Groupe de travail Réseau
**Request for Comments : 4744**
Catégorie : Sur la voie de la normalisation

E. Lear, Cisco Systems
K. Crozier
décembre 2006
Traduction Claude Brière de L'Isle

# Utilisation du protocole NETCONF sur le protocole extensible d'échange de blocs (BEEP)



**Résumé**
Le présent document spécifie une transposition de protocole d'application pour le protocole de configuration de réseau (NETCONF, *Network Configuration Protocol*) sur le protocole d'échange de blocs extensible (BEEP, *Blocks Extensible Exchange Protocol*).

## Table des matières



## 1. Introduction

Le protocole NETCONF [RFC4741] définit un mécanisme simple pour gérer un appareil du réseau. NETCONF est conçu pour être utilisable sur divers protocoles d'application. Le présent document spécifie une transposition de protocole d'application pour NETCONF sur le protocole extensible d'échange de blocs (BEEP) [RFC3080].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

### 1.1 Pourquoi BEEP ?

L'utilisation de BEEP est naturelle comme protocole d'application pour le transport de XML. Comme protocole

d'homologue à homologue, BEEP fournit un moyen facile de mettre en œuvre NETCONF, quel que soit le côté de la connexion qui est l'initiateur. Cette "bidirectionnalité" permet au gestionnaire ou à l'agent d'initier une connexion. C'est particulièrement important pour prendre en charge un grand nombre d'appareils connectés de façon intermittente, ainsi que les appareils qui doivent inverser la connexion de gestion en présence de pare-feu et de traducteurs d'adresse réseau (NAT, *network adress translator*).

BEEP utilise l'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*) [RFC4422]. Le profil SASL utilisé par BEEP permet une transposition simple et directe en le modèle de sécurité existant pour l'interface de ligne de commande (CLI, *command line interface*) alors que la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC4346] fournit un mécanisme de chiffrement fort, bien vérifié, avec l'authentification du côté serveur ou des deux côtés serveur et client.

## 2. Transposition de transport BEEP

Toutes les mises en œuvre NETCONF sur BEEP DOIVENT utiliser le profil et la transposition fonctionnelle entre NETCONF et BEEP comme décrit ci-dessous.

Pour les besoins de ce document, un gestionnaire est un client NETCONF, et un agent est un serveur NETCONF. L'utilisation du langage client/serveur dans BEEP est évitée à cause de la notion courante que dans le réseautage les clients se connectent aux serveurs.

### 2.1 Établissement de session NETCONF

Les gestionnaires peuvent être des écoutants BEEP ou des initiateurs. De même, les agents peuvent être des écoutants ou des initiateurs. Pour établir une connexion, l'initiateur se connecte à l'écoutant sur l'accès TCP 831. Donc, l'échange initial a lieu sans considération de si un gestionnaire ou l'agent est l'initiateur. Après l'établissement de la connexion de transport, lorsque les messages d'accueil sont échangés, ils DEVRAIENT chacun annoncer leur prise en charge de TLS et facultativement de SASL. Une fois que les messages d'accueil BEEP sont échangés, si TLS va être utilisé et est disponible aux deux parties, l'écoutant commence un canal avec le profil TLS.

Une fois que TLS a commencé, un nouveau message d'accueil BEEP est envoyé par l'initiateur et par l'écoutant, comme exigé par la spécification de BEEP.

Après l'échange de tous les messages d'accueil BEEP afin que les rôles soient clairs, l'agent DOIT annoncer le profil NETCONF. Le gestionnaire NE DOIT PAS annoncer le profil NETCONF. Si le côté agent de la communication (l'initiateur ou l'écoutant) reçoit un élément BEEP <greeting> qui contient le profil NETCONF, il DOIT clore la connexion. De même, si aucun côté ne produit de profil NETCONF, c'est également une erreur, et l'écoutant DOIT clore la connexion.

À ce point, si SASL est désiré, l'initiateur ouvre un canal BEEP pour effectuer un échange SASL pour s'authentifier. À l'achèvement de l'authentification, le canal est clos. C'est-à-dire que le canal est exclusivement utilisé pour authentifier.

On trouvera des exemples des deux profils TLS et SASL dans la [RFC3080].

Il est prévu que le mécanisme SASL PLAIN sera largement utilisé en conjonction avec TLS [RFC2595]. Dans ce cas, en accord avec la RFC 2595, le mécanisme PLAIN NE DOIT PAS être annoncé dans le premier <greeting> BEEP, mais seulement dans celui qui suit une négociation TLS réussie. Cela s'applique seulement si les mécanismes PLAIN TLS et SASL sont tous deux utilisés. Pour éviter le risque d'espionnage, le mécanisme SASL PLAIN NE DOIT PAS être utilisé sur des canaux non chiffrés. Les spécificités de l'utilisation de SASL et TLS sont mentionnées dans les considérations de sécurité ci-dessous.

Une fois l'authentification réalisée, il n'est plus nécessaire de distinguer entre initiateur et écoutant. On distingue maintenant le gestionnaire et l'agent, et on suppose que chacun connaît son rôle dans la conversation.

### 2.2 Lancement d'un canal pour NETCONF

Le gestionnaire établit maintenant un nouveau canal et spécifie le seul profil NETCONF. Par exemple :

(G = gestionnaire ; A = agent)

```
G : MSG 0 1 . 10 48 118
G : Content-type: application/beep+xml
G :
G  <start number="1">
G :   <profile uri="http://iana.org/beep/netconf" />
G : </start>
G : FIN

A : RPY 0 1 . 38 87
A : Content-Type: application/beep+xml
A :
A : <profile uri="http://iana.org/beep/netconf" />
A : FIN
```

À ce point, on est prêt à procéder aux opérations NETCONF sur le canal BEEP 1.

Les messages NETCONF sont transmis avec un en-tête Type de contenu réglé à "text/xml".

Ensuite le gestionnaire et l'agent échangent des éléments NETCONF <hello> sur le nouveau canal afin que chaque côté apprenne les capacités de l'autre. Cela se produit par un MSG. Chaque côté va alors répondre positivement. L'exemple suivant est adapté du paragraphe 8.1 de la [RFC4741] :

```
A : MSG 1 0 . 0 457
A : Content-type: application/beep+xml
A :
A : <?xml version='1.0' encoding="UTF-8"?>
A : <hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
A :   <capacités>
A :     <capacité>
A :       urn:ietf:params:netconf:base:1.0
 A:     </capacité>
A :     <capacité>
A :       urn:ietf:params:netconf:capability:startup:1.0
A :     </capacité>
A :     <capacité>
A :       http://exemple.net/router/2.3/core#macaractéristique
A :     </capacité>
A :   </capacités>
A :   <session-id>4</session-id>
A : </hello>
A : FIN

G : RPY 1 0 . 0 0
G : FIN
```

De futures capacités NETCONF pourront exiger des canaux BEEP supplémentaires. Quand de telles capacités seront définies, une transposition BEEP devra aussi être définie.

À ce point, la session NETCONF est établie, et les capacités ont été échangées.

### 2.3 Utilisation de la session NETCONF

Presque toutes les opérations NETCONF sont exécutées à travers l'élément <rpc>. Pour produire un appel de procédure distante (RPC, *remote procedure call*) le gestionnaire transmet sur le canal opérationnel un message BEEP contenant le RPC et ses arguments. En accord avec la norme BEEP, les demandes RPC peuvent être partagées sur plusieurs trames BEEP.

Une fois reçues et traitées, l'agent répond avec des messages BEEP RPY sur le même canal avec la réponse au RPC. En accord avec la norme BEEP, les réponses peuvent être partagées sur plusieurs trames BEEP.

### 2.4 Suppression de session NETCONF

À réception du <close-session> du gestionnaire, une fois que l'agent a achevé toutes les RPC, il va clore le canal BEEP 0. Quand un agent a besoin d'initier une fermeture, il va le faire en closant le canal BEEP 0. Bien qu'il ne soit pas obligé de faire ainsi, l'agent devrait permettre une période raisonnable pour qu'un gestionnaire libère tout verrou existant avant d'initier une clôture. Une fois que l'agent a clos le canal 0, tous les verrous sont libérés, et chaque côté suit les procédures de suppression comme spécifié dans la [RFC3081]. Ayant reçu un BEEP close ou ayant envoyé <close-session>, un gestionnaire NE DOIT PAS envoyer d'autres demandes. Si il y a des activités supplémentaires dues à des capacités étendues, il DOIT cesser d'une manière ordonnée et ce devrait être décrit de façon appropriée dans la transposition de capacités.

### 2.5 Profil BEEP pour NETCONF

Identification de profil : http://iana.org/beep/netconf
Messages échangés durant la création de canal : non applicable
Messages commençant les échanges réciproques : "hello", "rpc", "rpc-reply"
Messages de réponses positives : "rpc-reply"
Messages de réponses négatives : "rpc-reply"
Messages dans des échanges de un à plusieurs : aucun
Syntaxe de message : [RFC4741]
Sémantique de message : [RFC4741]
Informations de contact : voir la Section "Adresse des auteurs" de ce mémoire.

## 3. Considérations sur la sécurité

Les informations de configuration sont par nature sensibles. Leur transmission en clair et sans vérification d'intégrité laisse les appareils ouverts aux classiques attaques "par interposition". Les informations de configuration contiennent souvent des mots de passe, des noms d'utilisateurs, des descriptions de services, et des informations topologiques, qui sont toutes sensibles. Un protocole d'application NETCONF doit donc au minimum prendre en charge les options de confidentialité et d'authentification.

La transposition BEEP décrite dans le présent document vise la confidentialité et l'authentification d'une manière flexible par l'utilisation des profils TLS et SASL. La confidentialité est fournie via le profil TLS et est utilisée comme discuté ci-dessus. De plus, le certificat de serveur devra servir à l'authentification du serveur auprès du client. Le client DOIT être prêt à reconnaître et valider un certificat de serveur et DEVRAIT par défaut rejeter les certificats invalides.

Afin de valider un certificat, le client doit être capable d'accéder à une ancre de confiance. Bien que de telles méthodes de validation sortent du domaine d'application de ce document, elles vont dépendre du type d'appareil et des circonstances. Celui qui met en œuvre et l'administrateur doivent être conscients des dépendances circulaires que les diverses méthodes peuvent introduire. Par exemple, les serveurs du protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol*) peuvent n'être pas disponibles dans un scénario de démarrage à froid du réseau et il ne saurait être conseillé aux routeurs centraux de dépendre de la configuration reçue à l'amorçage.

Il y a plusieurs options pour l'authentification côté client. Le client PEUT fournir un certificat durant la phase d'initialisation de TLS, auquel cas le sujet de ce certificat devra être considéré comme le principal pour les besoins de l'authentification. Là encore, les mises en œuvre de serveur devraient être conscientes de toute interdépendance qui pourrait être créée à travers les protocoles utilisés pour valider les ancres de confiance.

Les points d'extrémité TLS peuvent être autorisés sur la base d'un nom de sujet ou d'une autorité de certification (CA), selon les circonstances. Par exemple, il serait malavisé pour un routeur du cœur de l'Internet de permettre une connexion d'agent netconf sur la simple base d'un certificat valide signé par une CA commune, mais pas déraisonnable de permettre une connexion à partir d'un agent avec un nom distinctif particulier. Par ailleurs, il serait souhaitable que les entreprises fassent confiance aux certificats signés par les CA de leur équipe de fonctionnement de réseau.

Dans le cas où le client ne s'est pas authentifié par TLS, le serveur DEVRAIT annoncer un ou plusieurs profils SASL, entre lesquels le client choisirait. Dans le cas particulier de l'établissement de TLS, le profil minimum PEUT être PLAIN. Autrement, les mises en œuvre DOIVENT prendre en charge le profil DIGEST-MD5 décrit dans la [RFC2831], et elles

PEUVENT prendre en charge d'autres profils comme le mécanisme de mot de passe à usage unique (OTP, *One-Time Password*) [RFC2444].

Différents environnements peuvent permettre des droits différents avant et après l'authentification. Le présent document ne spécifie pas un modèle d'autorisation. Quand une opération n'est pas proprement autorisée, une simple rpc-error contenant "permission refusée" est alors suffisante. Noter que les informations d'autorisation peuvent être échangées sous la forme d'informations de configuration, ce qui est une raison de plus pour assurer la sécurité de la connexion.

## 4. Considérations relatives à l'IANA

L'IANA a alloué l'accès TCP (831) à NETCONF sur BEEP.

## 5. Remerciements

Ce travail a été produit par le groupe de travail NETCONF de l'IETF, et de nombreuses personnes ont contribué à la discussion sur NETCONF. On notera Rob Ens, Phil Schafer, Andy Bierman, Wes Hardiger, Ted Goddard, et Margaret Wasserman qui ont tous contribué d'une certaine façon à ce travail, qui devait à l'origine se trouver dans la spécification du protocole NETCONF de base. Merci aussi à Weijing Chen, Keith Allen, Juergen Schoenwaelder, Marshall Rose, et Eamon O'Tuathail de leur participation très constructive. Les auteurs remercient aussi Elwyn Davies de sa relecture constructive.

## 6. Références

### 6.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2595] C. Newman, "Utilisation de TLS avec IMAP, POP3 et ACAP", juin 1999. (*MàJ par* RFC4616, 7817, 8314) *(P.S.)*

[RFC2831] P. Leach et C. Newman, "Utilisation de l'authentification par résumé comme mécanisme SASL", mai 2000. (*Obsolète, voir* RFC6331)

[RFC3080] M. Rose, "Cœur du protocole extensible d'échange de blocs (BEEP)", mars 2001. *(P.S.)*

[RFC3081] M. Rose, "Transposition du cœur BEEP en TCP", mars 2001. *(P.S.)*

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

[RFC4422] A. Melnikov et K. Zeilenga, éd, "Authentification simple et couche de sécurité (SASL)", juin 2006. *(P.S.)*

[RFC4741] R. Enns, éd., "Protocole de configuration NETCONF", décembre 2006. *(P.S.)*

### 6.2 Références pour information

[RFC2444] C. Newman, "Mécanisme SASL de mot de passe à utilisation unique", octobre 1998. *(P.S.)*

[XML] Sperberg-McQueen, C., Paoli, J., Maler, E., and T. Bray, "Extensible Markup Language (XML) 1.0 (Second Edition)", World Wide Web Consortium, First Edition, http://www.w3.org/TR/2000/REC-xml-20001006 , octobre 2000.

## Adresse des auteurs

Eliot Lear
Cisco Systems
Glatt-com
CH-8301 Glattzentrum, Zurich
CH
mél : lear@cisco.com

Ken Crozier
mél : ken.crozier@gmail.com

## Déclaration complète de droits de reproduction



**Remerciement**
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF.