Groupe de travail Réseau
Request for Comments : 5343
RFC mise à jour : 3411
Catégorie : Sur la voie de la normalisation

J. Schoenwaelder, Jacobs University Bremen

septembre 2008
Traduction Claude Brière de L'Isle

Découverte de l'identifiant de moteur dans un contexte de protocole simple de gestion de réseau (SNMP)

Résumé
Le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) version trois (SNMPv3) exige qu'une application connaisse l'identifiant (snmpEngineID) du moteur de protocole SNMP distant afin de restituer ou manipuler les objets conservés sur l'entité SNMP distante.

Le présent document introduit un localEngineID bien connu et un mécanisme de découverte qui peut être utilisé pour apprendre le snmpEngineID d'un moteur de protocole SNMP distant. Le mécanisme proposé est indépendant des caractéristiques fournies par les modèles de sécurité de SNMP et peut aussi être utilisé par d'autres interfaces de protocole qui fournissent l'accès aux objets gérés.

Ce document met à jour la RFC 3411.

Table des matières

1. Introduction

Pour restituer ou manipuler des informations de gestion en utilisant la version trois du protocole simple de gestion de réseau (SNMPv3, *Simple Network Management Protocol*) [RFC3410], il est nécessaire de connaître l'identifiant du moteur de protocole SNMP distant, dit "snmpEngineID" [RFC3411]. Alors qu'un snmpEngineID approprié peut en principe être configuré dans chaque application de gestion pour chaque agent SNMP, il est souvent désirable de découvrir automatiquement le snmpEngineID.

Le présent document introduit un mécanisme de découverte qui peut être utilisé pour apprendre le snmpEngineID d'un moteur de protocole SNMP distant. Le mécanisme proposé est indépendant des caractéristiques fournies par les modèles de sécurité de SNMP. Le mécanisme a été conçu pour coexister avec les mécanismes de découverte qui peuvent exister dans les modèles de sécurité SNMP, comme la découverte d'identifiant de moteur d'autorité du modèle de sécurité fondé sur l'utilisateur (USM, *User-based Security Model*) de SNMP [RFC3414].

Le présent document met à jour la [RFC3411] en précisant les règles de l'IANA pour la maintenance du registre de format SnmpEngineID.

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].

2. Fondements

Dans un domaine administratif, un moteur SNMP est identifié de façon univoque par une valeur de snmpEngineID [RFC3411]. Une entité SNMP, qui consiste en un moteur SNMP et plusieurs applications SNMP, peut fournir l'accès à plusieurs contextes.

Un contexte SNMP est une collection d'informations de gestion accessibles par une entité. SNMP. Un élément d'information de gestion peut exister dans plus d'un contexte et une entité SNMP a potentiellement accès à de nombreux contextes [RFC3411]. Un contexte est identifié par la valeur de snmpEngineID de l'entité qui héberge les informations de gestion (aussi appelée un contextEngineID) et un nom de contexte qui identifie le contexte spécifique (aussi appelé un contextName).

Pour identifier un élément individuel des informations de gestion au sein d'un domaine administratif, un quadruplet est utilisé qui consiste en :
1. un contextEngineID,
2. un contextName,
3. un type d'objet, et
4. son identification d'instance.

Les deux derniers éléments sont codés dans une valeur d'identifiant d'objet (OID, *Object IDentifier*). Le contextName est une chaîne de caractères (suivant la convention textuelle SnmpAdminString de la MIB de cadre SNMP [RFC3411]) tandis que le contextEngineID est une chaîne d'octets construite selon les règles définies au titre de la convention textuelle SnmpEngineID de la MIB de cadre SNMP [RFC3411].

Les opération du protocole SNMP et les unités de données de protocole (PDU, *Protocol Data Unit*) opèrent sur des OID et traitent les types et instances d'objet [RFC3416]. L'architecture SNMP [RFC3411] introduit le concept d'une scopedPDU comme une structure de données contenant un contextEngineID, un contextName, et une PDU. Le format de message de SNMP version 3 (SNMPv3) utilise les ScopedPDU pour échanger les informations de gestion [RFC3412].

Dans le cadre SNMP, les contextEngineID servent d'identifiant de bout en bout. Cela devient important dans des situations où des mandataires SNMP sont déployés pour traduire entre les versions de protocole ou pour traverser des boîtiers de médiation comme les traducteurs d'adresse réseau. De plus, les snmpEngineID séparent l'identification d'un moteur SNMP des adresses de transport utilisées pour communiquer avec un moteur SNMP. Cette propriété peut être utilisée pour corréler facilement les informations de gestion, même dans des situations où plusieurs transports différents ont été utilisés pour restituer les informations ou lorsque les adresses de transport peuvent changer de façon dynamique.

Pour restituer les données d'un agent SNMPv3, il est nécessaire de connaître le contextEngineID approprié. Le modèle de sécurité fondé sur l'utilisateur (USM) de SNMPv3 fournit un mécanisme pour découvrir le snmpEngineID du moteur SNMP distant, car c'est nécessaire pour des raisons de traitement de la sécurité. Le snmpEngineID découvert peut ensuite être utilisé comme contextEngineID dans une ScopedPDU pour accéder aux informations de gestion locales du moteur SNMP distant. D'autres modèles de sécurité, comme le modèle de sécurité du transport (TSM, *Transport Security Model*) [RFC5591], n'ont pas une telle procédure et peuvent utilisr le mécanisme de découverte défini dans le présent mémoire.

3. Procédure

Le mécanisme de découverte proposé consiste en deux parties, à savoir (i) la définition d'une valeur spéciale de snmpEngineID bien connue, appelée le localEngineID, qui se réfère toujours à un contexte local par défaut, et (ii) la définition d'une procédure pour acquérir le scalaire snmpEngineID de la MIB cadre de SNMP [RFC3411] en utilisant la valeur spéciale de localEngineID locale bien connue.

3.1 EngineID local

Un répondant à la commande SNMP qui met en œuvre la présente spécification DOIT enregistrer ses types de PDU en utilisant la valeur de snmpEngineID de localEngineID (définie ci-dessous) en invoquant l'interface de service abstrait (ASI, *Abstract Service Interface*) registerContextEngineID() définie dans la [RFC3412]. Cet enregistrement est fait en plus de l'enregistrement normal sous le snmpEngineID du moteur SNMP. Ceci est cohérent avec la spécification de SNMPv3 car elle permet explicitement l'enregistrement de plusieurs engineID et de plusieurs pduType [RFC3412].

La convention textuelle SnmpEngineID [RFC3411] définit qu'une valeur de snmpEngineID DOIT faire entre 5 et 32 octets. La présente spécification propose d'utiliser le format de longueur variable 3) de la convention textuelle SnmpEngineID et d'allouer la valeur de format réservée non utilisée de 6, en utilisant l'identifiant d'entreprise 0 pour le localEngineID. Une définition ASN.1 pour localEngineID ressemblerait à :

```
localEngineID CHAÎNE D'OCTETS ::= '8000000006'H
```

La valeur de localEngineID fournit toujours l'accès au contexte par défaut d'un moteur SNMP. Noter que la valeur de localEngineID est destinée à être utilisée comme valeur spéciale pour le champ contextEngineID dans la ScopedPDU. Elle NE DOIT PAS être utilisée comme valeur pour identifier un moteur SNMP ; c'est-à dire, cette valeur NE DOIT PAS être utilisée dans le scalaire snmpEngineID.0 [RFC3418] ou dans le champ msgAuthoritativeEngineID dans les securityParameters du modèle de sécurité fondés sur l'utilisateur (USM, *User-based Security Model*) [RFC3414].

3.2 Découverte de EngineID

La découverte du snmpEngineID est faite en envoyant une opération de protocole de classe lecture (voir le paragraphe 2.8 de la [RFC3411]) pour restituer le scalaire snmpEngineID en utilisant le localEngineID défini ci-dessus comme une valeur d'un contextEngineID. Les mises en œuvre DEVRAIENT n'effectuer cette étape de découverte que quand elle est nécessaire. En particulier, si des modèles de sécurité sont utilisés qui découvrent déjà le snmpEngineID distant (comme avec USM) aucune autre découverte n'est nécessaire. C'est aussi vrai dans des situations où l'application connaît déjà une valeur convenable de snmpEngineID.

La procédure pour découvrir le snmpEngineID d'un moteur SNMP distant peut être décrite comme suit :

1. Vérifier si une valeur convenable de contextEngineID est déjà connue. Si oui, utiliser la valeur de contextEngineID fournie et arrêter la procédure de découverte.

2. Vérifier si le modèle de sécurité choisi prend en charge la découverte du snmpEngineID distant (par exemple, USM avec son mécanisme de découverte). Si oui, laisser le modèle de sécurité effectuer la découverte. Si la valeur de snmpEngineID distant a déjà été déterminée, l'allouer au contextEngineID et arrêter la procédure de découverte.

3. Envoyer une opération de classe de lecture au moteur SNMP distant en utilisant la valeur de localEngineID comme contextEngineID afin de restituer le scalaire snmpEngineID.0 de la MIB de cadre SNMP [RFC3411]. Si cela réussit, régler le contextEngineID à la valeur restituée et arrêter la procédure de découverte.

4. Retourner une indication d'erreur qu'un contextEngineID convenable n'a pas pu être décuovert.

La procédure mentionnée ci dessus est un exemple et peut être modifiée pour restituer plus de variables dans l'étape 3, comme le scalaire sysObjectID.0 ou le scalaire snmpSetSerialNo.0 de la MIB SNMPv2 [RFC3418].

4. Considérations relatives à l'IANA

La RFC 3411 demandait que l'IANA crée un registre pour les formats SnmpEngineID. Cependant, la RFC 3411 ne demandait pas à l'IANA d'enregistrer les allocations initiales faites par la RFC 3411 et ne précisait pas les règles d'allocation. Pour régler ce problème, les règles suivantes sont établies ici.

L'IANA tient un registre des formats de SnmpEngineID. Les quatre premiers octets d'un SnmpEngineID portent un numéro d'entreprise, tandis que le cinquième octet dans une valeur de longueur variable de SnmpEngineID, appelé l'octet de format, indique comment sont formés les octets suivants. Les valeurs de format suivantes ont été allouées dans la [RFC3411] :

Format	Description	Références
0	réservé, non utilisé	[RFC3411]
1	adresse IPv4	[RFC3411]
2	adresse IPv6	[RFC3411]
3	adresse MAC	[RFC3411]
4	texte alloué administrativement	[RFC3411]
5	octets alloués administrativement	[RFC3411]
6-127	réservé, non utilisé	[RFC3411]
128-255	spécifique d'entreprise	[RFC3411]

L'IANA peut allouer de nouvelles valeurs de format hors de l'espace réservé de numéros originellement alloués de 1 à 127. Pour de nouvelles allocations dans cet espace de numéros, une spécification est exigée confromément à la [RFC5226]. L'espace de numéros 128 à 255 est spécifique de l'entreprise et n'est pas contrôlé par l'IANA.

Selon le présent document, l'IANA a fait l'allocation suivante :

Format	Description	Références
6	moteur local	[RFC5343]

5. Considérations sur la sécurité

SNMP version 3 (SNMPv3) fournit la sécurité cryptographique pour protéger les appareils contre l'accès non autorisé. La présente spécification recommande d'utiliser les services de sécurité fournis par SNMPv3. En particulier, il est RECOMMANDÉ de protéger l'échange de découverte.

Un snmpEngineID peut contenir des informations comme l'adresse MAC d'un appareil, l'adresse IPv4, l'adresse IPv6, ou du texte alloué administrativement. Un attaquant situé derrière un routeur / pare-feu / traducteur d'adresse réseau peut n'être pas capable d'obtenir ces informations directement, et il pourrait donc découvrir les valeurs de snmpEngineID afin d'obtenir ces sortes d'informations sur l'appareil.

Dans de nombreux environnements, rendre les valeurs de snmpEngineID accessibles via un niveau de sécurité de noAuthNoPriv va bénéficier aux outils légitimes qui essayent de déterminer algorithmiquement certaines informations de base sur un appareil. Pour cette raison, la configuration par défaut du modèle de contrôle d'accès fondé sur la vue (VACM, *View-based Access Control Model*) de l'Appendice A de la [RFC3415] donne un accès en lecture noAuthNoPriv au snmpEngineID. De plus, le mécanisme de découverte USM défini dans la [RFC3414] utilise des messages non protégés et révèle les valeurs de snmpEngineID.

Dans des environnements très sûrs, les valeurs de snmpEngineID peuvent être protégées en utilisant le mécanisme de découverte décrit dans le présent document avec un modèle de sécurité qui n'échange pas de messages SNMP en clair, comme avec le modèle de sécurité du transport (TSM, *Transport Security Model*) [RFC5591].

La primitive de service abstrait isAccessAllowed() du sous système de contrôle d'accès SNMP ne prend pas en compte le contextEngineID dans la vérification des droits d'accès [RFC3411]. Par conséquent, il n'est pas possible de définir une vue particulière pour la découverte du contexte de engineID. Une demande avec un localEngineID est donc traitée comme une demande avec le snmpEngineID correct par le sous système de contrôle d'accès. Ceci est en ligne avec la conception de SNMPv3 où l'identité authentifiée est le securityName (avec les informations de securityModel et securityLevel) et les adresses de transport ou la connaissance des valeurs de contextEngineID n'impactent pas la décision de contrôle d'accès.

6. Remerciements

Dave Perkins a suggéré l'introduction d'un contextEngineID "local" durant la réunion intermédiaire du groupe de travail ISMS (modèle de sécurité intégré pour SNMP) à Boston, en 2006. Joe Fernandez, David Harrington, Dan Romascanu, et Bert Wijnen ont fourni une relecture et des retours utiles qui ont aidé à améliorer ce document.

7. Références

7.1 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)

[RFC3411] D. Harrington, R. Presuhn, B. Wijnen, "Architecture de description des cadres de gestion du protocole simple de gestion de réseau (SNMP)", décembre 2002. (*MàJ par* RFC5343) (STD0062)

[RFC3412] J. Case et autres, "Traitement et distribution de message pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3414] U. Blumenthal, B. Wijnen, "Modèle de sécurité fondée sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau (SNMPv3)", décembre 2002. (STD0062)

[RFC3416] R. Presuhn, éd., "Version 2 des opérations de protocole pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC3418] R. Presuhn, éd., "Base de données d'informations de gestion (MIB) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

7.2 Références pour information

[RFC3410] J. Case et autres, "Introduction et déclarations d'applicabilité pour le cadre de gestion standard de l'Internet", décembre 2002. *(Information)*

[RFC3415] B. Wijnen, R. Presuhn, K. McCloghrie, "Modèle de contrôle d'accès fondé sur la vue (VACM) pour le protocole simple de gestion de réseau (SNMP)", décembre 2002. (STD0062)

[RFC5591] D. Harrington, W. Hardaker, "Modèle de sécurité du transport pour le protocole simple de gestion de réseau (SNMP)", juin 2009. *(P. S.)*

Adresse de l'auteur

Juergen Schoenwaelder
Jacobs University Bremen
Campus Ring 1
28725 Bremen
Germany
téléphone : +49 421 200-3587
mél : j.schoenwaelder@jacobs-university.de

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.