

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 correctement 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

Frontends SSL

Nom	Domaine	Début	Fin	Statut		
SSL	testsrv	09/15/09 11:38:58	09/13/19 11:38:58	Chaîne invalide		

Nouveau

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.

Frontend: SSL

Certificat:

Sujet: /C=FR/ST=IdF/L=Paris/O=Exotest/CN=testsrv/emailAddress=me@exotest
Emetteur: /C=FR/ST=IdF/L=Paris/O=Exotest/CN=Exotest CA/emailAddress=me@exotest
Validité: 09/15/09 11:38:58 - 09/13/19 11:38:58
Statut: Valide

```
-----BEGIN CERTIFICATE-----
MIIDijCCAvOgAwIBAgIBATANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEw
JGUjEMMAoGA1UECBMSWRGMQ4wDAYDVQQHEwVQYXJpczEQMA4GA1UEChMH
...
0ZDjY4Gtb+k9J5sUWACMFZd76pwkoa8KdRS1WVG1WvAuyZmKmja49F4fdZ
/oMuhwWpwW2rhIh1j/fYidw/V1DEdUzKZQni7CPGdqsGa3801TJlzQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDKzCCApSgAwIBAgIJALzRcyPQOTNiMA0GCSqGSIb3DQEBBQUAMG0xCz
AJBgNVBAYTAKZSMQwwCgYDVQQIEwNJZEYxZDjAMBgNVBAcTBVBhcm1zMRAw
...
RgK0G3XDnAPICUYm0u6r883X6scrSFTkGBOAnLPmD4fMyqGycrQnGqX2Vc
UomkAd2QiXhVGIASqsNW19qX0KdbmxV9NX35LyL4LTA=
-----END CERTIFICATE-----
```

Annuler

MàJ



Certificat final

Certificats intermédiaires

Certificat racine

RESULTAT OBTENU

Frontends SSL

Nom	Domaine	Début	Fin	Statut		
SSL	testsrv	09/15/09 11:38:58	09/13/19 11:38:58	Valide		

Nouveau

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.