# ALOHA LOAD BALANCER MISE EN ŒUVRE DU SSL – CERTIFICATS CHAINES

## « APPNOTES » #0024 — MISE EN ŒUVRE DU SSL – CERTIFICATS CHAINES

Cette note applicative a pour vocation de vous aider à implémenter la gestion du SSL via des certificats chaînés au sein de la solution ALOHA Load Balancer.

#### **CONTRAINTE**

Avoir en sa possession toute la chaîne de certificats jusqu'à l'Autorité de certification Trusted Root CA.

### **OBJECTIF**

Implémenter correctemet les certificats chaînés et supprimer l'erreur «invalid chain» dans l'interface de l'Aloha.

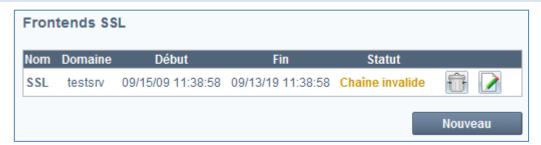
## **COMPLEXITE**



#### **VERSIONS CONCERNEES**

V 3.x et ultérieures

#### MESSAGE D'ERREUR

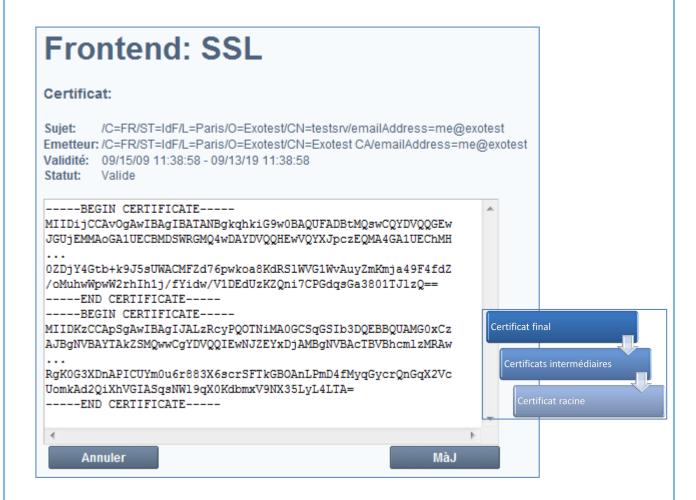


## ORDONNANCEMENT DES CERTIFICATS

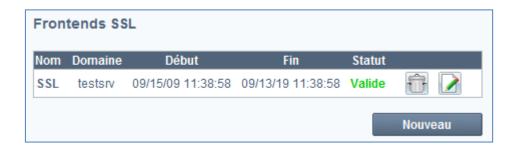


Pour mettre en œuvre des certificats chaînés, il faut que la chaîne de certificat puisse être vérifiée.

L'Aloha a donc besoin de connaître précisément l'ensemble et l'ordre des certificats qui constituent la chaîne.



#### **RESULTAT OBTENU**



L'Aloha ne vérifie pas si le certificat racine a été délivré ou non par une autorité de certification « Trusted root CA ». De ce fait, bien que le statut soit valide sur l'Aloha, le navigateur peut indiquer que le certificat de sécurité présenté n'a pas été émis par une autorité de certification approuvée.

## BASIC TROUBLESHOOTING

Si malgré tout, vous continuez un statut non valide, vous devez vérifier si l'un des certificat intermédiaires ou le certificat racine n'a pas expiré.