Documentation d'installation



Installation autorité de certification





18/03/2018

Yohan Fresneau

Sommaire

1.	Prérequis	. 3
2.	Qu'est-ce qu'un certificat	. 3
3.	Installation autorité de certification	. 3
4.	Configuration de apache2	. 4
5.	Ajout du certificat sur le navigateur	. 5
6.	Vérification du fonctionnement du certificat	. 6

1. Prérequis

Nous devons avoir une machine Linux, avec une IP fixe et un nom de machine qui permet de l'identifier facilement, ainsi que son réseau fonctionnel.

2. Qu'est-ce qu'un certificat

Une autorité de certification est une tierce de confiance, qui nous permet de certifier que c'est bien cette machine qui à créer le certificat, à quel serveur il est destiné et à quel site. Un certificat est un moyen d'identifier un serveur et permet de chiffrer les échanges. Cela est très utile, car cela permet de rajouter une sécurité, car le certificat nous permet de certifier que nous somme bien sur le bon site et non un site pirate.

3. Installation autorité de certification

Pour créer nos clés et notre certificat, nous devons effectuer ces commandes



openssl genrsa -out cletestlogin.key { taille clé défaut : 2048 }

openssl req -new -key cletestlogin.key -out testlogin.csr

Country Name (2 letter code) [AU]: FR

State or Province Name (full name) [Some-State]: Centre-val-de-loire

Locality Name (eg, city) []: Tours

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Lycée Paul Louis Courier

Organizational Unit Name (eg, section) []: **BTS SIO** Common Name (e.g. server FQDN or YOUR name) []: **testlogin.freshome.lan** Email Address []: **yohan.fresneau@outlook.fr**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: Toor01

An optional company name []:

Informations à saisir lors de la commande

openssl x509 -req -in testlogin.csr -out testlogin.crt -CA freshomecertgen.crt -CAkey clefreshome.key -CAcreateserial -CAserial ca.srl

Une fois cette commande effectuée, un message nous informe que l'on est bien signé.

4. Configuration de apache2

Nous allons activer le module qui nous permet de passer notre site en mode SSL

a2enmod ssl

Permet d'activer le module "SSL"

Nous allons maintenant activer le site SSL

a2ensite default-ssl

Permet d'activer notre site "SSL"

Nous allons spécifier notre certificat et notre clé privé

nano /etc/apache2/sites-available/default-ssl.conf

ServerName testlogin.freshome.lan

SSLCertificateFile /certificats/testlogin.crt

SSLCertificateKeyFile /certificats/cletestlogin.key

Fichier modifié "**/etc/apache2/sites-available/default-ssl.conf**"

Nous allons rediriger le flux non sécurisé du port 80 vers 443

nano /etc/apache2/sites-available/000-default.conf

ServerName testlogin.freshome.lan

Redirect / https://testlogin.freshome.lan/

Fichier modifié "/etc/apache2/sites-available/000-default.conf"

4/6

Nous devons redémarrer le serveur afin d'appliquer les modifications

<u>/etc/init.d/apache2 restart</u>

Nous allons créer ces dossiers sur les deux serveurs web

mkdir /certificats/

chmod 777 /certificats/

Permet de créer le dossier et mettre les permissions de lecture et d'écriture à tout le monde

Nous allons maintenant mettre nos clés et certificats sur nos serveurs web. Nous allons les déplacer grâce au SSH.

scp testlogin.crt administrateur@testlogin1.freshome.lan:/certificats/

scp testlogin.crt administrateur@testlogin2.freshome.lan:/certificats/

scp cletestlogin.key administrateur@testlogin1.freshome.lan:/certificats/

scp cletestlogin.key administrateur@testlogin2.freshome.lan:/certificats/

Permet d'envoyer depuis le serveur de certification les certificats vers notre serveur web

5. Ajout du certificat sur le navigateur

Pour récupérer le certificat, nous pouvons utiliser "Filezilla" client ou "WinSCP".

Nous devons prendre le fichier portant le nom : freshomecertgen.crt

Ce fichier se trouve dans : /etc/ssl/clés/

Options X	+		
-)→ C' û	€ Firefox about:preferences#privacy	✿ Q Rechercher	
	Ø Rechercher dans les ontions		
Général	complementaires		
Q Recherche	Empêcher les services d'accessibilité d'avoir accès à votre navigateur. En savoir plus		
Vie privée et sécurité	Collecte de données nar Firefox et utilisation		
a			
Compte Firefox	Nous nous efforçons de vous laisser le choix et de recueillir uniquement les informations dont nous		
	avons besoin pour proposer et ameliorer Firetox pour tout le monde, Nous demandons toujours		
	Politique de confidentialité		
	Autoriser Firefox à envoyer des données techniques et des données d'interaction à Mozilla		
	En savoir plus		
	Autoriser Firefox à envoyer les rapports de plantage à Mozilla En savoir plus		
	Sécurité		
	Protection contre les contenus trompeurs et les logiciels dangereux		
	Bloquer les contenus dangereux ou trompeurs En savoir plus		
	Bloquer les téléchargements <u>d</u> angereux		
	Signaler la présence de logiciels indésirables ou peu communs		
	Certificats		
	Lorsqu'un serveur demande votre certificat personnel		
	En sélectionner un automatiquement		
	<u>Y</u> ous demander à chaque fois		
	Interroger le répondeur OCSP pour confirmer la validité de vos		
	certificats Périnhériques de sécurité		

Nous devons nous rendre dans les options de Firefox, puis "Vie privée et sécurité" et pour finir "Afficher les certificats"

Nous allons importer notre certificat de confiance dans le navigateur

Gestionnaire de certificats			
Vos certificats Personnes Serveurs Autorités	Autres		
Vous possédez des certificats enregistrés identifiant ces autori	tés de certification		
Nom du certificat	Périphérique de sécurité	EL.	
✓AC Camerfirma S.A. Chambers of Commerce Root - 2008 Global Chambersign Root - 2008 √AC Camerfirms 54 (CF #42743287)	Builtin Object Token Builtin Object Token		
Camerfirma Chambers of Commerce Root Camerfirma Global Chambersign Root VACCV	Builtin Object Token Builtin Object Token		fres
ACCVRAIZ1 ×Actalis S.p.A./03358520967	Builtin Object Token		
Actalis Authentication Root CA ~AddTrust AB	Builtin Object Token	~	
Voir Modifier la confiance Importer Expo	rter Supprimer ou ne plus faire confiance		
		ОК	

Pour ajouter le certificat, on doit aller dans "Autorités", puis "Importer" et on choisit notre fichier "freshomecrtgen.crt"

On confirme l'ajout du certificat

Téléchargement du certificat On vous a demandé de confirmer une nouvelle autorité de certification (AC). Voulez-vous faire confiance à « ca.freshome.lan » pour les actions suivantes ? Oconfirmer cette AC pour identifier des sites web. Oconfirmer cette AC pour identifier les utilisateurs de courrier. Oconfirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
On vous a demandé de confirmer une nouvelle autorité de certification (AC). Voulez-vous faire confiance à « ca.freshome.lan » pour les actions suivantes ? Confirmer cette AC pour identifier des sites web. Confirmer cette AC pour identifier les utilisateurs de courrier. Confirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	×
Voulez-vous faire confiance à « ca.freshome.lan » pour les actions suivantes ? Confirmer cette AC pour identifier des sites web. Confirmer cette AC pour identifier les utilisateurs de courrier. Confirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
 Confirmer cette AC pour identifier des sites web. Confirmer cette AC pour identifier les utilisateurs de courrier. Confirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible). 	
Confirmer cette AC pour identifier les utilisateurs de courrier. Confirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Confirmer cette AC pour identifier les développeurs de logiciels. Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Avant de confirmer cette AC pour quelque raison que ce soit, vous devriez l'examiner elle, ses méthodes et ses procédures (si possible).	
Voir Examiner le certificat d'AC	
OK Annuler	

On coche toutes les cases, puis on clique sur "**Ok**" afin d'ajouter le certificat

6. Vérification du fonctionnement du certificat

Lorsque l'on se rend sur le site <u>https://testlogin.freshome.lan/</u>, nous avons une redirection transportant vers le port 443 et nous avons bien le SSL active indentifiable au cadenas vert.

