Gestion des certificats

Présentation

Le SNS Stormshiel permet d'exporter pour un serveur ou un utilisateur :

- le **certificat** : le format d'export contient des données en base64 (.pem) ou des données binaires (.der). Le fichier exporté contient le **certificat du porteur** mais également les **certificats des autorités** présentes dans la **chaîne de confiance** de ce certificat.
- L'**identité**: l'identité est constituée de la **clé privée** du porteur, de son **certificat** (qui contient sa clé publique), et des **certificats de la chaîne de confiance**. Le fichier d'export est un container .pem ou un container PKCS#12 (ou .p12). l'identité contient une **clé privée**, donnée sensible et son export doit être protégé par un **mot de passe**, qui permet de **chiffrer la clé privée** qu'il contient.

Extraire les certificat et la clé privée avec OpenSSL

Lien : https://www.ssl.com/fr/comment/exporter-la-cl%C3%A9-priv%C3%A9e-des-certificats-du-fichier-pkcs12-avec-openssl/

Installer un certificat SSL sur un serveur Web

Bonjour, c'est Bing. Je suis heureux de vous aider avec votre question sur l'installation d'un certificat SSL sur Apache2 Debian.

Un certificat SSL est un fichier qui permet de sécuriser la communication entre votre serveur web et vos clients. Il crée un canal chiffré qui empêche les attaques par eavesdropping ou par modification des données. Pour installer un certificat SSL sur Apache2 Debian, vous devez suivre les étapes suivantes :

Créer un dossier pour stocker les fichiers du certificat SSL, comme /etc/ssl/cles et /etc/ssl/certificats. Créer un fichier de clé privée (.key) dans le dossier /etc/ssl/cles avec la commande touch /etc/ssl/cles/votre-domaine.fr*private*key.key. Créer un fichier de certificat (.crt) dans le dossier /etc/ssl/certificats avec la commande touch /etc/ssl/certificats/votre-domaine.fr*ssl*certificate.cer. Créer un fichier intermédiaire (.cer) dans le dossier /etc/ssl/certificats avec la commande touch /etc/ssl/certificats/votre-domaine.fr*ssl*certificate*INTERMEDIATE.cer. Copier le contenu du fichier .crt dans le fichier .cer avec la commande cat /etc/ssl/certificats/votre-domaine.fr*ssl*certificate.cer > /etc/ssl/certificats/votre-domaine.fr*ssl*certificate*INTERMEDIATE.cer. Copier le contenu du fichier .key dans le fichier .crt avec la commande cat /etc/ssl/cles/votre-domaine.fr*private*key.key > /etc/ssl/certificats/votre-domaine.fr*ssl*certificate.cer. Créer un fichier de configuration pour votre site web Apache2 dans le répertoire /etc/apache2/sites-available avec la commande touch /etc/apache2/sites-available/votre-domaine.fr.conf. Ouvrir le fichier de configuration avec un éditeur de texte comme nano ou vim et ajouter les lignes suivantes : <VirtualHost *:80> ServerName votre-domaine.fr ServerAdmin postmaster@votre-domaine.fr DocumentRoot /var/www/votre-domaine # Available loglevels: trace8, ..., trace1, debug, info, notice, warn, # error, crit, alert, emerg. # It is also possible to configure the loglevel for particular # modules, e.g. #LogLevel info ssl:warn ErrorLog ${APACHE*LOG*DIR}/error.log CustomLog ${APACHE*LOG*DIR}/access.log combined

For most configuration files from conf-available/, which are # enabled or disabled at a global level, it is possible to # include a line for only one particular virtual host. For example the # following line enables the CGI configuration for this host only # after it has been globally disabled with "a2disconf". Include conf-available/serve-cgi-bin.conf

Redirect permanent 8 </VirtualHost>

<VirtualHost *:443> ServerName votre-domaine.fr ServerAdmin postmaster@votre-domaine.fr DocumentRoot /var/www/votre-domaine

ErrorLog ${APACHE*LOG*DIR}/error.log CustomLog ${APACHE*LOG*DIR}/access.log combined

SSLEngine on

SSLCertificateFile ${APACHE*DOCUMENT*ROOT}/certificados/${votre*domain}.crt SSLCertificateKeyFile *${APACHE*DOCUMENT*ROOT}/certificados/${votre*domain}.key

SSLCertificateChainFile ${APACHE*DOCUMENT*ROOT}/certificados/${votre*domain}*intermediate.cer

</VirtualHost>

Enregistrer le fichier de configuration en utilisant la commande a2ensite votre-domaine.fr et activer Apache2 en utilisant la commande apachectl configtest. Si tout s'est bien passé, vous devriez voir un message indiquant que votre configuration est correcte. Redémarrer Apache2 en utilisant la commande apachectl restart. Voilà, vous avez installé un certificat SSL sur Apache2 Debian. Vous pouvez maintenant accéder à votre site web en HTTPS en utilisant l'adresse https://votre-domaine.fr. Vous pouvez vérifier que votre site web est bien protégé en utilisant l'outil SSL Checker.

J'espère que cette réponse vous a été utile. Si vous avez d'autres questions sur Apache2 Debian ou sur d'autres sujets liés à l'informatique, n'hésitez pas à me les poser. Je suis toujours prêt à vous aider.