

Génération des certificats ssl aux différents formats

Sommaire

1 Présentation	1
2 Procédure LINUX	1
3 Procédure WINDOWS	1
4 Procédure TOMCAT	1
5 Attention Important	2
6 Déployer le certificat à tous les serveurs windows:	2

Présentation

Cette documentation présente comment générer les certificats aux différents formats

Procédure LINUX

Les certificats sont déjà au bon formats .key, .cer et chain.txt pour apache

Pour HAproxy, il faut générer un fichier pem avec clé privée, pour cela ajouter le contenu du fichier key a la fin du fichier pem:

```
cat certificat.cer > certificat.20XX.pem
```

```
cat cert_chain.txt >> certificat.20XX.pem
```

```
cat certificat.20XX.key >> certificat.20XX.pem
```

Procédure WINDOWS

Pour Windows il faut générer le fichier pfx:

Se connecter sous linux

Passer la commande suivante pour récupérer le pfx

- openssl pkcs12 -export -out wildcard.delta-assurances.net.pfx -inkey /root/wildcard.delta.key -in /root/wildcard.cer.2017
- Il faut le fichier de clé:/root/wildcard.delta.key
- Le fichier certificat résultant:/root/wildcard.cer.2017

Procédure TOMCAT

Nous allons générer la signature au format p12

Se connecter sous linux

Passer la commande suivante pour récupérer le p12

```
openssl pkcs12 -export -in certificat.cer -inkey key.key -chain -CAfile chain.txt -name Alias du certificat -out Nom.p12
```

Exemple:

```
openssl pkcs12 -export -in cert-1476690814-726944.cer -inkey wildcard.key.txt -chain -CAfile chain-1476690814-726944.txt -name wildcard.delta-assurances.net -out wildcard.p12
```

- cert-1476690814-726944.cer =certificat
- wildcard.key.txt =private key
- wildcard.p12 = store format P12
- wildcard.delta-assurances.net=alias du certificat dans le store
- chain-1476690814-726944.txt =chaîne de certification

Si vous avez le message d' erreur suivant: Error unable to get issuer certificate getting chain:

Il manque un certificat dans la chaîne, ouvrez le fichier chaîne pour voir lequel manque.

Au pire ouvrez le pfx sous windows, pour visualiser la chaîne complète

Le récupérer via une recherche sur google (tjs fournis par tbs!), et ajouter dans l' ordre dans le fichier chaîne.

Attention Important

- Stocker le mot de passe du certificat dans RDM
- Stocker le dossier comportant l' ensemble des fichiers

Déployer le certificat à tous les serveurs windows:

Lancer la commande suivante sur chaque serveur

```
certutil.exe -f -p PASSWORD -importpfx "cert.pfx"
```