NF16227 — GÉNÉRATION AUTOMATIQUE DE CERTIFICATS SSL VALIDE

Voir la carte de la fonctionnalité : [A classer](#)

Le hairpinning (capacité de deux machines placées derrière un même routeur NAT de communiquer entre-elles en utilisant l'adresse IP de sortie/box) n'est pas supporté par toutes les box, notamment celles d'Orange.

Ce problème est contournable par l'utilisation de l'IPv6 mais cette option n'est visiblement que très peu envisageable chez les clients d'Orange Pro.

Nous allons donc contourner ce problème en modifiant nos app de sorte qu'elles puissent essayer de se connecter sur l'adresse privée de son point de référence (service de réplication) quand l'IP publique ne répond pas.

L'idée est donc la suivante :

- le bindage des applications est entièrement revu : les applications sont distribuées désormais depuis internet `https://pl-LICENCE.apps.polarisgestionmag.net` (début de mise en place du store d'app) ;
- le service de réplication distribue un certificat SAN dont le CN l'identifie directement `nurX.pl-LICENCE.polarisgestionmag.net` ; mais également un nom alternatif : `i-nurX.pl-LICENCE.polarisgestionmag.net` ;
- il détermine son adresse IP locale (privée au sens du RFC 1918) et la communique lors du relevé d'IP au manager ;
- le manager stocke l'adresse IP et l'associe à une entrée DNS publique de la forme `i-nurX.pl-LICENCE.polarisgestionmag.net` ;
- quand une application est jumelée, le service de réplication détermine si l'adresse `i-nurX.pl-LICENCE.polarisgestionmag.net` est résolvable sur le DNS interne (ou celui du FAI dans le cas d'une box). Si c'est le cas, alors il distribue l'application par son l'adresse `https://i-nurX.pl-LICENCE.polarisgestionmag.net/` ; sinon, par `https://nurX.pl-LICENCE.polarisgestionmag.net/`.
- l'application quant à elle envoie ses requêtes API alternativement sur `i-nur` puis `nur`, en commençant par son point de montage (l'url de l'appli) et en intervertissant dès qu'une erreur "hôte injoignable" ou "l'hôte ne répond pas" ou "hôte inconnu" se produit (bref, toute erreur sauf erreur émise par le service = service ne répond pas).

Note : étant donné que la résolution DNS publique sur des adresses privées (RFC 1918) n'est pas supportée par tous les FAI (comme Free) et part en ServFail, nous ne pourrions pas assumer que cette solution fonctionne en permanence. Néanmoins, elle présente deux avantages :

- elle fonctionne (pour l'instant) chez les dns Orange que nous avons pu tester ;

- l'échec de résolution et l'échec de tentative de communication vers une IP RFC 1918 sur un téléphone cellulaire non connecté à un WIFI est immédiat, aussi l'utilisation systématique du lien interne en premier permettra d'accélérer les transferts sans retarder les cas où il n'est pas supporté !