Groupe de travail Réseau
Request for Comments : 4742
Catégorie : Sur la voie de la normalisation

M. Wasserman, ThingMagic
T. Goddard, ICEsoft Technologies, Inc.
décembre 2006
Traduction Claude Brière de L'Isle

Utilisation du protocole de configuration NETCONF sur Secure Shell (SSH)

Résumé
Le présent document décrit une méthode pour invoquer et faire fonctionner le protocole de congiguration de réseau (NETCONF, *Network Configuration Protocol*) au sein d'une session Secure Shell (SSH) comme un sous système SSH.

Table des Matières

1. Introduction

Le protocole NETCONF [RFC4741] est un protocole fondé sur XML utilisé pour gérer la configuration d'un équipement de réseautage. NETCONF est défini comme étant indépendant de la couche de session et de transport, permettant de définir des transpositions pour plusieurs protocoles de couche session ou transport. Le présent document définit comment NETCONF peut être utilisé au sein d'une session Secure Shell (SSH) en utilisant le protocole de connexion SSH [RFC4254] sur le protocole de transport SSH [RFC4253]. Cette transposition va permettre à NETCONF d'être exécuté à partir d'une session Secure Shell par un utilisateur ou une application.

Dans ce document, les termes "client" et "serveur" sont utilisés pour se référer aux deux extrémités de la connexion de transport SSH. Le client ouvre activement la connexion SSH, et le serveur écoute passivement la connexion SSH entrante. Les termes "gestionnaire" et "agent" sont utilisé pour se référer aux deux extrémités de la session de protocole NETCONF. Le gestionnaire produit des commandes d'appel de procédure distante (RPC, *remote procedure call*) NETCONF, et l'agent répond à ces commandes. Quand NETCONF fonctionne sur SSH en utilisant la transposition définie dans le présent document, le client est toujours le gestionnaire, et le serveur est toujours l'agent.

2. Terminologie des exigences

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].

3. Lancer NETCONF sur SSH

Pour faire fonctionner NETCONF sur SSH, le client va d'abord établir une connexion de transport SSH en utilisant le protocole de transport SSH, et client et serveur vont échanger les clés pour l'intégrité et le chiffrement du message. Le client va alors invoquer le service "ssh-userauth" pour authentifier l'utilisateur, comme décrit dans le protocole d'authentification SSH [RFC4252]. Une fois que l'utilisateur a bien été authentifié, le client va invoquer le service "ssh-connection", aussi appelé protocole de connexion SSH.

Après que le service ssh-connection est établi, le client va ouvrir un canal de type "session", qui va résulter en une session SSH.

Une fois la session SSH établie, l'utilisateur (ou l'application) va invoquer NETCONF comme un sous système SSH appelé "netconf". La prise en charge de sous système est une caractéristique de SSH version 2 (SSHv2) et n'est pas incluse dans SSHv1. Faire fonctionner NETCONF comme un sous système SSH évite le besoin que le descriptif reconnaisse les invites de shell ou saute les informations étrangères, comme un message système qui est envoyé au démarrage de shell. Cependant, même quand un sous système est utilisé, certains messages étrangers peuvent être imprimés par les descriptifs de démarrage de l'utilisateur. Les mises en œuvre DOIVENT sauter ces messages en cherchant une directive de démarrage 'xml', qui DOIT être suivie par un élément <hello> dans l'espace de noms 'NETCONF'.

Afin de permettre au trafic NETCONF d'être facilement identifié et filtré par les pare-feu et autre appareils du réseau, les serveurs NETCONF DOIVENT par défaut ne fournir l'accès au sous système "netconf" SSH que quand la session SSH est établie en utilisant l'accès TCP <830> alloué par l'IANA. Les serveurs DEVRAIT être configurables à permettre l'accès au sous systèmes netconf SSH sur d'autres accès.

Un utilisateur (ou application) pourrait utilisr la ligne de commande suivante pour invoquer NETCONF comme un sous système SSH sur l'accès alloué par l'IANA :

```
[utilisateur@client]$ ssh -s serveur.exemple.org -p <830> netconf
```

Noter que l'option -s cause l'invocation de la commande ("netconf") comme un sous système SSH.

3.1 Échange de capacités

Le serveur DOIT indiquer ses capacités en envoyant un document XML contenant un élément <hello> aussitôt que la session NETCONF est établie. L'utilisateur (ou l'application) peut analyser ce message pour déterminer quelles capacités NETCONF sont prises en charge par le serveur.

Le client doit aussi envoyer un document XML contenant un élément <hello> pour indiquer au serveur les capacités du client. Le document contenant l'élément <hello> DOIT être le premier document XML que le client envoie après l'établissement de la session NETCONF.

L'exemple suivant montre un échange de capacités. Les messages envoyés par le client sont marqués d'un "C:", et ceux envoyés par le serveur sont marqués d'un "S:".

```
S: <?xml version="1.0" encoding="UTF-8"?>
S: <hello>
S:   <capabilities>
S:     <capability>
S:       urn:ietf:params:xml:ns:netconf:base:1.0
S:     </capability>
S:     <capability>
S:       urn:ietf:params:ns:netconf:capability:startup:1.0
```

```
S:    </capability>
S:  </capabilities>
S:  <session-id>4<session-id>
S: </hello>
S: ]]>]]>

C: <?xml version="1.0" encoding="UTF-8"?>
C: <hello>
C:  <capabilities>
C:    <capability>
C:      urn:ietf:params:xml:ns:netconf:base:1.0
C:    </capability>
C:  </capabilities>
C: </hello>
C: ]]>]]>
```

Bien que l'exemple montre le serveur qui envoie un message <hello> suivi par le message du client, les deux côtés vont envoyer le message aussitôt que le sous système NETCONF est initialisé, peut-être simultanément.

Comme l'illustre l'exemple ci-dessus, une séquence de caractères spéciale,]]>]]>, DOIT être envoyée par le client et le serveur après chaque document XML dans l'échange NETCONF. Cette séquence de caractères ne peut pas légalement apparaître dans un document XML, de sorte qu'elle peut être sans ambiguïté utilisée pour identifier la fin du document courant, permettant une resynchronisation de l'échange NETCONF en cas d'erreur de syntaxe ou d'analyse XML.

4. Utilisation de NETCONF sur SSH

Une session NETCONF sur SSH consiste en l'échange de documents XML complets entre le gestionnaire et l'agent. Une fois la session établie et les capacités échangées, le gestionnaire va envoyer au serveur des documents XML complets contenant des éléments <rpc>, et l'agent va répondre avec des documents XML complets contenant des éléments <rpc-reply>.

Pour continuer l'exemple précédent, une session NETCONF sur SSH pour restituer un ensemble d'informations de configuration pourrait ressembler à ceci :

```
C: <?xml version="1.0" encoding="UTF-8"?>
C: <rpc message-id="105"
C: xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
C:  <get-config>
C:    <source><running/></source>
C:    <config xmlns="http://exemple.com/schema/1.2/config">
C:     <users/>
C:    </config>
C:  </get-config>
C: </rpc>
C: ]]>]]>

S: <?xml version="1.0" encoding="UTF-8"?>
S: <rpc-reply message-id="105"
S: xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
S:  <config xmlns="http://exemple.com/schema/1.2/config">
S:    <utilisateurs>
S:      <utilisateur><nom>racine</nom><type>super utilisateur</type></utilisateur>
S:      <utilisateur><nom>fred</nom><type>admin</type></utilisateur>
S:      <utilisateur><nom>barney</nom><type>admin</type></utilisateur>
S:    </utilisateurs>
S:  </config>
S: </rpc-reply>
S: ]]>]]>
```

5. Sortie du sous système NETCONF

La sortie de NETCONF est réalisée en utilisant l'opération <close-session>. Un agent va traiter les messages RPC provenant du gestionnaire dans l'ordre de leur réception. Quand l'agent traite une commande <close-session>, il devra répondre et clore le canal de session SSH. L'agent NE DOIT PAS traiter d'autre commande RPC reçue sur la session courante après la commande <close-session>.

Pour continuer l'exemple utilisé dans les sections précédentes, une session de sous système NETCONF existante pourrait être close comme suit :

```
C: <?xml version="1.0" encoding="UTF-8"?>
C: <rpc message-id="106"
C: xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
C:   <close-session/>
C: </rpc>
C: ]]>]]>

S: <?xml version="1.0" encoding="UTF-8"?>
S: <rpc-reply id="106"
S: xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
S:   <ok/>
S: </rpc-reply>
S: ]]>]]>
```

6. Considérations sur la sécurité

NETCONF est utilisé pour accéder aux informations de configuration et d'état et modifier les informations de configuration, de sorte que la capacité d'accéder à ce protocole devrait être limitée aux utilisateurs et systèmes autorisés à voir la configuration et l'état de l'agent ou à modifier la configuration de l'agent.

L'identité du serveur DOIT être vérifiée et authentifiée par le client en accord avec la politique locale avant que des données d'authentification fondées sur le mot de passe ou des données de configuration ou d'état soient envoyées ou reçues du serveur. L'identité du client DOIT aussi être vérifiée et authentifiée par le serveur en accord avec la politique locale pour s'assurer que la demande de client entrante est légitime avant tout envoi ou réception de données de configuration ou d'état au ou du client. Aucun des côtés ne devrait établir une connexion NETCONF sur SSH avec une identité inconnue, inattendue, ou incorrecte de l'autre côté.

Les données de configuration ou d'état peuvent inclure des informations sensibles, comme des noms d'utilisateur ou des clés de sécurité. Donc, NETCONF devrait seulement être utilisé sur des canaux de communications qui fournissent un chiffrement fort pour la confidentialité des données. Le présent document définit une transposition de NETCONF sur SSH qui assure la prise en charge d'un chiffrement et d'une authentification forts.

Le présent document exige que par défaut les serveurs n'accordent l'accès au sous système "netconf" SSH que quand ils utilisent un accès TCP spécifique alloué à cette fin par l'IANA. Cela permettra que le trafic NETCONF sur SSH soit aisément identifié et filtré par les pare-feu et autre nœuds du réseau. Cependant, cela permettra aussi que le trafic NETCONF sur SSH soit plus aisément identifié par des attaquants.

Le présent document recommande aussi que les serveurs soient configurables pour permettre l'accès au sous système "netconf" SSH sur d'autres accès. L'utilisation de cette option de configuration sans les changements correspondants de configuration des pare-feu ou appareils du réseau peut résulter en la capacité involontaire de nœuds extérieurs au pare-feu ou autre frontière administrative d'obtenir l'accès au sous système "netconf" SSH.

7. Considérations relatives à l'IANA

L'IANA a alloué un numéro d'accès TCP qui est l'accès par défaut pour les sessions NETCONF sur SSH comme défini dans le présent document.

L'IANA a alloué l'accès <830> à cette fin.

Il est aussi demandé à l'IANA d'allouer "netconf" comme nom de service SSH tel que défini dans la [RFC4250]:

Nom de service	**Référence**
netconf	RFC 4742

8. Remerciements

Le présent document a été écrit en utilisant l'outil xml2rfc décrit dans la [RFC2629].

Des apports nombreux ont été reçus des autres membres de l'équipe de conception NETCONF, incluant: Andy Bierman, Weijing Chen, Rob Enns, Wes Hardaker, David Harrington, Eliot Lear, Simon Leinen, Phil Shafer, Juergen Schoenwaelder, et Steve Waldbusser. Les personnes suivantes ont aussi relu le présent document et fourni des commentaires précieux : Olafur Gudmundsson, Sam Hartman, Scott Hollenbeck, Bill Sommerfeld, et Bert Wijnen.

9. Références

9.1 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)

[RFC4250] S. Lehtinen et C. Lonvick, éd., "Numéros alloués du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8268)

[RFC4252] T. Ylonen et C. Lonvick, éd., "Protocole d'authentification Secure Shell (SSH)", janvier 2006. *(P.S .; MàJ par* RFC8308, 8332)

[RFC4253] C. Lonvick, "Protocole de couche Transport Secure Shell (SSH)", janvier 2006. *(P.S., MàJ par* RFC6668, 8268, 8308, 8332, 8709)

[RFC4254] T. Ylonen et C. Lonvick, éd., "Protocole de connexion Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

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

9.2 Références pour information

[RFC2629] M. Rose,"Écrire des I-D et des RFC en utilisant XML", juin 1999. *(Information ; Remplacée par* RFC7749)

Adresse des auteurs

Margaret Wasserman
ThingMagic
One Broadway, 5th Floor
Cambridge, MA 02142
USA
téléphone : +1 781 405-7464
mél : margaret@thingmagic.com
URI : http://www.thingmagic.com

Ted Goddard
ICEsoft Technologies, Inc.
Suite 300, 1717 10th St. NW
Calgary, AB T2M 4S2
Canada
téléphone : +1 403 663-3322
mél : ted.goddard@icesoft.com
URI : http://www.icesoft.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.