dirigent vers le blog dupliqué et pas vers le blog principal. Voir notre guide [Cross-Posting for Advocacy](#) pour des conseils sur l'utilisation de cette technique
- Si vous avez un compte Facebook, vous pouvez facilement importer votre blog dupliqué. Vous pouvez utiliser le plugin [WPBOOK](#) qui ajoutera votre blog WordPress comme application Facebook. Assurez-vous d'utiliser l'URL du blog dupliqué.



À propos des auteurs



Sami Ben Gharbia: blogueur et militant tunisien basé aux Pays-Bas. Sami dirige [Global Voices Advocacy](#) et a eu l'idée du projet de cartographie [Threatened Voices](#) (Voix menacées). Il a également cofondé [nawaat.org](#) (un blog politique tunisien blog collectif), [cybversion.org](#) (un blog qui suit la censure du web en Tunisie), [babtounes](#) (un agrégateur des tweets sur la Tunisie basé sur WordPress) et de nombreux autres projets numériques militants.



Rebekah Heacock: est assistante de recherches de l'[OpenNet](#) OpenNet Initiative au [Berkman Center for Internet and Society](#) de l'université d'Harvard. Elle publie des articles sur la technologie, l'aide au développement, les transports en commun d'Afrique de l'Est sur [Jackfruity](#). Elle fait également de la recherche technologique pour le réseau Global Voices [Technology for Transparency Network](#).



Jeremy Clarke: de Montréal, se définit comme "hacker" spécialiste en PHP, HTML, CSS et WordPress. Il a conçu et développé les sites de [Global Voices](#) tout en participant à des logiciels open-source comme [wordpress](#). Son blog personnel s'appelle [SimianUprising.com](#). Pour en savoir plus sur la manière dont Global Voices a été conçu aller sur notre page [Design and Tech](#). Vous pouvez voir l'introduction sur la thématisation WordPress que Jeremy a faite sur [wordpress.tv](#).



Ce guide est publié sous une licence [Creative Commons](#)