Admins - Demande #3067

Normaliser la conf nginx de bastion

05/04/2018 13:07 - Quentin Gibeaux

Statut:	Fermé	**Début:**	05/04/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	Christian P. Momon	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Mai 2019	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Il semblerait que les configurations nginx de bastion ne soit pas toutes bien écrites. Étudier la conf dans son ensemble et voir pour normaliser/nettoyer.
Notamment photos.april.org

Historique

#1 - 05/04/2018 13:18 - Quentin Gibeaux

- Description mis à jour

#2 - 05/04/2018 13:32 - Christian P. Momon

- Statut changé de Nouveau à En cours de traitement

#3 - 05/04/2018 13:58 - François Poulain

Ça veut dire quoi, « pas bien écrites » ?

#4 - 05/04/2018 14:23 - Christian P. Momon

En fait, lors de la migration du site photos.april.org, j'ai eu des incompréhensions multiples sur le fichier de conf nginx de photos.april.org sur la VM bastion :
1) plusieurs listen 80 pour le même service_name (en fait, y a un « photo » et un « photos », je viens de le voir…) ;
2) pas de conf https forcée (alors que sur certains navigateurs, ça fonctionne) ;
3) pourquoi pas de include /etc/nginx/hsts.conf; ? (comme dans candidats.fr, www.april.org, etc.) ;
4) pourquoi location /register.php ?
5) pourquoi location /identification.php ?
6) le servername photo a pour fichiers de log photos* donc indistinguables ;
7) usage rewrite sans rewrite ON ;
8) …

#5 - 05/04/2018 14:46 - François Poulain

Christian P. Momon a écrit :

> En fait, lors de la migration du site photos.april.org, j'ai eu des incompréhensions multiples sur le fichier de conf nginx de photos.april.org sur la VM bastion :
> 1) plusieurs listen 80 pour le même service_name (en fait, y a un « photo » et un « photos », je viens de le voir…) ;

Ok beh comme tu vois c'est pas injustifié. Même si ça pourrait être fait avec moins de duplication.

> 2) pas de conf https forcée (alors que sur certains navigateurs, ça fonctionne) ;

Oui car historiquement je trouve peu utile de forcer le https sur du contenu public. Le jour où let's encrpyt tombera on va rigoler avec https et hsts mis partout pour juste « le plaisir » (c'est pas une éventualité folle; le coup du challenge https-sni m'a fait un peu suer...).

> 3) pourquoi pas de include /etc/nginx/hsts.conf; ? (comme dans candidats.fr, www.april.org, etc.) ;

À demander aux gens qui ont déployé hsts. :)

> 4) pourquoi location /register.php ?
> 5) pourquoi location /identification.php ?

Pour forcer le https au niveau des pages de connexion. C'est le pendant logique de 2).

> 6) le servername photo a pour fichiers de log photos* donc indistinguables ;

Il n'y a aucun besoin de les distinguer. L'existence de photo.april et photos.april est juste pour gérer l'ambiguité.

> 7) usage rewrite sans rewrite ON ;

Tu as une page de doc qui décrit ça ?

Du coup, je ne dis pas qu'il ne faut pas uniformiser, mais attention certains paramètres sont choisi à dessin et ne sont pas tous des accidents de parcours. Du coup, avant de changer il faut veiller un peu à ce que les changements soient compris et leur influence monitorée.

Sinon, blague à part, attention dans les changements de conf : nginx est un bijou mais il n'est pas dénué de blagues, cf par ex https://agir.april.org/issues/1840#note-7 .

#6 - 03/05/2018 09:48 - Quentin Gibeaux

- Version cible changé de Avril 2018 à Mai 2018

Poursuite sur le mois de mai

#7 - 13/05/2018 10:36 - Christian P. Momon

François Poulain a écrit :

> Christian P. Momon a écrit :
>
> > En fait, lors de la migration du site photos.april.org, j'ai eu des incompréhensions multiples sur le fichier de conf nginx de photos.april.org sur la VM bastion :
> > 1) plusieurs listen 80 pour le même service_name (en fait, y a un « photo » et un « photos », je viens de le voir…) ;
>
> Ok beh comme tu vois c'est pas injustifié.

J'avoue :)

> Même si ça pourrait être fait avec moins de duplication.

Dans ce cas précis, je suis pour plus de duplication. Le fait de mélanger dans un même fichier la configuration de plusieurs site web, brrrr, ça concourt à rendre moins visible, moins lisible (voire invisible dans mon cas ;*>).

> > 2) pas de conf https forcée (alors que sur certains navigateurs, ça fonctionne) ;
>
> Oui car historiquement je trouve peu utile de forcer le https sur du contenu public.

Pour « chiffrer du contenu public », ok. Mais que fais-tu des données personnelles de navigations (telle page vue à telle heure depuis tel endroit par untel) ?

Le fait est qu'en retournant une page non chiffrée, nous permettons à certains tiers de récupérer des données de navigation d'un utilisateur. Quelque part, cela fait de nous les complices du traçage des webonautes.

En HTTPS, certes, les trackeurs sauront qu'un certain visiteur est venu sur le site, mais il ne saura pas quels albums il a consulté ni quelles photos en particulier l'ont intéressé. C'est déjà beaucoup.

Au nom d'un « droit à l'intimité numérique », ne devons-nous pas considérer que nous avons le devoir de chiffrer même du contenu public ?

> > 4) pourquoi location /register.php ?
> > 5) pourquoi location /identification.php ?
>
> Pour forcer le https au niveau des pages de connexion. C'est le pendant logique de 2).

Effectivement.

> > 6) le servername photo a pour fichiers de log photos* donc indistinguables ;

> Il n'y a aucun besoin de les distinguer. L'existence de photo.april et photos.april est juste pour gérer l'ambiguité.

Besoin de distinguer ? J'aurai formuler dans l'autre sens : quel besoin de les mélanger ? Car, par défaut, le besoin est de suivre/coller à la nature de ce que l'on fait (deux sites web). De plus, ici, impossible de répondre à la question : photo.april.org est-il utile ? Combien de fois par an est-il utilisé ? En cas de debuggage, impossible de suivre le flux exacte des choses.

Bon, d'un autre côté, je reconnais que ces questions ne sont pas posées depuis des années…

> 7) usage rewrite sans rewrite ON ;

> Tu as une page de doc qui décrit ça ?

Ha ok, nous sommes dans nginx et non Apache2, donc pas besoin de directive « Rewrite ON »…

> Du coup, je ne dis pas qu'il ne faut pas uniformiser, mais attention certains paramètres sont choisi à dessin
> et ne sont pas tous des accidents de parcours. Du coup, avant de changer
> il faut veiller un peu à ce que les changements soient compris et leur influence monitorée.

J'approuve totalement. D'où ma démarche et ce ticket. Si l'intitulé du ticket est très ambitieux (le SM a de l'élan :*>), son origine est plus modeste : lors de la migration de la VM photos, j'ai constaté des incompréhensions de ma part et certaines différences dans les configurations. Donc je me proposais de mieux comprendre l'existant et potentiellement d'harmoniser un ou deux trucs au passage en mode jardinage.

Donc, pas de volonté de tout changer juste pour changer, ouf ;)

> Sinon, blague à part, attention dans les changements de conf : nginx est un bijou mais il n'est pas dénué de blagues, cf par ex https://agir.april.org/issues/1840#note-7 .

Hola, oui, en effet, merci \o/

#8 - 14/05/2018 09:22 - François Poulain

> Même si ça pourrait être fait avec moins de duplication.

> Dans ce cas précis, je suis pour plus de duplication. Le fait de mélanger dans un même fichier la configuration de plusieurs site web, brrrr, ça concourt à rendre moins visible, moins lisible (voire invisible dans mon cas ;*>).

:)

> Au nom d'un « droit à l'intimité numérique », ne devons-nous pas considérer que nous avons le devoir de chiffrer même du contenu public ?

Beh c'est un vaste débat. Juste pour préciser ce qui me chiffonne : un jour peut être il sera impossible de venir au local de l'April sans être surveillé par un tiers malveillant. Est-ce que, lorsque ce jour pointera son nez, la contre mesure la plus pertinente sera de forcer les visiteurs du local à venir maquillés et déguisés ? Perso je ne pense pas.

L'analogie à ses limites, mais je pense que le https everywhere et la protection des libertés individuelles ne sont pas intangiblement colinéaires. Et pour y parvenir, du fait des mécanismes d'AC, on perd une large part de notre indépendance à publier du contenu. Le jour où Lets Encrypt tombera, on va maudire hsts et autres.

> Besoin de distinguer ? J'aurai formuler dans l'autre sens : quel besoin de les mélanger ? Car, par défaut, le besoin est de suivre/coller à la nature de ce que l'on fait (deux sites web). De plus, ici, impossible de répondre à la question : photo.april.org est-il utile ? Combien de fois par an est-il utilisé ? En cas de debuggage, impossible de suivre le flux exacte des choses.
>
> Bon, d'un autre côté, je reconnais que ces questions ne sont pas posées depuis des années…

Oui et puis ça ne mange pas de pain. :)

> Du coup, je ne dis pas qu'il ne faut pas uniformiser, mais attention certains paramètres sont choisi à dessin
> et ne sont pas tous des accidents de parcours. Du coup, avant de changer
> il faut veiller un peu à ce que les changements soient compris et leur influence monitorée.

> J'approuve totalement. D'où ma démarche et ce ticket. Si l'intitulé du ticket est très ambitieux (le SM a de l'élan :*>), son origine est plus modeste : lors de la migration de la VM photos, j'ai constaté des incompréhensions de ma part et certaines différences dans les configurations.

> Donc je me proposais de mieux comprendre l'existant et potentiellement d'harmoniser un ou deux trucs au passage en mode jardinage.

Ack. :)

#9 - 20/05/2018 10:21 - Christian P. Momon

François Poulain a écrit :

> > Au nom d'un « droit à l'intimité numérique », ne devons-nous pas considérer que nous avons le devoir de chiffrer même du contenu public ?
>
> Beh c'est un vaste débat. Juste pour préciser ce qui me chiffonne : un jour peut être il sera impossible de venir au local de l'April sans être surveillé par un tiers malveillant. Est-ce que, lorsque ce jour pointera son nez, la contre mesure la plus pertinente sera de forcer les visiteurs du local à venir maquillés et déguisés ? Perso je ne pense pas.

Je vois deux points faibles à cette analogie :

1. avec HTTPS le maquillage et le déguisement sont automatiques, donc pas de contrainte sur l'utilisateur ;
2. HTTPS ne sert pas à cacher une visite mais son contenu, alors qu'un déguisement servirait à cacher une visite et non son contenu. L'intimité des échanges avec les visiteurs du local est protégée :)

> L'analogie à ses limites, mais je pense que le https everywhere et la protection des libertés individuelles ne sont pas intangiblement colinéaires.

Devant l'impossibilité de protéger les libertés numériques individuelles uniquement en comptant sur la bonne volonté humaine, et devant le constat des abus répétés (traçage…), le recours au chiffrement est une solution puissante, efficace et simple.

> Et pour y parvenir, du fait des mécanismes d'AC, on perd une large part de notre indépendance à publier du contenu.

Chiffrer n'est pas authentifier, donc on se met une contrainte supplémentaire en effet. Mais c'est incontournable dans la problématique de l'intimité numérique.

L'alternative serait de considérer que c'est au visiteur de se débrouiller pour protéger son intimité numérique, ce qui est vain si on regarde les pratiques en cours actuellement. Ou alors faudrait-il rendre le site uniquement accessible via Tor ? Voui, vaste le débat.

> Le jour où Lets Encrypt tombera, on va maudire hsts et autres.

Quelles seront alors nos possibilités :

1. passer à un équivalent de Let's Encrypt (ça existe ? on a tellement attendu qu'un Let's Encrypt existe…) ;
2. payer cher des certificats chez d'autres fournisseurs ;
3. passer en certificats auto-signés ;
4. revenir au HTTP ;
5. autres ?

Le fait que Let's Encrypt soit unique en son genre, cela fait prendre conscience qu'il faudrait peut-être « multiplier » les sources de cette dépendance pour la rendre moins centralisée, moins fragile. Bien que cela resterait une dépendance, cela la rendrait-elle plus soutenable/acceptable ?

#10 - 22/05/2018 14:18 - François Poulain

> avec HTTPS le maquillage et le déguisement sont automatiques, donc pas de contrainte sur l'utilisateur ;

Tellement automatique que sans les AC on est perdus.

> HTTPS ne sert pas à cacher une visite mais son contenu, alors qu'un déguisement servirait à cacher une visite et non son contenu.

Les deux masquent le transport. On sait que quelque chose passe, on connait les deux bouts du trafic, mais on ne connait pas la nature de ce qui passe.

> devant le constat des abus répétés (traçage…)

L'essentiel des abus constatés (traçage à des fins publicitaires) n'est nullement empêché par https. Https ne sert qu'à se protéger des intermédiaires techniques et des potentiels vampires sur la ligne ; mais ce ne sont pas ces acteurs qui en veulent le plus à ta vie privée.

> Le fait que Let's Encrypt soit unique en son genre, cela fait prendre conscience qu'il faudrait peut-être « multiplier » les sources de cette dépendance pour la rendre moins centralisée, moins fragile. Bien que cela resterait une dépendance, cela la rendrait-elle plus

> soutenable/acceptable ?

Oui clairement mais aujourd'hui personne d'honnête ne peut devenir une autorité de certification. C'est déjà un demi-miracle que LE ait réussi.

> 1. payer cher des certificats chez d'autres fournisseurs ;

Pour rappel c'est en partie notre situation actuelle.

#11 - 22/05/2018 14:30 - François Poulain

> Chiffrer n'est pas authentifier, donc on se met une contrainte supplémentaire en effet. Mais c'est incontournable dans la problématique de l'intimité numérique.

Et vu le nombre de rogues certificates qu'on a vu passer, il va devenir cavalier de penser que https authentifie. :)

#12 - 30/05/2018 21:26 - Quentin Gibeaux

Décision prise de tout passer en https, pour les problèmes techniques on verra suivant les remontés

#13 - 31/05/2018 13:14 - Quentin Gibeaux

- Version cible changé de Mai 2018 à Juin 2018

#14 - 28/06/2018 13:27 - Quentin Gibeaux

- Version cible changé de Juin 2018 à Été 2018

#15 - 06/09/2018 13:33 - Quentin Gibeaux

- Version cible changé de Été 2018 à Septembre 2018

#16 - 04/10/2018 09:54 - Quentin Gibeaux

- Version cible changé de Septembre 2018 à Octobre 2018

#17 - 08/11/2018 12:27 - Quentin Gibeaux

- Version cible changé de Octobre 2018 à Novembre 2018

#18 - 06/12/2018 10:21 - Quentin Gibeaux

- Version cible changé de Novembre 2018 à Décembre 2018

#19 - 10/01/2019 11:52 - Quentin Gibeaux

- Version cible changé de Décembre 2018 à Janvier 2019

#20 - 31/01/2019 13:18 - Quentin Gibeaux

- Version cible changé de Janvier 2019 à Février 2019

#21 - 28/02/2019 11:47 - Quentin Gibeaux

- Version cible changé de Février 2019 à Mars 2019

#22 - 28/03/2019 09:46 - Quentin Gibeaux

- Version cible changé de Mars 2019 à Avril 2019

#23 - 25/04/2019 14:46 - Quentin Gibeaux

- Version cible changé de Avril 2019 à Mai 2019

#24 - 28/05/2019 01:00 - Christian P. Momon

Notes sur la normalisation du forçage du HTTPS.

Dans les différentes fichiers NGINX, on trouve de très nombreuses diverses variantes :

```
force-ssl.conf    location / {
force-ssl.conf        rewrite ^/(.*) https://$host/$1 permanent;
force-ssl.conf    }

candidats.fr    server {
candidats.fr            […]
candidats.fr            include /etc/nginx/force-ssl.conf;
candidats.fr    }

listes.april.org    server {
listes.april.org    […]
listes.april.org        return 301 https://$host$request_uri;
listes.april.org    }

webmail.april.org    location / {
webmail.april.org        return 301 https://webmail.april.org/;
webmail.april.org    }

apr1.org    location / {
apr1.org        return 301 https://apr1.org/;
apr1.org    }

piwik.april.org    location / {
piwik.april.org        return 301 https://$host$request_uri;
piwik.april.org    }

webmail.april.org    location / {
webmail.april.org        return 301 https://webmail.april.org/;
webmail.april.org    }

pouet.april.org    server {
pouet.april.org    […]
pouet.april.org         # On redirige tout en HTTPS
pouet.april.org         return 301 https://pouet.april.org$request_uri;
pouet.april.org    }

photos.april.org    location / {
photos.april.org        rewrite ^/(.*) http://photos.april.org/$1 permanent;
photos.april.org    }

boutique.april.org    location / {
boutique.april.org        rewrite ^(.*)$ https://boutique.april.org$1 permanent;
boutique.april.org    }

valise.april.org    server {
valise.april.org            […]
valise.april.org            rewrite ^ https://valise.april.org$request_uri? permanent;
valise.april.org    }

informatiquedeloyale.info    location / {
informatiquedeloyale.info        rewrite ^ http://www.april.org/informatique-deloyale permanent;
informatiquedeloyale.info    }
```

Dans la documentation officielle de NGINX, on trouve :
https://www.nginx.com/blog/creating-nginx-rewrite-rules/

```
Again, return is preferable to the equivalent rewrite, which follows.
The rewrite requires interpreting a regular expression – ^(.*)$  – and
creating a custom variable ($1) that in fact is equivalent to the built-in $request_uri variable.

# NOT RECOMMENDED
rewrite ^(.*)$ $scheme://www.domain.com$1 permanent;
```

Donc actions :
1) modification de force-ssl.conf pour utiliser return :

```
force-ssl.conf    server{
force-ssl.conf        […]
force-ssl.conf        return 301 https://$host$request_uri;
force-ssl.conf    }
```

2) Reload et vérification des sites utilisant déjà force-ssl.conf
grep force-ssl *
adherents.april.org: include /etc/nginx/force-ssl.conf;

april-food-inc.april.org: include /etc/nginx/force-ssl.conf;
candidats.fr: include /etc/nginx/force-ssl.conf;
candidats.fr: include /etc/nginx/force-ssl.conf;
education.april.org: include /etc/nginx/force-ssl.conf;
formatsouverts.education: include /etc/nginx/force-ssl.conf;
pad.april.org: include /etc/nginx/force-ssl.conf;
wiki.april.org: include /etc/nginx/force-ssl.conf;

3) conversion et vérification des autres sites utilisant return

admin.april.org: return 301 https://$host$request_uri;
april.poll-o.fr: return 301 https://$host$request_uri;
backuppc2.april.org: return 301 https://$host$request_uri;
listes.agendadulibre.be: return 301 https://$host$request_uri;
listes.agendadulibre.org: return 301 https://$host$request_uri;
listes.april.org: return 301 https://$host$request_uri;
listes.candidats.fr: return 301 https://$host$request_uri;
listes.freesoftwarepact.eu: return 301 https://$host$request_uri;
listes.informatiquedeloyale.info: return 301 https://$host$request_uri;
listes.informatiquedeloyale.info: return 301 https://listes.april.org/wws/;
listes.libre-en-fete.net: return 301 https://$host$request_uri;
piwik.april.org: return 301 https://$host$request_uri;
pouet.april.org: return 301 https://pouet.april.org$request_uri;
questionaires.april.org: return 301 https://$host$request_uri;
statistiques.april.org: return 301 https://$host$request_uri;
webchat.april.org: return 301 https://$host$request_uri;
webmail.april.org: return 301 https://webmail.april.org/;

Ignoré car pas trivial :
apr1.org: return 301 http://apr1.org/;
apr1.org: return 301 https://apr1.org/;

4) conversion et vérification des autres sites utilisant rewrite
agir.april.org: rewrite ^/(.*)$ https://agir.april.org/$1 permanent;
candidats.april.org: rewrite ^/(.*)$ https://candidats.fr/$1 permanent;
informatiquedeloyale.info: rewrite ^ https://www.april.org/informatique-deloyale permanent;
listes.april.org: rewrite ^/(.*)$ https://listes.april.org/$1 permanent;
listes.april.org: rewrite ^/(.*)$ https://listes.april.org/$1 permanent;
mumble.april.org: rewrite ^/(.*)$ https://wiki.april.org/w/Mumble permanent;
stats.april.org: rewrite ^/(.*)$ https://stats.april.org/$1 permanent;
valise.april.org: rewrite ^ https://valise.april.org$request_uri? permanent;
valise-new.april.org: rewrite ^ https://valise-new.april.org$request_uri? permanent;
www.april.org: rewrite ^/(.*) https://www.april.org/$1 permanent;
www-test.april.org: rewrite ^/(.*) https://www-test.april.org/$1 permanent;
www-test.april.org: rewrite ^ https://www-test.april.org$request_uri? permanent;

Ignoré car pas trivial :
apr1.org: rewrite ^/(admin*)$ https://apr1.org/$1 permanent;
apr1.org: rewrite ^/(admin/.*)$ https://apr1.org/$1 permanent;
apr1.org: rewrite ^/(yourls-api.php/.*)$ https://apr1.org/$1 permanent;
apr1.org: rewrite ^/(yourls.php/.*)$ https://apr1.org/$1 permanent;
apr1.org: rewrite ^/(yourls.php)$ https://apr1.org/$1 permanent;
boutique.april.org: rewrite ^(.*)$ https://boutique.april.org$1 permanent;

Tout ça commité.

#25 - 28/05/2019 20:03 - Christian P. Momon

- Statut changé de En cours de traitement à Résolu

D'autres actions pourraient être menées mais les motivations à l'origine de ce ticket ont été satisfaites. Donc proposition de fermeture du ticket.

#26 - 29/05/2019 21:42 - Quentin Gibeaux

- Statut changé de Résolu à Fermé