RFC 8808 : A YANG Data Model for Factory Default Settings

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 septembre 2020

Date de publication du RFC : Août 2020

https://www.bortzmeyer.org/8808.html

Ce RFC décrit un modèle YANG pour permettre la « remise aux réglages d'usine » d'un équipement, quand celui-ci est trop bizarrement configuré pour qu'il y ait une autre solution que l'effacement radical.

YANG (RFC 6020 [1]) est un langage de description des équipements réseau et de leurs capacités, afin de permettre de la gestion automatisée de ces équipements via des protocoles comme NETCONF (RFC 6241) ou RESTCONF (RFC 8040).

Ce RFC définit un nouveau RPC, `factory-reset`, qui va remettre tous les réglages de la machine aux réglages qu'elle avait à la sortie d'usine. C'est l'équivalent YANG de manipulations physiques comme « appuyez sur les boutons Power et VolumeDown simultanément pendant cinq secondes » ou bien « insérez un trombone dans ce petit trou ».

La section 2 du RFC décrit plus précisément ce que veut dire « retourner aux réglages d'usine ». Les entrepôts ("*datastore*", cf. RFC 6020, RFC 7950 et RFC 8342) comme `<running>` reprennent les valeurs qu'ils contenaient lorsque l'équipement a quitté l'usine. Toutes les données générées depuis sont jetées. Cela inclut (le RFC utilise des exemples de répertoires Unix, que je reprends ici, mais ce sont juste des exemples, l'équipement n'utilise pas forcément Unix) les certificats (`/etc/ssl`), les journaux (`/var/log`), les fichiers temporaires (`/tmp`), etc. Par contre, il faut garder des informations qui étaient spécifiques à cet engin particulier (et différent des autres du même modèle) mais qui ont été fixés avant le premier démarrage, par exemple des identificateurs uniques ou des clés privées ou mots de passe générées automatiquement au début du cycle de vie. Les données sensibles doivent être effacées de manière sûre, par exemple en écrivant plusieurs fois sur leur emplacement (cf. section 6). À noter que

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6020.txt`

cette remise au début peut couper la communication avec la machine de gestion : l'équipement se comportera comme s'il sortait du carton, ce qui peut nécessiter une configuration nouvelle.

Notre RFC normalise également un nouvel entrepôt ("*datastore*"), `factory-default`, qui contient ces réglages d'usine et permet donc à un client NETCONF ou RESTCONF de savoir en quoi ils consistent. Appeler `factory-reset` revient donc à appliquer `factory-default`. Cet entrepôt suit les principes du RFC 8342, annexe A, et est en lecture seule.

La section 4 présente le module complet, qui est disponible en (en ligne sur `https://www.bortzmeyer.org/files/ietf-factory-default.yang`). Il s'appuie sur le module du RFC 8342 et sur celui du RFC 8341.

L'URN de ce RFC, `urn:ietf:params:xml:ns:yang:ietf-factory-default` a été enregistré à l'IANA <`https://www.iana.org/assignments/xml-registry/xml-registry.xml#ns`> (registre du RFC 3688), et le module `ietf-factory-default` dans le registre des modules <`https://www.iana.org/assignments/yang-parameters/yang-parameters.xml#yang-parameters-1`>.

Quelques mots sur la sécurité pour terminer. Comme le but de ce module est de permettre à des clients NETCONF ou RESTCONF d'appeler ce RPC `factory-reset`, et que ce RPC a des conséquences...sérieuses pour l'équipement, il faut comme d'habitude veiller à ce que les accès NETCONF et RESTCONF soient bien sécurisés (par exemple via SSH, cf. RFC 6242 et via les contrôles d'accès du RFC 8341).